Security Bombshell: did a trusted antivirus program help steal data?

Kaspersky security has always been well-regarded as a top-notch third-party security provider for PCs, though some folks have always had a lingering suspicion of using a Russian company to watch out for their data. Now it looks as if some of those fears might have been confirmed.

Reports in two major newspaper link the hacking of classified material by the Russians to the use of Kaspersky antivirus on the home computer of an NSA employee. The scenario plays out like this. An employee who worked for the NSA developing hacking tools took some classified files home to work on using his home computer. (Obviously a big, no-no.) Russian hackers were able to target those files by using Kaspersky security software on the PC to identify them.

This was some important info detailing America's strategy for both defending against cyber-attacks and launching them. The government no longer allows federal agencies to use Kaspersky's security software.

Assuming this is actually how the hackers accessed the data, that wouldn't necessarily mean Kaspersky was involved. They could have been hacked by Russian government agents as well. Though that doesn't speak too well of the security their software is providing.

It's also possible that the Russian government may demand access to Kaspersky's servers the same way that the NSA could get an order to force an American company to hand over their files.
In an online statement, the company said, "Kaspersky Lab has not been provided any evidence substantiating the company’s involvement in the alleged incident...However, as the trustworthiness and integrity of our products are fundamental to our business, we are seriously concerned about the article’s implications that attackers may have exploited our software. We reiterate our willingness to work alongside U.S. authorities to address any concerns they may have about our products and respectfully request any relevant information that would enable the company to begin an investigation at the earliest opportunity." The statement went on to deny any inappropriate ties with the Russian government. So far, the company has not been officially charged or even officially accused of doing anything wrong.

Here's the bottom line. Any security software you use is going to be able to see the files on your PC. That's the only way they can check for viruses or malware. If there are bad actors working for that company or those with criminal intent are able to hack their servers, they can get that information. However, if you don't have security software, you run the risk of exposing your information to hackers. The question ultimately comes down to who you trust to watch your information.