Rootkit

aus Wikipedia, der freien Enzyklopädie

Ein **Rootkit** (englisch etwa: „Administratorenbausatz“; root ist bei unixähnlichen Betriebssystemen der Benutzer mit Administratorrechten) ist eine Sammlung von Softwarewerkzeugen, die nach dem Einbruch in ein Softwaresystem auf dem kompromittierten System installiert wird, um zukünftige Anmeldevorgänge („logins“) des Eindringlings zu verbergen und Prozesse und Dateien zu verstecken.

Der Begriff ist heute nicht mehr allein auf unixbasierte Betriebssysteme beschränkt, da es längst auch Rootkits für andere Systeme gibt. Antivirenprogramme versuchen, die Ursache der Kompromittierung zu entdecken. Zweck eines Rootkits ist es, Schadprogramme („malware“) vor den Antivirenprogrammen und dem Benutzer durch Tarnung zu verbergen.

Eine weitere Sammlung von Softwarewerkzeugen oder Bootloadern ist das „Bootkit“.

Inhaltsverzeichnis

Geschichte

Die ersten Sammlungen von Unix-Tools zu den oben genannten Zwecken bestanden aus modifizierten Versionen der Programme ps, passwd usw., die dann jede Spur des Angreifers, die sie normalerweise hinterlassen würden, verbergen und es dem Angreifer so ermöglichten, mit den Rechten des Systemadministrators root zu agieren, ohne dass der rechtmäßige Administrator dies bemerken konnte.

Backdoor-Funktionalitäten

Ein Rootkit versteckt normalerweise Anmeldevorgänge, Prozesse und Logdateien und enthält oft Software, um Daten von Terminals, Netzwerkverbindungen und Tastaturanschläge und Mausklicks sowie Passwörter vom kompromittierten Systems abzugreifen. Hinzu können Backdoors (Hintertüren) kommen, die es dem Angreifer zukünftig vereinfachen, auf das kompromittierte System zuzugreifen, indem beispielsweise eine Shell gestartet wird, wenn an einen bestimmten Netzwerkport eine Verbindungsanfrage gestellt wurde. Die Grenze zwischen Rootkits und Trojanischen Pferden ist fließend, wobei ein Trojaner eine andere Vorgehensweise beim Infizieren eines Computersystems besitzt.

Technische Umsetzung

Das Merkmal eines Rootkits ist es, dass es sich ohne Wissen des Administrators installiert und dem Angreifer die Basis zum Installieren von z. B. Viren oder die Möglichkeit zum Distributed-Denial-of-Service (engl. für *verteilte Diensteblockade*) bietet. Rootkits können neue Hintertüren („backdoors“) öffnen. Zudem versuchen Rootkits, den Weg ihres Einschleusens zu verschleiern, damit sie nicht von anderen entfernt werden.

Application-Rootkits

Application-Rootkits bestehen lediglich aus modifizierten Systemprogrammen. Wegen der trivialen Möglichkeiten zur Erkennung dieser Art von Rootkits finden sie heute kaum noch Verwendung.

Heutzutage finden sich fast ausschließlich Rootkits der folgenden drei Typen:

Kernel-Rootkits

Kernel-Rootkits ersetzen Teile des Kernels durch eigenen Code, um sich selbst zu tarnen („stealth“) und dem Angreifer zusätzliche Funktionen zur Verfügung zu stellen („remote access“), die nur im Kontext des Kernels („ring-0“) ausgeführt werden können. Dies geschieht am häufigsten durch Nachladen von Kernelmodulen. Man nennt diese Klasse von Rootkits daher auch *LKM-Rootkits* (LKM steht für engl. „loadable kernel module“). Einige Kernel-Rootkits kommen auch ohne LKM aus, da sie den Kernelspeicher direkt manipulieren. Unter Windows werden Kernel-Rootkits häufig durch die Einbindung neuer `.sys`-Treiber realisiert.

Ein solcher Treiber kann Funktionsaufrufe von Programmen abfangen, die beispielsweise Dateien auflisten oder laufende Prozesse anzeigen. Auf diese Weise versteckt das Rootkit seine eigene Anwesenheit auf einem Computer.

Userland-Rootkits

„Userland-Rootkits“ sind vor allem unter Windows populär, da sie keinen Zugriff auf der Kernel-Ebene benötigen. Sie stellen jeweils eine DLL bereit, die sich anhand verschiedener API-Methoden (*SetWindowsHookEx, ForceLibrary*) direkt in alle Prozesse einklinkt. Ist diese DLL einmal im System geladen, modifiziert sie ausgewählte API-Funktionen und leitet deren Ausführung auf sich selbst um („redirect“). Dadurch gelangt das Rootkit gezielt an Informationen, welche dann gefiltert oder manipuliert werden können.

Speicher-Rootkits

Speicher-Rootkits existieren nur im Arbeitsspeicher des laufenden Systems. Nach dem Neustart („reboot“) des Systems sind diese Rootkits nicht mehr vorhanden.

Prominente Rootkits der letzten Jahre

- Die Firma *Sony BMG* kam in die Schlagzeilen und musste diverse Musik-CDs zurückrufen, nachdem bekannt geworden war, dass sich der von *Sony* eingesetzte Kopierschutz XCP („E**x**tended **C**opy **P**rotection“) für Musik-CDs mit Methoden eines Rootkits in Windows-Systemen einnistete. Obwohl selbst kein Virus bzw. Trojanisches Pferd, eröffnet allein dessen Existenz weiteren Schadprogrammen Tür und Tor.[1]
- Zwischenzeitlich gab es auch einen USB-Stick mit Fingerabdruckleser[2] von *Sony*, dessen Software zur vollen Funktionsfähigkeit ein Rootkit im Windows-Verzeichnis versteckte. Allerdings wurde einer Pressemitteilung von *Sony* zufolge die Produktion und der Vertrieb dieses USB-Sticks Ende August 2007 wieder eingestellt.[3]
- Die Firma *Kinowelt* verkaufte 2006 in Deutschland DVDs mit einem von *Settec* entwickelten Kopierschutz, der unter Windows ebenfalls ein *Userland-Rootkit* zum Verstecken von Prozessen installiert.[4]
- Forscher der *University of Michigan* haben eine Variante entwickelt, virtuelle Maschinen als Rootkits („Virtual Machine Based Rootkits“) zu verwenden. Die Arbeit an diesem Projekt mit Namen *SubVirt* wurde unter anderem von *Microsoft* und *Intel* unterstützt. Das Rootkit, das mittlerweile von Wissenschaftlern und *Microsoft*-Mitarbeitern entwickelt wurde, sollte auf dem „*IEEE Symposium on Security and Privacy*“ im Mai 2006 präsentiert werden.
- Auf der Konferenz *Black Hat* im Januar 2006 wurde ein möglicher Rootkit-Typ vorgestellt, der selbst eine Neuinstallation des Betriebssystems oder ein Neuformatieren der Festplatte überlebt, indem er das ACPI („Advanced Configuration and Power Interface“) manipuliert oder sich im PC-BIOS festsetzt.[5]
- Die Firma EA hat in ihrem im September 2008 veröffentlichten Spieletitel *Spore* im DRM-Paket des Programms ein Rootkit zur Anwendung gebracht, das dem Zweck dient, den Kopierschutz mit Online-Authentifizierung vor dem Benutzer zu verbergen. Darüber ist eine bis jetzt noch kontroverse Diskussion entstanden.[6]

Entfernung von Rootkits

Da eine hundertprozentige Erkennung von Rootkits unmöglich ist, ist die beste Methode zur Entfernung die vollständige Neuinstallation des Betriebssystems.[7] Da sich bestimmte Rootkits im BIOS verstecken, bietet selbst diese Methode keine hundertprozentige Sicherheit über die Entfernung des Rootkits.[8] Um eine Infizierung des BIOS im Voraus zu verhindern, sollte das BIOS hardwareseitig mit einem Schreibschutz versehen werden, z. B. durch einen Jumper auf der Hauptplatine.

Jedoch gibt es für viele Rootkits von offiziellen Herstellern, z. B. das Sony Rootkit, bereits Programme zur Erkennung und Entfernung.

Siehe auch

- Dropper
- Hook (Informatik)

Weblinks

- c't-Artikel „Kostenloser Spürhund, RootkitRevealer spürt Hintertüren auf“ (http://www.heise.de/security/artikel/58158) vom 4. April 2005 zu Rootkits unter Windows XP (siehe auch www.heise.de/security/artikel/38057/0 (http://www.heise.de/security/artikel/38057/0))

- SonyBMGs digitaler Hausfriedensbruch – Ein Review der Ereignisse (http://www.netzpolitik.org/2005/rookit-sonys-digitaler-hausfriedensbruch/)
- 10 Dinge, die Sie über Rootkits wissen sollten (http://www.diagramm.net/index.php?id=5455&d=a&i=NuN)

Einzelnachweise

1. www.heise.de/newsticker/Sony-BMGs-Kopierschutz-mit-Rootkit-Funktionen--/meldung/65602 (http://www.heise.de/newsticker/Sony-BMGs-Kopierschutz-mit-Rootkit-Funktionen--/meldung/65602) Heise Verlag
2. Golem.de (http://www.golem.de/0708/54381.html) „Sonys USB-Sticks mit Rootkit-Funktion“
3. GameStar.de (http://www.gamestar.de/news/pc/hardware/sony/1473404/sony.html) „Sony: Produktion der USB-Sticks mit Rootkit wieder eingestellt“
4. DVD-Kopiersperre Alpha-DVD: Update oder Uninstaller (http://www.heise.de/newsticker/meldung/DVD-Kopiersperre-Alpha-DVD-Update-oder-Uninstaller-111677.html) - heise.de
5. www.heise.de (http://www.heise.de/security/meldung/Wieder-einmal-Rootkit-im-PC-BIOS-209207.html) Wieder einmal: Rootkit im PC-BIOS
6. heise.de (http://www.heise.de/newsticker/Spore-Aerger-ueber-Kopierschutz-Update--/meldung/115804) Spore: Ärger über Kopierschutz
7. technet.microsoft.com (http://technet.microsoft.com/de-de/sysinternals/bb897445.aspx#inp) Sysinternals über die Entfernung von Rootkits
8. Jürgen Schmidt: *Hacking Team verwendet UEFI-Rootkit.* (http://www.heise.de/security/meldung/Hacking-Team-verwendet-UEFI-Rootkit-2750312.html) heise.de, 14. Juli 2015, abgerufen am 6. August 2015.

Kategorien: Schadprogramm | IT-Sicherheit | DRM
