



How boot-time scans can help you win the battle against malware

INTRODUCTION

While boot-time scanning might appear to be an unnecessary impediment to speedy start-up times, it does in fact represent a critical tier of protection against today's sophisticated malware. This white paper explains why boot-time scanning is necessary and provides a technological overview of the advanced boot-time scanner in avast! antivirus solutions.

THE BENEFITS OF BOOT-TIME SCANNING

Computer viruses used to be basic programs and both detection and removal were relatively easy processes. But that is no longer the case. Modern malware uses extremely sophisticated techniques in order to evade detection by antivirus products and, in some cases, can actually bite back and disable any antivirus product installed. Consequently, not all malware can be reliably detected and removed once the operating system has booted and is running.

Rootkits, which account for a high percentage of infections, can be particularly problematic. If a rootkit is present in the system, it may hook itself into the file system handling code and modify the requests passing through there. For example, if an antivirus program asks the operating system to open a particular malware file so it can be scanned, the rootkit can change the information flow and open a harmless file instead, hiding the infection. More commonly, rootkits hide by interfering with the operating system's file enumeration code – the code that browses the file system structures and lists the files present – to exclude infected files from being listed. These files are, in effect, completely hidden to both the operating system and the antivirus software. In short, a rootkit can render a computer completely untrustworthy.

The Conficker worm is an example of malware which can defeat antivirus scanners running within Windows. When Conficker is active, it locks its files so that they cannot be examined by an antivirus scanner (the scanner's logs will simply show an "Unable to open: file in use" message). To detect and clean such malware, it is necessary to scan the system before the malware is running.

As the name implies, a boot-time scan runs at start-up before most of the operating system and any applications have loaded. The main benefit of this is that in most cases, malware will still be in a dormant

state and unable to take action to conceal its presence on the system.

The avast! boot-time scan uses direct disk access and bypasses the Windows file system drivers that are normally used for enumerating and opening files. In other words, avast! reads the raw data on the partition and parses the file system structures without using or in any way depending on the corresponding operating system code. Consequently, while a threat may be able to hide from both the operating system and any antivirus solution running within the operating system, it usually cannot hide from the avast! boot-time scanner.

TECHNOLOGICAL OVERVIEW OF THE avast! BOOT-TIME SCANNER

The boot-time scanner is a special avast! feature for detecting and removing viruses and rootkits. The user can "schedule" a boot-time scan from the avast! user interface, and the scan will automatically run the next time the computer is started or restarted.

The avast! boot-time scan is started very early in the boot-process, before the swap or paging file has been initialized, before the Win32 subsystem has been loaded and before the **HKEY_LOCAL_MACHINE\Software** hive has been loaded. This means that the scan runs before auto-start entries such as **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run** and users' StartUp folders have been processed and, consequently, any malware that

may be registered in these auto-start locations is still inactive. Since the malware is not yet active, it cannot actively fight against its detection or removal and so the boot-time scanner can detect malicious software that would normally be hidden or locked.

The boot-time scanner is a native application and does not depend on the Win32 subsystem (the KERNEL32.DLL library, for example). It is very similar to Microsoft Chkdsk – which is also started during the boot process – and is a user-mode application, running under the LOCALSYSTEM account. To schedule a boot-time scan, an entry is written to the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager** registry key and so the action must be performed from an account with administrative privileges. The boot-time scanner executable is installed into the System folder as running the scanner from the avast! installation folder is not reliable.

The scanning engine of the boot-time scanner is identical to the ordinary Windows version of the avast! engine, although the unpacking capabilities are slightly restricted: a few of the more complex file archive types (such as 7-ZIP) are not processed. However, all

runtime packers (packed/protected executables) are scanned, just as in the Windows version.

Since the Windows GUI is not running at the time the scanner runs, its user interface is simple and text-based, though interactive. Support for non-English characters is restricted; the loaded font supports code-page 437 only, so some of the localized versions are either not available at all and must stay in English (Japanese and Chinese, for example), or have to use Latin transliteration (Cyrillic, Greek).

The boot-time scanner uses a direct disk access and does not rely on the usual operating system API functions to work with files; instead, it reads the raw partition data and parses the file system structures itself. The FAT16, FAT32 and NTFS file systems are supported.

If a rootkit driver is already active when the boot-time scanner starts (some kernel-mode drivers will start even before the boot-time scan), it may interfere with the file system processing code to hide its files from enumeration or prevent removal of its files. However, as the boot-time scanner does not rely on the usual file-access API, it is not affected by such actions –

files remain visible, the content can be read, and the files can be deactivated and removed. This enables the boot-time scanner to remove even the most sophisticated and stubborn rootkits and viruses.

Currently, the boot-time scanner is only available in 32-bit versions of Windows.

ABOUT AVAST SOFTWARE

Based in the Czech Republic, AVAST Software a.s. (formerly ALWIL Software a.s.) has been producing industry-leading security solutions since 1991 and is the developer of the award-winning avast! product line. As a global company, AVAST has partners all around the world who contribute to the continuous development and improvement of their products and provide technical support to clients in their native language.

AVAST's mission is to provide both home users and businesses with solutions that are easy-to-use, affordable and exceptionally effective.

To find out more about AVAST Software and the avast! product line, please visit www.avast.com.