White Paper

Root Out Rootkits

An inside look at McAfee® Deep Defender

Table of Contents

Researchers discover an average of 2,000 rootkits each day, according to McAfee® Labs™. Rootkits are an increasingly common form of malware built explicitly to hide malicious code. Once installed, a rootkit conceals itself and looks innocent to traditional file-based scans. The longer it stays hidden, the more damage the rootkit can do, especially when rootkits conceal secondary malware components, a common line of attack.

To prevent the rootkit from installing and cloaking itself and related malware, McAfee has invented endpoint detection more sophisticated than malware signatures and operating-system level heuristics. This paper describes how McAfee Deep Defender moves endpoint security beyond the operating system. McAfee Deep Defender gets hardware assistance from Intel and uses a privileged early load position to uncloak, block, and remove the kernel-mode activities of stealthy rootkits. Once McAfee Deep Defender has neutralized the rootkit, any malicious user-mode payload the rootkit was concealing lies exposed for detection and clean up by the traditional file-based scanning of McAfee VirusScan® Enterprise software. Both products interact with McAfee Global Threat Intelligence™ to minimize time to protection for the system and other potential targets.

McAfee Labs has identified:

- More than 2.8 million unique rootkits
- 180,000 new rootkits each quarter
- 2,000 new rootkits per day

Rootkits: Rotten Code in the Core

Rootkits may seem like just another type of malware—another virus, Trojan, or worm—but they can be far more dangerous. Two characteristics—the concealment enabled by low-level operation and their role in hiding complex threats—distinguish rootkits from the traditional malicious code that we expect file-based antivirus and host intrusion prevention systems to catch.

Rootkits cloak and disable defenses

The most distinctive attribute of a rootkit is its ability to conceal its presence. There are two types of rootkits: user mode and kernel mode. Kernel-mode rootkits are the hardest to detect and clean because they lie deep inside the operating system. They load before most boot or other drivers and before traditional user-mode level protections. Kernel-mode rootkits use this early load position to hide their presence by manipulating the kernel, memory, and other system elements. These rootkits can control basic computing functions, so in addition to hiding their own existence, they can

- Disable protections (including antivirus)
- Reinfect if they are removed
- Conceal other code, such as a payload within the rootkit or separate elements of the attack
- Deny read/write access to rootkit files to block removal[1]

> *"Rootkits can target any system, from database servers to point-of-sale terminals, from mobile phones to automobile electronics. Because rootkits can operate within and below the operating system, they can disguise or conceal the files, processes, and registry keys touched by other malware. These traits make rootkits a vital component of multistage threat operations."*
>
> —Dave Marcus and Thom Sawicki
> *The New Reality of Stealth Crimeware*

“Modern rootkits do not elevate access, but instead are used to make another typically malicious software payload undetectable by adding stealth capabilities. The payload might covertly steal user passwords, credit card information, or computing resources, or conduct other unauthorized activities. Due to the stealthy nature of this malicious activity, the attack may go unnoticed for an extended length of time, perhaps years.”

—Jason Brown
McAfee Deep Defender Best Practices Guide[3]

Designed to conceal a payload

A rootkit can make system changes or create system policies that compromise security. Using these tactics, the rootkit’s primary job is to conceal other malware, malicious payloads in the form of viruses, Trojans, or worms until the time is right for attack. That’s why rootkits are a preferred tool in stealthy threats like Stuxnet or Necurs.[2] The low-level control of the rootkit allows it to cloak the presence of that secondary malware, hiding it from traditional operating system (OS) and application-level security products. Often, the attacker applies creativity to building the rootkit and then leverages off-the-shelf malware payloads for the rest of the crime: data theft, keylogging, and reconnaissance. Both parts of the attacker’s task have become easier with malware toolkits that rival commercial development tools. When user-mode and kernel-mode rootkits are used together, an attacker leverages kernel-level access to disguise the attack and user-level functionality to manipulate the system, resulting in a sophisticated and essentially invisible attack.

Meet Koutodoor and TDSS

While a few attacks—like Stuxnet and its derivative, DuQu—received widespread news attention, other rootkit families like Koutodoor and TDSS have had greater impact with less fanfare. The Koutodoor progeny represent 21 percent of the rootkit zoo.[4] In the case of Koutodoor, cybercoders have been perfecting this brainchild since 2007.[5]

Koutodoor operates in several stages:

- Installs Trojan (as rootkit)
- Installs secondary malware from its download sites
- Secondary malware sends traffic to specific URLs, generating “clicks” on banner ads and web counters

This sequence drives revenue based on the pay-per-click Internet business model. By installing the rootkit on infected systems, the criminals boost click-through income without having too many clicks originate from the same address.[6]

Koutodoor has many clever attributes. It uses polymorphic droppers to avoid recognition and changes a function value and read-write privileges to deny file access and persist on infected systems. Also, it changes its file name at every boot. Like many rootkits, it can prevent the launch of legitimate programs, including antivirus. Its ingenuities seem endless: it adds 11 files to the system, changes the timestamp, adds and removes six files (one mysteriously labeled dogkiller.exe), and creates or changes several dozen registry elements.[7,8]

All of these actions are designed to conceal the presence or ensure the survival of the rootkit on the host. As long as the rootkit can conceal the various Koutodoor files, the attack remains active.

Modern Cyberwarfare

“Some of today’s tools work against some of today’s rootkits. Tools like virus scanners and host intrusion prevention systems operate at the operating system and above. They can examine memory and monitor user-mode privileges to detect and remediate the relatively high-level, user-mode rootkits. However, stealth techniques that operate at the kernel-level and below fly underneath the radar of traditional operating system, vulnerability, and virus scanning tools. Kernel-mode rootkits have system-level privileges, so they are harder to detect and repair.

Stuxnet and Zeus demonstrate how much more sophisticated cybercrime is today compared to just a few years ago.

The Stuxnet attack appears to have been designed to disrupt industrial control systems within Iranian nuclear programs. Stuxnet used both user- and kernel-mode rootkits, plus a rootkit within the programmable logic controller (PLC), a usage not previously seen in the wild. The user and kernel-mode rootkits hid files and decrypted and injected code in running processes. The spring 2010 version of the kernel-mode rootkit included stolen signed device drivers, so that the rootkit looked like legitimate code.”

—*The New Reality of Stealth Crimeware*
www.mcafee.com/stealthcrimeware

Rootkits Dodge Detection

Many user-mode rootkits and the increasing number of kernel-mode rootkits go undetected by traditional file-based tools like antivirus and intrusion prevention systems (IPS). Detection requires low-level instrumentation and active system monitoring actions below and within the kernel level of the operating system that are not part of standard and IPS.

If and when rootkits are detected, cleanup is messy. Since the rootkit likely acted to replicate itself and hide other malicious components, system administrators must become or bring in forensic investigators to understand the complete attack sequence and find and remove any other attack components, particularly data-stealing malware. For many, the easiest and safest remediation is a complete re-image with a productivity tax of an average of 10 hours per system.[9] Without a reimage, the rootkit may just reinstall itself from another part of the system and repeat the cloaking effort on the malware, or contact its command and control center to reinitiate the attack sequence.

Another rootkit, TDSS, represents more than 37 percent of the rootkit zoo and shows how adeptly rootkit families evolve to stay ahead of antivirus tools. For example, a recent incarnation infected the Master Boot Record to load ahead of other drivers and all antivirus solutions, allowing it to disable antivirus and operating system protections, debuggers, and other tools. TDSS also infects existing files as a parasite. It creates and maintains an encrypted file system where it will store its payload. Password stealers and other threats stored in the rootkit's vault are undetectable by on-access scanners; they are off the grid.[10]

In addition, some rootkits will hook, or intercept, function tables to disguise themselves. For example, the system service dispatch table (SSDT) is an internal dispatch table within Microsoft Windows that houses core OS functions. When a rootkit hooks this table, it can conceal itself and related components by providing fake memory values to any code in search of a pointer. Hooking of this table allows a rootkit to "stealth" anything, from files and folders to processes to parts of the registry.

Win at Rootkit Limbo[11]

Through a development partnership with Intel, McAfee has created a new tier of security products that acts beyond the operating system. The first of these, McAfee® Deep Defender, can monitor and control functions low in the system stack, revealing and then disabling rootkits in the kernel. Unlike static scanning tools that need to be told to run, McAfee Deep Defender sits inline, monitoring and evaluating kernel events in real time. When it sees suspicious or malicious events, it can block them and, if you choose, remediate malicious code within the kernel.

McAfee Deep Defender works in conjunction with McAfee VirusScan Enterprise software. While McAfee Deep Defender drives effective, real-time protection into the kernel itself to fight rootkits, McAfee VirusScan Enterprise detects and remediates other kinds of malware at the user level using both signature-based and real-time, cloud-based malware systems. The two products should be used together to detect and clean up rootkits and their companion files throughout the software stack, as well as unstealthy malware in the user and application levels.

McAfee Deep Defender with McAfee DeepSAFE take out kernel-mode malware

McAfee Deep Defender is the first product built with McAfee DeepSAFE™ technology, an advanced integration of Intel hardware and McAfee security expertise. McAfee DeepSAFE technology provides real-time memory monitoring via hardware features in the Intel Core i3, i5, and i7 processors. Specifically, McAfee DeepSAFE uses the Intel Virtualization Technology or VT-x to get an unfettered view of system memory. Leveraging McAfee DeepSAFE, McAfee Deep Defender has a great, unprecedented vantage point to witness and selectively intervene in the flow of events in the lowest levels of the operating system.

If a rootkit or other stealth malware is active, McAfee DeepSAFE will catch its attempt to load into memory and alert the McAfee Deep Defender agent. McAfee Deep Defender identifies peculiar actions at kernel memory locations and makes the connection between these suspicious memory I/O events and other threats on the disk. McAfee Deep Defender can then unload or blacklist these malicious or infected drivers to render them useless.

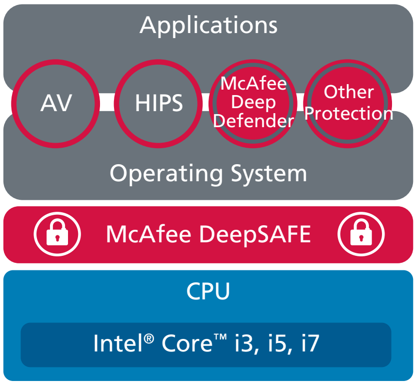

Figure 1. McAfee DeepSAFE technology provides low-level monitoring to enable rootkit detection and removal.

Updates the cloud

Since it is monitoring memory activity and triggering on suspicious behavior, McAfee Deep Defender will detect zero-day malware. To alert other systems to a zero-day rootkit, McAfee Deep Defender will transmit telemetry data to the McAfee Global Threat Intelligence™ (McAfee GTI™) cloud. The data it communicates—a hash of the blacklisted driver that attempts to load and its metadata, such as file size, path name, service name, digital signature information, and file fingerprint—informs McAfee research and analysis. The telemetry data will be converted into cloud-based protection, as well as a .DAT signature. The .DAT signature can be used by McAfee VirusScan Enterprise software on any system—even those without McAfee DeepSAFE or McAfee Deep Defender—to protect against installation of that rootkit on those systems. McAfee GTI-enabled products benefit second-hand from this hardware-assisted security, gaining more accurate detection.[12]

McAfee VirusScan Enterprise can remove related malware

Once the kernel-mode rootkit is exposed and removed, any user-mode malware it has been hiding becomes visible. McAfee VirusScan Enterprise software may detect it upon the next scan if it is a known virus, Trojan, worm, or other malware. If the revealed malware is not yet known (does not yet have a .DAT signature), McAfee VirusScan Enterprise software may consult the McAfee GTI file reputation service for a risk assessment of the suspicious file. If McAfee GTI confirms the file as a threat, McAfee VirusScan Enterprise will block and clean the malware.

Inside the Detection and Scanning Functions

McAfee DeepSAFE, McAfee Deep Defender, and McAfee VirusScan Enterprise components all perform scanning, but each scan is a bit different. The resources, access, and characteristics of the level in which they operate determine the types of scans and remediations they perform. For example, the lowest level McAfee DeepSAFE component lives in the limited world of kernel operations. It has lightweight logic focused entirely on memory access—what's normal and what's anomalous. It has the power to block drivers from loading and suspend kernel threats. For the actual removal of the code, it passes the information it has gleaned about the driver's misbehavior up the stack to the McAfee Deep Defender agent.

The McAfee Deep Defender agent has more resources (both time and compute) to perform more robust analysis. It receives the information from McAfee DeepSAFE and considers its implications. The McAfee Deep Defender agent has a focused set of antivirus content that looks at file, registry, stealth memory, and process scanning techniques. If its analysis identifies a rootkit family, it can initiate additional scanning and remediation.

Real-time visibility into memory

Through real-time insight into both memory accesses and the interactions of malicious code, McAfee Deep Defender can perform rich, subtle detection and remediation that is unlike the file-oriented scanning of traditional antivirus. The visibility into memory and kernel-level events also gives McAfee Deep Defender more information than that available to intrusion prevention systems.

A few other things differentiate McAfee Deep Defender from traditional user-mode security tools.

- An on-demand scan will only detect when it is run, either manually or as part of a scheduled task. If a malicious rootkit has already been installed, the rootkit has had time to cloak itself and replicate or activate its self-healing regimes before the scan gets a chance to find it.
- Traditional tools are visible to rootkits. They can be manipulated by rootkits, for example, by deactivating the antivirus driver.
- The first driver to load wins. Via McAfee DeepSAFE, the McAfee Deep Defender driver always loads first

Scenarios

To highlight the technical magic in McAfee Deep Defender, let's walk through a few use cases: a clean laptop and an infected system. First, you will install McAfee Deep Defender on a laptop with an Intel i3/i5/i7 CPU with VT-x enabled. The system is already running McAfee VirusScan Enterprise (VSE) and a McAfee ePolicy Orchestrator® (McAfee ePO™) agent.

Clean installation

McAfee Deep Defender uses the same McAfee ePO policy and agent infrastructure as McAfee VirusScan Enterprise. To deploy, you just check in a new McAfee ePO package, and the McAfee agent will pull it down to the endpoints. McAfee DeepSAFE technology is included in the same McAfee ePO package. McAfee Deep Defender gains low-level visibility through two McAfee DeepSAFE components: the McAfee DeepSAFE memory layer and the McAfee DeepSAFE loader/in-band agent. Once you have installed the McAfee Deep Defender package, either locally or over the network, you reboot the system.

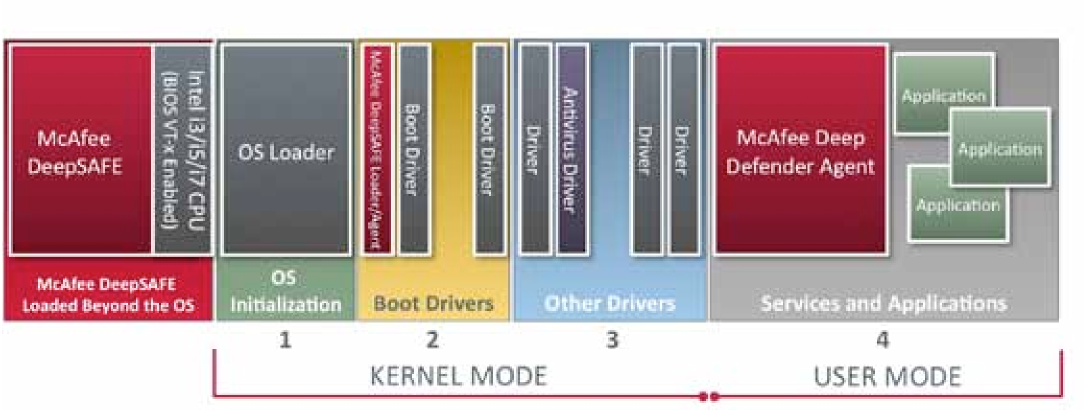

Figure 2. McAfee Deep Defender installation and initial execution after first boot.

1. The system's OS loader begins initialization of the Microsoft Windows operating system. Boot drivers begin to load. The first of these is the McAfee DeepSAFE loader/in-band agent. This agent contains lightweight detection logic that analyzes activity, notes when a driver is behaving suspiciously, and exposes any rootkits. We use multiple methods to ensure that the McAfee driver always loads first. For example, rootkits often alter registry keys. McAfee locks the specific registry keys used to change load order, so our agent will always load ahead of other code. This guaranteed early load process ensures that McAfee DeepSAFE can monitor and inspect each driver loaded after it and prevents other drivers from compromising the McAfee DeepSAFE agent.

   NOTE: With this load position and memory monitoring, we can see a kernel-mode driver attempting to make a memory change and act before anything bad happens. Other security systems that load later, after the driver or higher in the stack, would only see what the malicious driver wanted them to see—the altered reality created by the rootkit's manipulation of memory. Instead, we see the *attempt* to alter memory and can act before any change is made. McAfee does not need to have prior knowledge (a signature or pattern) of the rootkit. We catch it trying to do its job. This gives you true zero-day detection.

2. Next, other standard drivers, including the McAfee VirusScan driver, load. Other McAfee products, such as McAfee SiteAdvisor® and McAfee Host Intrusion Prevention, have drivers loading in this space as well.

3. User-level services and applications start to load, including the McAfee Deep Defender agent. This agent contains the higher-end, heavier-weight logic of remediation and removal. Where the lightweight logic in the kernel-mode McAfee DeepSAFE loader/agent will detect a malicious driver, the heavyweight rules in McAfee Deep Defender pinpoint other components involved in the attack.

A phishing attack

That's the overview of where the McAfee components live in the system and what they do. Now, let's put them to work detecting unknown rootkits on the fly. Today, the user of this machine gets a phishing email with a compelling offer to attend an industry seminar for free if they sign up through a special website. The value-conscious user clicks through to the link, and a rootkit Trojan downloads in the background as the user is filling out the form.

Normally, the rootkit would attempt to hide in the kernel as a boot driver. However, this time, McAfee DeepSAFE catches the rootkit's attempt to load into memory. The McAfee DeepSAFE component alerts the McAfee Deep Defender agent, which blocks and remediates the rootkit. Here's how it works:

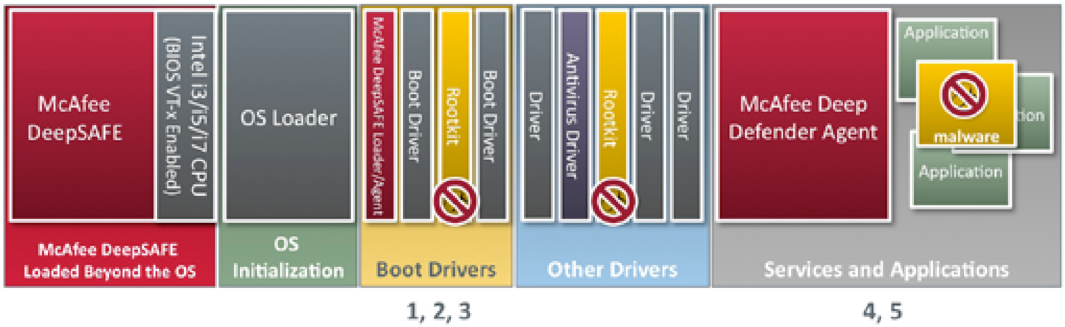

Figure 3. McAfee Deep Defender operation during malicious attack.

1. A new kernel driver (mal.sys) loads. At this point, the driver has not been classified as good (and therefore not whitelisted) or bad (and also not blacklisted) and so is classified as unknown by the McAfee DeepSAFE loader/agent.
2. Mal.sys behaves suspiciously by attempting to load the interrupt descriptor table (IDT) at a new address. This operation is normally something only the OS would attempt to perform. Alternatively, the driver may try to patch the SSDT, a construct we described earlier.
3. Since the mal.sys driver is classified as unknown, McAfee Deep Defender blocks the attempted load of the IDT, blacklists the driver, and generates an event as a result of the attempted action.
4. The event is escalated to heavyweight rules (HWRs) for processing by the McAfee Deep Defender agent when the system enters user mode. The HWRs use more complex detection and removal logic to clean mal.sys; this part of McAfee Deep Defender has the capability of quarantining the file, for example. In this case, the HWRs prompt the system to reboot in order to eject the malware driver. After reboot, the malware driver attempts to load, but it is denied by the blacklist. This denial triggers a rescan of the kernel driver.

A rootkit in residence

Alternatively, you might install McAfee Deep Defender on a system already infected with one or more rootkits. In the example below, you have two classes of rootkits, "boot driver rootkits" and rootkits that are just standard kernel-mode drivers. The latter category is the most common.

With rootkits already in residence, we install McAfee Deep Defender using McAfee ePO software as before. When we reboot, our boot sequence starts out the same, but McAfee Deep Defender protection kicks in during the startup process, and McAfee VirusScan Enterprise helps with remediation:

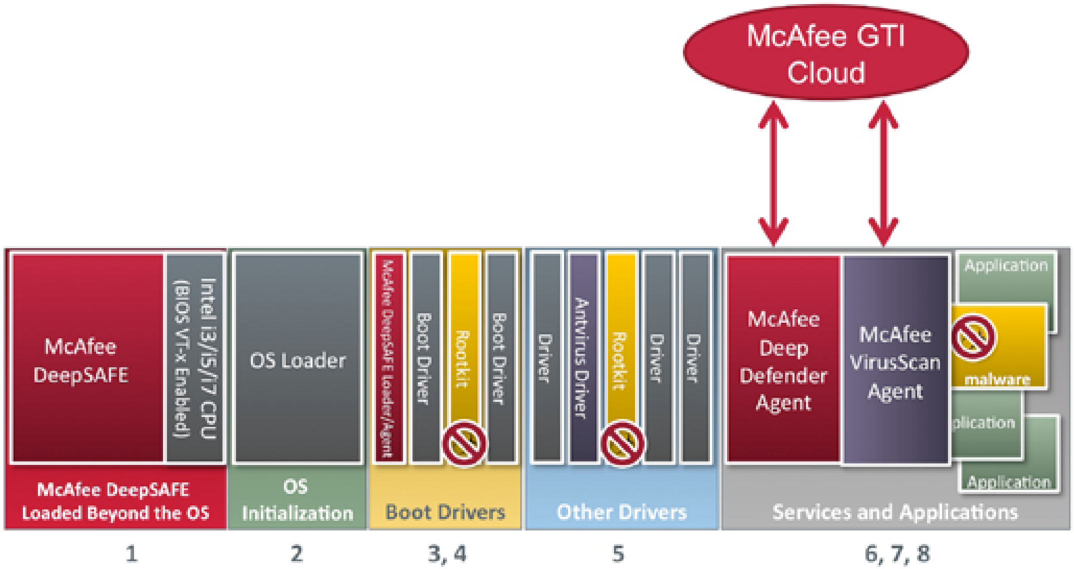

Figure 4. McAfee Deep Defender detecting and cleaning an existing rootkit.

1. As the system initializes, the first component of McAfee DeepSAFE becomes active in the memory layer.

2. The systems' OS loader begins initialization of the Windows operating system.

3. Boot drivers begin to load, starting with the McAfee DeepSAFE loader/agent.

4. The remaining boot drivers load. A driver attempts to modify the kernel, and the McAfee DeepSAFE memory component (from step 1) sees the action and relays the attempt to the McAfee DeepSAFE loader/agent (from step 3). The McAfee DeepSAFE agent will process its activity against its lightweight detection logic. If we identify the memory access as malware, the McAfee DeepSAFE loader/agent will block the malicious boot driver's activities. The rootkit will be neutralized, but it won't yet be gone from the system.

5. Windows loads the other standard drivers, including the McAfee VirusScan driver. McAfee DeepSAFE detects another attempt to modify the kernel and, as before, tells the McAfee DeepSAFE loader/agent to step in and block that malicious code.

   Note: The antivirus driver—or other security drivers in this level such as the IPS or SiteAdvisor driver—could load before the malicious driver, but they wouldn't see anything wrong unless the driver happened to exhibit known bad behavior (something detected by the product's heuristic file or behavior identification). Any new, or zero-day, behavior would go unnoticed. Only McAfee DeepSAFE technology provides the real-time visibility into rootkit kernel memory accesses.

6. As before, the user-level services and applications start to load, including the McAfee Deep Defender agent.
7. The McAfee Deep Defender agent removes both malicious driver rootkits.
8. Once the kernel mode code that provided camouflage is gone, the malware it was hiding becomes visible. The next time the malicious file is accessed or executed, if the malware is known, a McAfee VirusScan Enterprise on-access scan will detect and clean it, or it will be detected at the next scheduled scan. If the malware is unknown but suspicious, McAfee VirusScan Enterprise will use McAfee GTI lookups and potentially identify and clean this non-rootkit malware.

Conclusion

Rootkits represent just the latest escalation in the decades-long battle between malware developers and security researchers. By inserting previously unavailable monitoring and control operations within the kernel, McAfee Deep Defender offers enterprises a way to fight back against these stealthy attacks. McAfee Deep Defender works alongside other host protections and within the familiar McAfee ePO management to make it easy to layer in a new baseline of protection.

This solution leverages Intel hardware capabilities to provide the strongest McAfee software protection for the system—protection that goes beyond the operating system. Unlike static scans and user-mode protections, McAfee Deep Defender monitors memory operations in real time, stopping unknown, zero-day infections before they have a chance to do damage. If the rootkit has been concealing secondary malware, that malware will be revealed for cleanup by user-level protections like McAfee VirusScan Enterprise.

McAfee Deep Defender, built on McAfee DeepSAFE technology, provides must-have protection for endpoints on the front line. It can free your system of rootkits and related payloads so multistage attacks never get past the first contact. Learn more at www.mcafee.com/deepdefender and www.mcafee.com/deepsafe.

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world’s largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by its unrivaled global threat intelligence, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee is relentlessly focused on constantly finding new ways to keep our customers safe. http://www.mcafee.com

[1] "Predicting the Future of Stealth Attacks," *October 2011 Virus Bulletin*, Kapoor and Mathur

[2] http://blogs.mcafee.com/mcafee-labs/signed-malware-you-can-runbut-you-cant-hide

[3] Contact your sales representative for access to this resource.

[4] McAfee Labs

[5] "Predicting the Future of Stealth Attacks," *October 2011 Virus Bulletin*, Kapoor and Mathur

[6] http://www.eset.eu/encyclopaedia/win32-koutodoor-hm-trojan-e-backdoor-cep-gen-cq?lng=en

[7] "Predicting the Future of Stealth Attacks," *October 2011 Virus Bulletin*, Kapoor and Mathur

[8] http://home.mcafee.com/virusinfo/virusprofile.aspx?key=568093#none

[9] Costs average five hours for each IT administrator and user per system reimaged (10 hours total), for an approximate cost per endpoint of $585; at a 5,000 node company, a 1 percent infection rate would equate to $30,000 in cleanup costs.

[10] "Predicting the Future of Stealth Attacks," *October 2011 Virus Bulletin*, Kapoor and Mathur

[11] The traditional party game where the winner is the person that gets lowest to the ground: http://www.partycity.com/product/inflatable+cactus+limbo+game.do.

[12] Find out how to activate McAfee GTI in your McAfee product at https://kc.mcafee.com/corporate/index?page=content&id=KB70130

McAfee
An Intel Company

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