

Microsoft's Kernel Patch Protection Endangers Third-party Security Software Vendors

Overview

New security measures introduced by Microsoft under the name "Kernel Patch Protection" are being presented to the world as bringing a new level of security to users. This security will be provided by a combination of Microsoft security software and Windows operating system kernel design.

Agnitum security experts have analyzed these new measures, and it is their informed opinion that these measures will actually cause more harm than good, for two primary reasons:

- It will be more complicated for third-party security software companies to install and maintain their software on Windows PCs. In some circumstances, kernel patch protection may even block the installation of third-party security software.
- It will be easier for hackers to share and use this new technology than for legitimate software developers.

Let's take a look behind the scenes and see why this is the case.

Technical Background

To provide proactive protection, security software solutions need to get control over low-level system activities like file and registry operations.

To achieve this level of control, one approach uses a documented API provided by Microsoft. However, this API does not allow ISVs (independent software vendors) to control system activity pre-emptively and on the fly. It limits the number of file and registry operations that can be controlled. It does not allow control of process memory modification and imposes a number of other restrictions. This does not help independent software vendors to provide system protection using native interfaces.

An alternate approach requires modification or replacement of code or critical structures in the kernel of the Microsoft Windows operating system using internal system calls—so-called *kernel patching*. Essentially, kernel patching bypasses actual Windows kernel code to invoke third-party code. However, this approach opens up Windows to attack by malicious third-party code as well as legitimate attempts to extend Windows functionality.

One of the most commonly used approaches to implementing proactive protection involves changing and monitoring the *Service Dispatch Table (SDT)*, which is used by the OS to transfer control from user-mode to kernel (low-level system mode). Developers sometimes patch the kernel by changing the service number in the SDT, and when a call is made to invoke a system service, the third-party code is invoked instead of the kernel code.

Security vendors, including Agnitum, often use this approach. Unlike other techniques suggested by Microsoft, this approach enables third-party software to protect the OS by gaining full control over file and registry operations. Microsoft, however, prefers that developers not use this approach. In fact, the company has gone so far, in the x64 versions of Windows, as to prevent call redirection involving 32-bit SDT pointers. Sadly, this poses no problem for hackers, as there are unused areas in the kernel code that can be used to create so-called "connectors." In theory, Windows Patch Guard should interrupt this process after doing a memory space check, but hackers already know how to disable this protection.

And now, along comes Kernel Patch Protection

In a recent update, Microsoft removed the ability for developers to legitimately change the service number in the SDT, introducing so-called *kernel patch protection* for x64-based versions of Windows Server 2003 SP1, Windows XP and later versions of Windows for x64-based systems.

Microsoft believes kernel patch protection defends code and critical structures in the Windows kernel against modification by unknown code or data. Kernel patch protection stores and periodically verifies checksums of specific kernel memory areas (network components); if a checksum mismatch is found, the result is the dreaded Blue Screen of Death (BSOD). According to Microsoft, this technique should prevent SDT modification and thwart the intentions of a number of rootkits.

Research by Agnitum security experts has determined that, in practice, kernel patch protection does not prevent hackers from reverse engineering specific OS code areas to re-acquire the desired capabilities. While it does disable compatibility with future kernel versions, quality-assurance is not a big concern for most malware writers.

So where does this leave legitimate security software developers?

Microsoft seems to be saying that it is enough to use just standard built-in protection tools. Agnitum and other third-party security developers would strongly disagree with that position. Third-party security solutions create a much-needed additional level of protection, and having a variety of these tools available empowers the user while handicapping the hacker. Simply put, it is much harder for malware writers to adapt malicious code for different protection mechanisms from multiple vendors than it is to attack a single-vendor solution that purports to be a universal fix.

Kernel patch protection restricts ISVs to two alternatives:

1. Use the "legitimate" API provided by Microsoft and be unable to implement proactive system protection.
2. Use "shady" methods—in effect, use hacker techniques to compete with Microsoft and enforce a level playing field.

Kernel patch protection does complicate rootkit writers' lives. But they can use quick-and-dirty techniques, because they don't need to worry about compatibility with existing system and application software.

Besides, does it make sense to consider triggering a Blue Screen of Death as a way to defend against rootkits?

Under Microsoft's proposed solution, a rootkit that could previously be detected by and remedied with anti-virus software will now cause the BSOD. The same result will occur after installation of security software that is not compatible with kernel patch protection technology.

The security experts at Agnitum believe this move by Microsoft is designed to force users to rely on Microsoft and only Microsoft for Windows security, removing the option to use third-party security solutions that, if past experience is anything to go by, are likely to be more robust and provide better protection than Microsoft offerings.

We believe that Microsoft owes users a better solution.

For further reference, see

http://www.microsoft.com/whdc/driver/kernel/64bitpatch_FAQ.msp

<http://support.microsoft.com/kb/914784>

by Igor Pankov,
Agnitum Ltd., www.agnitum.com

Press contacts:
pr@agnitum.com