Symantec™
Security Response

Rootkits

Contents

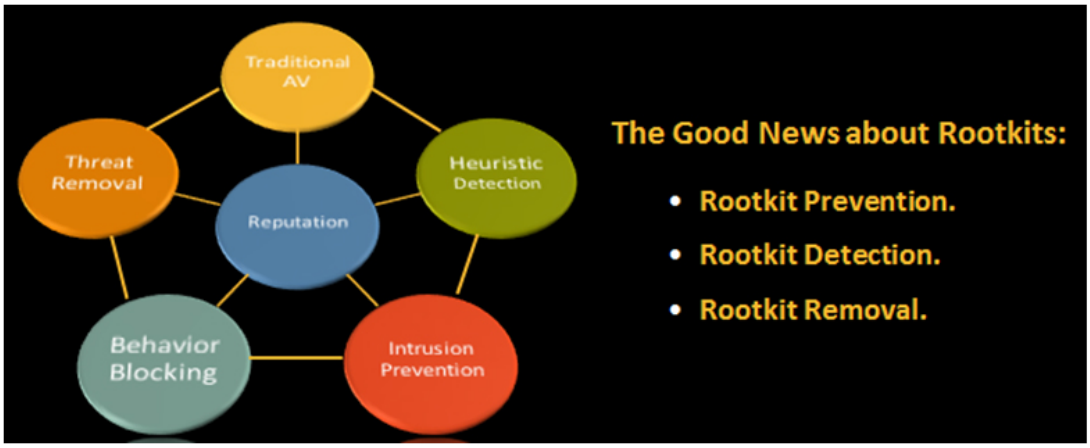
Overview

Computer security has become a hot topic for the news industry. Hardly a week passes without some new threat or data breach making headlines. Increased media coverage of these attacks reflects the growing need for everyone to be educated about secure computing, not just system administrators and security professionals. As with news in general, the more sensational or frightening the security story, the more attention it will get. A regular candidate for these stories are rootkits. Writers and editors, aided by the security community, spook users with tales of malicious rootkits with cryptic names such as **Duqu** and **Stuxnet** that are capable of no end of damage.

Rootkits have been around for some time—longer than many other types of malware. They still make the news, though, because they are scary. And they really are scary...if you lack proper protection. The good news is that Symantec security products such as Norton Internet Security and Symantec Endpoint Protection provide powerful protection against these malicious tools. Our security products use a broad range of technologies to prevent against, detect, and remove rootkits (figure 1).

Figure 1

Symantec Solutions For Blocking Rootkits



What are Rootkits?

Broadly defined, a rootkit is any software that acquires and maintains privileged access to the operating system (OS) while hiding its presence by subverting normal OS behavior. A rootkit typically has three goals:

1. **Run:** A rootkit wants to be able to run without restriction on a target computer. Most computer systems (including Windows) have mechanisms such as Access Control Lists (ACLs) in place to prevent an application from getting access to protected resources. Rootkits take advantage of vulnerabilities in these mechanisms or use social engineering attacks to get installed so that they have no restrictions on what they are able to do.

2. **Hide**: Specifically, the rootkit does not want an installed security product to detect that it is running and remove it. The best way to prevent this is to appear invisible to all other applications running on the machine.

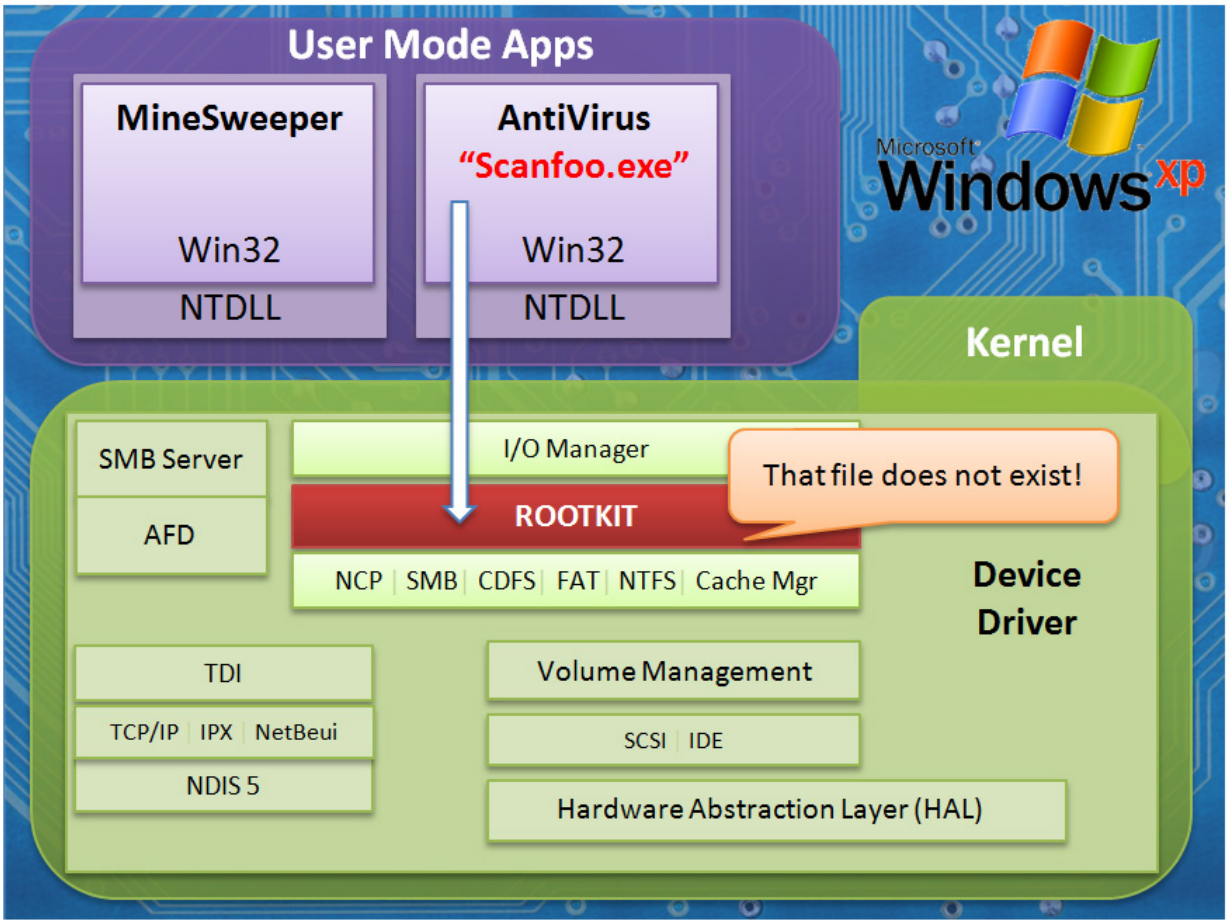
3. **Act**: A rootkit has specific actions it wants to take (often referred to as its payload). Running and being hidden are all well and good, but a rootkit author wants to get something from the compromised computer, such as stealing passwords or network bandwidth, or installing other malicious software.

So what does it mean that a rootkit "subverts" normal OS behavior? This subversion occurs when a rootkit hides by lying to other software on the computer. Most software relies on the OS to provide information about the environment in which it is running. For example, an application may have files that it needs to run, or data files that it needs to write to, or registry keys that are used for configuring the application. The application asks the OS about those files and registry keys using the application programming interface (API) provided by the operating system. (Examples include FindFirstFile to enumerate files, or RegOpenKeyEx to get access to the registry). The OS then returns the appropriate information to the application.

These same APIs are often used by security software when scanning for malicious software. In order to hide, rootkits hijack these APIs and watch for any question an application may ask that might be incriminating. So imagine that an application asks, "Operating system, can you show me the contents of the file at c:\foo.exe?" The rootkit intercepts the question before it gets to the operating system and quickly replies (as if it were the operating system), "That file does not exist." (figure 2)

The same sort of conversation might take place when looking at registry settings, which are used to configure individual applications and the OS itself. The best rootkits will not only prevent their files from being read (as in the "foo.exe" example), but will completely hide their existence from other software running on the machine.

Figure 2
Rootkit subversion



There are a number of techniques a rootkit can use to subvert normal operating system behavior:

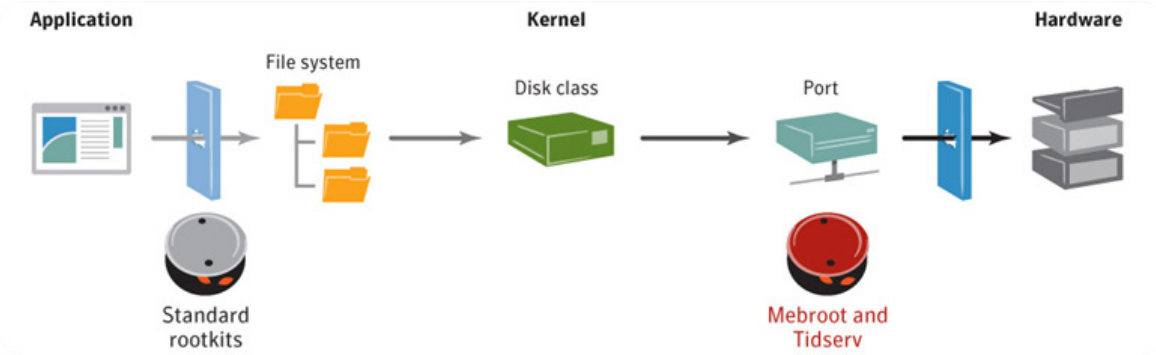
1. **Hooking operating system APIs**: Some rootkits re-route OS APIs by changing the address of these APIs to point to their own code. This can be done both in user mode (where most applications run) and kernel mode (where device drivers run) and is often referred to as "hooking." When an application calls a hooked API, the system looks up the address of the API in a table (such as the System Service Dispatch Table in kernel mode or the Import Address Table in user mode). The operating system then executes the code at that address. If a rootkit has hooked the API, it has changed the address in the table to point to its own code so that its code runs, rather than the expected system functionality. This allows the rootkit to intercept requests that might reveal its presence.

2. **Hiding in unused space on the machine's hard disk**: This unused space is invisible to normal OS APIs that are used to look for files on the hard disk. The rootkit will then modify a commonly used driver (such as atapi.sys) so that when that driver loads it will look in this unused space to find the rest of the rootkit's code.

3. **Infecting the master boot record (MBR)**: The rootkit may also infect the MBR in order to get its code into memory. **The MBR is used to bootstrap a system**, helping make the transition from the hardware portion of a computer's startup routine to loading the operating system itself. If a rootkit can control that process, then it can control what code gets loaded into memory before the OS even has a chance to protect itself.

Regardless of the technique used, a rootkit is trying to get its code running while hiding its presence from other applications running on the machine.

Figure 3
Rootkit Sophistication



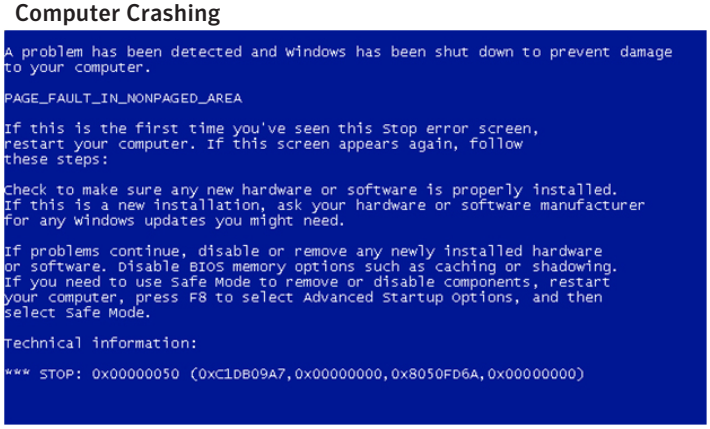
The combination of privilege and stealth make rootkits a particularly dangerous threat. In recent years, one of the most sensational examples of a rootkit was the **Tidserv family** of malware. Tidserv arrives on a machine much like any other piece of malware: through a drive-by download, from peer-to-peer file sharing software, bundled with other threats, or through a social-engineering attack (via email, SMS, etc.). When activated and depending on the version of the threat, Tidserv might hide in unused space, infect commonly used drivers, or infect the MBR in order to get itself running on the victim's system. Once Tidserv is running (and largely undetectable), the threat begins earning its keep by directing the victim to malicious websites, manipulating Web search results, displaying ads, or prompting the user to install more (usually malicious) software. Additionally, it can contact remote servers in order to update itself with new functionality. A computer infected with Tidserv is truly owned by the malicious software and, ultimately, by the attacker at the other end controlling it.

Although rootkits can effectively enable malware to keep a low profile while maintaining an infection, there are a few reasons why rootkits are not more widely used than they are. First, rootkit technology requires a higher level of sophistication to develop and maintain than more common malware techniques. Second, since rootkits typically rely on undocumented and unsupported features in the operating system, they are very sensitive to operating system changes. In February 2010, **many Tidserv rootkit infections surfaced when boot-time crashes started being reported after an unrelated Windows update**. The update had invalidated some of the assumptions Tidserv had made about the operating system, which resulted in the crash.

Rootkit Prevention

Imagine discovering one day that your computer simply will not boot. No matter what you try, every time you try to reboot it, you are shown the cryptic blue screen of death. You borrow a friend's computer and start looking for a solution, only to find that Microsoft is telling you that you were probably infected with a very nasty rootkit. As you start looking for your recovery disks you realize that this going to be a very bad day.

Figure 4
Computer Crashing



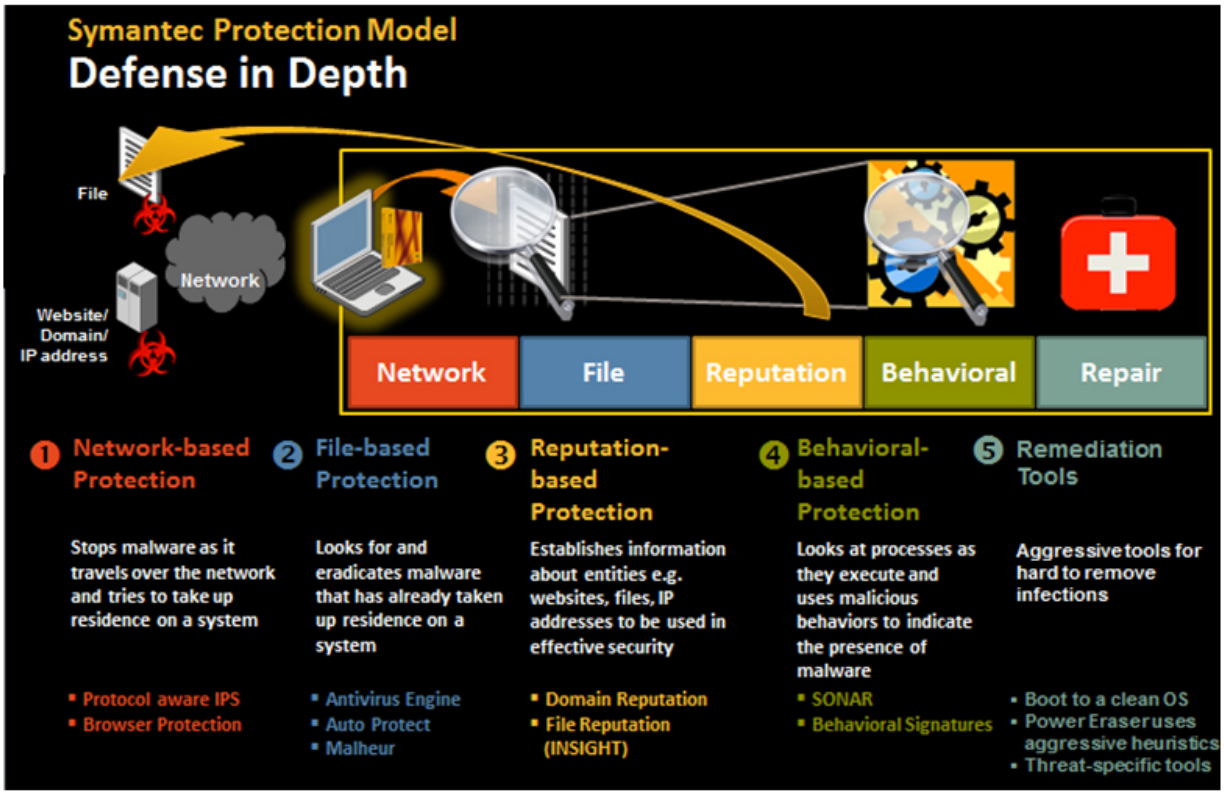
So what can you do (other than re-build your machine every time you suspect it is infected)? Even if you do not suspect anything is wrong with your computer (since that is what rootkit authors want), how can you be certain that some malicious code is not hiding there? When news stories cover these threats, they usually say that users should make sure that they are running security software and that it is up to date. But if a rootkit is already running and hiding from your security software, how does keeping it up to date help?

Symantec security products such as Norton Internet Security and Symantec Endpoint Protection include a number of technologies that are designed to prevent, detect, and

remove rootkits without being fooled by the tricks rootkits use to remain hidden. Using a variety of technologies working individually and together, these products provide top-quality protection against rootkits. The components work together as a protection stack by monitoring a variety of inputs and behaviors on a protected system and sharing that information in order to get a complete picture of a potential attack, while still maintaining a low false-positive rate.

The components that provide this protection technology are delivered by the **Security Technology and Response (STAR)** organization within Symantec. This organization researches malware threats and trends, and builds technology to prevent and remediate all kinds of threats, including rootkits. The **STAR protection stack** combines network-, file-, reputation-, and behavior-based protection. These layers of protection enable Symantec products to prevent and detect rootkits. In addition to these layers of protection built into the products, we also provide tools for removing rootkits from computers that have already been infected. Figure 5, below, shows how our various layers of protection protect your computer against the different phases of a rootkit's attack.

Figure 5
Symantec Defense-in-Depth Protection



With rootkits, as with all threats, the best defense is a good offense. Almost all rootkits start off on a computer with a simple application that may be an .exe-based installer or some user-mode shell code that will install the actual rootkit and hide itself. For example, when Tidserv first arrives on a machine, and before it has installed its driver, it is just a regular executable file that is probably dropped on the machine by other malware or via a drive-by download. Obviously, a good security solution will detect the rootkit before it can get its hooks into the system.

Network-Based Protection

The first layer of protection in the STAR security solution is our intrusion prevention system (IPS), which blocks threats that attempt to get onto a machine. As noted earlier, a common way malware gets onto computers is when users visit an otherwise innocuous website that has been compromised and is hosting an attack toolkit that serves up drive-by downloads. If the attack toolkit can exploit a bug in out-of-date or vulnerable browser software that the user is running, it then silently downloads malware such as a rootkit onto the vulnerable visitor's computer. Since most malware is now delivered via Web-based attacks, this is often the first opportunity for a Symantec IPS to detect and prevent an attack. Our IPS

technology intercepts network traffic when it sees malicious patterns of Web-attack toolkits or characteristics of vulnerabilities being exploited from a malicious website. Symantec IPS also adds protection into the browser to safeguard it against threats designed to take advantage of browser vulnerabilities—even if they are obfuscated or include complex JavaScript. Thus, if a user visits a site hosting malicious content that tries to infect the user's computer with a rootkit, IPS can block the threat either at the network layer or in the browser before it has a chance to download—thus protecting the user's system.

Network-based detection is one of the most powerful ways to block malware in general. It is much easier for malware authors to modify their files than it is for them to modify their network traffic patterns. Strong IPS protection allows Symantec to prevent malware from ever landing on a machine. Blocking threats at this level is the fastest, safest way to keep a computer clean. In recent years, Symantec has observed a marked increase in the percentage of threats blocked by our IPS engines as compared to more traditional antivirus engines. In 2010, for example, half of the threats that Symantec detected were blocked using network-based protection.

File-Based Protection

In the rare case that malware evades network defenses, or is introduced onto a user's computer through a non-network-based vector such as a USB key, Symantec employs the additional defense of file-based protection. When a file is written to the computer's disk or accessed by the user, the file is immediately scanned by Symantec AutoProtect technology and our antivirus engines. The scan looks for known signatures as well as for known malicious patterns. Additionally, the Symantec MalHeur (short for Malware Heuristics) engine is able to detect previously unknown malicious files based on patterns developed from our having previously detected millions of other threats. The MalHeur engine compares the characteristics of the potentially malicious file against the attributes of millions of sample files (both benign and malicious) to logically detect previously unseen malware. Thus, Symantec technologies can quickly identify and remove potentially malicious files that appear similar to other known rootkit installers before they are ever allowed to run.

Reputation-Based Protection

What about a completely new threat that does not resemble any known rootkit installers and that defies pattern identification? This is where Symantec's reputation technology comes into play. Norton Internet Security and Symantec Endpoint Protection receive anonymous telemetry information about executable files installed and running on our customers' machines. By combining information from millions of users, we can build a file's reputation. For example, if we determine that a file exists on millions of our customers' machines and that those machines are not reporting errors, we can be fairly certain that the file is not malicious. On the other hand, the likelihood that we will investigate a file as being potentially malicious increases if that file exists only on a handful of machines. Along with the prevalence of the file, the length of time we have known about the file also contributes to its reputation.

Symantec's Download Insight technology uses this reputation profile for any new executable content our customers download. If the file has a bad reputation (or no reputation) we can block the file before it gets a chance to infect the system. Thus, a previously unknown rootkit installer that is unwittingly downloaded onto a Symantec protected machine will not get to run specifically because we have never seen it before.

Behavioral-Based Protection

Finally, if a rootkit installer is introduced by removable media, there is Symantec's SONAR behavioral-based protection technology. SONAR monitors more than 1300 different application behaviors in real time. This means that, as an application launches, SONAR scans the application for potentially malicious activity. SONAR tracks whether an application tries to install new services or drivers, wants to inject code into other processes, or if it tries to modify system files or perform other malicious actions. SONAR also checks the reputation of the file that is attempting to run. If SONAR determines that the application is malicious, it can quarantine it before it is able to infect the system. SONAR technology successfully provided zero-day protection for such high-profile threats as **Hydraq**, **Imsolk** and Stuxnet.

Rootkit Detection Techniques

The technologies discussed thus far are all excellent at preventing a rootkit from ever being installed on a system. It should not be surprising then, that these same technologies also prevent every other type of malware from infecting a system. In other words, the prevention of rootkits and prevention of other types of threats all rely on similar mechanisms. If a rootkit has already infected a system, though, the detection and removal of the rootkit requires much more sophisticated techniques than are required for a typical infection. Basically, the best prevention relies on the fact that the rootkit has not yet had a chance to hide itself in the system. Once the rootkit installer has been able to do its work, though, things get trickier.

That is why products that use the STAR protection stack, such as Norton Internet Security and Symantec Endpoint Protection, do not stop at prevention. Rather than relying on the OS to return accurate values when asked straightforward questions, our products dig deep beneath the OS to find the truth. This is done by building technologies that directly scan and safeguard the system's registry, disk, and memory.

Direct Registry Scanning

The registry is basically the brains of the Windows OS. Windows uses the registry to store important information such as which applications and drivers should run upon each bootup (figure 6). Windows provides APIs (RegOpenKeyEx, RegGetValue, RegSetValue, etc.) for storing and retrieving information in the registry. As noted, these APIs can be subverted by rootkits to return incorrect or incomplete information.

The registry itself, however, is ultimately stored as a set of files on the computer's hard disk. STAR technology, though, can read the registry directly from disk without relying on signals from the OS APIs. For example, the STAR ERASER engine, which is responsible for checking that drivers and applications that run at startup are not malicious, uses this direct registry access technology. Thus, even if a rootkit is using system APIs to lie to everyone else, ERASER can detect what is really going on. In this way, it can find rootkits that load and attempt to hide on start up.

Direct Disk Scanning

Imagine, though, that a rootkit driver is hidden in the registry AND in the file system. Even if ERASER knows the driver should be present because the registry points to it, if it cannot find it on the disk, then it cannot scan and detect it. ERASER solves this issue using Veritas VxMS technology to bypass the OS APIs for file system access and scanning the disk directly (figure 7). If the scan reveals that the file is malicious, ERASER then renames the file on the next boot up before the OS has a chance to load the malicious driver. We refer to this patented mechanism as the "one-and-a-half boot solution for malware removal." Once the file is renamed, it will not be loaded by the OS, and regular remediation actions are then launched to remove the threat.

Kernel Memory Scanning

Sometimes, though, even the ability to scan a file as it appears on disk is not enough to detect the file. This can happen because the file on disk may be obfuscated or constructed in such a way that it evades traditional signature detection. In this case, the ERASER component, acting in conjunction with traditional Symantec antivirus engines, has the ability to scan the memory when the rootkit is loaded (figure 8). To do this, ERASER

Figure 6
Direct Registry Scanning

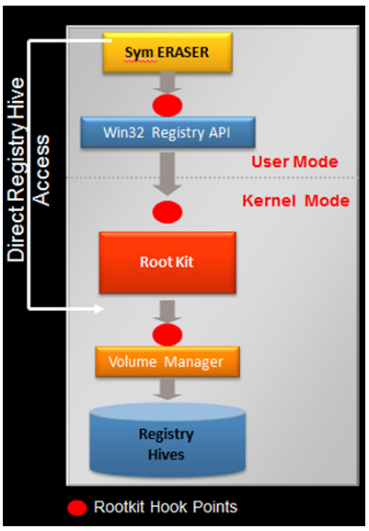


Figure 7
Direct Disk Scanning

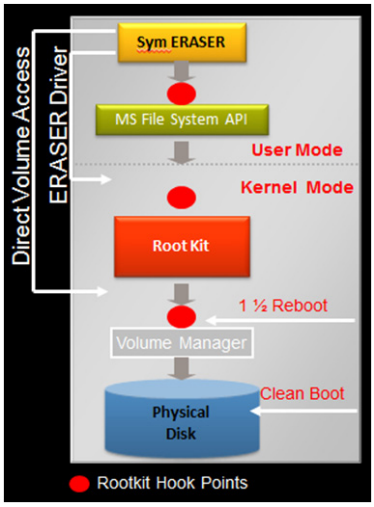
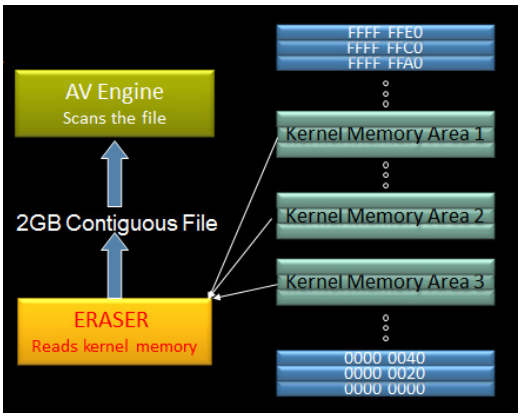


Figure 8
Kernal Memory Scanning



reads the entire kernel memory space and then passes it to our antivirus engine for scanning. In this way, we can detect threats that may try to hide on disk, but which are still loaded and running in kernel memory.

Network Activity Scanning

Another very powerful tool we use to detect rootkits relies, again, on our network-threat protection technology. Just as our IPS technology watches for attacks on protected machines, it also watches for traffic being sent from the computer that is possibly being generated by installed malicious applications. A rootkit successfully installed and hidden on a computer and evading antivirus software still needs to occasionally "phone home" to its control server. As mentioned earlier, it is much easier for rootkit authors to change what their files look like than it is for them to change the pattern of their network traffic. When our IPS technology detects a traffic pattern that we know comes from a rootkit, we can notify the user to take specific actions to remove the threat. For example, using our IPS technology, we regularly detect Tidserv-infected computers due to the network traffic pattern of that threat, and then provide customers with tools to remove it.

Rootkit Removal Techniques

If the rootkit is hiding, though, how can we remove it? What if our IPS technology determines that a rootkit is installed on the system but it is evading removal? What if the computer is infected but does not have our solutions already installed? To handle these tough cases, the STAR team provides some powerful tools to rip the rootkit from the computer.

Symantec Power Eraser and **Norton Power Eraser** provide our customers with the best tools to root out and destroy all types of malware (figure 9). These products use STAR's Symantec Maximum Repair library (SMR) to track down and eliminate threats. Power Eraser uses many of the same detection techniques used in ERASER, but combines them with a very aggressive, updatable conviction engine. This additional level of aggression comes at the cost of possibly convicting applications which are not malicious. In that case, though, these "false positives" are filtered out using our reputation technology. Power Eraser also uses aggressive techniques to remove detected threats. Since Power Eraser is a stand-alone tool, it can be used on computers that have no security product installed. This is a great help when trying to clean up an unprotected machine that is badly infected with rootkits or other malware.

Beyond the detection and removal capabilities of Power Eraser, we also build targeted tools to quickly get fixes for specific threats into the field. An example of this is our **Tidserv tool**. This tool was developed to specifically detect and remove the Tidserv rootkit. Because we were able to get the tool into the field quickly, we were able to get help to existing and new customers who needed to restore their compromised computers back to health. Since its release, this tool has been rolled into SMR and is now available as part of Power Eraser. Having the ability to quickly release tools for new threats allows us to get protection to our customers without requiring that they wait for a new product release.

In addition to these very powerful tools, we also provide the **Norton Bootable Recovery Tool** and the **Symantec Endpoint Recovery Tool**. These tools allow users to create a bootable CD that can be used to detect and remediate a machine completely outside the scope of the influence of the rootkit.

All of these removal tools are in addition to the excellent remediation capabilities already built into the products themselves. Symantec security products can readily handle the vast majority of threats, usually without even letting threats such as rootkits be installed on a computer. Users will only need these special removal tools when they suspect that something has gotten past their security product or to clean a machine without having these products installed.

Summary

Rootkits make it into the news because they are scary. Even though they are scary, products such as Symantec Endpoint Protection and Norton Internet Security protect you against rootkit attacks every day. By looking below the operating system, we find rootkits where they are hiding. And by using aggressive, targeted tools and techniques, we give even novice users a simple, easy to use, and safe way to eradicate rootkits from infected systems. And we do all this without you having to reinstall or image your entire operating system—so you can stop looking for those recovery disks. Rootkits may be scary, but with the amount of protection and remediation we provide you, the good news is that the rootkits should be scared of us.

Symantec
Security Response

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Moutain View, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

Credits

Spencer Smith
Technical Director
Security Technology and Response
Symantec Corporation

John Harrison
Group Product Manager, Product Management
Security Technology and Response
Symantec Corporation

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527-8000
www.symantec.com