McAfee 5800 Scan Engine and .DATs

Get effective malware protection for embedded systems.

The primary function of any anti-malware product is to find and remove viruses, worms, and other types of threats. The key measure of a product's anti-malware effectiveness is how well it isolates a threat and prevents it from spreading. It sounds easy, but it's a complex endeavor. The nature of threats has changed significantly in recent years, and is much more sophisticated and distributed.

Alongside traditional virus threats, there are now email worms, internet worms, distributed denial-of-service (DDoS) attacks, backdoor and remote access Trojans, spyware, rootkits, and advanced persistent threats. Many of these threats combine multiple attack vectors to maximize their chances of spreading quickly through global corporate networks. It's not uncommon to see threats that blend multiple attack techniques, including mass mailing, infection via network shares, autoruns, exploits, or rootkits. Some try to terminate existing security controls, while others install Trojans, rootkits, or keyloggers to steal and exfiltrate credentials and data.

These advanced persistent threats have had a particularly marked effect, combining the use of system exploits—formerly associated with hacking activities—with the stealth capabilities of rootkits and backdoors. An increasing number of advanced persistent threats are designed to cash in on vulnerabilities in operating systems and applications. Threats that once required hours or days to propagate from one region to another are now exploited globally in minutes or less.

No matter how the exploits against our systems and data evolve, the challenge for our security controls remains the same—to find and remove the threat. The advanced scanning technology in the McAfee® 5800 Scan Engine—battle-tested over many years—is the foundation of our response to the threats of yesterday, today, and tomorrow.

The 5800 Scan Engine: McAfee Core Technology

A scan engine examines different types of objects for signs of infection. The McAfee 5800 Scan Engine contains the functionality necessary to inspect 32-bit and 64-bit program executables, Microsoft Office files, Adobe PDF and Flash, Oracle Java, boot sectors, and other file formats that could conceal or be exploited by

McAfee Protection for Embedded Systems

- Includes the McAfee 5800 Scan Engine, .DAT files, and SDK
- Scans 32-bit and 64-bit program executables, Microsoft Office files, Adobe PDF and Flash files, Oracle Java, boot sectors, and other file formats
- Sees through the encryption used in compressed, archived, packed, and protected files
- Advanced heuristic analysis evaluates code behavior
- Generic detection identifies and cleans many viral variants
- Rigorous .DAT file testing minimizes false alarms
- Whitelisting of known clean files enhances scanning performance

a piece of malicious code. Additionally, our scan engine has the ability to see through the encryption used in compressed, archived, packed, and protected files. That's why it's essential to keep the engine updated. Each time a new operating system appears or a new type of file format becomes susceptible to infection, McAfee adds support for it—always keeping the scan engine up to date and ready to protect your data.

Virus definitions

Understanding how to inspect different file structures is only part of the solution. It's just as important to know what to look for. The what-to-look-for information (that is, specific characteristics that identify a particular virus, worm, or Trojan) is stored in the virus definition files, also known as .DAT files. DAT files are released daily, with interim emergency releases for threats rated medium or higher by McAfee Labs.

Protection for McAfee customers

The scan engine and virus definition files operate in tandem to deliver effective protection for our customers. This core technology is wrapped into different product solutions, as appropriate for each platform and operating system. The same scan engine is integrated into all McAfee self-managed, antivirus solutions—McAfee VirusScan® software and McAfee Security for Email Servers, Messaging, and McAfee Web Security appliances—and it forms the foundation of the McAfee Total Protection suites.

The McAfee Scan Engine Software Developers Kit (SDK)

Using the McAfee Scan Engine SDK, application and managed service providers can integrate advanced scanning technology directly into their own solutions, enhancing what they offer to their customers. With the increase in outsourcing, customers have come to expect that effective protection from today's malicious code is automatically included in such services. Our scan engine software development kit (SDK), with its easy-to-implement, C-based application programming interface (API), makes it easy for McAfee embedded partners to deliver the protection their customers demand.

Comprehensive scanning for today's and tomorrow's threats

The McAfee 5800 Scan Engine delivers comprehensive detection for all of today's threats—not only those found in the field, but also those that might become widespread at some point in the future. New threats appear all the time, and many of today's viruses, worms, and other threats travel at internet speed—they strike fast and move quickly. So a scan engine's ability to flag new, unknown pieces of malware is more important than ever.

Supported Platforms

- Microsoft Windows (on Intel x86 and x64): Windows, XP, Vista 7, 8 and 10; Server 2003, 2008, 2008 R2, and 2012
- Linux 32-bit distributions shipping with version 2.6 and 3.x production kernels, libc6 (glibc), gcc versions 3.2 onwards, and with libstdc++.so.6 installed
- Linux 64-bit distributions shipping with version 2.6 and 3.x production kernel, with libstdc++.so.6 installed
- Sun Solaris (on SPARC): Versions 9, 10, and 11 with the latest Solaris OS recommended cluster installed
- Sun Solaris (on Intel x86 and x64): Version 10 and 11 with the latest Solaris OS recommended cluster installed
- FreeBSD (on Intel x86 and x64): FreeBSD 8.x – 10.x
- IBM AIX (on RS6000): Versions 6.1 and 7.1
- Apple Mac OS X 10.6 Snow Leopard, OS X 10.7 Lion, OS X 10.8 Mountain Lion, OS X 10.9 Mavericks, and OS X 10.10 Yosemite
- HP-UX (on PA-RISC): Versions 11i v1 – v3

Heuristic detection

Our advanced heuristic analysis lets us look through the code in a file to determine if the actions it takes are typical of a virus. The more virus-like code that's found, the more likely the file is to be infected. To reduce the risk of false alarms—identifying a virus when there isn't one—we combine positive heuristics with negative heuristics to search for those things that are distinctly non-virus like.

Generic detection and cleaning

Generic detection involves using a single virus definition to detect and clean many variants of the same virus family. Of course, all threats must be detected, but it is much less efficient to build individual signatures for each one as they appear. Piecemeal detection isn't just less efficient—it also means that a new variant has the opportunity to spread before the scanner is able to detect it. The use of generics has also helped in managing the size of the DAT files as the number of threats grows at a geometric rate.

The McAfee generic detection capability, developed over several years, has brought enormous benefits to McAfee customers by protecting them from threats such as Ransomware, Spyware, Fake AV, Conficker, Sality, Virut, Zeus, and many others.

Reliable and accurate

False alarms—mistakenly flagging a clean file as being infected—cost money and undermine confidence in a company's antivirus defenses. That's why it is essential to minimize the risk of false alarms. Every day, our .DAT files undergo rigorous quality assurance testing on a test server containing multiple terabytes of real-world applications, minimizing the risk of costly false alarms.

Whitelisting technology

Our scan engine uses whitelisting technology for known clean Microsoft Windows operating system and popular software application files. This provides a significant performance benefit for both on-access and on-demand scanning when these files are accessed. We continue to update the whitelist with qualifying information in line with new releases of popular software files.

Maintaining business continuity

McAfee scanners make full use of the engine's important ability to clean infected files. If a scanner simply flags an infection, the system administrator must replace the file—either from an original master disk, an installation DVD (in the case of .EXE files), or from a backup (for documents and spreadsheets)—if a backup even exists. If the scanner is able to clean the infected file, business continuity is maintained, downtime is minimized, and costs are reduced.

System Requirements

- At least 512 MB of free hard disk space
- At least an additional 512 MB of free hard disk space reserved for temporary files
- At least 512 MB of RAM (1024 MB recommended minimum)
- At least 1024 MB of RAM for updating operations

Key features of the McAfee 5800 Scan Engine:

- Enhancements to PDF format to improve exploit detection capabilities
- Improved handling of Windows executable format
- Improved unpacking of .NET, Shockwave Flash, VBA, and generic unpacking improvements to detect more threats
- Enhancements to live memory scanning in Windows for detecting and removing malicious processes, threads, and files
- Performance optimizations around initialization and scanning
- New supported platforms: Windows 10, FreeBSD 10.x, Solaris 11 for SPARC
- End-of-Life (EOL) platforms: IBM AIX 5.3, FreeBSD 7.x, Solaris 8 on SPARC and Linux Kernel 2.4
- Scan engine SDK for easy integration into third-party applications

Learn More

For more information visit
www.mcafee.com/embedded

McAfee
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

62048ds_scan-engine_0915
SEPTEMBER 2015