# Cross-View based Rootkit Detection

## Neue Wege in der digitalen Forensik

**Wilhelm Dolle**
**Director Information Technology**
**interActive Systems GmbH**

**Competence Center For Applied Security Technology (CAST) - Forum Forensik**
**18. August 2005, Darmstadt**

COMPETENCE CENTER FOR
APPLIED SECURITY TECHNOLOGY
CAST

# Agenda

- Bedrohung der Systemsicherheit durch Rootkits
- Arbeitsweise der „cross-view“-basierten Erkennung
- Verfügbare Werkzeuge
- Pro und Contra des „cross-view“-basierten Ansatzes

# Bedrohungssituation

- **Steigende Anzahl von Angriffen / Sicherheitsvorfällen**
- **Verfügbarkeit von (einfachen) Angriff-Tools**
- **Unterschiedlicher Kenntnisstand der Täter**
  - Hacker / Cracker
  - Script Kiddies
  - Innen- / Aussentäter
  - …
- **Unterschiedliche Motivation der Täter**
  - Wirtschaftliche Gründe
  - „Testen“ von technischem Know-How
  - (Industrie)Spionage
  - …

# Typischer Angriffsablauf

- Footprinting (Netzstruktur aufklären)
- Protokoll- und Portscans (aktiv / passiv)
- Enumeration (Betriebssystemerkennung, Bannergrabbing, Verwundbarkeitsscans)
- Ausnutzen einer Sicherheitslücke durch Anwendung eines Exploits (z.B. Buffer Overflow)
- Verstecken / Festsetzen (Hintertüren, Sniffer, Keylogger, ...)
- Einbruchsspuren verwischen
- System missbrauchen

# Was sind Rootkits?

- Keine Angriffswerkzeuge („Admin Bausatz“)

- Leichte Installation
- Verbergen Spuren (Dateien, Prozesse, Netzverbindungen, ...)
- Trojanisierte Systemprogramme und andere Tools
- Schaffen dauerhaften Zugang zum System (Backdoor)
- Enthalten zusätzlich oft Keylogger, Sniffer, Logfilecleaner

- Memory-Based Rootkits / Persistent Rootkits

- Dateibasierte/-modifizierende Rootkits
- Kernelbasierte/-modifizierende Rootkits

# Historie von Rootkits

- Ende 80‘er: manipulieren von Logdateien
- 1989: Phrack-Magazin: Umgehen von Unix-Überwachung
- 1994: erster CERT Hinweis auf eine Sammlung von Programmen
- Erste Erwähnung von „Rootkits“ in Zusammenhang mit SunOS
- 1996: erste Linux-Rootkits
- 1997: Phrack-Magazine: LKM-Rootkits vorgeschlagen (zunächst für Linux verfügbar später auch für andere Unix-Varianten)
- 1998: Non-LKM kernel patching von Silvio Cesare
- 1997: heroin
- 1999: knark / adore LKM
- 1999: Kernel Rootkits für Windows (NT-Rootkit)
- 2000: T0rnkit v8 libproc library Rootkit veröffentlicht
- 2001 KIS, SucKIT manipulieren den Kernel direkt im Hauptspeicher (Technik 1998 beschrieben)
- Ab 2002: Sniffer Backdoors in Rootkits

# Cross-View based Rootkit-Detection

- **Problem**
  - Rootkits fangen Systemaufrufe ab um z.B. nicht mehr in der Prozessliste zu erscheinen, Dateien zu verstecken oder liefern falsche Registry-Schlüssel zurück
  - Herkömmliche Antiviren- und Antispyware-Programme versagen hier

- **Lösungsansatz (am Beispiel von 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
  - Verdächtige Unterschiede geben Hinweise auf mögliche Rootkits

# RootkitRevealer

- Veröffentlicht: 22. Februar 2005 (SysInternals)
- Vergleicht Windows-API mit rohem Inhalt des Dateisystem bzw. eine Registry-Hive-Datei
- 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

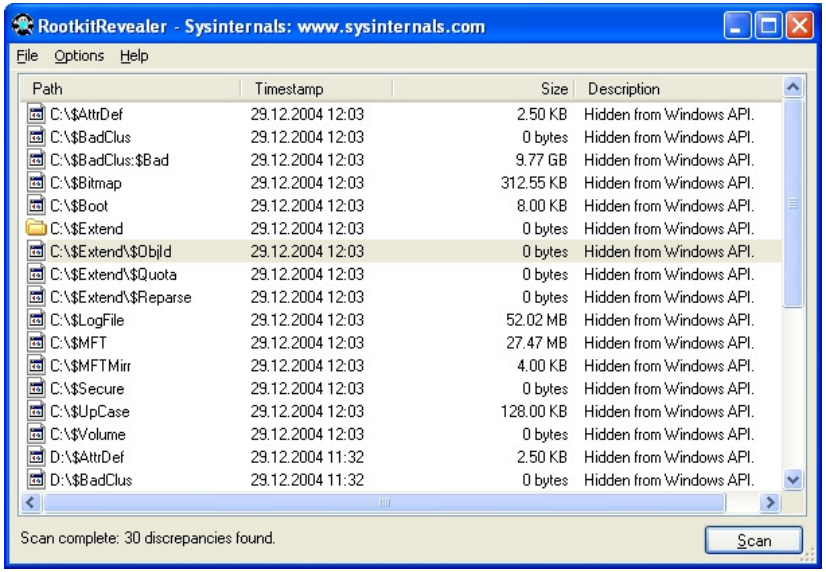
# Abweichungen die RootkitRevealer findet

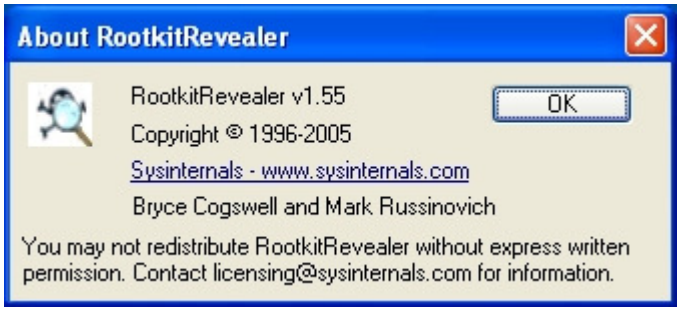
- **Mögliche Abweichungen**
  - Hidden from Windows API (typische Rootkit-Meldung)
  - Access is Denied (sollte nie vorkommen)
  - Visible in Windows API, directory index, but not in MFT
  - Visible in Windows API, but not in MFT or directory index
  - Visible in Windows API, MFT, but not in directory 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

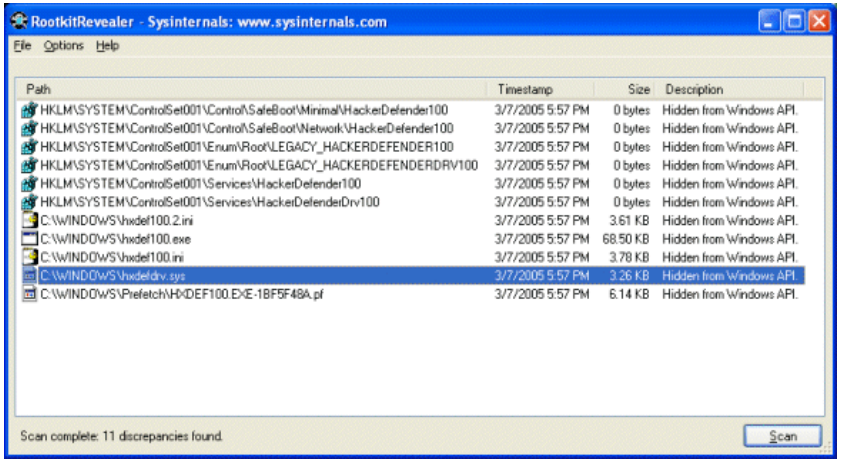
- **Die Ausgabe von RootkitRevealer muss eigenständig interpretiert werden**

# RootkitRevealer bei der Arbeit

- Anzeige von versteckten Registry-Einträgen und Dateien des HackerDefender Rootkits (rechts unten)



# BlackLight™

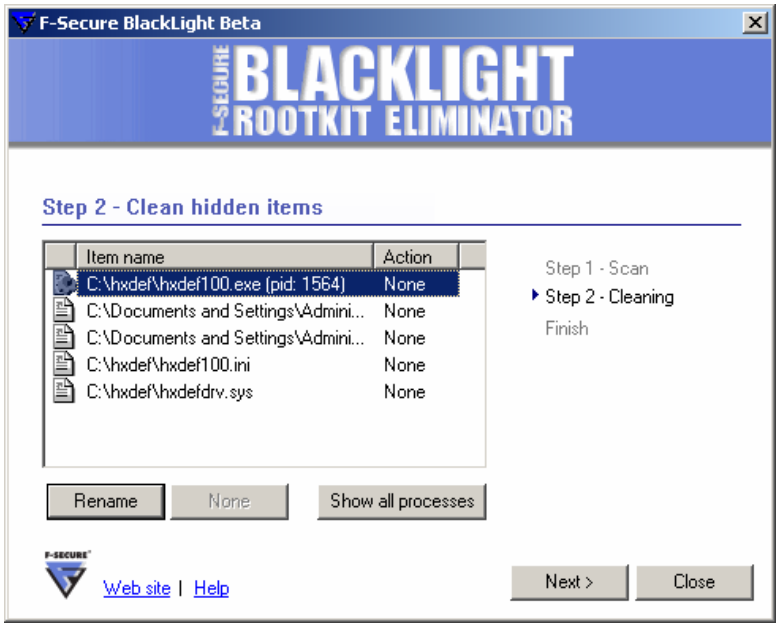

- **Veröffentlicht: 10. März 2005 (F-Secure), Beta-Version (kostenlos nutzbar bis 1. Oktober 2005)**

- **Features**
  - Erkennt und entfernt Rootkits (z.B. HackerDefender, FU), aber teilweise auch Spyware, Trojanische Pferde und Würmer
  - Interpretiert die Scan-Ergebnisse selber
  - Läuft im Hintergrund des Rechners mit (kein Reboot nötig)

- **F-Secure hat für 2005 weitere Produkte mit der BlackLight-Technologie™ angekündigt**

# BlackLight™ bei der Arbeit

- Anzeige von versteckten Einträgen des HackerDefender Rootkits

# Strider GhostBuster Rootkit Detection


- **Noch nicht veröffentlich von Microsoft**
- **3 verschiedene Versionen**
- **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

# Contra

- **Rootkits die Ihre Existenz prinzipiell nicht verbergen werden nicht gefunden (dafür sollten aber herkömmliche Antiviren- bzw. Antispyware-Programme erfolgreich sein)**
- **Rootkit muss zum Zeitpunkt des Scans aktiv sein (Rootkits können den Betrieb zeitweise einstellen wenn sie in der Prozessliste einen Scanner entdecken, z.B. HackerDefender)**
- **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 natürlich auch der Aufwand für die Detektoren)**

# Pro

- **Kombination von High-Level- (online) mit Low-Level-Scans (offline) und einem Antivirenscanner wäre ein sehr guter Ansatz**
  - Reboot-Häufigkeit von Destops / Servern?
- **Die Messlatte für Rootkits wird höher gelegt: Rootkits müssen einen größeren Aufwand betreiben um sich sicher zu verstecken**

# Links

- „Heimliche Hintertüren - Rootkits aufspüren und beseitigen“; Wilhelm Dolle, Thomas Fritzinger, Jürgen Schmidt; Online-Artikel zum Start der Seite „Heise Security“; Juli 2003; http://www.heise.de/security/artikel/38057
- SysInternals RootkitRevealer; www.sysinternals.com/Utilities/RootkitRevealer.html
- F-Secure BlackLight™; www.f-secure.de/blacklight/
- Microsoft Strider GhostBuster Rootkit Detection; www.research.microsoft.com/rootkit/
- The Online Rootkit Magazin; www.rootkit.com
- „Thoughts about Cross-View based Rootkit Detection“; Joanna Rutkowska; www.invisiblethings.org/papers/crossview_detection_thoughts.pdf

# Fragen?

## Vielen Dank für die Aufmerksamkeit

**Wilhelm Dolle, CISA, CISSP, IT-Grundschutz-Auditor**
**Director Information Technology**

**iAS interActive Systems GmbH**
**Dieffenbachstrasse 33c**
**D-10967 Berlin**

**phone** +49-(0)30-69004-100
**fax** +49-(0)30-69004-101
**mail** wilhelm.dolle@interActive-Systems.de
**web** http://www.interActive-Systems.de