10+ things you should know about rootkits

Version 1.0
September 17, 2008

By Michael Kassner

Rootkits are complex and ever changing, which makes it difficult to understand exactly what you're dealing with. Even so, I'd like to take a stab at explaining them, so that you'll have a fighting chance if you're confronted with one.

1 What is a rootkit?

Breaking the term *rootkit* into the two component words, *root* and *kit*, is a useful way to define it. *Root* is a UNIX/Linux term that's the equivalent of Administrator in Windows. The word *kit* denotes programs that allow someone to obtain root/admin-level access to the computer by executing the programs in the kit -- all of which is done without end-user consent or knowledge.

2 Why use a rootkit?

Rootkits have two primary functions: remote command/control (back door) and software eavesdropping. Rootkits allow someone, legitimate or otherwise, to administratively control a computer. This means executing files, accessing logs, monitoring user activity, and even changing the computer's configuration. Therefore, in the strictest sense, even versions of VNC are rootkits. This surprises most people, as they consider rootkits to be solely malware, but in of themselves they aren't malicious at all.

One famous (or infamous, depending on your viewpoint) example of rootkit use was Sony BMG's attempt to prevent copyright violations. Sony BMG didn't tell anyone that it placed DRM software on home computers when certain CDs were played. On a scary note, the rootkit hiding technique Sony used was so good not one antivirus or anti-spyware application detected it.

3 How do rootkits propagate?

Rootkits can't propagate by themselves, and that fact has precipitated a great deal of confusion. In reality, rootkits are just one component of what is called a *blended threat*. Blended threats typically consist of three snippets of code: a dropper, loader, and rootkit.

The dropper is the code that gets the rootkit's installation started. Activating the dropper program usually entails human intervention, such as clicking on a malicious e-mail link. Once initiated, the dropper launches the loader program and then deletes itself. Once active, the loader typically causes a buffer overflow, which loads the rootkit into memory.

Blended threat malware gets its foot in the door through social engineering, exploiting known vulnerabilities, or even brute force. Here are two examples of some current and successful exploits:

- **IM.** One approach requires computers with IM installed (not that much of a stretch). If the appropriate blended threat gains a foothold on just one computer using IM, it takes over the IM client, sending out messages containing malicious links to everyone on the contact list. When the recipient clicks on the link (social engineering, as it's from a friend), that computer becomes infected and has a rootkit on it as well.
- **Rich content.** The newest approach is to insert the blended threat malware into rich-content files, such as PDF documents. Just opening a malicious PDF file will execute the dropper code, and it's all over.

4 User-mode rootkits

There are several types of rootkits, but we'll start with the simplest one. User-mode rootkits run on a computer with administrative privileges. This allows user-mode rootkits to alter security and hide processes, files, system drivers, network ports, and even system services. User-mode rootkits remain installed on the infected computer by copying required files to the computer's hard drive, automatically launching with every system boot.

Sadly, user-mode rootkits are the only type that antivirus or anti-spyware applications even have a chance of detecting. One example of a user-mode rootkit is Hacker Defender. It's an old rootkit, but it has an illustrious history. If you read the link about Hacker Defender, you will learn about Mark Russinovich, his rootkit detection tool called Rootkit Revealer, and his cat-and-mouse struggle with the developer of Hacker Defender.

5 Kernel-mode rootkit

Malware developers are a savvy bunch. Realizing that rootkits running in user-mode can be found by rootkit detection software running in kernel-mode, they developed kernel-mode rootkits, placing the rootkit on the same level as the operating system and rootkit detection software. Simply put, the OS can no longer be trusted. One kernel-mode rootkit that's getting lots of attention is the Da IOS rootkit, developed by Sebastian Muniz and aimed at Cisco's IOS operating system.

Instability is the one downfall of a kernel-mode rootkit. If you notice that your computer is blue-screening for other than the normal reasons, it just might be a kernel-mode rootkit.

6 User-mode/kernel-mode hybrid rootkit

Rootkit developers, wanting the best of both worlds, developed a hybrid rootkit that combines user-mode characteristics (easy to use and stable) with kernel-mode characteristics (stealthy). The hybrid approach is very successful and the most popular rootkit at this time.

7 Firmware rootkits

Firmware rootkits are the next step in sophistication. This type of rootkit can be any of the other types with an added twist; the rootkit can hide in firmware when the computer is shut down. Restart the computer, and the rootkit reinstalls itself. The altered firmware could be anything from microprocessor code to PCI expansion card firmware. Even if a removal program finds and eliminates the firmware rootkit, the next time the computer starts, the firmware rootkit is right back in business. John Heasman has a great paper called "Implementing and Detecting a PCI Rootkit" (PDF).

8 Virtual rootkits

Virtual rootkits are a fairly new and innovative approach. The virtual rootkit acts like a software implementation of hardware sets in a manner similar to that used by VMware. This technology has elicited a great deal of apprehension, as virtual rootkits are almost invisible. The Blue Pill is one example of this type of rootkit. To the best of my knowledge, researchers haven't found virtual rootkits in the wild. Ironically, this is because virtual rootkits are complex and other types are working so well.

9 Generic symptoms of rootkit infestation

Rootkits are frustrating. By design, it's difficult to know if they are installed on a computer. Even experts have a hard time but hint that installed rootkits should get the same consideration as other possible reasons for any decrease in operating efficiency. Sorry for being vague, but that's the nature of the beast. Here's a list of noteworthy symptoms:

- If the computer locks up or fails to respond to any kind of input from the mouse or keyboard, it could be due to an installed kernel-mode rootkit.
- Settings in Windows change without permission. Examples of this could be the screensaver changing or the taskbar hiding itself.
- Web pages or network activities appear to be intermittent or function improperly due to excessive network traffic.

If the rootkit is working correctly, most of these symptoms aren't going to be noticeable. By definition, good rootkits are stealthy. The last symptom (network slowdown) should be the one that raises a flag. Rootkits can't hide traffic increases, especially if the computer is acting as a spam relay or participating in a DDoS attack.

10 Polymorphism

I debated whether to include polymorphism as a topic, since it's not specific to rootkits. But it's amazing technology that makes rootkits difficult to find. Polymorphism techniques allow malware such as rootkits to rewrite core assembly code, which makes using antivirus/anti-spyware signature-based defenses useless. Polymorphism even gives behavioral-based (heuristic) defenses a great deal of trouble. The only hope of finding rootkits that use polymorphism is technology that looks deep into the operating system and then compares the results to a known good baseline of the system.

11 Detection and removal

You all know the drill, but it's worth repeating. Be sure to keep antivirus/anti-spyware software (and in fact, every software component of the computer) up to date. That will go a long way toward keeping malware away. Keeping everything current is hard, but a tool such as Secunia's Vulnerability Scanning program can help.

Detection and removal depends on the sophistication of the rootkit. If the rootkit is of the user-mode variety, any one of the following rootkit removal tools will most likely work:

- F-Secure Blacklight
- RootkitRevealer
- Windows Malicious Software Removal Tool
- ProcessGuard
- Rootkit Hunter (Linux and BSD)

The problem with these tools is that you can't be sure they've removed the rootkit. Albeit more labor-intensive, using a bootable CD, such as BartPE, with an antivirus scanner will increase the chances of detecting a rootkit, simply because rootkits can't obscure their tracks when they aren't running. I'm afraid that the only way to know for sure is to have a clean computer, take a baseline, and then use an application like Encase to check for any additional code.

Final thoughts

Opinions vary when it comes to rootkit removal, as discussed in the NetworkWorld article "Experts divided over rootkit detection and removal." Although the article is two years old, the information is still relevant. There's some hope, though: Intel's Trusted Platform Module (TPM) has been cited as a possible solution to malware infestation. The problem with TPM is that it's somewhat controversial. Besides, it will take years before sufficient numbers of computers have processors with TPM.

If you're looking for additional information, I recommend the book *ROOTKITS: Subverting the Windows Kernel*, by Gary Hoglund and James Butler, of HPGary.

Michael Kassner has been involved with wireless communications for 40-plus years, starting with amateur radio (K0PBX) and now as a network field engineer for Orange Business Services and an independent wireless consultant with MKassner Net. Current certifications include Cisco ESTQ Field Engineer, CWNA, and CWSP.

Additional resources

- TechRepublic's Downloads RSS Feed XML
- Sign up for the Downloads at TechRepublic newsletter
- Sign up for our IT Leadership Newsletter
- Check out all of TechRepublic's free newsletters
- Detect rootkits and rootkit behavior with these techniques
- 10 things to look for in an anti-spyware application
- 10 things you should know about fighting spyware in Windows XP

Version history

Version: 1.0
Published: September 17, 2008