No News Is Big News for Sana Security

April 23 2007

Sana Security today announced version 2.2 of the Primary Response SafeConnect anti-malware utility, which works exactly the same in Vista as in Windows XP.

Sana Security today announced version 2.2 of the Primary Response SafeConnect behavior-based anti-malware utility, now compatible with Windows Vista. The big news for the Vista version is that there's no news. It works exactly the same in Vista (32-bit or 64-bit) as in Windows XP. That's no small feat given Vista's changed driver model and added security, especially the PatchGuard protection in 64-bit Vista's kernel.

PRSC detects malicious software by monitoring the behavior of all running programs. When it detects evil behavior it terminates the offending program and removes all traces of it, without any need for a predefined signature. In testing, the previous version was quite effective - it blocked all of the malware samples except a couple that apparently didn't do anything malicious during the test period. Version 2.2 does monitor a few new behaviors and adds a regularly updated bulletin on malware Sana Security has detected in the wild.

I asked Sana's Chief Technology Officer Vlad Gorelik whether a product like PRSC is even necessary, given the added security built into Vista. According to Gorelik, Sana's experience is that Vista completely blocks about two thirds of existing malware from running. But turn that around - one in three is Vista-compatible. Not all of them trigger User Access Control, and you can be sure that some users will blindly click Allow. Fortunately if the program that an unwitting user released is a

stinker, PRSC will catch it as soon as it gets out of line.

Gorelik pointed out that Vista has to be compatible with existing programs; otherwise it would never be accepted. And malicious programs are just a subset of existing programs. Even 64-bit Vista requires a compatibility layer for 32-bit programs, so it's theoretically vulnerable. He suggested that when 64-bit Vista becomes more prevalent, hackers may dig into that compatibility layer.

He also observed that there's a lot of money in malware these days. Internet Explorer is supposed to block installation of unknown ActiveX controls, but the bad guys can afford to commission fancy-looking Flash animations that encourage the user to work around this limitation with step-by-step instructions. Gorelik suggests that similar social engineering attacks will be used in Vista, though we don't yet know exactly what form it will take.

"I think Vista is great," he said, "but you're going to have the same problems under Vista - just a little different flavor. Vista has to run programs, and malicious programs are programs. Any platform that's so broadly deployed is a target."

Primary Response SafeConnect 2.2 comes in two versions, one for Windows XP and 32-bit Vista and another specifically for 64-bit Vista. Windows 2000 is no longer supported in this version. A one-year subscription costs $29.95.

https://phys.org/news/2007-04-news-big-sana.html