Prepared by
CMS Consulting Inc.
September 2005
Confidential

CMS Consulting Inc.

Hidden Rootkits in Windows

Presented by: Brian Bourne, CISSP, MCSE:Security
Christopher Diachok, MCSE

Microsoft Infrastructure and Security Experts

Microsoft GOLD CERTIFIED Partner for Security Solutions

CMS Consulting Inc.

Microsoft Infrastructure and Security Experts

Active Directory - Windows Server - Exchange - SMS - ISA
MOM - Clustering - Office - XP - SQL - Terminal Services
Office - Security Assessments - Lockdown - Wireless

Clients Include

Microsoft Canada - Dell - CIBC - RBC - PwC - Sears - Government Agencies - CFL - Ontario Hospitals - Take Two Interactive

Visit us online: www.cms.ca

Downloads – Resources – White Papers

CMS CONSULTING INC.

Microsoft GOLD CERTIFIED Partner

For Security Solutions
For Advanced Infrastructure
For Network Solutions

AGENDA

- Overview
- Types of rootkits
- Popular rootkits
- What can they hide
- DEMO – Hacker Defender Anatomy 101
- How they hide and go undetected
- DEMO - Hacker Defender In Action!
- DEMO – Covert Channels
- Detection
- DEMO – Rootkit Revealer
- Protection and Removal
- Trends

Overview

- What is a rootkit?
  - A root kit is a set of tools used by an intruder after cracking a computer system. These tools can help the attacker maintain his or her access to the system and use it for malicious purposes. Root kits exist for a variety of operating systems such as Linux, Solaris, and versions of Microsoft Windows

Reference: http://en.wikipedia.org/wiki/Rootkit

Types of rootkits

- **Persistent Rootkits**
  A persistent rootkit is one associated with malware that activates each time the system boots. Because such malware contain code that must be executed automatically each system start or when a user logs in, they must store code in a persistent store, such as the Registry or file system, and configure a method by which the code executes without user intervention.

- **Memory-Based Rootkits**
  Memory-based rootkits are malware that has no persistent code and therefore does not survive a reboot.

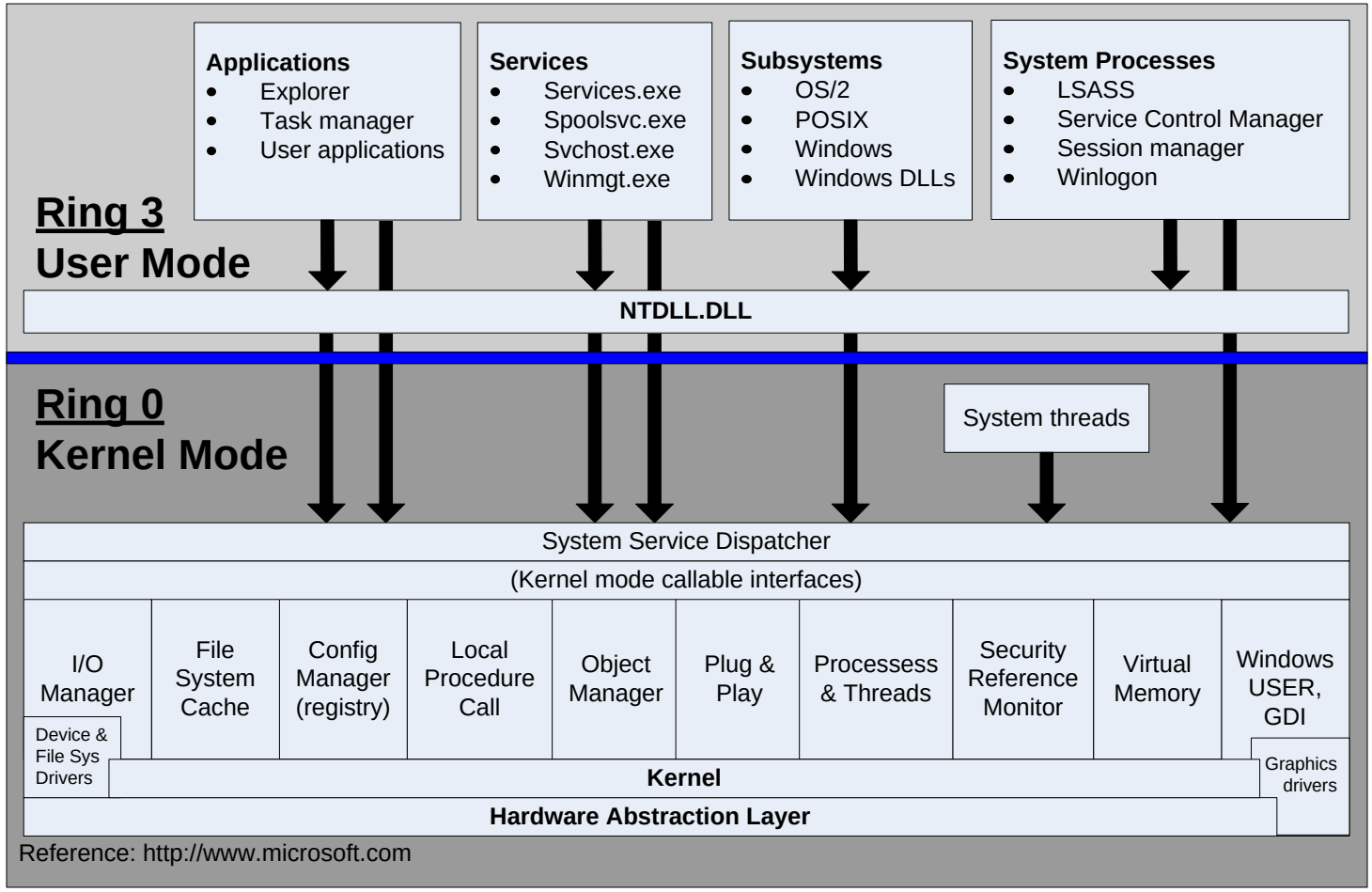
Reference: http://www.sysinternals.com

Types of rootkits

- **User-mode Rootkits**
  There are many methods by which rootkits attempt to evade detection. For example, a user-mode rootkit might intercept all calls to the Windows FindFirstFile/FindNextFile APIs, which are used by file system exploration utilities, including Explorer and the command prompt, to enumerate the contents of file system directories. When an application performs a directory listing that would otherwise return results that contain entries identifying the files associated with the rootkit, the rootkit intercepts and modifies the output to remove the entries.
- **Kernel-mode Rootkits**
  Kernel-mode rootkits can be even more powerful since, not only can they intercept the native API in kernel-mode, but they can also directly manipulate kernel-mode data structures. A common technique for hiding the presence of a malware process is to remove the process from the kernel's list of active processes. Since process management APIs rely on the contents of the list, the malware process will not display in process management tools like Task Manager or Process Explorer.

Reference: http://www.sysinternals.com

Windows Architecture



Reference: http://www.microsoft.com

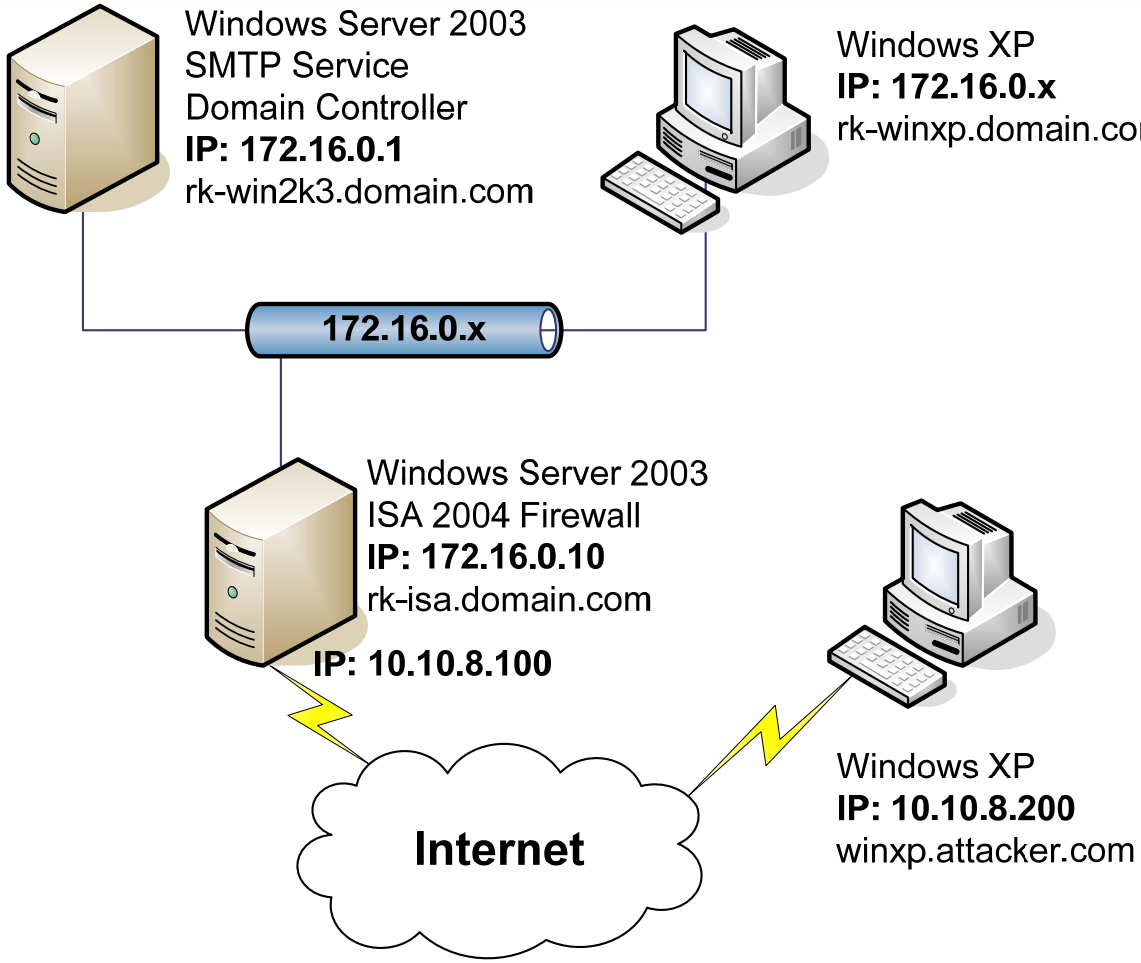
Popular rootkits

- AFX Rootkit 2005
- FU
- Hacker Defender
- HE4Hook
- NT Root
- NTFSHider
- NTIllusion
- Vanquish
- Winlogon Hijack

What can they hide

- Covert Channels
- Custom GINA’s
- Files and Directories
- Processes
- Registry Keys
- Services
- TCP/UPD ports

DEMO Network



DEMO

- **Hacker Defender - Anatomy 101**
  - Hxdef100.exe
  - Hxdef100.ini
  - Hxdefdrv.sys (Embedded in hxdef100.exe)

  - Rdrbs100.exe
  - Rdrbs100.ini
  - Bdcli100.exe

Reference: http://hxdef.czweb.org

Hヲィンェキ ゥエォエウゥェキ 100 キェサョクョケェウ

HACKER DEFENDER 100 REVISITED

- **Released September 1st 2005**
  - compiler define for disabling NtOpenFile hook
  - outbound TCP connection hiding
  - separation between hidden files and processes - Hidden Processes
  - hidden files in Prefetch are deleted during initialization
  - disabling incompatible McAfee Buffer Overflow protection
  - found and fixed several bugs, source code cleanup

How they hide and go undetected

- **Kernel Native API hooking**
  - SDT
    - This technique is typically implemented by modifying the ServiceTable entries in the Service Descriptor Table (SDT).
      - Directly unlinking the process's EPROCESS entry from ActiveProcessLink.
- **User Native API hooking**
  - Import Address Table (IAT) / Export Address Table (EAT)
    - Each process and module(DLL) have their own Import Address Table (IAT) that contains the entry-point addresses of the APIs that are used. These addreseses will be used whenever the process makes a call to the repective APIs. Therefore, by replacing the entry-point address of an API (in the IAT) with that of a replacement function, it is possible to redirect any calls to the API to the replacement function.
    - Every DLL has an Export Address Table (EAT) that contains the entry-point addresses of the APIs that are implemented within the DLL. Hence, by replacing the entry-point of an API within the EAT with the relative address of the replacement function, we can cause GetProcAddress to return the address of the replacement function instead.
- **Dynamic Forking of Win32 EXE**
  - Under Windows, a process can be created in suspend mode using the CreateProcess API with the CREATE_SUSPENDED parameter. The EXE image will be loaded into memory by Windows but execution will not begin until the ResumeThread API is used. Before calling ResumeThread, it is possible to read and write this process's memory space using APIs like ReadProcessMemory and WriteProcessMemory. This makes it possible to overwrite the image of the original EXE with the image of another EXE, thus enabling the execution of the second EXE within the memory space of the first EXE.
- **Direct Kernel Object Manipulation (DKOM) in memory**
  - A device driver or loadable kernel module has access to kernel memory
  - A sophisticated rootkit can modify the objects directly in memory in a relatively reliable fashion to hide.
- **Interrupt Descriptor Table (IDT)**
  - Interrupts are used to signal to the kernel that it has work to perform.
  - By hooking one interrupt, a clever rootkit can filter all exported kernel functions.

Reference: http://www.security.org.sg / http://www.hbgary.com

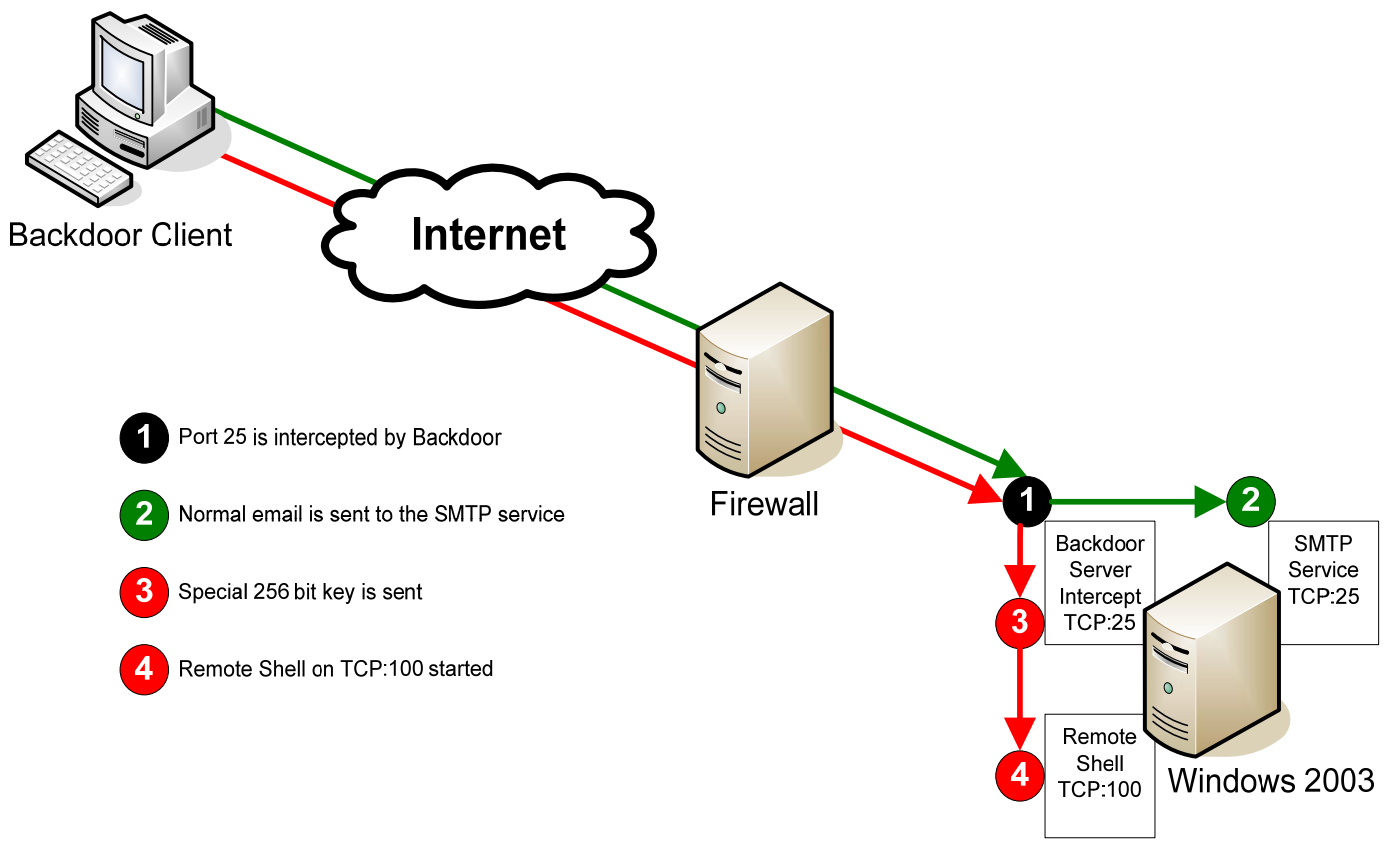
DEMO

- Hacker Defender – In Action!
  - Security Compromise - Exploit
  - Avoiding Antivirus Detection
  - Hiding Folders/Files
  - Hiding Services
  - Hiding TCP Ports

DEMO

- Hacker Defender – Covert Channel
  - Backdoor shell access via SMTP

Covert Channel Summary



Detection

- How to detect rootkits?

Find Hidden Service (aka FHS)	1.1
F-Secure BlackLight Beta	2.1.1018
Kernel PS (aka knlps)	1.0
Kernel SC (aka knlsc)	1.3
Klister	0.4
KProcCheck	0.2-beta1
Malicious Software Removal Tool	v1.8 Sept 13 2005
Process Magic by WinEggDrop	1
RootKit Shark	3.11
RootkitRevealer	1.55
Strider (Microsoft)	beta
TaskInfo	6.1.2.162 Beta
UnHackMe	2.5

DEMO

- Detecting rootkits
  - Rootkit Revealer

Detection Results

Name	Version	AFX Rootkit 2005	FU	Hacker Defender	Vanquish	Notes
Blacklight	2.1.1018	Yes	Yes	Yes	Yes	
Flister	0.1	Yes	No ***1***	Yes	Yes	Need to type in the exact dir path
Keensense	2.0	Yes	Yes	Yes	No	Installs system driver and requires a reboot. Unstable.
Process Guard	3.150	Yes	Yes	Yes	Yes	Install requires a reboot. All Global Protection optiosn manually turned on. Needs to "learn" a baseline of the system.
Rootkit Revealer	1.55	Yes	No	Yes	Yes	
Strider	beta	Yes	No ***1***	Yes	Yes	Hidden directory/file compare of comprimised state and clean state from a WinPE boot CD using windiff.

1 Could not detect FU because it does not hide folders/files. Only processes.

Detection Summary

- All “stock” rootkits discovered with various detection tools
- Custom recompiled rootkits by pass antivirus detection
- Commercially available rootkits that hide files, services, processes, registry keys would not be detected in the compromised OS

Protection

- Defence in Depth practices!
- Application Layer firewalls
- Add rootkit detection software to your toolkit
- Baseline your systems in another kernel (WinPE) using the Microsoft Strider technique for comparing modified/added binaries on a regular basis

Removal

- Rootkit removal tools (eg. “Unhackme” by Greatis Software)
- Clean from another kernel (eg. Knoppix, WinPE, etc)
- Use technology that reverts back to a previous state if your environment allows for it:
  - Undo disks in Microsoft Virtual PC/Server
  - Faronics Deep Freeze
  - Symantec Norton GoBack
  - Winternals Recovery Manager
- Once a machine has been compromised, the only true cleaning method is to format and reload the OS!

Trends

It’s a cat and mouse game

- As rootkit detection methods/signatures are updated; so are the techniques/methods of the rootkits evading detection; just like viruses but much more sophisticated
- Encrypting the memory pages where the rootkit is running to avoid detection
- Spyware and Viruses utilizing functions of rootkits to hide their presence and payload; This has already happened and will continue to escalate to an extremely “stealthy” version

Trends

- Memory Hiding (e.g. Shadow Walker)
- Using other system writeable memory locations. (e.g. VideoCardKit, MTDWin)
- Boot sector rootkits (e.g. BootRootKit)
- Database rootkits (presented in concept by Alexander Kornbrust at BH2005)

Need to Know

Prevention

- Stop rootkits from entering and executing in your environment.

Response

- Non-critical systems can be cleaned and/or reloaded.
- Critical systems require professional assistance, particularly if forensic evidence is desired.

Learn More

- You're in the "Emerging Threats" track!
- http://www.rootkit.com
- Participate in the Toronto Area Security Klatch

CMS Consulting Inc.

Q & A

Thank You!

Visit: CMS Consulting at http://www.cms.ca

Join: Toronto Area Security Klatch at http://www.task.to

CMS CONSULTING INC.

Microsoft Infrastructure and Security Experts

Microsoft GOLD CERTIFIED Partner for Security Solutions