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?

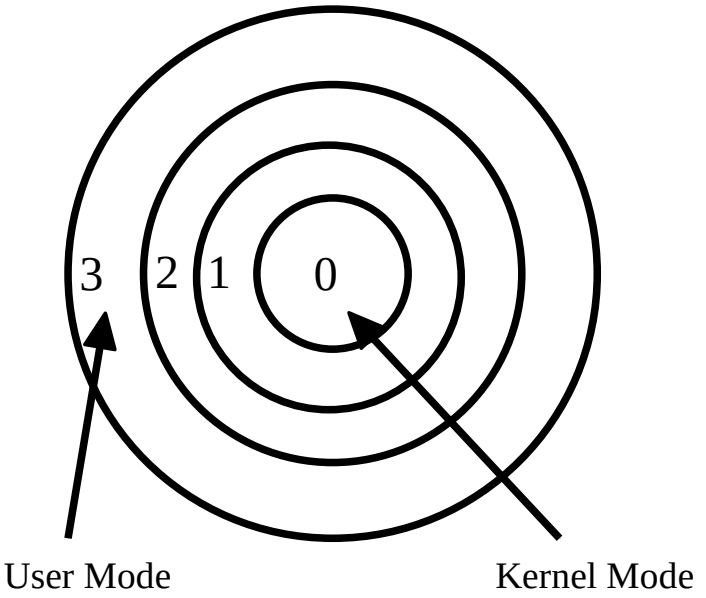
- „Ein Rootkit ist ein Satz von Programmen der **dauerhafte** und **nicht aufzuspürende** Gegenwart auf einem Computer erlaubt.“ (Hoglund, Butler)
- Der Fokus von Rootkits ist die **Heimlichkeit** (auch für legale Zwecke?)
- Weitere Funktionen
  - Hintertüren
  - Fernsteuerung von Rechnern
  - Spyware (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 nutzten 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

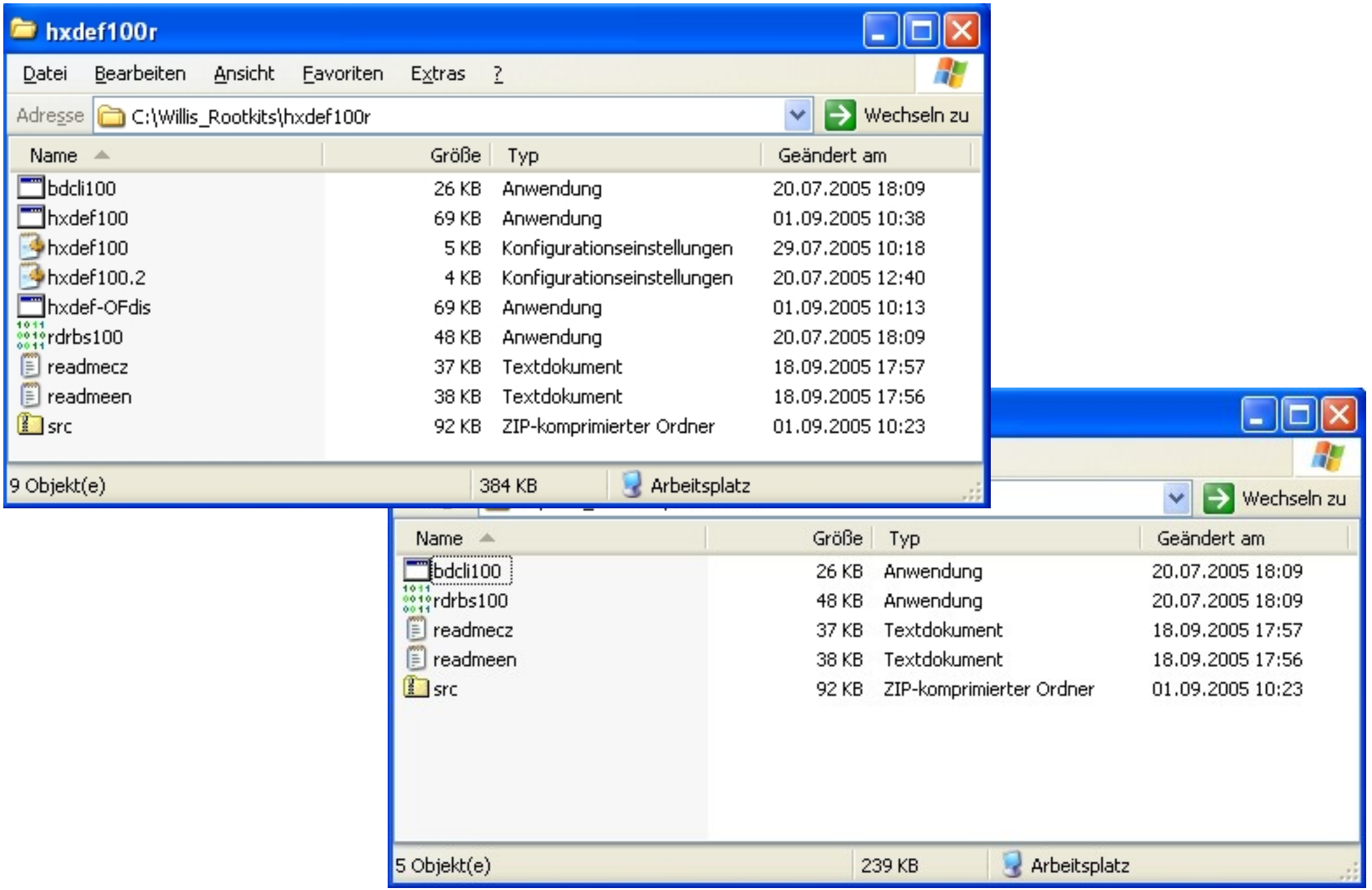
- Manipulation von Tabelleneinträgen (Hooking)
  - Klassische Technik, u.a. systemweit Dienste aus System Service Descriptor Table (SSDT) bzw. aus Import Address Table (IAT) im Adressraum eines Programmes
- Runtime-Patching
- Geschichtete Treiber
- Direkte Manipulation von Kernel-Objekten (Direct Kernel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

HackerDefender Rootkit

- Kostenlose Version nebst Quellcode erhältlich

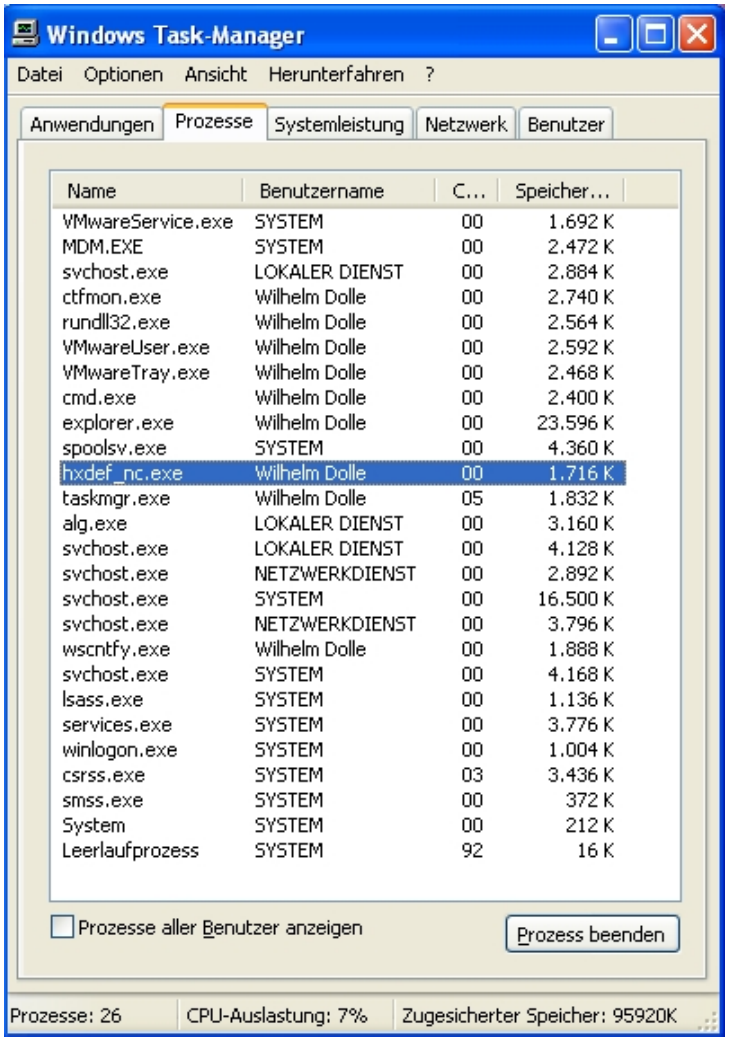
- Features
  - Verstecken von Dateien, Verzeichnissen, Prozessen und Registry-Einträgen die mit einer bestimmten Zeichenkette anfangen (default „hxdef“)
  - Leicht verständliche Konfigurationsdatei
  - Startet nach Aktivierung beliebige (versteckte) Programme
  - Versteckt TCP- und UDP-Ports auf denen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

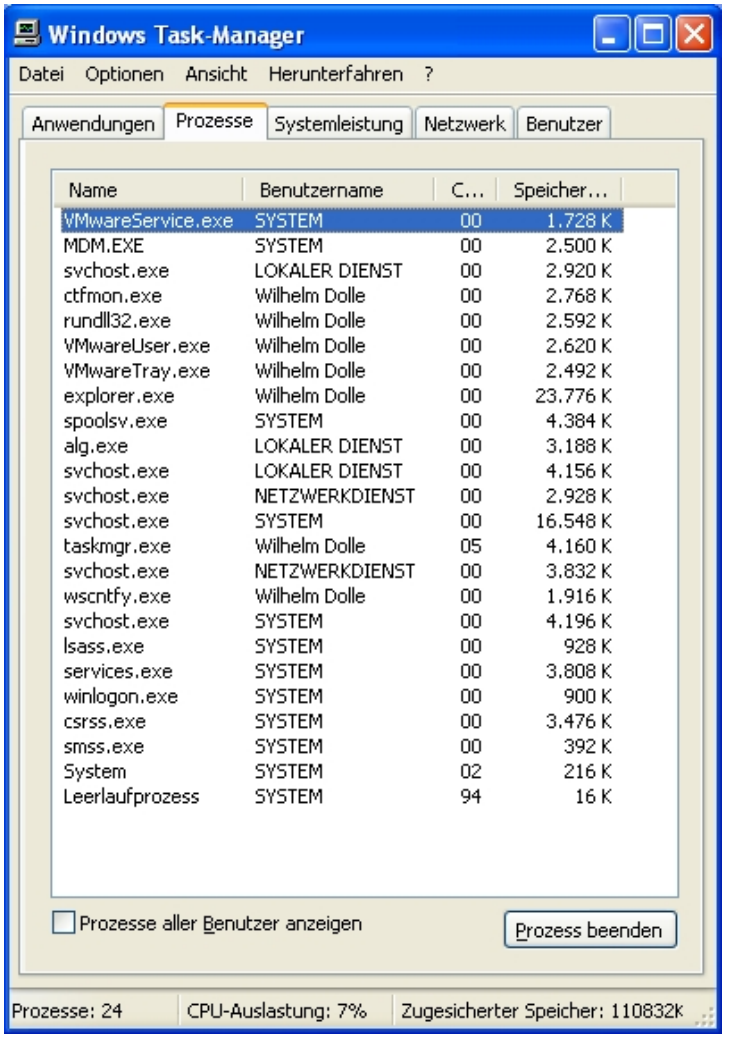
HackerDefender – Verstecken von Dateien



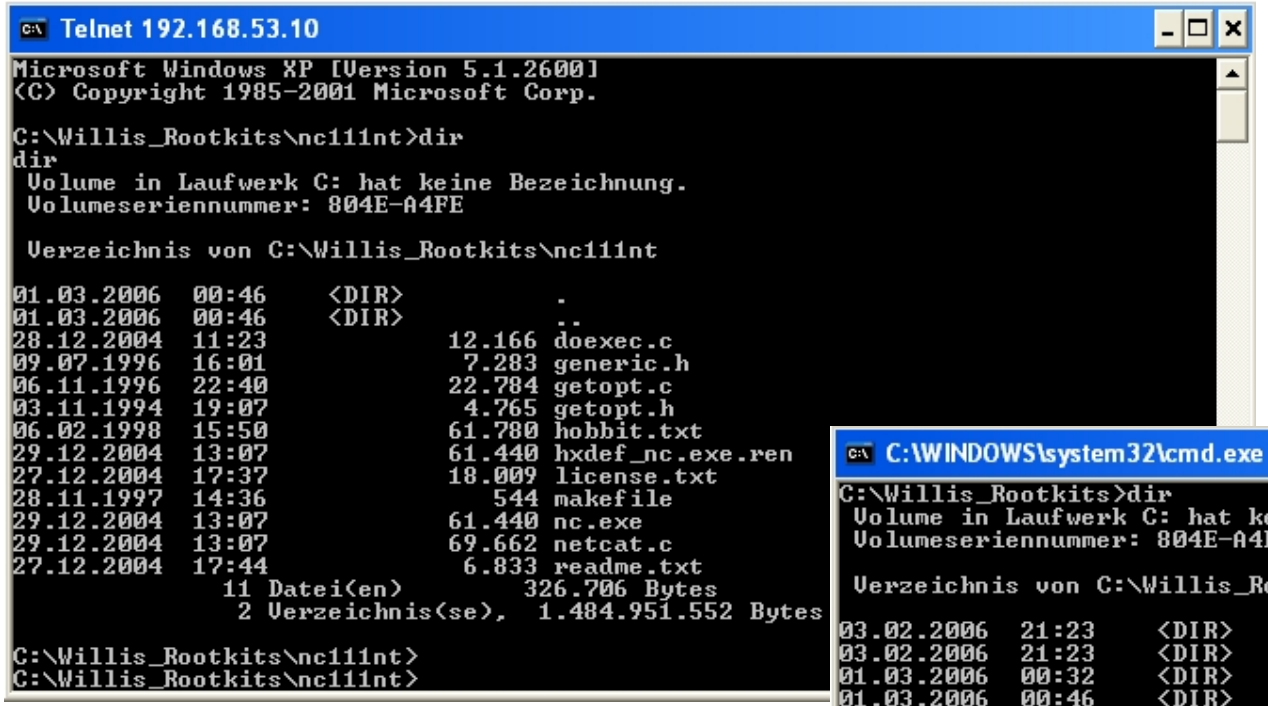
HackerDefender – Verstecken von Prozessen

- „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*

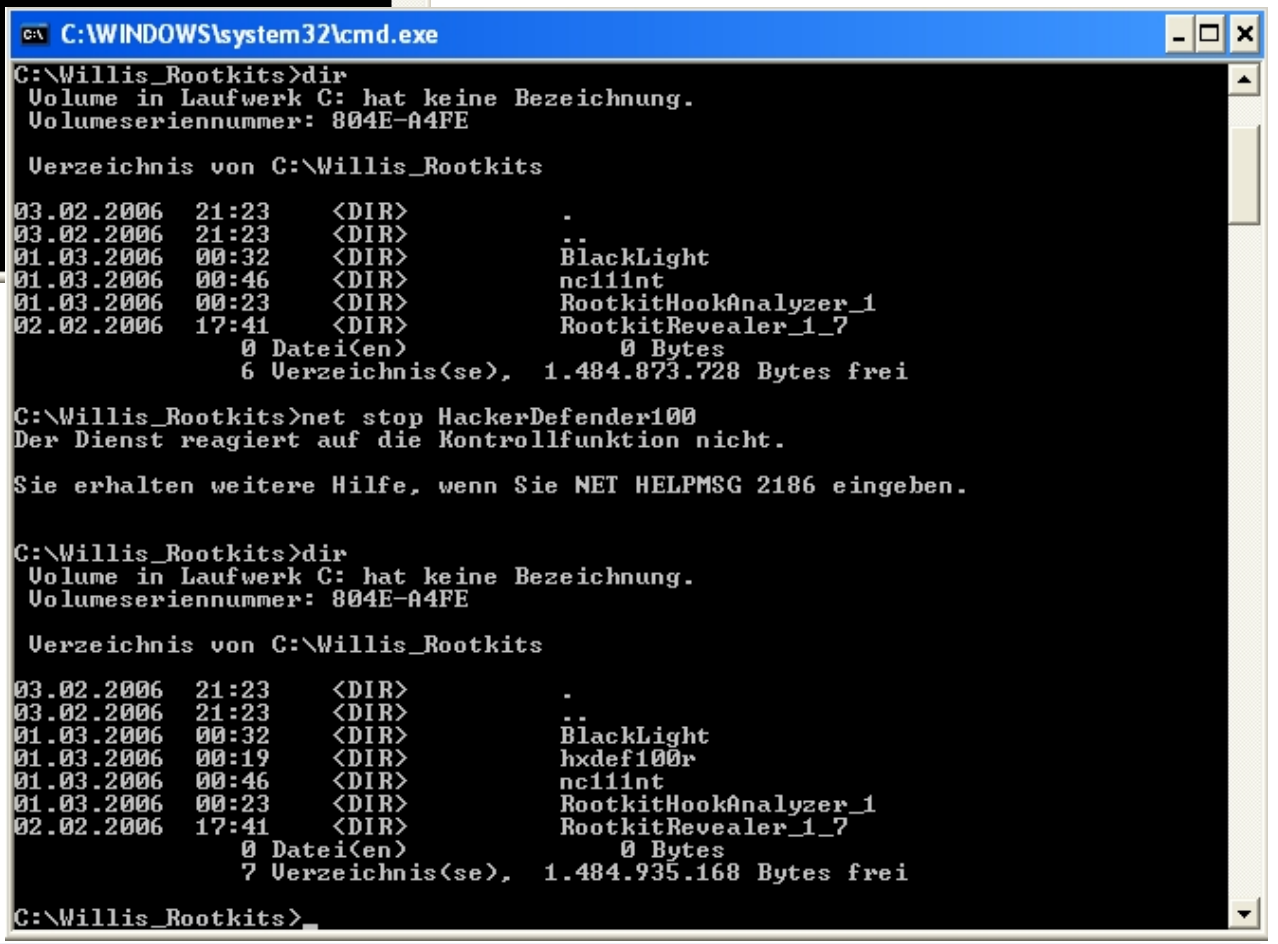




HackerDefender – Backdoor / Beenden



- Telnet-Verbindung zur netcat-“Backdoor“

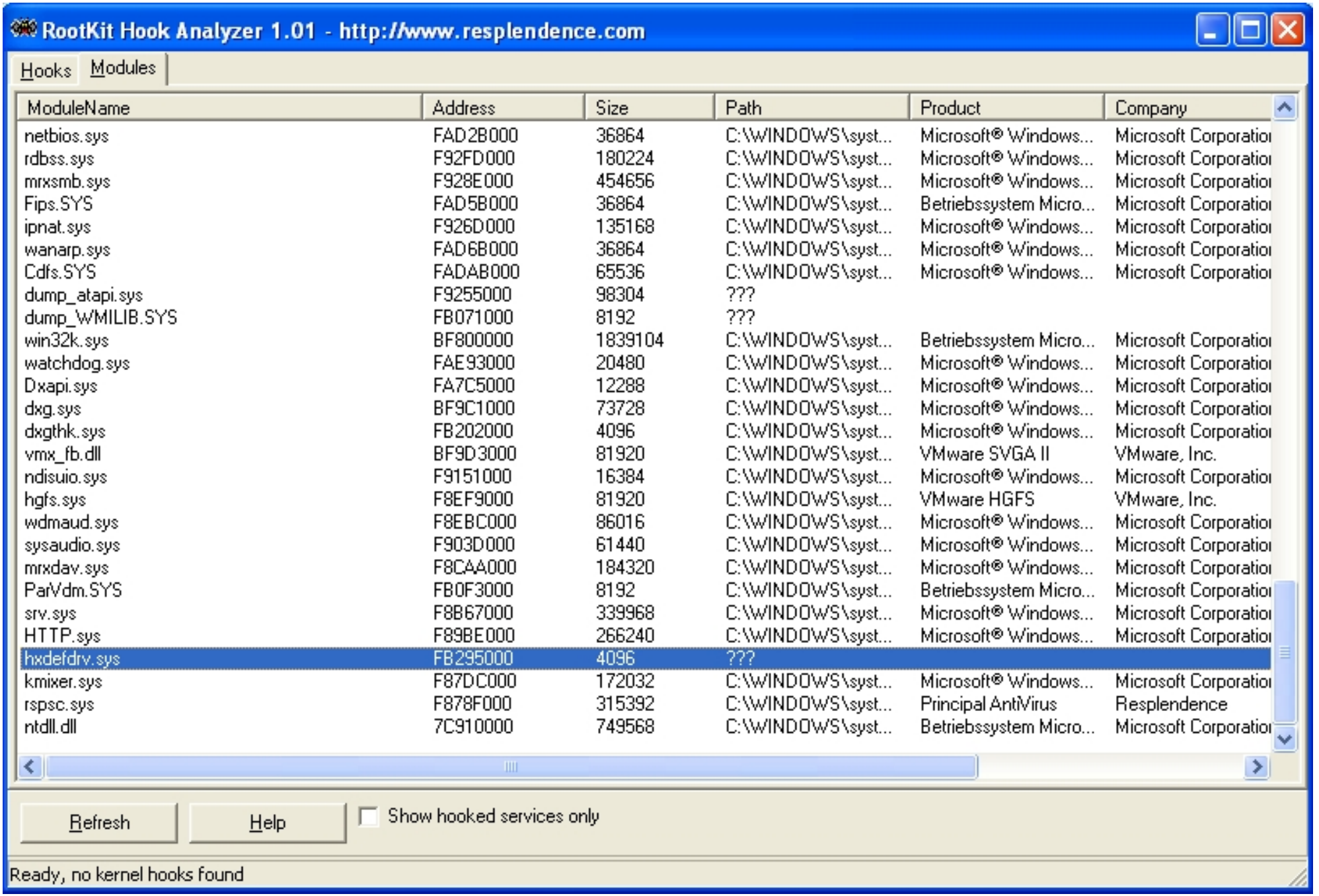


- Beenden des Rootkit-Dienstes mit
  net stop HackerDefender100

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 Virginity Verifier (testet analog zu VICE die Integrität von Betriebssystemstabellen)

RootKit Hook Analyzer



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

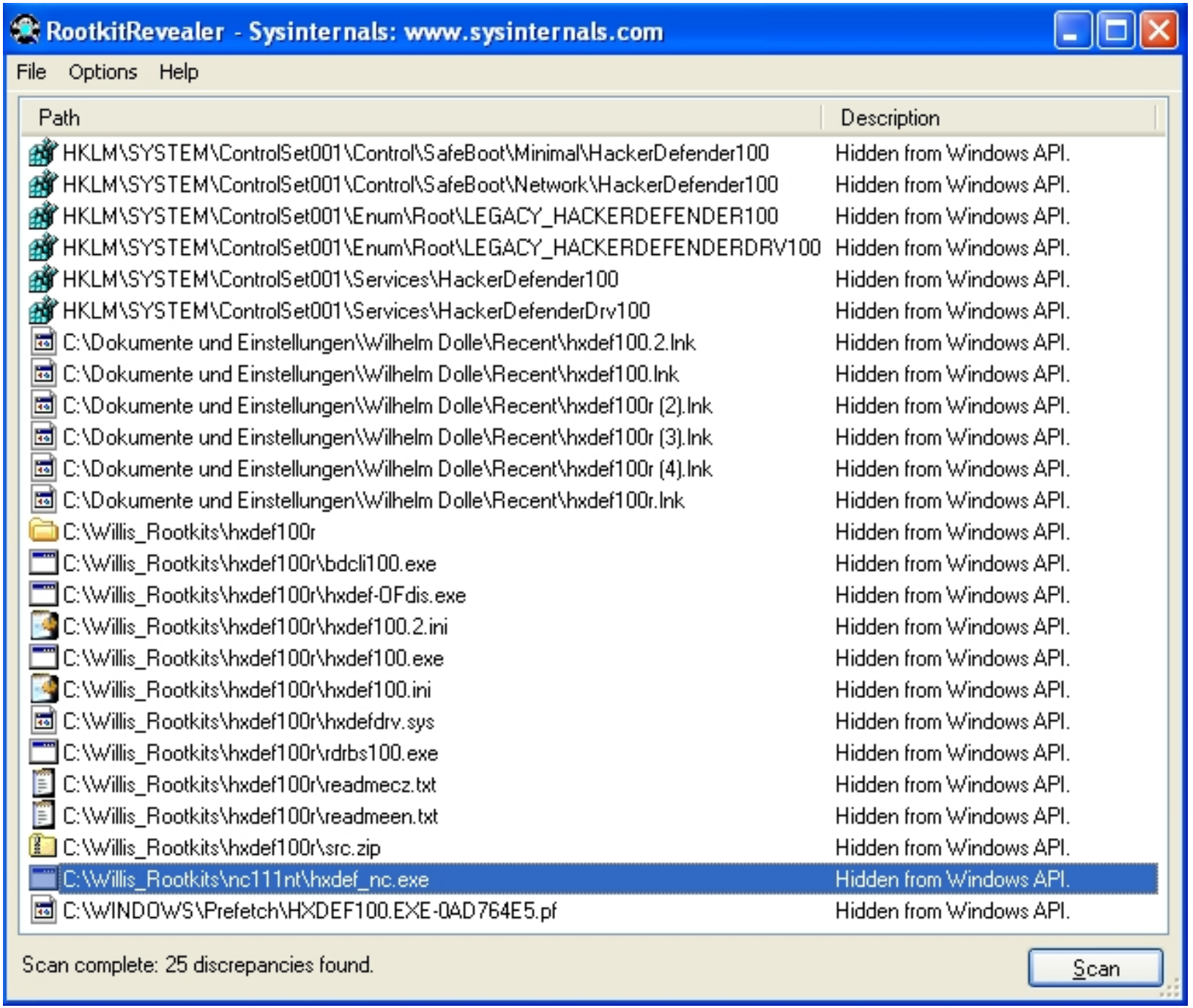
- Veröffentlicht: 22. Februar 2005 (SysInternals)

- Features:
  - Vergleicht Windows-API mit rohem Inhalt des Dateisystem bzw. eine Registry-Hive-Datei
  - Untersucht keine Prozesse
  - Erkennt alle auf www.rootkit.com 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 mismach between Windows API and raw hive data
- Key name contains embedded nulls
- Data mismatch between Windows API and raw hive data

RootkitRevealer im Einsatz

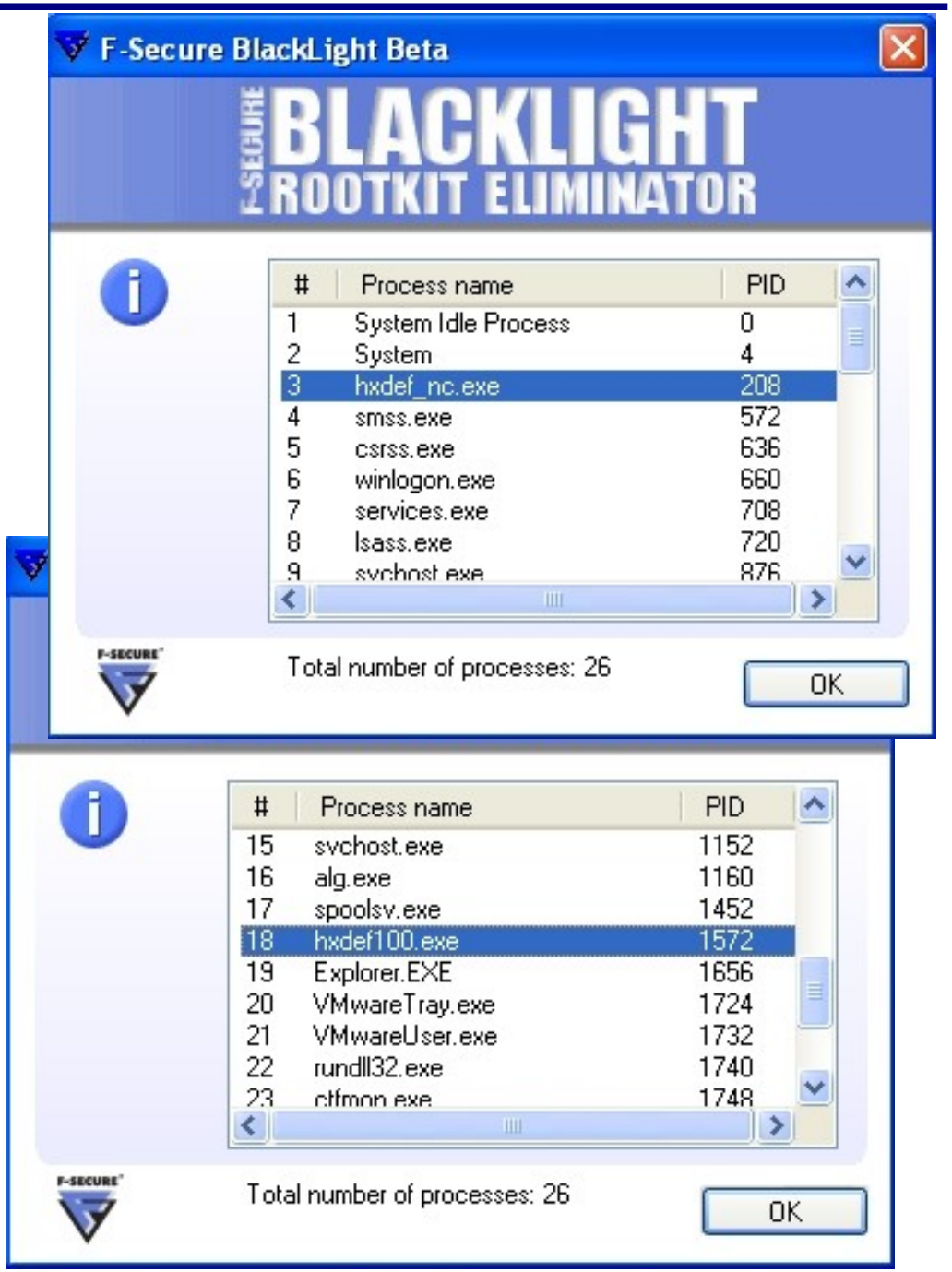


BlackLight™

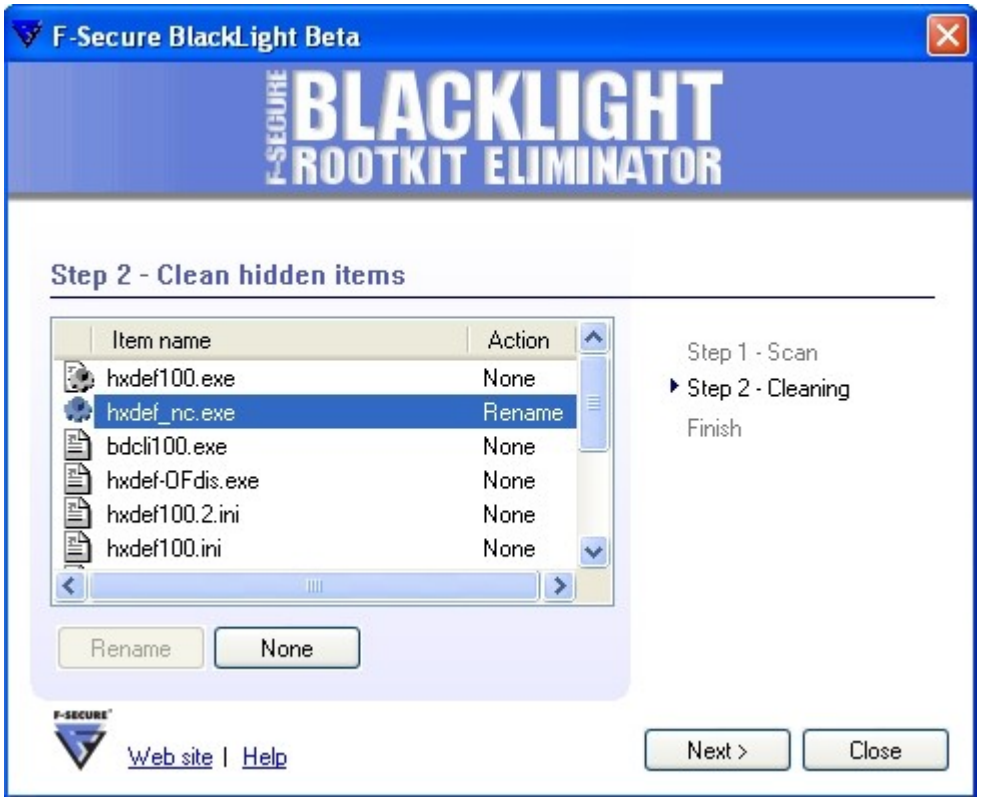
- Veröffentlicht: 10. März 2005 (F-Secure), Beta-Version (kostenlos nutzbar bis 1. Mai 2006)

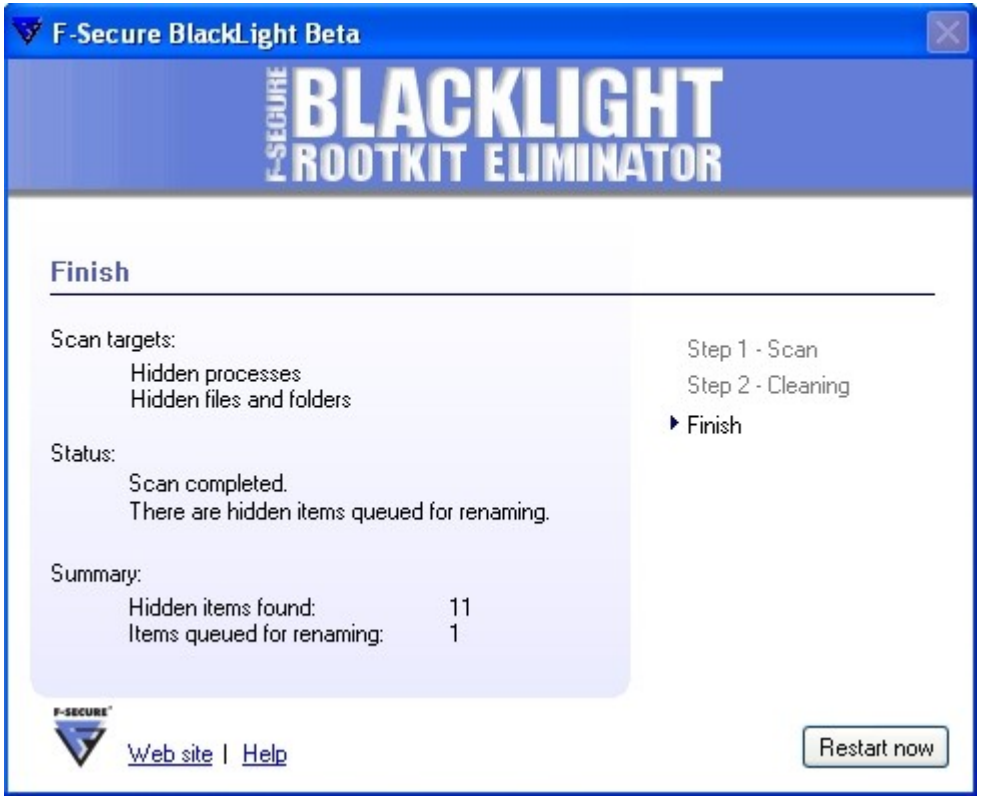
- Features
  - Findet verdächtige Dateien, Verzeichnisse und Prozesse
  - Interpretiert die Scan-Ergebnisse selber und macht dem Benutzer Vorschläge
  - Erkennt und entfernt Rootkits (z.B. HackerDefender, FU), aber teilweise auch Spyware, Trojanische Pferde und Würmer
  - Entfernung erfolgt durch umbenennen 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 infacted 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

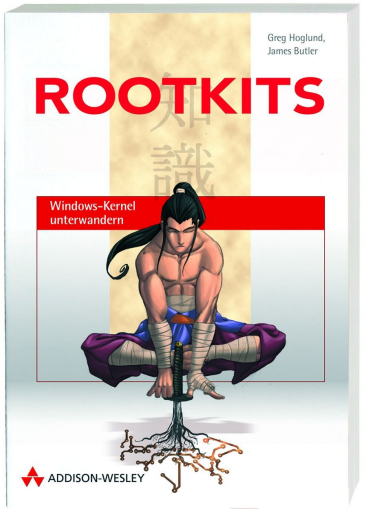
- Anhand der gefundenen Spuren im Internet nach Informationen und Hinweisen zur Entfernung des Rootkits suchen
  - Module entfernen
  - Manipulierte Dateien durch Originale ersetzen
  - Startscripte säubern

- **Wann immer möglich System komplett neu aufsetzen!**

Fazit (CVBRD)

- Kombination von High-Level- (online) mit Low-Level-Scans (offline) und einem Antivirenscanner 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 Destops / 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/