Rootkits 101

Wes Miller

wmiller@coretrace.com
Director of Product Management
CoreTrace ™

January 2008

CORETRACE

What is a Rootkit, Anyway?

- Hoglund and Butler write in “Rootkits: Subverting the Windows Kernel”:

  A rootkit is a set of programs and code that allows a permanent or consistent, undetectable presence on a computer.

- Mark Russinovich’s original definition:

  Software that hides itself or other objects, such as files, processes, and Registry keys, from view of standard diagnostic, administrative, and security software.

CORETRACE

Evolving Definitions

- Hoglund's revised definition from Rootkit.com on February 4:

  A rootkit is a tool that is designed to hide itself and other processes, data, and/or activity on a system.

- When Mark Russinovich publicized the Symantec NProtect rootkit, he qualified his definition:

  Its rootkit-like if it benefits the user, otherwise it's a rootkit

CORETRACE

The History of Rootkits

- The first rootkit was actually the first PC virus, Brain
  - Appeared in January 1986
  - Infects boot sector and hooks BIOS INT 13 to provide view of uninfected boot sector
- First use of “rootkit” label on SunOS in 1994
  - Root is UNIX super user
  - “Rootkit” was collection of tools for obtaining and maintaining root access
    - Replacements for system processes such as *ps*, *ls*
    - Compromised processes omit malware-related output
- Rootkits started appearing on Windows in the late 1990s

Modern Rootkits

- Rootkits can hide virtually anything:
  - Processes
  - Files, directories, Registry keys
  - Services, drivers
  - TCP/IP ports
- There are several types of rootkit technology:
  - User-mode hooking
  - Kernel-mode hooking
  - Code patching
  - Hiding in other processes
- www.rootkit.com is the primary rootkit forum

CORETRACE

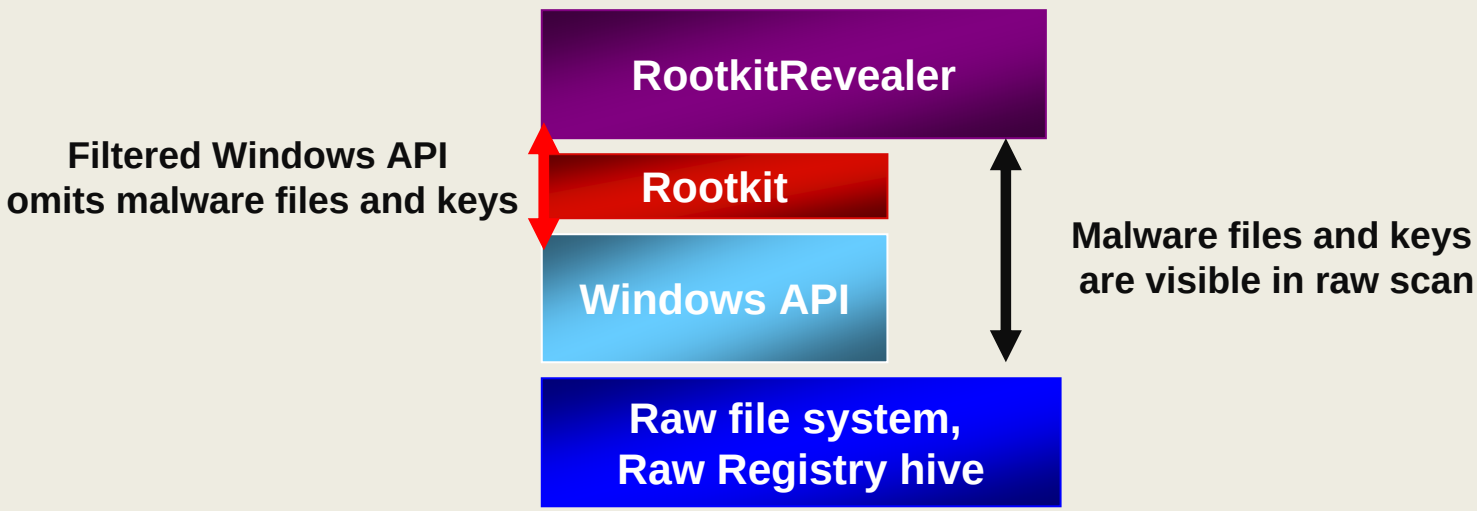
The Evolution of Malware

- Malware, including spyware, adware and viruses want to be hard to detect and/or hard to remove
- Rootkits are a fast evolving technology to achieve these goals
  - University of Connecticut found a rootkit on a server in June that had been there for two years
- There's been a steady growth in rootkit-based malware over the last year:
  - W32.Maslan.A@mm
  - W32.Opasa@mm
  - Trojan.Comxt.B
  - Backdoor.Shellbot
  - Backdoor.Ryejet
  - The list goes on and on…

CORETRACE

RootkitRevealer

- RootkitRevealer (RKR) runs online
- RKR tries to bypass rootkit to uncover cloaked objects
  - All detectors listed do the same
  - RKR scans Registry and the file system
  - Performs Windows API scan and compares with raw data structure scan

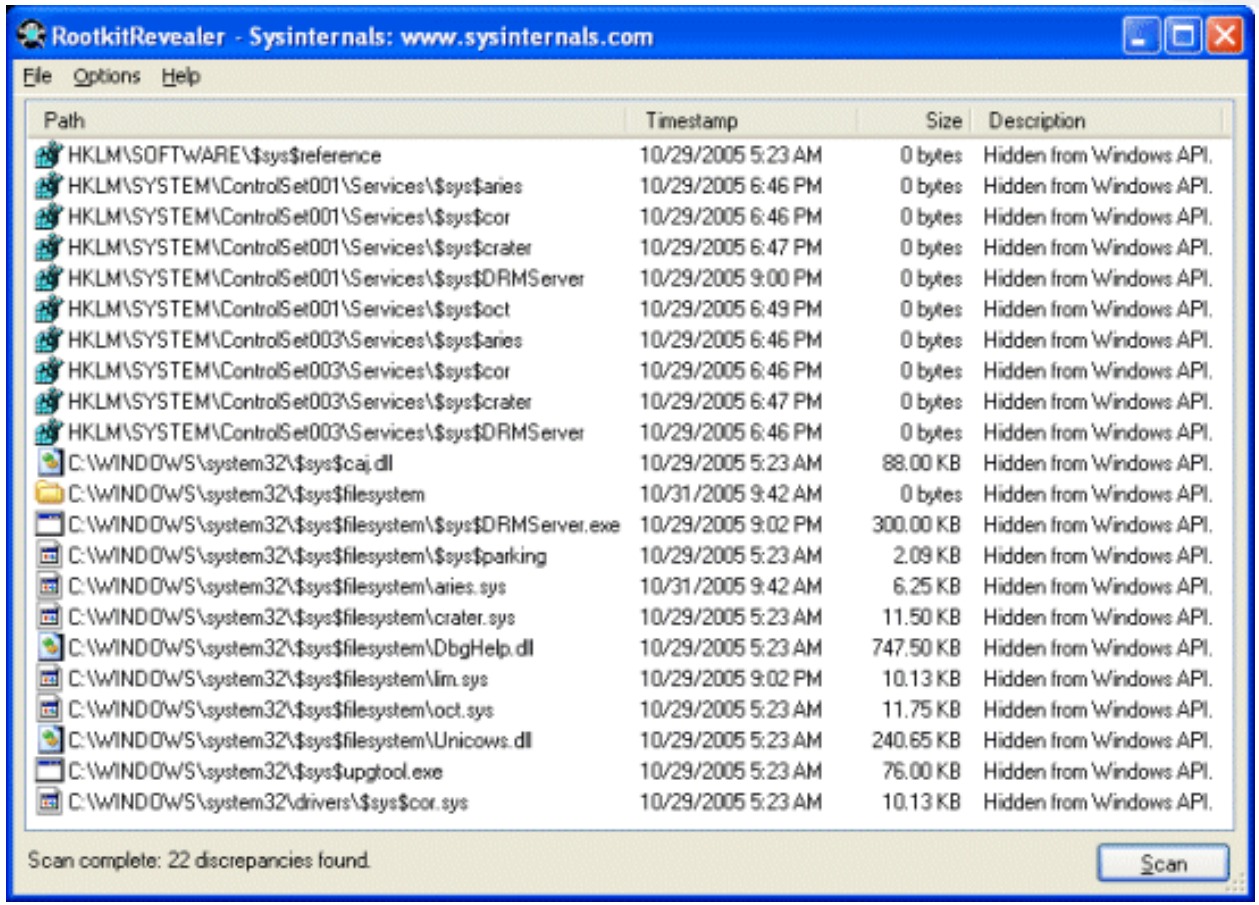


Discovery

- Late October, 2005: RootkitRevealer reports hidden files and directories
- Examined system-call table with Windbg
  - Saw evidence of system-call hooking by Aries.sys
- Looked at Aries.sys company name: “First 4 Internet”
  - Web site advertised DRM solutions
- Suspected connection with content-protected CD
- Confirmed by watching with Filemon

CORETRACE

Sony's Rootkit Revealed



CORETRACE

Announcement

- Published “Sony, Rootkits and Digital Rights Management Gone Too Far” Blog post on October 31
- Immediate media attention:
  - /.’d that evening (story covered on /. over 15 times)
  - AP, CNET, NY Times, USA Today, BBC, CBC, Rolling Stone, Billboard, Business Week,…


Software in more than 50 Sony BMG CDs

SONY

Cover story

CD woes may have had roots in merger

By Jefferson Graham • USA TODAY

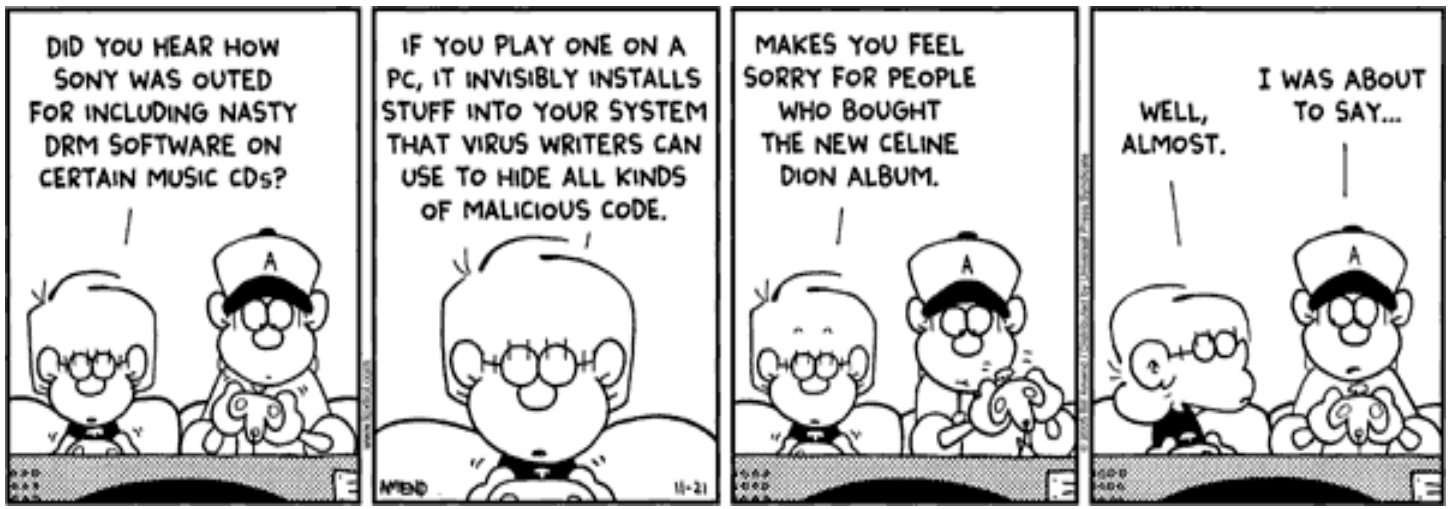
It sounded like music to record executives' ears. Copy-protection software that would to do the impossible: make CDs that couldn't be repeatedly copied.

How Sony responded

- Several viruses took advantage of the cloak
  - AV, including Microsoft, start disabling the cloak
- DHS says “Its your content, not your computer”

CORETRACE

Foxtrot



CORETRACE

Sony's Response

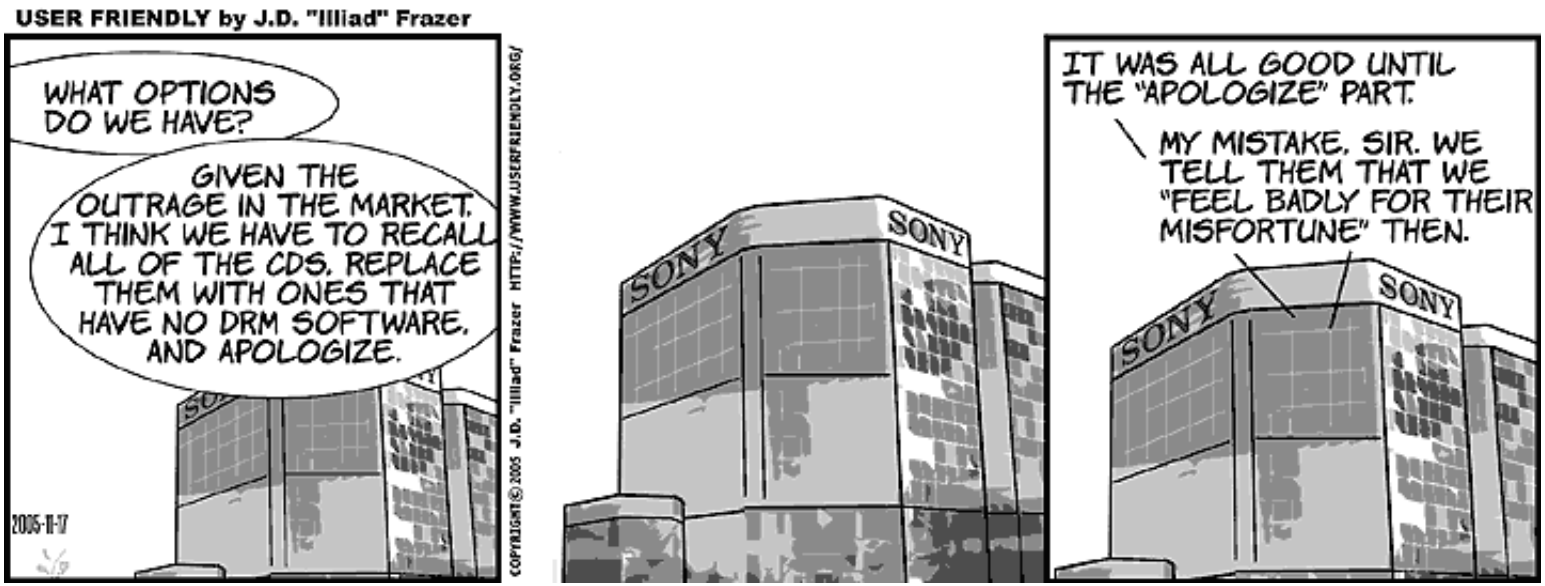
- November 4: Thomas Hesse, head of Sony digital business states in NPR interview:

> "*Most people, I think, don't even know what a Rootkit is, so why should they care about it?*"

- Then Sony released patch to remove cloak
  - Required registration
  - Doubled as update to DRM code
  - Available only as ActiveX control that contained security vulnerabilities
- On November 16 Sony announced recall, consumer trade-in program and plans to release stand-alone uninstaller

CORETRACE

Sony Feels Bad

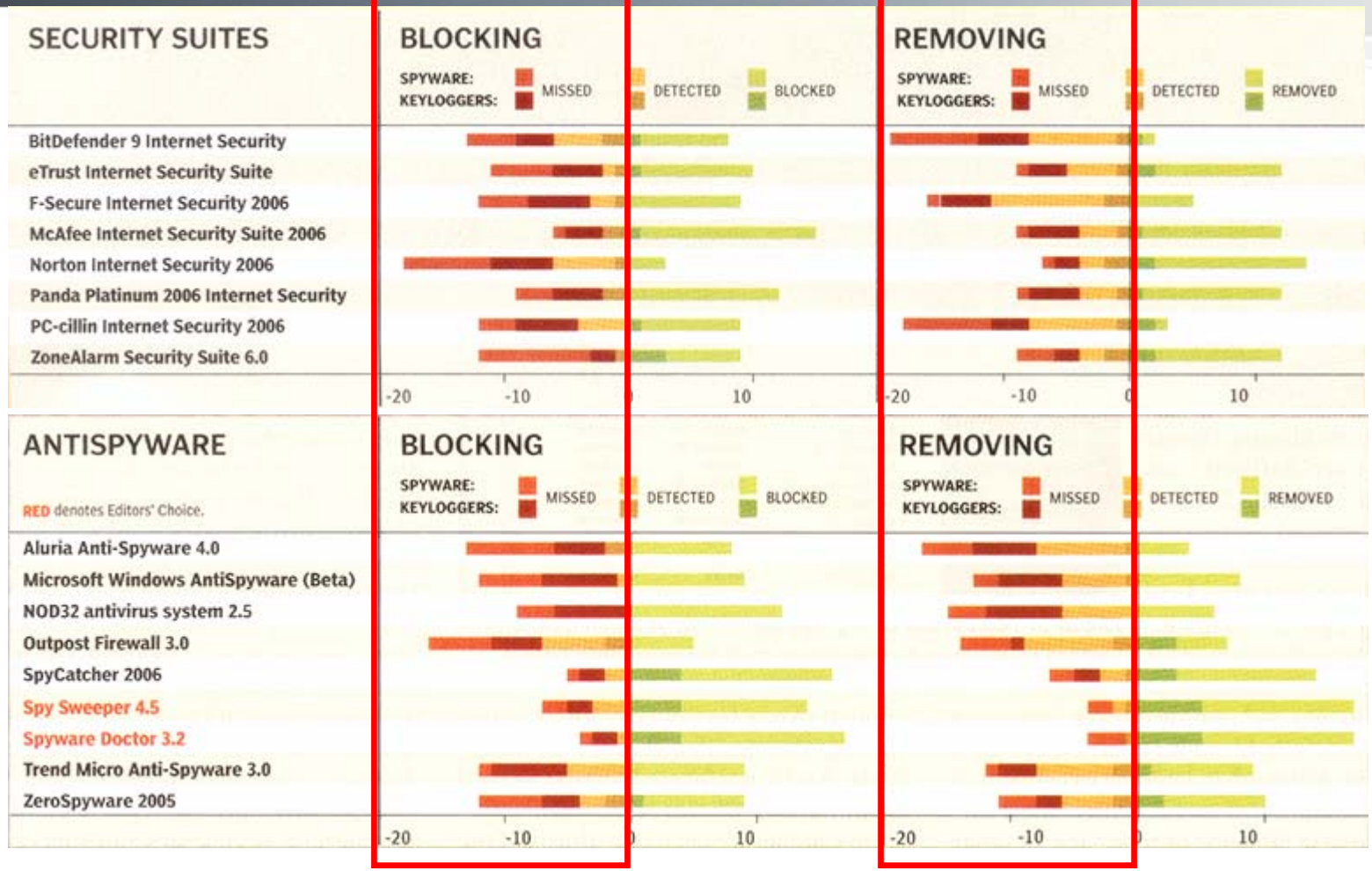


CORETRACE

Legal Action

- Lawsuits started flying:
  - 5 class-action lawsuits filed
  - Electronic Freedom Foundation (EFF) files suit
  - Texas Attorney General sued for violations of Texas Antispyware law
- Mark served as expert for NY attorney Scott Kamber
  - Kamber filed first action November 1 so had national class
- Kamber and Sony reached a quick settlement:
  - November 21: Scott meets with Sony attorneys
  - December 29: Settlement filed in court
  - January 9: Preliminary approval
  - Final hearing: May 22

Antimalware Isn't Enough



CORETRACE

General Rootkit Detection

- All cloaks have holes
  - Leave some APIs unfiltered
  - Have detectable side effects
  - Can’t cloak when OS is offline
- Rootkit detection attacks holes
  - Cat-and-mouse game
- General rootkit detectors:
  - RKDetect
  - F-Secure BlackLight
  - Sysinternals RootkitRevealer

CORETRACE

RootkitRevealer Limitations

- Rootkits have already attacked RKR directly by not cloaking when scanned
  - RKR is given true system view
  - Windows API scan looks like raw scan
- RKR has been modified to be a harder to detect by rootkits
  - RKR is adopting anti-signature techniques
  - Rootkit authors will continue to find ways to detect RKR
  - It’s a game nobody can win
- All rootkit detectors suffer the same vulnerability

CORETRACE

Cleaning Rootkits

- Clean rootkits at your own risk
  - Don’t trust that you’ve found all the malware

If the system has sensitive
Information, ***you should reinstall***

- Most rootkits require off-line cleaning
  - Require additional tools to identify malware components
    - E.g. Process Explorer, Autoruns
  - Even delete-on-reboot is easily circumvented
  - WinPE or ERD Commander

CORETRACE

Defending Against Rootkits

- The only real defense is to stop them from installing
  - Run as non-admin
  - Apply defense-in-depth
- Microsoft is making it harder for rootkits to install

CORETRACE

Microsoft's Anti-Rootkit Efforts

- Data Execution Protection and the /GS switch
  - Hardens against buffer-overflow based propagation
- Patchguard on Windows XP 64-bit and Vista 64-bit
  - Prevents system-call hooking
  - Prevents Interrupt Dispatch Table hooking
  - Prevents kernel patching
- Vista User Account Control
  - Makes it easier to run as limited user
  - Only apps that need admin run as admin
- Vista 64-bit signed drivers
  - Requires *all* kernel-mode code to be digitally signed

CORETRACE

Rootkits Will Always Find a Way

- Malware will adapt to any countermeasure:
  - User-mode rootkits will destroy accounts
  - Social engineering will circumvent UAC
  - Standard driver architecture allows for cloaking
  - Malware will get digitally signed
  - Bugs will allow malware to punch holes
  - The rootkit doomsday scenario
  - Legacy systems will be around a long time…
- Detection will continue to be important

CORETRACE

Resources

- Rootkit.com
- *Rootkits: Subverting the Windows Kernel*, Hoglund and Butler, Addison-Wesley
- *Sysinternals:*
  - Malware forum
  - RootkitRevealer forum

CORETRACE