IT@Intel Brief

Intel IT
Information Security and Stealth Malware Protection
February 2013

Evaluating McAfee Deep Defender* for the Enterprise

- Ability to prevent kernel-mode rootkits in real-time before they take hold
- Faster identification, analysis, and response to stealth malware attacks
- Ability to detect and remediate instead of having to rebuild systems
- Excellent companion product to McAfee Host Intrusion Prevention for Desktops* and McAfee VirusScan Enterprise*

Intel IT conducted an initial pilot to evaluate the potential business value of McAfee Deep Defender* at Intel. During the pilot, this software was able to detect and block stealth malware threats that no anti-malware application currently deployed at Intel could have prevented in such a timely manner. Based on these promising results, in 2013 we plan to deploy Deep Defender to target internal organizations through a production pilot and will investigate the viability of a wider deployment following a successful production pilot.

Deep Defender uses real-time detection to help stop zero-day malware—those threats that exploit a previously undisclosed vulnerability in a computer application or OS. In particular, this software can detect and block stealth malware attacks that use kernel rootkits. This hardware-enhanced security is enabled by McAfee DeepSAFE* technology.

Researchers at McAfee Labs have identified more than 3.7 million unique stealth rootkits. We found that Deep Defender can help Intel IT threat management personnel reduce the time required to detect and analyze malware variants. In addition, real-time detection can enable us to remediate systems, rather than rebuild them—saving time and effort. Because Deep Defender detects, blocks, and remediates stealth malware attacks in such a timely manner, this software will be a valuable addition to Intel's existing information security portfolio (Figure 1).

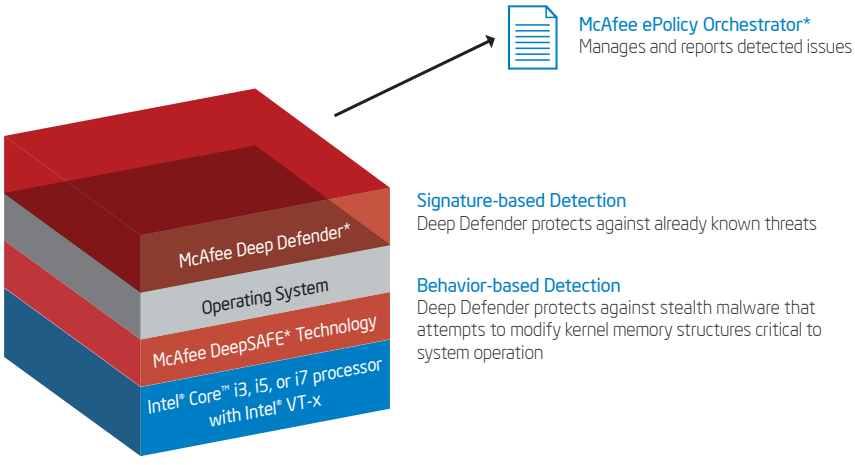

Figure 1. McAfee Deep Defender* uses both signature-based and behavior-based detection to provide real-time protection against stealth malware on Intel® Core™ i3, i5, or i7 processor with Intel® Virtualization Technology (Intel® VT) for IA-32, Intel® 64, and Intel® architecture (Intel® VT-x).

"The frequency of threats attacking Microsoft Windows below the kernel is increasing. Some of the critical assets targeted include the BIOS, master boot record (MBR), volume boot record (VBR), GUID Partition Table (GPT), and NTLoader. Although the volume of these threats is unlikely to approach that of simpler attacks on Windows and applications, the impact of these complex attacks can be far more devastating. We expect to see more threats in this area during 2013."

Source: "2013 Threats Predictions" published by McAfee Labs, 2012

Background

Even before Intel acquired McAfee in 2010, Intel had been working with McAfee to develop technology to detect and block stealth malware attacks on the OS. The companies knew that stealth malware attacks would continue to advance, especially as hackers realized that they could sell malware. Intel and McAfee began collaborating on a technology whereby a software agent could utilize features within the hardware to enable new, unique protections from *outside* the OS. The result of this collaboration is the McAfee DeepSAFE* technology, which is implemented in McAfee Deep Defender*.

Today, the volume of new malware continues to increase, and those creating malware are constantly evolving the techniques and tools they use to attack confidential and sensitive information. The stealth techniques that cybercriminals use to gain access to a PC or network are becoming more sophisticated and easier to implement. Cybercriminals are now creating stealth malware that is designed to circumvent current security protections.

Of particular concern are stealth kernel-mode rootkits, which can load in advance of the computer OS and applications and operate at the kernel level of the OS (Figure 2). Rootkits are used in zero-day attacks[1] to hide other malware components that target a computer application or the OS.

As of the end of 2012, McAfee Labs, a team of 500 multidisciplinary researchers in 30 countries, had identified more than 3.7 million unique stealth rootkits. McAfee Labs predicts an increase in covert and persistent attacks deep within and beneath Microsoft Windows*.

[1] For more information on zero-day attacks, refer to www.mcafee.com/us/resources/data-sheets/ds-deep-defender.pdf.

REAL-TIME DETECTION HELPS BLOCK ZERO-DAY THREATS

Deep Defender complements Intel IT's existing antivirus, security monitoring, and security intelligence platforms by adding real-time, hardware-enhanced memory monitoring and protection to each user device.

Stealth malware can be detected two ways; Deep Defender uses both methods.

- **Signature-based detection – detecting threats that are already known.** Detects static strings within a code file that identifies that file as malware. Most antivirus applications use this approach, but by itself signature-based detection can protect only against threats that have already been identified and entered into detection tables. Also, this detection method occurs after the stealth malware has already had an opportunity to infect and damage the PC.
- **Behavior-based detection – detecting zero-day threats in real time.** Monitors system memory for attempts by malware to modify kernel memory structures critical to system operation. This approach enables the detection of zero-day malware, such as rootkits, as the threat occurs.

Deep Defender provides real-time stealth malware protection by *combining* signature-based detection to combat known threats with behavior-based detection to block zero-day threats, such

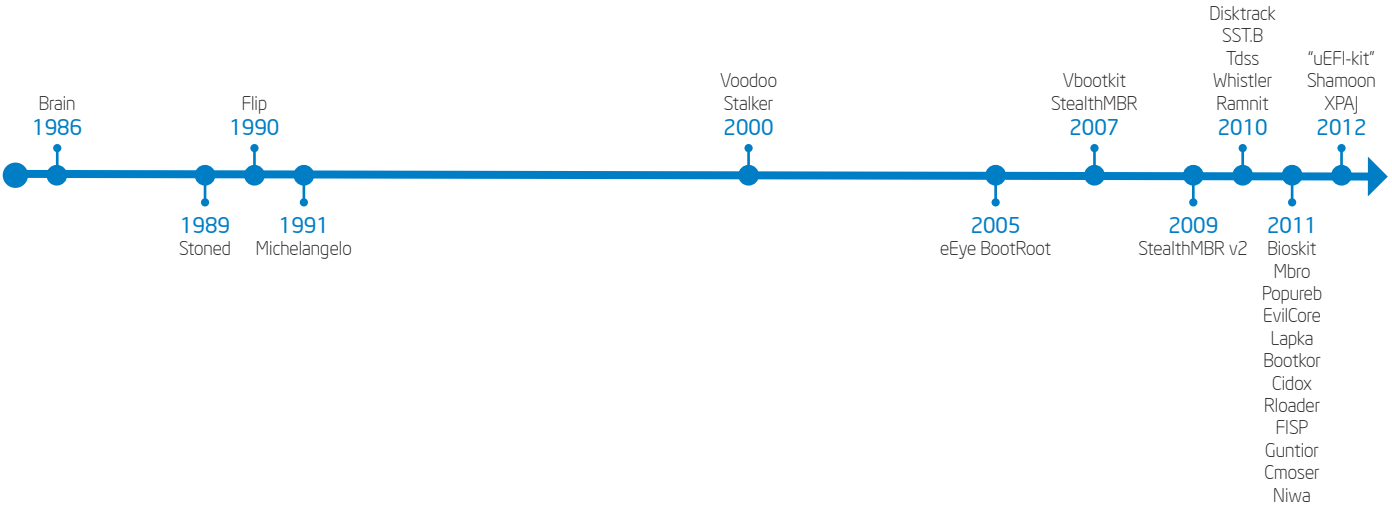

Figure 2. The increased frequency of kernel-level attacks makes McAfee Deep Defender* an important component of Intel's overall information security portfolio.

as kernel rootkits. This combination of protection methods is a significant improvement over the traditional signature-only approach to security. Deep Defender's hardware-enhanced security is enabled by McAfee DeepSAFE technology, which interacts with the Intel® processor to provide a new perspective on security—outside the OS.

If a behavior is flagged as suspicious but turns out to be a legitimate behavior such as a driver upgrade, the driver can be added to a whitelist so Deep Defender does not alert the user. The ability to create whitelists and blacklists provides a method for tuning Deep Defender to fit different security environments and to improve performance and security protection.

A COLLABORATIVE EFFORT

The development of Deep Defender is an ongoing, joint undertaking between Intel and McAfee. McAfee DeepSAFE technology relies on Intel® Virtualization Technology (Intel® VT) for IA-32, Intel® 64, and Intel® architecture (Intel® VT-x). Intel architecture experts collaborated with McAfee product developers to help them develop a product that uses features of the Intel processor to protect the kernel.

Intel also provided insight and assistance in other aspects of product development, including:

- Significantly reducing performance overhead
- Enhancing the integration of Deep Defender with McAfee ePolicy Orchestrator* (McAfee ePO*), McAfee's security management platform
- Identifying and resolving defects
- Helping address cybercriminal activities by developing protection against both 32-bit and 64-bit stealth malware variants

Intel IT continues to collaborate with McAfee in further reducing Deep Defender's performance impact and improving the overall product. For example, Intel and McAfee are actively developing additional features that rely on Intel® technologies to detect additional types of threats, such as BIOS attacks.

Initial Pilot

We conducted an initial pilot to evaluate the potential business value of utilizing McAfee Deep Defender at Intel. The 10-week pilot, with 320 participants, used version 1.0.1. We used our internal software distribution system to deploy the software and used the McAfee ePO server to manage and report detected issues. After the pilot concluded, we conducted a participant survey and analyzed the results of the pilot.

METHODOLOGY

We sent the pilot invitation to a wide variety of employees from different business groups located worldwide, to provide a mix of employee segments. The participants included those who are typically at high risk for receiving malware or a target for stealth malware attacks, such as those who:

- Have been previously impacted with malware
- Have access to sensitive data
- Travel and use hotels and hotspots for connectivity
- Interact frequently with customers and suppliers
- Use credit cards for corporate purchases and handle financial data

To participate in the pilot, an employee's PC had to meet the following criteria:

- Equipped with an Intel® Core™ i3, Core™ i5, or Core™ i7 processor with Intel VT
- Capable of using McAfee Agent* 4.6
- Does not have an incompatible hypervisor installed[2]

We sent interested employees an email containing the instructions for installing and enabling the software.

We created a client package for the pilot participants that included three components.

- Verification that the PC BIOS settings are set correctly for both Intel VT-x and Execute Disable Bit
- McAfee Agent 4.6 software
- McAfee Deep Defender 1.0.1 software

If the BIOS check detected any incorrect settings, most resets were done automatically. However, for any settings that needed to be changed manually, we gave employees detailed reset instructions.

We configured the McAfee Agent 4.6 to work with a test McAfee ePO server. We configured the test ePO server to include the McAfee Deep Defender 1.0.1 extensions so that any malware detection events would be logged at the ePO server. We also developed and applied ePO policy settings to the ePO server so that if, for example, zero-day malware was detected, Deep Defender would block and remediate the malware. We plan to base future Deep Defender deployments at Intel on this client package.

[2] Software products utilizing Intel® Virtualization Technology (Intel® VT) are not compatible with each other. Therefore systems running a hypervisor utilizing Intel VT are not candidates to run McAfee Deep Defender*.

KEY LEARNINGS AND BUSINES VALUE

Prior to conducting the initial pilot, we anticipated that Deep Defender would enable faster threat analysis of malware variants as well as have the potential to detect and remediate threats in real time, instead of reactively rebuilding systems after the attack occurred.

The pilot confirmed these expectations. During the pilot, there were three detections of malware, demonstrating significant business value.

No malware detection application currently deployed at Intel would have been able to detect or block these particular threats in such a timely manner. For example, our antivirus application did not detect any of the threats. The new software detected the rootkit's attempt to load and stopped the kernel-level compromise by blocking and remediating the malware. If the threat had not been blocked, it would have been necessary to rebuild these systems, involving hours of IT effort and lost employee productivity.

Had the malware gone undetected, financial or document theft might have occurred on each of the affected systems and spread to other employees' systems through file-sharing activities.

We also experienced several driver-detection events, where drivers legitimately changed kernel-level information. We can use this information to whitelist these drivers so they do not trigger events in the future.

Based on the business value demonstrated during the pilot, we have already identified several use cases, particularly systems used by Intel employees that are at high risk for being impacted by stealth malware. Deep Defender will be a valuable addition to existing information security protections already in use at Intel, such as antivirus and host-intrusion prevention applications.

During the pilot, we developed processes to integrate Deep Defender into our existing real-time monitoring and interpretation of security events on the network. For example, the software works with McAfee ePO, our security management platform, which centralizes and streamlines the management of end-point, network, content security, and compliance solutions. We are also working on integrating Deep Defender with our Security Information Event Management tool.

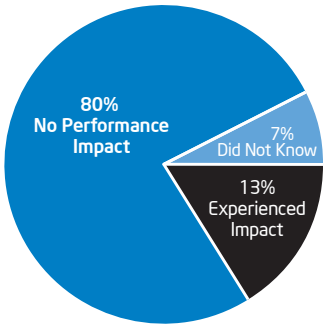

Figure 3. Survey responses after the initial pilot were encouraging—80 percent of respondents did not see a performance impact when running McAfee Deep Defender* software.

McAfee Deep Defender* and Microsoft Windows* 8

Intel IT is standardizing on Windows 8 Enterprise as the primary OS for business Ultrabook™ devices and Intel® architecture-based tablets, and we plan to eventually make the new OS available for laptops and desktop PCs.

While Windows 8 provides additional security during the boot process through the early launch anti-malware (ELAM) driver and Unified Extensible Firmware Interface (UEFI) Secure Boot support, these security measures apply only to drivers already blacklisted. McAfee Deep Defender provides several unique advantages for zero-day malware on Windows 8.

- Profiles malware's access to protected memory locations and reacts to malicious behavior
- Loads before the OS to monitor kernel memory in real time.
- Detects the malware at runtime, as the threat is attempting to load, whereas the built-in Windows 8 features provide protection only at reboot—meaning the time between infection and reboot could be days or weeks, allowing stealth malware to hide and propagate.

SURVEY RESULTS

At the end of the pilot, we conducted a participant survey and received 222 responses. As shown in Figure 3, 80 percent of respondents did not see a performance impact when running Deep Defender software. Another 7 percent responded "do not know" indicating that performance impact was essentially transparent to these users as well. This was an impressive finding because typically users do experience a performance impact when running malware detection and remediation software. We will continue to track performance impact as we move into the production pilot.

NEXT STEPS

We have identified Deep Defender as a valuable addition to Intel's information security portfolio. We currently estimate the number of PCs in use at Intel that could benefit from the installation and use of Deep Defender at about 70,000. As Deep Defender continues to evolve, we believe it will become even more valuable. Key upcoming features planned for availability in Release 1.6, scheduled for release in Q2 2013, include the following:

- **BIOS monitoring.** Prevents changes to PC start-up operations.
- **Intel® Xeon® processor support.** Provides real-time malware prevention to protect servers and their critical business functions and data.
- **Microsoft Windows 8 support.** Provides kernel and BIOS protection for stealth malware threats occurring on the Windows 8 OS.
- **Support for the latest Intel architecture.** McAfee software will continue to take advantage of advances in hardware-enhanced security provided by Intel® microarchitecture.

Our future plans include upgrading the initial pilot participants to Release 1.5, evaluating Release 1.6, and deploying Deep Defender to target internal organizations through a production pilot.

Conclusion

McAfee Deep Defender uses real-time detection to help stop zero-day malware, such as attacks using kernel-mode rootkits, before they damage a system or spread to other PCs. In an initial pilot at Intel, this software was able to detect and block stealth malware threats that other anti-malware applications in use at Intel would not have detected or prevented in a timely manner.

The pilot also supported our expectations that the event data provided by Deep Defender can help Intel IT threat management personnel reduce the time required to detect and analyze malware variants. In addition, real-time detection can enable us to remediate systems in most cases, instead of having to rebuild them—saving time and effort.

Deep Defender, with its ability to detect and block stealth malware, will be a valuable companion product to the information security protections already in use at Intel, such as antivirus and host-intrusion prevention applications. In 2013, we plan to deploy Deep Defender to target internal organizations through a production pilot and will investigate the viability of a wider deployment following a successful production pilot.

For more straight talk on current topics from Intel's IT leaders, visit www.intel.com/it

AUTHORS

Greg Bassett
Security Engineer, Intel IT

Albert Gutierrez
Client Security Engineer, Intel IT

Stephanie Mahvi
Project Manager, Intel IT

Printed in USA ♻ Please Recycle 0213/ERAI/KC/PDF 327765-001US