COMPUTERWORLD

Security

http://www.computerworld.com/s/article/9138346/AV_tests_find_that_reputation_really_does_count

AV tests find that reputation really does count

Robert McMillan

September 21, 2009 (IDG News Service) New reputation-based antivirus systems are doing a better job of blocking malicious software than did their predecessors.

That's what testing and certification company NSS Labs discovered when it looked at how good antivirus software really is at blocking Web-based attacks.

NSS tested nine antivirus products by installing the software and then directing the PC to a battery of more than 3,000 Web sites that were known to be actively downloading malicious software to PCs. For two products -- built by Trend Micro and McAfee -- the tests took a look at how much so-called reputation-based malware detection systems really helped block malware. These reputation systems use a variety of techniques to size up a program and get a sense of whether it's trustworthy.

According to NSS President Rick Moy, antivirus products that ship with reputation systems tended to do better in the tests. "Not all AV is the same," he said. "There are huge differences between anti-malware products, and the reputation systems are making a considerable impact."

With Trend Micro Internet Security and McAfee Total Protection, NSS compared how the software did with reputation-based detection turned both on and off. Trend Micro's software improved by 23 percent with the system active; McAfee's improved by 8 percent.

Trend Micro and McAfee were also the two quickest companies to protect customers from new strains of malware, NSS said.

Overall, Trend Micro Internet Security performed best in the NSS tests, catching malware 96.4 percent of the time. The number-two-ranked product, Kaspersky Internet Security, also uses a reputation system, although NSS wasn't able to turn it off to see how much it helped with detection.

These reputation-measuring techniques are supposed to enhance traditional signature-based AV products. With signature detection, the antivirus company simply takes a kind of digital fingerprint of the code and then blocks any other program that has the same signature.

Reputation-based detection has become an important new area for antivirus vendors, as criminals have become expert at jumbling up their malicious software so that digital signatures no longer work. "There's a lot of malware being missed by the security industry because it's being changed for every single visitor," said Carey Nachenberg, a Symantec fellow who created the company's new reputation-based detection system.

Trend Micro's reputation system works because it blocks specific URLs. But reputation systems can use a variety of factors to determine whether to block a program. Nachenberg's Symantec Reputation Based Security system, used by the just-released Norton Internet Security 2010, uses complex algorithms to figure out a program's reputation. (This version wasn't available when NSS conducted its tests.)

In essence, it's a lot like the film-rating system of NetFlix, making a prediction based on a number of factors. How long has the program been around? Where did it come from? How many people use it? "All these pieces of information can be correlated together and used to drive a reputation rating for every piece of software," Nachenberg said.

The top 4 consumer AV products, as rated by NSS based on the percentage of malware caught, were as follows:

1) Trend Micro Internet Security 2009 / 96.4%

2) Kaspersky Internet Security 2009 / 87.8%

3) Norton Internet Security 2009 / 81.8%

4) McAfee Total Protection Suite 2009 / 81.6%