Alarmstufe Rot: Ihr PC wurde geentert!

Rootkits unter MS-Windows

Das Leben mit Computerviren, Würmern und Trojanern ist für Windows-Benutzer[1] schon seit langem selbstverständlich. Die mächtigsten und tückischsten aller Trojaner – bei Profi-Hackern sehr beliebt und bei Anwendern und Systemadministratoren entsprechend gefürchtet – sind die so genannten Rootkits. Der Name stammt aus der Unix-Welt, da hier die ersten Rootkits auftraten. *Root* in Unix entspricht dem *Administrator*-Nutzer unter Windows, er hat alle Rechte am System. Ein Rootkit ist also ein Softwarewerkzeug, das dem Eindringling alle Rechte des Administrators verschafft – und dies auf Dauer. Denn: Es versteckt seine Existenz vor allen, bis auf den Hacker selbst. Selbst die besten Suchwerkzeuge nach digitalem Ungeziefer versagen oft bei Rootkits. Zwar muss es dem Angreifer zunächst gelingen, einen Rechner zu knacken und das Rootkit zu installieren; anschließend ist dieses jedoch kaum mehr zu finden bzw. zu entfernen – auch nicht für Experten.

Feindliche Vorgangsweisen

„Blinde Passagiere" wie Trojaner oder Rootkits erhält man vorrangig durch administrative Nachlässigkeiten, die ihrerseits ihre Ursache in mangelndem Sicherheitsbewusstsein haben: Hacker scannen das Netzwerk nach angreifbaren Rechnern und nisten sich überall dort ein, wo sie leicht Unterschlupf finden. Besonders gefährdet sind auch Rechner, die für Hacker aus strategischen Gründen interessant sind – z.B. weil sie eine schnelle Internetanbindung haben oder sich in Netzen befinden, die ergiebige Spionagemöglichkeiten versprechen. Das einzige Mittel dagegen ist eine rigorose, umfassende Sicherheitspolitik, wie sie der ZID schon seit längerem empfiehlt (mehr dazu im Abschnitt *Was bleibt zu tun?*).

Rootkits sind – obwohl von einer hohen Dunkelziffer ausgegangen werden muss[2] – unter Windows zwar weniger verbreitet als Viren und Würmer, dafür aber umso unangenehmer. Beispielsweise hatte ein Administrator eines Institutsservers der Uni Wien zweimal ein Problem mit einem HE4Hook-Rootkit (siehe weiter unten), obwohl sich der Server hinter einer Firewall befand und sich der Administrator deshalb sicher wähnte. Beim ersten Mal fiel der Windows-Server dadurch auf, dass von ihm eine Netzwerkattacke ausging, die viel Bandbreite in Anspruch nahm. Virenscanner-Untersuchungen blieben erfolglos, die schädliche Aktivität war aber unleugbar. Der Server wurde also vom Netz genommen, und als der Administrator schließlich die Festplatte ausbaute und auf einem anderen, „sauberen" PC als Datenplatte durchsuchte, wurde das Rootkit sichtbar. Der Server wurde daraufhin komplett neu aufgesetzt; dennoch gelang es Hackern wieder, das System zu knacken (vermutlich war der Server nach einem Software-Update nicht sofort neu gestartet worden, sodass die Sicherheitsänderungen nur teilweise aktiv waren). Diesmal wurde der Server nach Strich und Faden ausspioniert – Serverdaten wurden analysiert und kopiert, Passwörter abgehört und in versteckten Bereichen gespeichert – und damit zu einer großen Gefahr für seine (Netzwerk-)Umgebung. Erst durch weitreichende, konsequent eingehaltene Sicherheitsmaßnahmen konnten die Hacker gestoppt werden.

Rechner an der Uni Wien spielen bei solchen Attacken leider allzu oft die Rolle des „dummen Opfers". Meist sind sie nicht das direkte Ziel des Hackers, sondern nur Mittel zum eigentlichen Zweck. Mit einem geenterten Universitäts-PC hat der Angreifer mehrerlei erreicht:

- Der PC dient ihm als Sprungbrett für weitere Attacken und zur Verschleierung seiner Herkunft.
- Der PC steht ihm als Spam-Verteilerknoten (als Schleuse für den Versand unerwünschter Massenmail) zur Verfügung.
- Der PC – mit seiner im Allgemeinen guten Ausstattung und Netzwerkbandbreite – kann im Rahmen eines netzwerkmäßig verteilten Großangriffs auf ein externes Ziel (*Distributed Denial of Service*, DDoS) als ferngesteuerter „Zombie" eingesetzt werden.
- Der PC ist der sprichwörtliche „Fuß in der Türe" zum Datennetz der Universität. Durch Abhören von Authentisierungsinformationen (z.B. Mailbox-Passwörter) kann der Angreifer weitere Systeme infiltrieren bzw. unter falscher Identität beliebig agieren.

Gut getarnt ist halb gewonnen

Wie unter Unix/Linux[3] gibt es auch unter Windows zwei grundsätzlich verschiedene Arten von Rootkits. Die **Usermode-Rootkits** sind klassische Trojaner und können daher im Allgemeinen mit einem geeigneten aktuellen Viren-

1) Alle Personenbezeichnungen in diesem Artikel sind geschlechtsneutral zu verstehen.

2) Das Jahr 2006 wurde von Sicherheitsexperten zum „Year of the Rootkit" gekürt.

3) siehe Artikel *Ihr Linux-Rechner wurde assimiliert – ist Widerstand zwecklos? Rootkits unter Linux* in *Comment 06/1*, Seite 19 bzw. unter `www.univie.ac.at/comment/06-1/061_19.html`

4) siehe Artikel *Sonys digitaler Hausfriedensbruch* in *Comment 06/1*, Seite 24 bzw. unter `www.univie.ac.at/comment/06-1/061_24.html`

scanner gefunden werden. Sie laufen im Usermode, d.h. mit den Rechten des Anwenders. Ihr Wirkprinzip ist die Unterdrückung relevanter Information bei der Ausgabe: Jedes Programm, das den Hacker verraten könnte, wird so umgeschrieben, dass die elektronischen Spuren des Angreifers verwischt werden und seine Anwesenheit im System verborgen bleibt. Usermode-Rootkits sind unter Windows (im Gegensatz zu Linux) selten, weil sie für die Hackergemeinschaft mit großem Aufwand verbunden sind: Aufgrund der proprietären und noch dazu komplexen grafischen Oberfläche von Windows müssen dafür sehr viele Anwendungen umprogrammiert werden.

Umso größerer Beliebtheit bei Hackern erfreuen sich die **Kernelmode-Rootkits**. Kernelmode-Rootkits sind äußerst effizient und daher der ultimative Schrecken jedes PC-Verantwortlichen oder Anwenders. Sie fälschen Informationen bereits *vor* der Ausgabe, auf der Ebene des Systemkerns. Das Ergebnis: Dateien verschwinden, Anwendungen des Hackers werden im laufenden System versteckt, offene Netzwerkzugänge dem eigentlichen Administrator vorenthalten, Systemregistraturdaten falsch angegeben, Einträge in der Ereignisanzeige von Windows unterdrückt oder gefälscht und vieles andere mehr. Jede Anwendung, die ein Nutzer oder Administrator aufruft, wird daran gehindert, korrekte Daten wiederzugeben. Daher ist der Schädling auf regulärem Weg kaum zu finden. Selbstredend können Kernelmode-Rootkits auch die Ausführung eines Virenscanners behindern oder gar unterdrücken, während sich der genasführte Administrator sicher wähnt; dasselbe gilt für den Zugriff auf Aktualisierungsdaten des Scanners im Internet. Windows-Firewalls werden ausgehebelt, Webseiten und Internetadressen werden umgelenkt, Kommunikation wird abgehört oder kontrolliert. Das Bedrohungspotenzial ist schier unerschöpflich.

Unter Windows werden Kernelmode-Rootkits häufig als Gerätetreiber oder als DLL (*Dynamic Link Library*) mit allen Rechten des Administrators – als Teil des Betriebssystems – installiert. Die alternative Methode ist, mit Hilfe eines einmalig aufzurufenden Programms die Systemschnittstellen im Speicher des PCs zu ändern, sodass jeder Systemaufruf einer Anwendung zuerst an dem im Speicher residierenden Rootkit vorbei muss. Einmal installiert, werden Rootkits beim Systemstart automatisch wieder geladen. Dank ihrer Versteck-Technik sind ihre Spuren nach dem Laden sofort verschwunden – wenn sich der Administrator anmeldet, hat der PC längst voll durchgestartet und der Spuk läuft. Wie schwierig das Entfernen eines solchen Rootkits sein kann, hat der Sicherheitsexperte Marc Russinovich am Beispiel von Sonys XCP-Rootkit[4] in seinem Weblog dokumentiert (`www.sysinternals.com/blog/blogindex.html`).

Das erste Kernelmode-Rootkit für Windows wurde 1999 von Greg Hoglund, einem Systemsicherheitsarchitekten, entwickelt (bis zu diesem Zeitpunkt waren alle trojanischen Aktivitäten Teil des Usermodes). Sein *NT Rootkit* ist in der Anwendung sehr einfach: Im Prinzip lässt es alle Informationen – Dateien, laufende Programme (Prozesse), Registratureinträge – vor den Augen des Anwenders verschwinden, die als Kennung den Text `_root_` vorangestellt haben. Es ist auch in der Lage, eine zweite Internetadresse für den PC zu vergeben, über die der Hacker unbehelligt in das System einsteigen kann. Alle Aktivitäten, die der Hacker über diese Internetadresse abwickelt, werden vom Rootkit getarnt. Das Rootkit versteckt sich zudem selbst: Nach der Installation ist es unsichtbar.

Wie gelangt nun der Hacker an die getarnten Daten? Ganz einfach: Wird ein verborgenes Programm mitsamt seiner Kennung aufgerufen, so ist die Tarnung dafür aufgehoben. Die Idee dahinter ist, dass nur der Hacker weiß, welche Programme vor den Augen des PC-Besitzers versteckt sind, und daher nur er selbst diese Programme ausführen kann. Kopiert er z.B. den Windows-Explorer und speichert die Kopie unter einem neuen Namen (mit Kennung), so wird beim anschließenden Aufruf dieser Kopie die Dateiansicht plötzlich wieder vollständig angezeigt. Ähnlich funktioniert das mit dem Task-Manager, dem Registratur-Editor etc. Ist ein Hacker nicht imstande, eine individuelle Kennung in das Rootkit zu programmieren, kann er vom Administrator auf diesem Weg enttarnt werden.

Das NT Rootkit ist heute mehr Konzept als taugliches Rootkit, dennoch wird es gerne als Anschauungsbeispiel für die Infektionsmöglichkeiten eines Windows-Betriebssystemkerns präsentiert. Die Janusköpfigkeit solcher Sicherheitsbemühungen zeigte sich schon bald: Die Ideen Hoglunds wurden natürlich von der Hackergemeinde aufgegriffen und verfeinert, sodass mittlerweile eine Vielzahl weit moderner und wesentlich flexiblerer Kernelmode-Rootkits existiert. Vier davon – HE4Hook, Vanquish, FU/FUTo und das AFX-Rootkit – werden im Folgenden näher vorgestellt.

Schurken im Schatten – und wie man sie aufspürt

Wie kann etwas Unsichtbares gefunden werden? Zum Glück gilt auch hier: *Tand, Tand ist das Rootkit aus des Hackers Hand*. Jedes Rootkit ist nur so gut wie sein Programmierer, sodass kleinere Fehler dann doch oft zur Enttarnung führen. Solche Fehler sind sowohl bei der Methode der Infektion des Systemkerns als auch bei deren Umsetzung möglich. Daher ist es grundsätzlich wichtig, den Gegner zu kennen, d.h. über die Funktionsweise von Rootkits Bescheid zu wissen.

HE4Hook

Das HE4Hook-Rootkit wird auch als „russisches Rootkit" bezeichnet. Es ist kein vollständiges Rootkit, d.h. es kann keine Registratureinträge und offenen Ports verschwinden lassen, versteckt aber Dateien und Programme (Prozesse). Auf Anfrage verhindert es auch das Löschen von Dateien oder das Stoppen von Prozessen, für den Fall, dass jemand zufällig ein getarntes Objekt ergattert. HE4Hook ist ein älteres Rootkit und läuft auf modernen Windows-Versionen

nicht. Beispielsweise erzeugt es unter Windows XP einen formidablen Absturz, wenn es geladen wird, hinterlässt dabei aber Spuren in der Ereignisanzeige (siehe **Abb. 1**). Unter Windows XP ServiceRelease 2 hingegen stürzt das Betriebssystem komplett ab. Falls also auf Ihrem PC unerklärliche Systemabstürze oder ähnliche Fehlermeldungen wie in Abb. 1 auftreten, könnte es sein, dass er von einem Hacker geentert wurde, der beim Installieren des Rootkits nicht erfolgreich war.

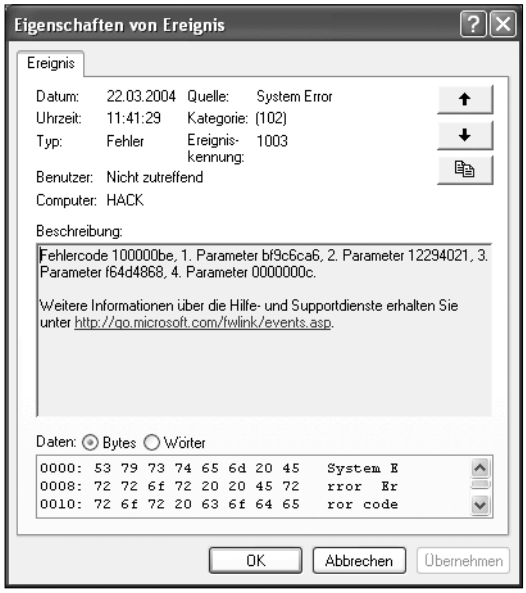

Abb. 1: Ereignisanzeige unter Windows XP nach Systemabsturz durch HE4Hook-Rootkit

Vanquish

Im Vergleich zu HE4Hook sind die Möglichkeiten des Vanquish-Rootkit relativ schlicht gehalten, dafür funktioniert es aber auch auf neueren Windows-Versionen – also auf Windows 2000, 2003 und XP. Wie das NT Rootkit verbirgt Vanquish alles, was als Kennung seinen Namen enthält (es kann allerdings noch keine Nutzer, Prozesse oder offenen Ports verstecken). Ein mit Vanquish kompromittiertes System lässt sich nicht mit vernünftigem Aufwand säubern: Das Rootkit installiert sich nicht nur über die DLLs und setzt sich vor die Programmschnittstellen (APIs) von Windows, sondern infiziert auch Prozesse und nistet sich in der Registratur ein. Nur Prozesse und Dateien, welche die Kennung aufweisen, werden von Vanquish verschont. Damit ist es im laufenden System faktisch nicht mehr sichtbar bzw. entfernbar. Zusätzlich protokolliert das Rootkit automatisch jedes eingegebene Passwort in der Datei `C:\vanquish.log`.

Da die Kennung `vanquish` wie bei Hoglunds erstem Rootkit fix vorgegeben ist, kann das Vorhandensein von Vanquish auf diesem Weg aufgedeckt werden: Man erstellt einfach eine Datei mit dieser Kennung im Namen; verschwindet sie, dann ist Vanquish installiert. Leider ist diese Methode nicht immer erfolgreich – versierte Hacker bauen eine andere Kennung in das Rootkit ein. Für einen stichhaltigeren Test muss man wissen, dass Vanquish lediglich Windows-APIs täuschen kann, also nur reine Windows-Anwendungen von ihm betroffen sind. Glücklicherweise gibt es aber unter Windows immer noch das gute alte DOS, das keine Windows-APIs verwendet und daher von Vanquish nicht betrogen werden kann. Wenn Sie also die Windows-Eingabeaufforderung (die „DOS-Box“, unter *Start – Ausführen* zu finden) mittels `command` – keinesfalls mit `cmd`[5] – aufrufen, so läuft DOS in einer Windows-Emulation. Mittels `dir C:\vanquish.log` unter `command` kann ein Standard-Vanquish gefunden werden. Hat der Hacker die Kennung geändert, dann muss die Ergebnisliste des Befehls `dir /s` unter `cmd` mit derjenigen des gleichen Befehls unter `command` verglichen werden. Zeigt `cmd` weniger Dateien als `command`, so ist mit großer Wahrscheinlichkeit ein Vanquish-Rootkit aktiv.

FU/FUTo

Das FU-(bzw. das neuere FUTo)-Rootkit[6] ist Hackern beim Verstecken von Prozessen behilflich. Der Windows-Systemkern hält an einer bestimmten Stelle im Hauptspeicher eine spezielle Liste von aktiven Programmen (Prozessen) für die Abfrage bereit, die durch den Windows Task-Manager angezeigt werden kann. In dieser Liste sind alle ausführbaren Programme eingetragen und durchnummeriert. Diese Nummerierung nennt man *Prozess-Identifikation* (PID). Da sich diese Liste in kurzer Zeit sehr oft ändern kann, wird jedes Programm zusätzlich mit einem Eintrag versehen, der auf das vorige bzw. das nächste Programm in der Liste verweist. Diese Prozess-Liste wird daher „Kette“ genannt. Fordert ein Hacker beim FU-Rootkit das Verstecken eines Programms an, werden die Verkettungseinträge des vorigen und nachfolgenden Eintrags so geändert, dass sie das zu tarnende Programm umgehen und somit unsichtbar machen. Da die PID aber noch existiert, kann das getarnte Programm trotzdem ausgeführt werden.

Abb. 2 zeigt solche Prozesslisten in der Ansicht des Task-Managers von Windows 2000 sowie in der Ansicht des FU-Rootkit. Noch ist alles in Ordnung. Der Hacker, der sich in diesem Fall bereits Administrator-Rechte angeeignet hat, bringt jetzt sukzessive alle Prozesse zum Verschwinden (siehe **Abb. 3**).

Natürlich ist es nicht sinnvoll, wenn der Hacker alle Prozesse verschwinden lässt. Diese Demonstration zeigt jedoch, dass mit Ausnahme des Leerlaufprozesses (das ist jenes Programm, das ausgeführt wird, wenn das System nichts zu tun hat) keine Einschränkungen für das Versteckspiel mit FU bzw. FUTo bestehen. Eine Spezialität von FU ist, dass Privilegien von beliebigen Prozessen im laufenden Betrieb geändert werden können. Beispielsweise ist es möglich, einem Programm, das von einem Hauptbenutzer gestartet wurde, nachträglich Administrator-Rechte zu geben. Darüber hinaus kann FU den Anmeldevorgang eines Nutzers „impersonalisieren“: Windows weiß dann nicht, welcher Nutzer

5) Der Unterschied zwischen dem DOS-Befehlsinterpreter `command` und seinem Windows-Äquivalent `cmd` ist, dass `cmd` sehr wohl Windows-APIs verwendet. Das äußert sich insbesondere bei langen Dateinamen: Während diese unter `cmd` vollständig dargestellt werden, werden sie unter `command` nach dem sechsten Zeichen abgeschnitten und mit einer Tilde (~) sowie einer Ziffer ergänzt.

6) FU steht für *fool the superuser* („täusche den Administrator“) und ist eine Anspielung auf den Unix-Befehl `su` (*substitute user*), mit dem im laufenden System ein Benutzerwechsel durchgeführt werden kann.

wirklich angemeldet wurde. Installiert wird FU über den Treiber `msdirectx.sys`, der aufgrund der Namensgebung leicht mit Microsofts Multimedia-Software DirectX verwechselt werden kann.

Wie verrät sich nun dieses Rookit? Das ältere FU-Rootkit produziert unter neueren Windows-Versionen (2003, XP) durchaus sporadische Systemabstürze. FUTo geht es mit Windows 2000 und XP ähnlich. Da Windows nicht nur für Prozesse, sondern auch für Anwendungen eine eigene Namensliste im Systemkern hält, können Programme, die explizit den Anwendungsnamen setzen (z.B. die schon erwähnte DOS-Box), durch FU/FUTo in der Anwendungsliste des Task-Managers nicht zum Verschwinden gebracht werden. Die Folge ist, dass Prozessliste und Anwendungsliste des Task-Managers nicht übereinstimmen – d.h. eine Anwendung läuft, es ist aber kein zugehöriger Prozess zu finden.

AFX

Das AFX-Rookit ist der Mercedes unter den hier genannten Windows-Rootkits: Es läuft unter Windows NT, 2000, 2003 und XP. AFX kann Prozesse, Dateien, Verzeichnisse, Systemmodule, Windows-Registratureinträge, offene Ports sowie System-Ikonen (*systray icons*) verstecken.

Eine Besonderheit von AFX ist, dass es auch Datei-Deskriptoren (*file handles*) verbergen kann. Ein Datei-Deskriptor ist eine Datenstruktur im Speicher des Systems, die zum Zeitpunkt des Lesens oder Schreibens einer Datei für diese zentral angelegt wird und mittels der die Verwaltung aller Dateien durchgeführt wird, die soeben geöffnet sind. Werkzeuge wie Filemon (siehe `www.sysinternals.com`), die anhand solcher Datei-Deskriptoren offene Dateien anzeigen und somit z.B. eine offene Datei `c:\vanquish.log` aufdecken können, sind gegen das AFX-Rootkit chancenlos.

Die Bedienung dieses Rootkits ist verblüffend einfach: Es versteckt jenes Verzeichnis, aus dem heraus es installiert wird. Der Verzeichnisname (genauer: die unterste Ebene des Pfades zum Installationsverzeichnis) wird dabei gleichzeitig zum Schlüssel für die Sichtbarkeit – wie `vanquish` bei Vanquish oder `_root_` bei Hoglunds NT Rootkit.

AFX hat – wie viele andere Windows-Rootkits – derzeit noch das Problem, dass es (z.B. unter Windows 2003 oder Windows XP) nicht mit mehreren gleichzeitig angemeldeten Nutzern umgehen kann. Ein möglicher Administrator-Trick ist daher, sich zunächst als unprivilegierter Hauptbenutzer anzumelden und dann erst auf den Administrator-Nutzer zu wechseln, wodurch das Rootkit zumindest teilweise sichtbar wird.

Das Wettrennen

Wie Linux-Rootkits sind auch Windows-Rootkits sehr abhängig von ihrer exakten Implementierung. Ändern sich im

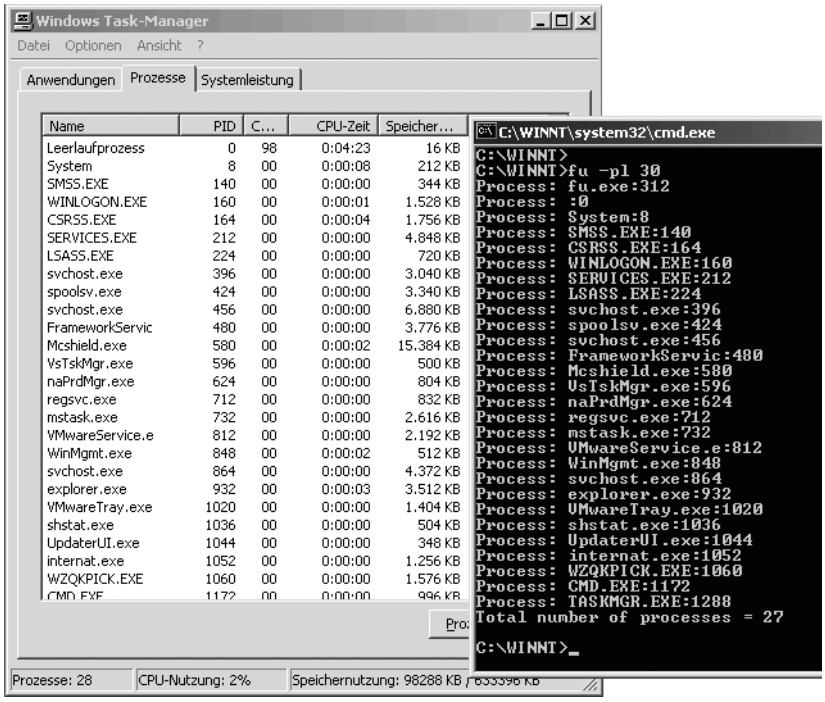

Abb. 2: Prozessliste im Task-Manager (links) und in der Ansicht des FU-Rootkits (rechts)

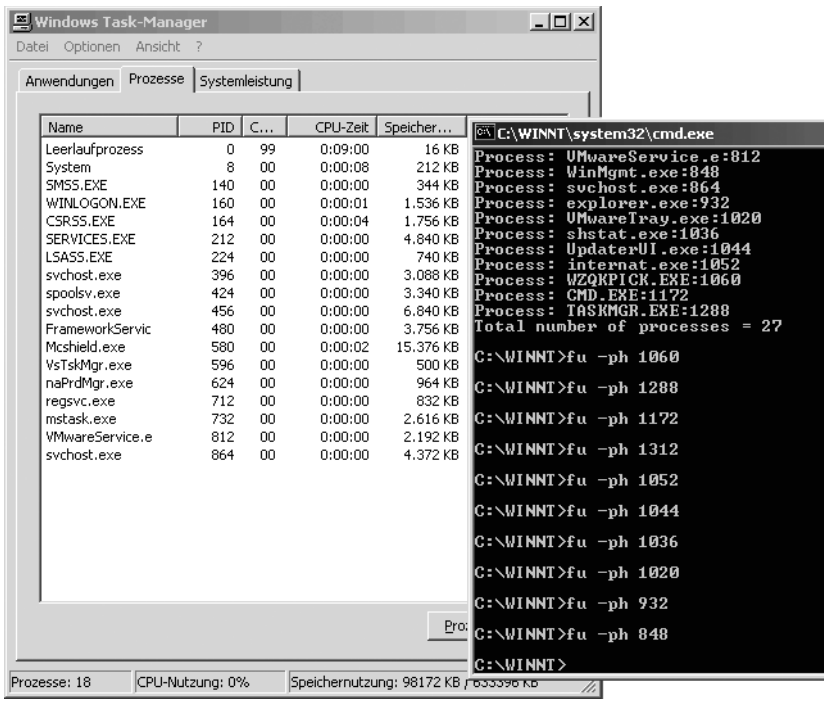

Abb. 3: Das FU-Rootkit kann bis auf den Leerlaufprozess alle Prozesse zum Verschwinden bringen.

Windows-Kern oder in den Programmschnittstellen wesentliche Teile durch ein Service-Release (wie z.B. das Service-Pack 2 von Windows XP), dann ist mit hoher Wahrscheinlichkeit das abgestimmte Zusammenspiel zwischen Rootkit und Systemkern nicht mehr möglich. Die Folge davon sind Abstürze von Programmen oder des gesamten Betriebssystems, die vor allem zu zwei Zeitpunkten auftreten: Wenn der wahre Administrator des Systems ein Upgrade auf ein neues Service-Release durchführt (also ein ServicePack einspielt) oder wenn der Hacker sein Rootkit in eine unpassende Windows-Version einspielt. Daher sind System- oder Programmabstürze – insbesondere des Windows-Explorers – vom Sicherheitsstandpunkt generell bedenklich und sollten analysiert werden.

Zwischen Betriebssystem-Herstellern und Hackern hat sich diesbezüglich ein richtiggehendes Wettrennen eingestellt: Die Systemhersteller schließen Lücken und machen den Hackern durch Änderungen an den Programmschnittstellen (APIs) das Leben schwer; die Hacker passen sich an und entwickeln ausgefeiltere Rootkits. Je nach aktuellem Software-Stand haben abwechselnd die „Guten“ oder die „Bösen“ die Nase vorne.

Explizite Rootkit-Scanner, wie sie unter Linux gebräuchlich sind, gibt es unter Windows nicht. Eine interessante Entwicklung zur Enttarnung von Rootkits sind jedoch die so genannten *Baseline*-Werkzeuge wie z.B. Patchfinder 2 oder das neuere Windows Memory Forensic Toolkit (zu finden unter `www.rootkit.com`). Jede Aktion eines Nutzers bewirkt eine Vielzahl von Systemaufrufen – wird beispielsweise der Windows-Explorer gestartet, so müssen Dateien gelesen und geschrieben, Registratureinträge gelesen bzw. geändert und Netzwerkschnittstellen verwendet werden. Ein Baseline-Werkzeug analysiert diese Systemaufrufe und merkt sich die Muster. Wird danach ein Rootkit (oder auch ein Virenscanner!) installiert, schlägt das Baseline-Werkzeug Alarm, da sich die Aufruf-Muster geändert haben. Selbstverständlich haben auch Baseline-Werkzeuge ihre Nachteile: Wie die Virenscanner brauchen sie viele Ressourcen vom System und sind hochgradig abhängig von der eingesetzten Windows-Version.

Machtlose Virenscanner

Das Aufspüren aktiver Kernelmode-Rootkits gestaltet sich schwierig. Ist ein Rootkit erst einmal erfolgreich installiert und auf Dateisystem-Ebene zum Verschwinden gebracht worden, entzieht es sich erfolgreich der Suche. In **Abb. 4** ist ein ergebnisloser Scan des McAfee Virenscanners nach einem laufenden HE4Hook-Rootkit zu sehen – obwohl er die Signatur von HE4Hook kennt, was nicht selbstverständlich ist: Beispielsweise ignorierten manche Scanner das FU-Rootkit mehr als zwei Jahre nach dessen Erscheinen noch immer.

Es gibt also keine zuverlässige Möglichkeit, bereits im System laufende Kernelmode-Rootkits mittels Virenscanner zu finden. Windows lässt sich jedoch durch rechtzeitiges Drücken der `F8`-Taste beim Start im „abgesicherten Modus“ laden. Viele Rootkits werden dann nicht gestartet, sodass ein anschließendes Aufspüren möglich wird.

Die beste Möglichkeit, Rootkits zu finden, besteht darin, die Festplatte in einen anderen Windows-PC zu transferieren und sie dann mittels Virenscanner zu untersuchen. Dieser PC sollte jedoch sehr sicher betrieben werden, da eventuelle dort installierte Rootkits das Ergebnis natürlich verfälschen würden. Am besten geeignet ist hier ein neu instal-

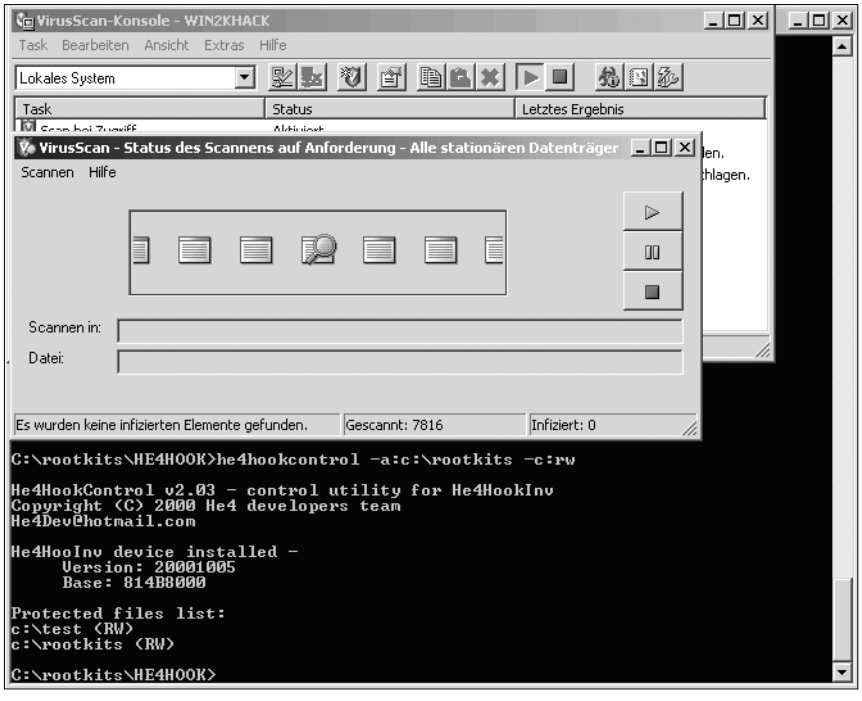

Abb. 4: HE4Hook wird trotz bekannter Signatur vom Virenscanner nicht gefunden.

7) siehe Artikel *Sicherheit von Anfang an* in *Comment 04/1*, Seite 20 bzw. unter `www.univie.ac.at/comment/04-1/041_20.html`

8) siehe Artikel *Department of Desktop Security: Red Alert bei Windows-Betriebssystemen* in *Comment 04/1*, Seite 18 bzw. unter `www.univie.ac.at/comment/04-1/041_18.html`

9) siehe *Artikel McAfee VirusScan – Ihr Goalkeeper im Einsatz gegen virale Offensiven* in *Comment 04/1*, Seite 21 bzw. unter `www.univie.ac.at/comment/04-1/041_21.html`

10) siehe Artikel *Phishing: Bitte nicht anbeißen!* in *Comment 06/2*, Seite 37 bzw. unter `www.univie.ac.at/comment/06-2/062_37.html`

11) siehe Artikel *Kammerjäger im Netz* in *Comment 06/1*, Seite 31 bzw. unter `www.univie.ac.at/comment/06-1/061_31.html`

12) siehe Artikel *Goldene Regeln für ein intaktes (Windows-)Betriebssystem* in *Comment 04/1*, Seite 16 bzw. unter `www.univie.ac.at/comment/04-1/041_16.html`

lierter Windows-PC, der von Beginn an sicher betrieben wurde.[7)]

Ein Säubern mittels Virenscanner, wie es bei sonstigem digitalen Ungeziefer üblich ist, reicht bei Rootkits jedoch nicht. Die einzig sinnvolle Methode zur „Rettung" eines derart aufgehackten PCs ist, ihn komplett neu aufzusetzen – d.h. man muss seine Daten sichern, die Festplatte formatieren und anschließend sowohl das Betriebssystem als auch die benötigten Anwendungsprogramme neu installieren, wobei das direkte Überspielen von Programmen zu vermeiden ist.

Was bleibt zu tun?

Es zeigt sich, dass die Suche nach bereits installierten Rootkits sehr mühsam und zeitintensiv, zugleich aber auch qualitativ unsicher ist. Wieder einmal ist Vorsorge der beste Schutz und ein Minimieren der Angriffsfläche die beste Waffe gegen Hacker:

- Halten Sie unbedingt Ihr System durch Security-Updates[8)] und regelmäßige Updates des Virenscanners[9)] am aktuellen Stand der Technik.

- Schränken Sie den Zugriff auf Ihren Rechner ein. Verwenden Sie die Windows-Firewall, wo immer es möglich ist, und erlauben Sie dabei nur das, was Sie wirklich brauchen.

- Schalten Sie Windows-Dienste ab, die Sie nicht benötigen. Leider ist dies nicht leicht zu beurteilen und sollte daher nur von versierten Benutzern durchgeführt werden; mit der Verwendung der Windows-Firewall ist jedoch bereits viel gewonnen.

- Meiden Sie generell dubiose Webseiten und verwenden Sie Ihren Browser nicht, wenn Sie als Administrator Ihres PCs angemeldet sind.

- Schalten Sie das automatische Ausführen von programmierten Webinhalten wie JavaScript und ActiveX nach Möglichkeit aus – stellen Sie den Browser vielmehr so ein, dass Sie zuvor gefragt werden, ob Sie das jeweilige Programm ausführen wollen. Das ist zwar lästig, aber im Zweifelsfall bewahrt es vor unreflektiert ausgeführten Programmen aus dem Internet.

- Seien Sie im Umgang mit dem Internet misstrauisch: Schon so mancher Rechner wurde durch eine Phishing-Attacke erfolgreich geentert.[10)] eMail-Nachrichten von (vorgeblich) Banken, der Polizei oder anderen scheinbar seriösen Institutionen, in denen Sie aufgefordert werden, umgehend einem Link zu folgen oder ein Attachment zu öffnen (paradoxerweise werden hierfür oft Sicherheitsgründe angeführt), zielen in aller Regel nur darauf ab, Sie zu einer unüberlegten Handlung zu verführen – z.B. zur Preisgabe Ihres Mailbox-Passworts oder der Anmeldeinformation für Ihren lokalen PC. Beliebt sind auch Word-Dokumente, bei deren Öffnen ein Makro aktiviert wird, das wiederum einen Trojaner auf Ihrem PC installiert. Lassen Sie sich nicht reinlegen – solche Mails können Sie getrost löschen!

Notebooks sind durch ihren häufigen Standortwechsel besonders gefährdet: Moderne Computer-Würmer melden ihr erfolgreiches Eindringen in ein System an zentraler Stelle und führen anschließend Befehle von dort aus.[11)] Hat sich ein Wurm in ein Notebook eingenistet, kann er damit auch hinter Firewalls verschleppt werden und sogar dort – in vermeintlich geschützter Umgebung – sein Unwesen treiben. Ein Notebook ist kein Server; daher sollten hier potentiell riskante Dienste wie integrierte Webserver, Datei- und Druckerfreigaben etc. unbedingt deaktiviert werden.

Einen Windows-Rechner „sauber" zu halten bedeutet Arbeit, manchmal sogar viel Arbeit. Der nötige Aufwand lässt sich stark reduzieren, indem Sie Ihren Arbeitsplatzrechner vom ZID im Rahmen des PC-Deployment managen lassen (siehe `www.univie.ac.at/ZID/fu/`). Richtiges Verhalten beim Umgang mit Netzwerkdiensten wie WWW, eMail und dergleichen[12)] lässt sich dadurch aber nicht ersetzen: Nur permanente Wachsamkeit und ein kritisches Überdenken der eigenen Sicherheitsstrategie kann einigermaßen verlässlich Ruhe verschaffen.

Weitere Informationen, Windows-Rootkits und Rootkit-Analysewerkzeuge finden Sie unter `www.rootkit.com`.

Aron Vrtala ■

Neue Standardsoftware

Neue Produkte (Stand: 2. Oktober 2006)

- Corel WordPerfect Office X3 für Win.
- Endnote X für Win. & Mac
- MS-Visual Studio 2005 Prof. für Win., deutsch (englisch ist seit längerem verfügbar)
- MS-Windows 2003 Server Standard R2
- ScanSoft PaperPort Prof. 11.0 für Win.
- SigmaPlot 10.0 für Win.
- SPSS 13.0 für Mac

Updates (Stand: 2. Oktober 2006)

- RSI IDL 6.3 für Win., Mac & Unix (bisher 6.2)

Alle Informationen zur Standardsoftware sind unter **`www.univie.ac.at/ZID/standardsoftware/`** zu finden. Eine Liste der Softwareprodukte, die im Rahmen der Fakultätsunterstützung (Ferninstallation und Softwarewartung von PCs) angeboten werden, finden Sie unter **`www.univie.ac.at/ZID/fu-windows/`**.

Peter Wienerroither