A *Podcast Briefing* produced by SearchSecurity.com

Rootkits: What They Are and How to Fight Them

TechTarget
The Most Targeted
IT Media

Sponsored By: webroot
SOFTWARE, INC.

SearchSecurity.com

Rootkits: What They Are and How to Fight Them

a Podcast Briefing presented by Gerhard Eschelbeck and Paul Gillin

■ This *Podcast Briefing* is based on a Webroot/TechTarget Podcast: "Rootkits: What They Are and How to Fight Them."

Rootkits: A Hidden Security Threat

Rootkits are the latest IT security threat to make the headlines. Anyone who has heard of rootkits knows their nasty reputation: They cannot be removed, they can live on a computer for years without being discovered, and they can wreak havoc with the operating system.

This *Podcast Briefing* gives computer users a clear explanation of what a rootkit is, separates the facts from the myths about rootkits, and provides recommendations on how users can defend against rootkit infections, and detect and remove them from their systems. It concludes with a question-and-answer session with a security expert who has many years of experience fighting rootkits.

"Rootkit" Defined

According to www.whatis.com, a rootkit is "a collection of tools that enable administrator-level access to a computer or a computer network."

According to security expert Greg Hoglund, a rootkit is "a tool that is designed to hide itself and other processes data and/or activity on a system." Despite their bad reputation, rootkits actually have some very useful applications, such as managing licenses or concealing files that a computer administrator does not want others to see. The problem with rootkits is that programs that conceal things and provide remote administrative access can also be exploited to cause trouble. Today, rootkits are most often used to compromise computer security, making it critical for users to be aware of them. Rootkits are basically a platform for spyware, Trojans, phishing software, and other harmful applications.

The Sony Story

Rootkits became a big story in the fall of 2005 when a security research firm discovered that rootkit software was being distributed on music CDs published by Sony Music. The CD actually installed a rootkit on unsuspecting users' computers when it was inserted into the disk drive. Sony had included the rootkit as part of its Digital Rights Management initiative, but failed to warn users that they were getting this payload as a hidden bonus. The incident was a headache for Sony, but it did raise awareness about the potential security threats of rootkit technology.

An Unlimited Potential for Harm

Rootkits by themselves are not harmful, but they can be exploited by malware writers to do harm. In their worst form, rootkits can be installed on a computer by a hacker, cracker, or other criminal to give a program administrator or other individual access that can be exploited at any time. Once a rootkit is installed, a harmful program may spread to other computers on the network. The fact that a single compromised computer can put the entire network at risk makes rootkits a particularly thorny problem for IT organizations.

An Ideal Tool in the Hands of Computer Criminals

Rootkits have become a bigger problem in recent years because today's computer criminals are financially motivated. The strength of a rootkit is that it allows a remote user to control an unsuspecting victim's system—precisely the tool a criminal wants. Once maldoers have a backdoor into an individual's computer, they can collect all kinds of information about where this person goes, what he or she

Inside...

buys, and what credit cards the victim uses to pay for things.

Rootkits are commonly used to exploit spyware and programs that monitor keystrokes. Rootkits can also serve as a launchpad for worms and viruses. In fact, some worms actually contain rootkits, which they install on infected computers to enable their proliferation throughout a network. The biggest danger of rootkits is that they can give a remote user so-called "shell access" to a system—meaning that the attacker has virtually complete control of that system. The harm that viruses in spyware can do is generally limited; not so for rootkits. By serving up control of almost any function on a computer, rootkits have an almost unlimited potential for mischief.

Their Insidious Reach

Rootkits can exist at the kernel, library, and application levels. Kernel rootkits are especially dangerous and are the focus of a great deal of attention because they can be so hard to detect. One of the really tricky characteristics of rootkits is that some types can actually bind themselves tightly to the operating system—so tightly, in fact, that they can be nearly impossible to detect. In effect, they take over the operating system in such a manner that the user cannot trust the information the operating system is giving him or her.

Conventional anti-spyware and antivirus programs are powerless in this situation because they rely on the operating system for status information, and the operating system itself has been compromised. Understandably, this nasty characteristic of rootkits has created some hysteria, giving rise to the myth that rootkits are simply impossible to remove short of reformatting the disk drive and reinstalling the Windows operating system. While some rootkits can indeed be very insidious, the fact is that almost all can be detected by shutting down an infected computer and restarting from a bootable disk. An inactive rootkit cannot hide itself—at least not yet.

What To Do If You Become Infected

One school of thought says that it is faster to simply back up your files and reformat the computer, but admittedly that is an extreme solution to the problem. A variety of freeware and open source rootkit detectors are available to address the problem, but the old admonition of "buyer beware" applies. Free rootkit detectors are typically not updated as often as commercial systems are, and with the pace of change in this technology, the user does not want to be behind the curve.

Because rootkits are so often used as a platform for spyware, the commercial vendors best equipped to attack the rootkit problem are those with extensive experience in spyware detection and removal. Just looking for erratic behavior is not enough. A good rootkit detection and removal program uses multiple vectors to identify a problem. The program should also have an up-to-date list of newly identified rootkits, so that "newcomers" do not slip in under the radar. This is one reason why it is so important for users to update their signature files.

It is also important to remember that not all rootkits are bad. Users do not want a rootkit detector that is simply going to destroy any violator it finds. The anti-rootkit software needs to be able to identify good and bad rootkits and let an administrator allow or disallow these programs.

Webroot Spy Sweeper Version 4.5

Webroot Software has been in the security business since 1997 and is a leading anti-spyware vendor. Webroot has proprietary technology that makes the company the leader in rootkit detection and removal. With 300 employees and millions of customers in numerous countries, Webroot has the expertise and the reach to track the latest in spyware and rootkit threats.

Its Spy Sweeper program has won many industry awards. Spy Sweeper Enterprise, the most effective anti-spyware solution available, protects corporate resources and users from damaging spyware such as rootkits, keyloggers, and Trojans. Real-time monitoring with Smart Shields adds additional protection by blocking spyware attempts before they reach the desktop. The new Spy Sweeper version 4.5 has won critical acclaim for its ability to find and destroy rootkits without disrupting the host computer. For more information, go to www.webroot.com.

The next section discusses the rootkit problem in greater detail, giving an overview of the changing threat landscape, how rootkits fit into that landscape, and how users can defend themselves against this new and growing threat.

Strategies for Detecting and Removing Rootkits: An Expert Weighs In

Paul Gillin: This segment discusses rootkit detection and removal with an expert in the computer security field. Gerhard Eschelbeck is Chief Technology Officer and Senior Vice President of Engineering at Webroot. With 15 years of experience in the field of computer security, Gerhard drives the overall product strategy at Webroot. Gerhard has testified before Congress, spoken at many major conferences, and been named one of InfoWorld's 25 Most Influential CTOs in 2003, 2004, and 2006.

Rootkits are not really a new technology. They have been around for some years. Why are they suddenly so much in the public consciousness?

Gerhard Eschelbeck: Rootkits have been around for many years in the Unix world, but over the past year or so, they have gotten significant attention, mostly because they have become prevalent in the Windows world as well. There have been a number of high-profile incidents where rootkits have been identified in various products in the industry, and that probably has contributed to this popularization of the concept of rootkits.

Gillin: If rootkits have been around for a long time and have not been doing any real damage, are they any more of a threat now than they were before all the recent publicity?

Eschelbeck: You have to look at the context to determine whether or not a rootkit is a threat. Hiding something is generally a bad idea, and the original intention of rootkits was to hide information or documentation. But, clearly, there is a fine line between the malicious and benign use of rootkits, and that fine line is really all about the intention. You have to ask yourself the following questions: First, how did this get on my computer? Was there an explicit attempt by someone to get this rootkit on my computer, or did this get on my computer in a very sneaky way? Second, could other malicious software hide itself within this rootkit? Answering these questions will allow you to determine whether the rootkit was intended for harmful or harmless purposes. There are certainly some good uses of rootkits, especially in the areas of license management, self-protection of some types of software for administrators, and so on.

Gillin: I understand that rootkits can so enmesh themselves at the operating system level that some can actually be impossible to remove. Have you found that to be the case?

Eschelbeck: It depends on how the rootkit is implemented. You can have implementations at the kernel level or at the user-mode level. In general, the intention of a rootkit is to hide information, to hide processes, to hide files from the user, and therefore, not only the removal but the detection is quite complicated and difficult. Users have to have some really sophisticated techniques to be able to identify rootkits on their machines, and then to remove them. Removal is even more complicated than detection, because you have to make sure that the operating system will continue to work after removing the rootkit. Most of today's rootkits can be removed from your system pretty safely, but a year or two from now, removing a rootkit may pose a significant challenge.

Gillin: You have done extensive work on rootkits for Webroot. Are you finding that the manner in which rootkits embed themselves in operating systems is getting stronger and more sophisticated?

Eschelbeck: Sure, but it is not only rootkits that have evolved over the past several years. The whole threat landscape has evolved significantly in recent years. Ten years ago, the virus was the big thing in the IT world, and then it was the worm circulating on the Internet, and now it is all about spyware, and spyware is driven a lot by financial motives. As a spyware writer, you make an effort to hide as much as you can. And that really was a big catalyst for the development of rootkit technologies as well, because spyware utilizes rootkit technologies to become stealthier, more hidden from the user, and more malicious. This is a very big challenge today for end-users, for consumers, and for enterprises as well.

Gillin: What are some of the most difficult aspects of detecting and removing rootkits?

Eschelbeck: The rootkit is all about hiding information. Essentially you cannot trust the operating system anymore. As soon as you have a rootkit on your machine, nothing the operating system tells you is necessarily trusted information. So, the first step in removing a rootkit from the operating system is to introduce technology that is capable of understanding the lowest levels of that system, for example, how hard disks are formatted. The technical capability to sit below the operating system allows you to identify any pieces on the operating system that potentially indicate the presence of a rootkit. So, clearly, a very high level of sophistication and knowledge about a particular operating system is necessary. A key requirement for the Webroot research and development team developing advanced rootkit detection, removal, and prevention techniques is knowledge of the Windows operating system.

Gillin: Are rootkits necessarily operating-system dependent? Is there such thing as a rootkit that will attack or work with Windows, Linux, and even the Macintosh?

Eschelbeck: Not today. Today's rootkits are pretty targeted to unique platforms. They are very specific in that they really take advantage of the unique capabilities in those operating systems.

Gillin: There are a lot of free rootkit detectors out there and really no way to tell whether one is better than another. What does Webroot bring to this technology that users cannot download as shareware?

Eschelbeck: Webroot has pioneered much of the anti-spyware and anti-rootkit technologies that are in use today. In the malware space, it is all about timing—how quickly you can get detection, removal, and prevention back to your customers to protect them from the latest keyloggers, Trojans, rootkits, and so on. One of the big advantages that Webroot offers is a system called Phileas. This is an automated research system that works like a search engine for malware, providing visibility on any new threats as they evolve. Our research team has access to those threats and can analyze and engineer them before any of our customers get infected.

Gillin: In testing the quality of some of the Freeware rootkit detectors out there, is Webroot in fact finding rootkits that others do not routinely find?

Eschelbeck: It is actually quite often the case that we have signatures of malware in our research lab before they are actually visible to the world or before they have had a chance to infect customers, mostly because of Phileas, our research system, which gathers and collects new pieces of malware from the Internet 24 hours a day. We can analyze these rootkits and provide our customers with detection and signatures before they even get infected.

Gillin: When you are detecting rootkits, do you look for certain patterns of behavior, or is it more a matter of just being aware of what is out there on the Internet and looking for signatures that you have discovered?

Eschelbeck: Rootkit detection is really a combination of both. Because these detection technologies sit well below the operating system, we can compare what the operating system sees on the machine versus what the technology is seeing at the lowest level of the operating system. If the two match up, the operating system is most likely clean and safe, but if there are discrepancies between the two, then you clearly have to take a closer look because it could be an indication of a potential rootkit infection. So, there are some generic capabilities that really do not need a signature whatsoever, because they basically look at behavior and patterns, but there are also some very specific signatures that look for certain instances of malware that cannot necessarily be detected by simple behavioral analysis capabilities. So, really it is a combination of the two that gives rootkit detection technologies their power.

Gillin: In your opinion, do most PC users have a rootkit installed and probably do not know it?

Eschelbeck: That is an interesting question. Our statistics for keyloggers and Trojans, which very often use rootkits to conceal themselves, show a significant increase in the numbers of these infections. For example, we saw an infection rate of about 29% earlier this year versus 24% for the latter part of last year.

Gillin: And is it correct that if people are using their standard anti-virus, anti-spyware products, they are probably not detecting these rootkits? Or has that become part of the standard security suite?

Eschelbeck: A big part of the challenge today is that users really do not know whether or not they are infected. Rootkits remain hidden from user view and users would rarely know they are installed on their computers. Many of the existing technologies do not have specific capabilities to identify rootkits on machines. So, the user really has to consider more advanced rootkit detection technologies to be able to detect the kinds of rootkits we have been talking about.

Gillin: Do users need to do anything more than just adding rootkit detection to their software suite? Do they need to change their behavior in some way?

Eschelbeck: Users can take a few steps to reduce the overall exposure and risk of rootkit infection. These are:

1. Keep your system healthy by making sure that computers are patched at the latest possible patch level, especially if you have a Microsoft operating system. Microsoft releases new patches the second Tuesday of every month, so it is important to keep those updated. This applies not only to Microsoft applica-

tions but to any other applications that are on the system as well.

2. Think about logging on to your computer as a non-administrative user. It is easier said than done, but the reality is that if you reduce your privileges by logging on as a regular user versus an administrative user, you are significantly reducing the risk and the potential for an infection on your computer.
3. Always update your antivirus and anti-spyware technologies at the same time.

Gillin: You mentioned earlier that rootkits are not necessarily bad. It is a technology that can be used to enable malware. What are some good applications of rootkits?

Eschelbeck: As I said before, there is a fine line between good uses and bad uses, and it is really all about the intent. There are certainly some applications where rootkits can be used in a meaningful and non-malicious way, such as license management or self-protection of software. Self-protection from malware is a classic scenario where rootkit technology may be helpful and supportive, but again it is really all about the intention. There are really two key criteria. Does the user know that this rootkit is on his or her system? And, is this rootkit a potential backdoor for somebody else to write malware that uses the rootkit to hide itself?

Gillin: Would you give a couple of examples of what could happen if you have a rootkit installed? How can it be leveraged to cause damage?

Eschelbeck: A good example would be the Sony CD copy-protection rootkit, which was very widely publicized at the end of October last year. As part of Sony's copy protection scheme, software was installed on users' computers without their knowledge when they put in the CD, and this software was fundamentally a rootkit. Sony basically did not disclose this to the user base and that was one reason why it created such media attention. But a second issue was discovered a few days later, which was probably the bigger part of it. The fact was that this rootkit was not just limited to Sony's use in making their CDs copy-protected. It could be used to write malware, and the malware writer could very easily hide the malware in the Sony rootkit. A lot of users who had this Sony rootkit became potential victims of malware that was taking advantage of that design flaw in the rootkit. So, it was a benign rootkit created by Sony for legitimate purposes, but it had a design flaw that made it potentially harmful.

Gillin: Tell us what you think the future holds. You said earlier that virus activity has actually died down somewhat and more activity has shifted to rootkits. In fact, is this going to be an evolution of the security battle? Will rootkits now be a more common enemy, or is this just one more problem that we have to worry about, and the other problems are just as bad as they ever were?

Eschelbeck: The threat landscape is shifting. There have not been any significant worm outbreaks since 2003. Today's malware writers target the user directly through web browsers and e-mail. And one of the big reasons why this is happening is because recent malware, particularly spyware, is all financially motivated. People want to make money with these particular malware distribution schemes, and that is why we are not going to see it go away anytime soon. As mentioned earlier, our research showed a 29% increase in keylogger interactions earlier this year. That is a pretty big number actually, if you think about it, and at the same time, we also saw a shift in where this malware is coming from. China now distributes 40% of the spyware that is out there, followed by the U.S. at 17%.

Gillin: What should users do to protect themselves from this latest threat to their security?

Eschelbeck: I always recommend that users beware of the many offers to download free software from the Internet. Free software is not necessarily free. Those "free" offers may contain malware or rootkits, and users can certainly take proactive steps to prevent these infections from happening. It is also very important to avoid questionable Internet sites where you could become a victim of spyware and malware writers. Try to focus on sites that are trusted and that give users a good level of protection. Next, always patch your systems. Keep your systems updated with the latest patches that are available. And lastly, keep your antivirus and anti-spyware technologies updated.

■ **Paul Gillin** is a veteran technology journalist with 19 years of editorial management experience, including positions as Chief Editor of TechTarget and Computerworld.

■ **Gerhard Eschelbeck** is Chief Technology Officer and Senior Vice President of Engineering at Webroot.

About TechTarget *Podcast Briefings*

TechTarget *Podcast Briefings* provide the pertinent information that senior-level IT executives and managers need to make educated purchasing decisions. Originating from our industry-leading Vendor and Expert Podcasts, TechTarget-produced *Podcast Briefings* turn Podcasts into easy-to-follow technical briefs, similar to white papers.

For inquiries and additional information, contact:
Dennis Shiao, Director of Product Management, Webcasts
dshiao@techtarget.com

About TechTarget

We deliver the information IT pros need to be successful.

TechTarget publishes targeted media that address your need for information and resources. Our network of technology-specific Web sites gives enterprise IT professionals access to experts and peers, original content, and links to relevant information from across the Internet. Our conferences give you access to vendor-neutral, expert commentary and advice on the issues and challenges you face daily. Our magazines—*CIO Decisions*, *Information Security*, *Storage*, and *WinStorage*—give you in-depth analysis and guidance on the critical IT decisions you face. Practical technical advice and expert insights are distributed via more than 80 specialized e-Newsletters, and our Webcasts allow IT pros to ask questions of technical experts.

What makes us unique

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals. We leverage the immediacy of the Web, the networking and face-to-face opportunities of conferences, the expert interaction of Webcasts and Web radio, the laser-targeting of e-mail newsletters and the richness and depth of our print media to create compelling and actionable information for enterprise IT professionals. For more information, visit www.techtarget.com.

TechTarget
The Most Targeted
IT Media