Antivirus software could make your company more vulnerable

	Antivirus software could make your company more vulnerable !

Security researchers are worried that critical vulnerabilities in antivirus products are too easy to find and exploit

Imagine getting a call from your company's IT department telling you your workstation has been compromised and you should stop what you're doing immediately.
You're stumped: You went through the company's security training and you're sure you didn't open any suspicious email attachments or click on any bad links; you know that your company has a solid patching policy and the software on your computer is up to date; you're also not the type of employee who visits non-work-related websites while on the job. So, how did this happen?

A few days later, an unexpected answer comes down from the security firm that your company hired to investigate the incident: Hackers got in by exploiting a flaw in the corporate antivirus program installed on your computer, the same program that's supposed to protect it from attacks. And all it took was for attackers to send you an email message that you didn't even open.
This scenario might sound far-fetched, but it's not. According to vulnerability researchers who have analyzed antivirus programs in the past, such attacks are quite likely, and may already have occurred. Some of them have tried to sound the alarm about the ease of finding and exploiting critical flaws in endpoint antivirus products for years.
Since June, researchers have found and reported several dozen serious flaws in antivirus products from vendors such as Kaspersky Lab, ESET, Avast, AVG Technologies, Intel Security (formerly McAfee) and Malwarebytes. Many of those vulnerabilities would have allowed attackers to remotely execute malicious code on computers, to abuse the functionality of the antivirus products themselves, to gain higher privileges on compromised systems and even to defeat the anti-exploitation defenses of third-party applications.
Exploiting some of those vulnerabilities required no user interaction and could have allowed the creation of computer worms – self-propagating malware programs. In many cases, attackers would have only needed to send specially crafted email messages to potential victims, to inject malicious code into legitimate websites visited by them, or to plug in USB drives with malformed files into their computers.

Attacks on the horizon

Evidence suggests that attacks against antivirus products, especially in corporate environments, are both possible and likely. Some researchers believe that such attacks have already occurred, even though antivirus vendors might not be aware of them because of the very small number of victims.
The intelligence agencies of various governments have long had an interest in antivirus flaws. News website The Intercept reported in June that the U.K. Government Communications Headquarters (GCHQ) filed requests in 2008 to renew a warrant that would have allowed the agency to reverse engineer antivirus products from Kaspersky Lab to find weaknesses. The U.S. National Security Agency also studied antivirus products to bypass their detection, according to secret files leaked by former NSA contractor Edward Snowden, the website said.

Réagissez à cet article

Source : *Antivirus software could make your company more vulnerable | Computerworld*