Whitepaper | April 2006

McAfee®
Proven Security™

Rootkits, Teil 1 von 3: Die wachsende Bedrohung

Inhaltsverzeichnis

Die Fakten 3

Kurzfassung 3

Eine kurze Geschichte der Stealth-Malware (Rootkits) 3

Rootkits, Malware und Kontroversen 4

Rootkit-Technologietrends 5

Quellenverzeichnis 8

Die Fakten

1. Innerhalb von gerade einmal drei Jahren hat der Einsatz von Stealth-Technologien in böswilliger Software (Malware) um mehr als 600 Prozent zugenommen.
2. In den Jahren von 2000 bis 2005 ist die Komplexität von Rootkits um mehr als 400 Prozent angestiegen, und im Jahresvergleich hat die Komplexität vom 1. Quartal 2005 bis 2006 um mehr als 900 Prozent zugenommen.
3. Der Anteil von Linux-basierten Technologien ist von einem Höchstwert von etwa 71 Prozent aller Malware-Stealth-Komponenten im Jahr 2001 auf eine vernachlässigbare Zahl im Jahr 2005 gefallen, während die Anzahl Windows®-basierter Stealth-Komponenten im selben Zeitraum um 2.300 Prozent angestiegen ist.
4. Diese zunehmende Verbreitung und Komplexität von Rootkit-Komponenten ist in erster Linie aufgrund der *Open-Source*-Umgebung sowie des Online-Teamworks in entsprechenden Sites und Blogs möglich.
5. Für Autoren von Malware stellt die Windows-Plattform ein attraktives Ziel dar – nicht nur aufgrund der überwältigenden Anzahl vorhandener Installationen, sondern auch wegen der aufregenden technischen Herausforderungen, die sie mit ihren vielen undokumentierten Programmierschnittstellen (Application Programming Interfaces, APIs) bietet.
6. Produkte, die Stealth-Technologien einsetzen, müssen nicht unbedingt selbst Rootkits sein. Sie unterstützen und begünstigen aber die Ausbreitung von Malware und tragen auf diese Weise dazu bei, dass sich Malware noch weiter verbreitet, als dies ohnehin der Fall sein würde.

Kurzfassung

Rootkits sind tief in das System eingreifende und schwer aufzuspürende Programme, die heutige Systeme bedrohen. Durch immer weiter entwickelte Stealth-Techniken wird das Aufspüren von Rootkits und das Eindämmen der Schäden, die sie anrichten, zu einer beträchtlichen Herausforderung. Im vorliegenden Dokument wird zwischen Stealth-Techniken, die einfache Strategien zum Verbergen von Dateien, Prozessen und Aktivitäten sind, und dem Begriff *Rootkit* unterschieden, der zu einem Synonym für Malware geworden ist, die ihre Aktivitäten verheimlicht. Außerdem wird ein kurzer Rückblick auf die Geschichte der Stealth- und Rootkit-Technologien geworfen, um besser verstehen zu können, wie sich diese Bedrohungen entwickelt haben. Es werden die Motivationen und Technologien analysiert, die dem zunehmenden Einsatz von Rootkits zugrunde liegen, aktuelle Trends untersucht und ein Ausblick auf die zukünftige Entwicklung dieser neuen Form von Malware gegeben.

Eine kurze Geschichte der Stealth-Malware (Rootkits)

Ursprünglich verstand man unter einem Rootkit einfach nur eine Sammlung von Tools, mit denen man auf Administrator-Ebene auf einen Computer oder ein Netzwerk zugreifen kann (was in der UNIX-Welt als "root"-Zugriff bezeichnet wird). Der Begriff bezog sich auf einen Satz neu kompilierter Unix-Tools wie etwa *ps*, *netstat*, *ls*, und *passwd*. Da diese Tools von einem Angreifer dazu verwendet werden konnten, die Spuren seines Eindringens zu verwischen, wurden Rootkits mit dem Begriff *Stealth* verknüpft. Als dieselben Strategien in Windows-Umgebungen Anwendung fanden, wurde dieser Begriff mit übernommen. Heutzutage dient der Begriff *Rootkit* meist als Beschreibung für Malware (wie Trojaner, Würmer und Viren), die ihre Präsenz und ihre Aktionen aktiv vor Benutzern und anderen Systemprozessen verbirgt.

Die Vorgehensweise, Malware vor den aufmerksamen Augen der Benutzer und vor Sicherheitsprodukten zu verstecken, geht zurück auf den allerersten PC-Virus – *Brain*[1] – der 1986 auftauchte. *Brain* entzog sich der Entdeckung, indem er Bootsektorabfragen bei PCs abfing und die Lesevorgänge an andere Stellen auf dem Datenträger umleitete. Virenautoren erkannten bald, dass die Lebensdauer eines Virus vor allem von Stealth-Techniken abhing: Der 1987 aufgetretene *Lehigh*-Virus[2] konnte kurz nach seiner Freisetzung eingedämmt werden, da er keinerlei Versuche unternahm, sich zu verbergen.

Von Ende der 1980er bis Anfang der 1990er Jahre entwickelten die Autoren von Malware immer komplexere DOS-Viren, indem sie ihren Viren innovative Stealth-Techniken zum Schutz vor Aufdeckung hinzufügten. Zu den beiden am häufigsten verwendeten Methoden gehörte es, Aufrufe von BIOS-E/A-Interrupts für Datenträger-Lesevorgänge (INT 13) abzufangen und mit manipulierten Ergebnissen zu ersetzen, und stets bei jedem Start eines Programms (einschließlich eines Antivirenscanners) Datenträgersektoren zu desinfizieren, die dann nach Abschluss des Programms wieder erneut infiziert wurden. Der Bootsektorvirus *Tequila*[3] (1991) und der Dateivirus *1689 Stealth*[4] (1993) setzten diese Techniken ein, um erhöhte Dateilängen zu verbergen, was andernfalls ein sicheres Anzeichen für eine Infektion gewesen wäre. Spätere DOS-Viren fingen Funktionen auf höherer Ebene ab (wie DOS-Treiberaufrufe), um ihre Präsenz zu verbergen oder die Infektion aufrechtzuerhalten.

Mitte der 1990er Jahre brachte das Aufkommen von Windows, das gegen DOS-Viren immun war, eine kurze Pause bei der Innovation von Stealth-Technologien. Die Virenautoren mussten erst einmal lernen, mit den Windows-APIs und der geschützten Speicherarchitektur umzugehen, bevor sie neue Wege ersinnen konnten, deren Verteidigung zu umgehen. Mit dem Auftauchen der Trojaner *NTRootkit*[5] Ende 2001 und später *HackerDefender*[6] (2003) endete die "Kampfpause" an der

Stealth-Front. Diese Trojaner griffen auf einer sehr grundlegenden Ebene auf das Betriebssystem zu und verdeckten auf diese Weise ihre Anwesenheit.

Ebenso wie die Computerumgebungen weiterentwickelt wurden, haben auch die Stealth-Technologien mit Schritt gehalten. Irreführende Benennungen, Netzwerkmanipulation und andere Techniken wurden entwickelt, damit sich Malware nicht einfach erkennen lässt. Eine der einfachsten und dennoch wirksamsten Methoden besteht darin, eine infizierte Datei umzubenennen, so dass sie wie eine zulässige System- oder Benutzerdatei aussieht. So könnte sich der Trojaner *scvhost.exe* oder *svehost.exe* neben der echten Datei *svchost.exe* im Windows-Verzeichnis *system32* befinden. Außerdem kann ein Trojaner namens *svchost.exe* aus dem *Windows*- bzw. *WINNT*-Verzeichnis ausgeführt werden. Im ersten Fall ist es die enge Ähnlichkeit mit der echten Datei, während es im zweiten Fall die Unkenntnis seitens der Benutzer ist, dass sich die echte Datei eigentlich im Windows-Verzeichnis *system32* befinden sollte, was Benutzer dazu verleitet, den Trojanerdateien zu vertrauen.

Mit dem Aufkommen des Internet ergaben sich dann sowohl für die Angreifer als auch für die Verteidiger neue Gelegenheiten und Möglichkeiten. Für Autoren von Malware hielt es neue Verbreitungswege und Massen potenzieller Opfer bereit. Systemverteidiger erhielten neue Hilfsmittel in Form von Echtzeit-Netzwerkerkennung mit IPS-Lösungen (Intrusion Prevention System, Systeme zum Schutz vor Eindringlingen) und andere Geräte zur Überwachung des Netzwerkverkehrs auf verräterische Anzeichen von bösartigen Aktivitäten.

Eine wirksame Stealth-Technologie muss heutzutage Dateien, Prozesse und Registrierungseinträge verstecken oder schützen. Malware muss seine Spuren in zunehmendem Maße durch Manipulieren von Datenpaketen im Netzwerk, TCP/IP-Stack, TCP/IP-Protokoll[7] und BIOS[23] verbergen, um den fortgeschritteneren Sicherheitstechnologien zu entgehen.

Rootkits, Malware und Kontroversen

Malware existiert in vielen Formen. Man unterschiedet jedoch explizit zwischen Viren, Trojanern, Würmern und potenziell unerwünschten Programmen (Potentially Unwanted Programs, PUPs). Viren sind (wie ihre biologischen Gegenstücke) sich selbst replizierende Programme, die auch vertrauliche Informationen stehlen, Systemressourcen blockieren, Informationen zerstören oder andere bösartige Aktionen durchführen können. Trojaner sind Programme, die wie gutartige oder sogar nützliche Softwareanwendungen aussehen, aber bösartigen Code enthalten. Auch wenn sich Trojaner nicht selbst replizieren, können sie doch einen infizierten Computer andere Malware herunterladen lassen, die dies kann. Würmer sind Malware, die sich repliziert, indem sie über freigegebene Netzwerke, Diskettenlaufwerke oder sogar USB-Laufwerk Kopien von sich selbst verbreiten – meist autonom ohne Mitwirkung des Benutzers. PUPs wiederum ähneln zwar den Trojanern und anderer Malware in dem Punkt, dass sie oftmals vertrauliche und private Informationen stehlen. Der Unterschied besteht jedoch darin, dass sie mit dem stillschweigenden Einverständnis des Benutzers installiert und ausgeführt werden.

Stealth-Technologie ist dabei nicht der einzige Einsatzbereich von Malware. PUPs und kommerzielle Softwareanwendungen setzen zunehmend Stealth-Technologien ein, um zu verhindern, dass sie entfernt werden. Im April 2005 wurde mit *Adware-Isearch*[9] eine der ersten Adware-Anwendungen gefunden, die Stealth-Technologie einsetzte. Seitdem wurden verschiedene weitere gefunden, wie *Apropos*[10], *Qoolaid*[11] und *DigitalNames*[12], die alle als Trojaner neu eingestuft wurden, da sie für den Benutzer eine beträchtliche Bedrohung darstellen.

Man darf jedoch nicht der Versuchung erliegen, jede Software mit Stealth-Technologie als Rootkit einzustufen, denn dies würde die Genauigkeit und Aussagekraft des Begriffes verwässern. McAfee® und andere haben diese Position übernommen und stufen kommerzielle Software, die Stealth Technologien einsetzen, nur als PUPs und nicht als Rootkit ein. Allerdings wird in der Sicherheits-Community von anderer Seite eingewendet, dass jeglicher Einsatz von Stealth-Technologien unerwünscht ist und somit den Begriff *Rootkit* in seiner negativen Bedeutung verdient hat.[13,14,15] Diese etwas akademische Debatte gipfelte in einer öffentlich viel beachteten Diskussion, als Mark Russinovich am 31. Oktober 2005[28] in seinem Blog enthüllte, dass die DRM-Software (Digital Rights Management, Digitale Rechteverwaltung) *Extended Copy Protection* (*XCP*) von Sony BMG unter Beschuss geraten ist, weil in ihr Stealth-Technologien eingesetzt werden, die Computer anfällig für Angriffe machen. Ende 2005 erkannte das McAfee AVERT™-Labor, dass sich diese kommerzielle Anwendung für bösartige Zwecke verwenden lässt, und kennzeichnete das Programm fortan als PUP.

XCP besitzt eine Gerätetreiberimplementierung, die Kernel-Berechtigungen umfasst. Dieser Treiber versteckt DRM-Dateien und -Prozesse, so dass der Benutzer sie nicht deaktivieren und illegale Kopien von Musikdateien anfertigen kann. Um diesen Schutz zu erzielen, wurde Kernel-Code geschrieben, der jede Datei, jeden Ordner und jeden Prozess versteckt, der mit der Zeichenfolge *sys* beginnt. Allerdings würde dies auch jede andere Malware, die mit derselben Zeichenfolge ähnlich benannt ist, vor den meisten Antivirenscannern verbergen.

Wie zu erwarten war, haben Autoren von Malware diese Gelegenheit beim Schopfe gepackt und Programme geschrieben, die die Sony-Software zum Verbergen ihrer Dateien nutzen. Dazu gehören beispielsweise Varianten des Wurms *W32/Brepibot*[17], der im November 2005 gemeldet wurde und sich über IRC-Kanäle (Internet Relay Chat) verbreitet.

Diese kommerzielle Anwendung wirft die Frage auf, welchen Nutzen es bringt, alle Programme als Rootkits zu kennzeichnen, die Stealth-Technologien einsetzen. Wenn Stealth zu einer gängigen Softwarepraxis wird, wäre es vielleicht besser, den Begriff *Rootkits* nur für Malware zu reservieren, die Stealth-Technologien einsetzt. McAfee und andere haben diese Position übernommen und stufen *XCP* deshalb nur als PUP und nicht als Rootkit ein.[18]

Die Kontroverse um Stealth-Techniken dauert derzeit noch an. Am 10. Januar 2006, weniger als zwei Monate nach der Aufdeckung von *XCP*, wurde die Antiviren-Community von der Enthüllung erschüttert, dass Symantec in einem seiner Produkte Stealth-Technologien zum Verstecken eines Verzeichnisses mit dem Namen *NProtect*[19] verwendet hat. Auch wenn dieses Sicherheitsrisiko geringer als bei *XCP* war, verbirgt *NProtect* doch Dateien in einem versteckten Verzeichnis vor Antivirenscans. Autoren von Malware könnten dies theoretisch zum Schutz ihrer Dateien nutzen, indem sie die Dateien in diesem *NProtect*-Verzeichnis unterbringen. Symantec verteidigt den Einsatz von Stealth-Technologien als ein wichtiges Werkzeug im Kampf gegen Malware, während viele Mitglieder der Community dem Unternehmen vorwerfen, dieselben Techniken zu übernehmen und zu legitimieren, die von deren Gegenspielern verteilt und gefördert werden.

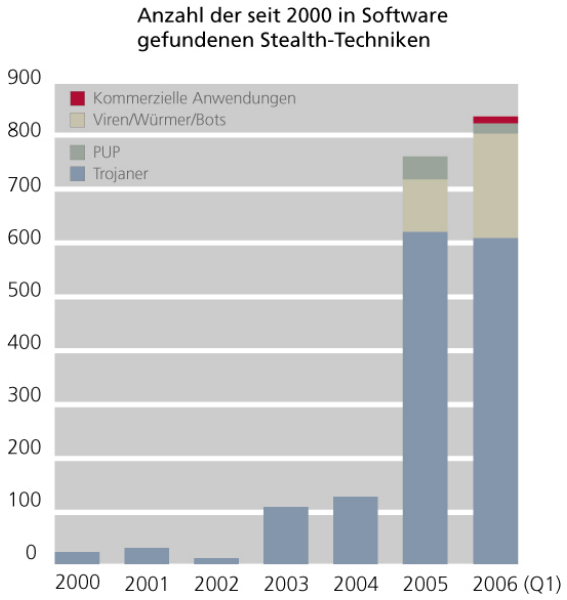
Die Enthüllung, dass das Kaspersky Anti-Virus (KAV)-Modul[24] iStreams-Technologie einsetzt, hat den Streit um Stealth-Techniken in kommerzieller Software weiter fortgeführt. Die iStreams-Technologie verbessert die Leistung des KAV-Scanmoduls, indem die Prüfsumme von Dateien gespeichert wird, die bereits in NTFS-ADS (Alternative Datenströme) gescannt wurden. Von Kaspersky wurde behauptet, dass durch das Speichern der NTFS-Streams keinerlei Bedrohung entsteht, da es interne Daten des Programms sind und somit selbst dann wiederhergestellt werden, wenn sie von bösartigem Code oder Daten überschrieben werden.[20] Auch wenn diese Technik zum Verstecken von Daten keine Gefahr darstellte, wurde sie in den Medien ebenfalls missbilligt.

Rootkit-Technologietrends

In diesem Abschnitt werden die Hintergründe der zunehmenden Einführung von Rootkits und deren Vielfalt, die Motivation der Autoren von Rootkits sowie die Technologietrends diskutiert, die die Zukunft der Rootkits bilden.

Trend 1: Rootkits verbreiten sich über Trojaner hinaus zu anderen Formen von Malware und PUPs

In den vergangenen drei Jahren hat sich die Häufigkeit von Stealth-Technologie in Malware, PUPs und kommerziellen Anwendungen mehr als versechsfacht. Wie im Diagramm 1 dargestellt, war der Einsatz von Stealth-Technologien 2005 nicht mehr ausschließlich auf Trojaner beschränkt, sondern tauchte auch in anderen Formen von Malware sowie in PUPs und kommerziellen Anwendungen auf.



Quelle: McAfee AVERT-Labor

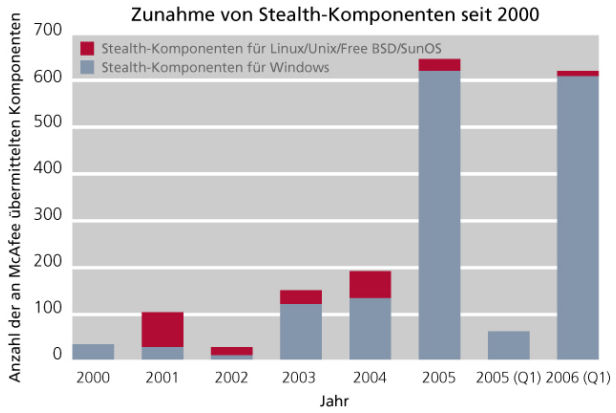
Diagramm 1: Die zunehmende Verbreitung von Stealth-Techniken in Software

Als Ursache für den rasanten Anstieg von Stealth-Technologien ließe sich die Zusammenarbeit im Internet bei den entsprechenden Forschungen auf diesem Gebiet nennen. Websites wie *www.rootkit.com* enthalten hunderte Zeilen von Rootkit-Code, der neu kompiliert und optimiert werden kann, sowie ausführbare Rootkit-Binärdateien. Verschiedene im Umlauf befindliche Rootkits stammen direkt von Stealth-Technologien von diesen Websites ab. Einige Beispiele dafür wären *AFXrootkit*, *NTRootkit*, *FURootkit*, *He4Hook* und *PWS-Progent*. Noch schlimmer ist, dass es auf diesen Websites auch Blog-Einträge gibt, in denen dem Leser sogar gezeigt wird, wie sich eine Erkennung durch Antivirenscans umgehen lässt. Da steht dann geschrieben: "Leute, das ist jetzt zwar nicht sehr kreativ, aber ihr könnt doch kompilieren, stimmt's? Gut, das soll heißen, dass Antivirenscanner nach exakt dieser Datei suchen. Und wenn man nun hier oder dort eine kleine Änderung vornimmt, könnte es passieren, dass diese Datei möglicherweise beim Scannen durch die Masche schlüpft. Zumindest für eine Weile."[13]

Trend 2: Rootkits werden immer komplexer

Die Zusammenarbeit im Internet geht aber über die einfache Verbreitung von Stealth-Technologien hinaus. Sie fördert auch die Entwicklung neuer, weiter entwickelter Stealth-Technologien. Ein Maß für die Komplexität ist die Anzahl der Komponentendateien in einem Softwarepaket. Wenn beispielsweise ein Rootkit-Paket mit dem Namen *a.exe* die Dateien *b.exe*, *c.dll* und *d.sys* installiert, wobei *d.sys* die Stealth-Komponente des Rootkits installiert, wird die Gesamtanzahl

der Komponenten als vier gezählt. An dieser Stelle wird davon ausgegangen, dass *d.sys* andere Dateien im Paket versteckt oder schützt. Das Diagramm 2 zeigt die zunehmende Komplexität von Rootkits in den letzten sechs Jahren. Im Jahr 2005 ist die Komplexität bei bekannten Rootkits um fast 200 angestiegen. Im Vergleich dazu wurden in den ersten drei Monaten von 2005 nur 60 Stealth-Komponenten an McAfee AVERT übermittelt. Diese Anzahl schnellte in den ersten drei Monaten von 2006 auf 612 Komponenten an – ein Anstieg von über 900 Prozent. Während die Anzahl der eingereichten Proben ebenfalls zunahm, ist für diesen Anstieg hauptsächlich die fortschreitende Weiterentwicklung der Rootkit-Technologie verantwortlich.



Quelle: McAfee AVERT-Labor

Diagramm 2: Verteilung von Stealth-Technologien nach Softwareplattformen

Trend 3: Rootkits konzentrieren sich zunehmend auf die Windows-Plattform

Die meisten derzeit beobachteten Rootkit-Aktivitäten sind auf die Windows-Plattform gerichtet. Nach einem Höchststand von beinahe 70 Prozent im Jahr 2001 sind Linux-basierte Stealth-Aktivitäten heute vernachlässigbar. Auch wenn man davon ausgehen darf, dass Linux-basierte Rootkits überleben werden, gehört die absehbare Zukunft doch ganz klar den Windows-basierten Rootkits. Dies liegt vor allem an der massenhaften Verbreitung von Windows mit seinen vielen undokumentierten APIs, die für jeden Rootkit-Autor eine technische Herausforderung darstellen.

Das Diagramm 3 zeigt den Anstieg der "reinen" Rootkits in Windows[F1] und den Trend zu deren Einbettung in anderen Malware-Kategorien. *NTRootkit* wurde zuerst 2001 beobachtet und war mit seinen Varianten bis 2005 verbreitet. Die Rootkits *HackerDefender*, *AFXRootkit* und *PWS-Progent* tauchten zuerst 2003 auf. Bei *HackerDefender* wurde in den letzten Jahren ein starker Anstieg verzeichnet, während Varianten von *AFXRootkit* und *PWS-Progent* erst gegen Ende 2005 entdeckt wurden. Unter den derzeit am meisten verbreiteten Rootkits sind relativ fortgeschrittene Rootkits wie *FURootkit*. In den letzten Monaten wurden auch Stealth-Technologien gefunden, die mit verschiedenen Formen von Malware eingebettet sind. Dazu gehören *Backdoor-CEB*, *AdClicker-BA*, *W32/Feebs*, *Backdoor-CTV*, *Qoolaid*, *PWS-LDPinch*, *Opanki.worm* und *W32/Sdbot.worm*.

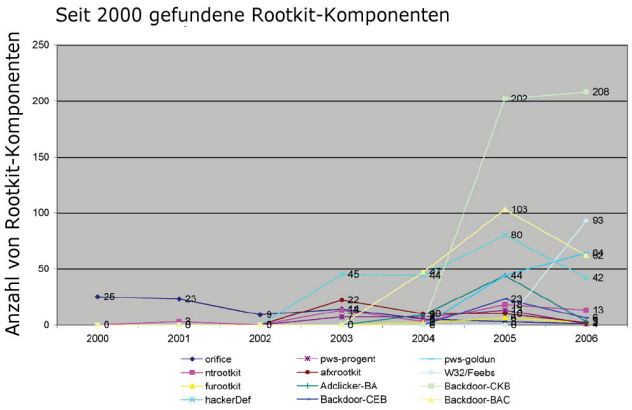


Diagramm 3: Zunahme der Anzahl von Komponenten in Rootkits

Trend 4: Angriffsvektoren für Rootkits sind sowohl in unseriöser als auch in seriöser Software vorhanden

Dank ihrer Vielseitigkeit haben Stealth-Technologien Eingang in beinahe jeden bekannten Angriffsvektor für Malware gefunden. Ihre Beliebtheit hat sogar kommerzielle Softwareanbieter davon überzeugt, sie in ihren Produkten einzusetzen. Wie in Abbildung 1 gezeigt wird, erstrecken sich die Eintrittsvektoren von Stealth-Technologien derzeit von Softwarezustellungsmethoden über Exploits, die Benutzereingriffe überflüssig machen, bis hin zu benutzerinstallierten, vertrauenswürdigen Anwendungen. Dieses breite Spektrum soll hier anhand einiger bekannter Rootkits und deren Angriffsvektoren veranschaulicht werden. *Backdoor-BAC* wurde über Spam-E-Mails, trojanische Downloader und direkte Exploits verbreitet.[22] *HackerDefender*[6] wird meist über Spam, Bots, direkte Exploits und Peer-to-Peer-Filesharing-Anwendungen verbreitet. Einige beobachtete Rootkits werden über Massen-Mailing-Würmer heruntergeladen, um komplexe, kombinierte Angriffe durchzuführen. Dies war bei *Backdoor-CEB*[16] der Fall, das von *W32/MyDoom.bb*[29], *W32/MyDoom.bc*[30] und *W32/MyDoom.d*[31] heruntergeladen wurde. *FURootkit*[32,33] wurde wohl aufgrund seiner hochkomplexen Struktur und leichten Bereitstellung von Bots wie *SDbot*[34] und *Opanki*[35] bevorzugt. *W32/Feebs*[36] war eines der ersten Rootkits, bei denen eine Verbreitung über E-Mail-Anhänge und Peer-to-Peer-Netzwerke beobachtet wurde.

[F1] "Reinform" steht für Proof-of-Concept-Rootkits (darunter *Ntrootkit* und *FURootkit*) mit innovativen Rootkit-Techniken.

Kombinierte Software, die Adware verbreitet, ist eine weitere häufige Quelle von Stealth-Technologien (meist in Form von PUPs). Ein Beispiel dazu wurde unter dem Namen *build2.exe* an McAfee übermittelt und als *Adware-Isearch*[9] erkannt. Es kombinierte ein Desktopsuchprogramm zusammen mit einem Firefox-Plug-In und erstellte Symbole, die für das Anti-Spyware-Programm spywareavenger (*www.spywareavenger.com*) und das Antivirenprogramm VirusHunter (*www.virushunter.com*) warben. Das Paket enthielt jedoch auch ein Adware-Programm namens *aBetterIntrnt*, von dem ein Dienstprogramm heruntergeladen wurde. Dieses Dienstprogramm hat dann einige weitere Adware-Programme auf dem Computer installiert. Abschließend hat *Adware-Isearch* dann ein Kernel-Mode-Rootkit aktiviert, um zu verhindern, dass die neu installierten Dateien von einem Benutzer, einem Antivirenscanner oder einem Anti-Spyware-Scanner entfernt werden konnten.[21]

In jüngster Zeit werden Stealth-Technologien über kommerzielle Software verbreitet – d. h. über vertrauenswürdige Programme – wie man am Beispiel von *XCP*[18] sehen konnte. Die meisten Benutzer hatten unbemerkt die Installation der *XCP*-Stealth-Technologie auf ihre Systeme zugelassen, da sie der Anwendung vertrauten und die kopiergeschützte Musik auf Sony-CDs abspielen wollten. Auf diese Weise haben sie jedoch gleichzeitig ernsthafte Sicherheitslücken geschaffen.

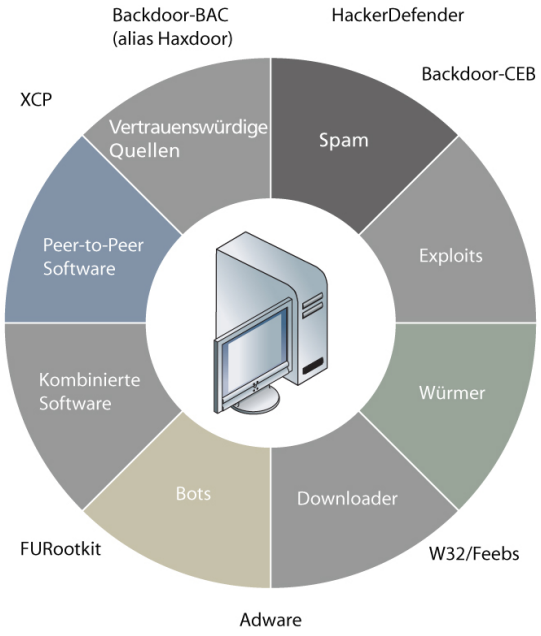


Abbildung 1: Vielfalt der Angriffsvektoren – Kanäle, über die sich Rootkits verbreiten

Trend 5: Das Einbetten von Stealth-Technologie wird einfacher

Die Verfügbarkeit von Rootkit-Code- und Stealth-Bausätzen macht es den Autoren von Malware leicht, Prozesse, Dateien und Registrierungen zu verstecken, ohne dabei detaillierte Kenntnisse über das Zielbetriebssystem besitzen zu müssen. Wie einfach dies ist, zeigt die Abbildung 2: Die Benutzeroberfläche des Stealth-Bausatzes *Nuclear Rootkit* benötigt nur den Namen einer Datei oder eines Verzeichnisses, und mit einem Mausklick wird ein benutzerdefinierter Binärcode erstellt, der mithilfe verschiedener Stealth-Technologien die Datei bzw. das Verzeichnis sowie Ports, Prozesse und Registrierungseinträge versteckt.

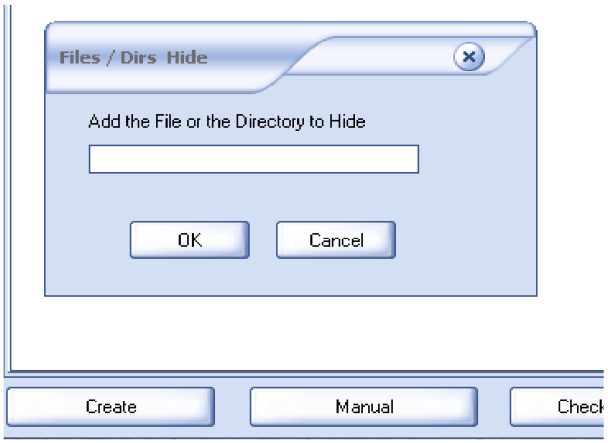


Abbildung 2: Die simple Benutzeroberfläche von Nuclear Rootkit

Obwohl der oben erwähnte Stealth-Bausatz kostenlos zum Download zur Verfügung steht, kann man hochkomplexe und benutzerdefinierte Stealth-Bausätze auch käuflich erwerben, wie zum Beispiel *A-311 Death* und die Gold Edition von *HackerDefender*. Die Preise reichen dabei von ca. 200 bis 2.000 US-Dollar. Was sich damit anrichten lässt, hat das erfolgreiche Phishing von *Backdoor-BAC* (alias *Haxdoor und A-311 Death*) eindrucksvoll demonstriert. Der Trojaner war in der Lage, für seinen Autor tausende PINs (Personal Identification Numbers), Kennwörter und andere vertrauliche Informationen zu sammeln.[22]

Angesichts der relativ geringen Startkosten und der Aussicht auf finanzielle Gewinne entwickeln Hacker und Autoren von Malware weiterhin neue Rootkits, die das Aufspüren durch Antivirenscanner und andere Sicherheitsprodukte unterbinden. Die Online-Kooperation dieser Straftäter über das Internet stellt für die Sicherheits-Community eine beträchtliche Herausforderung dar, da sich deren bösartige Programme mit der fortschreitenden Perfektionierung von Malware immer schwieriger verhindern, erkennen und entfernen lassen.

Ausblick

Im Jahr 2004 verzeichnete McAfee annähernd 15.000 Trojaner, von denen jedoch nur 0,87 Prozent Windows-Rootkits waren. 2005 registrierte McAfee etwa 30.000 Trojaner, wobei die Rootkits diesmal jedoch einen viel größeren Anteil belegten

(rund zwei Prozent) – was einem nominalen Wachstum von fast 400 Prozent entspricht. Bei allen in Malware und PUPs enthaltenen Rootkit-Komponenten hat McAfee im ersten Quartal 2006 eine Zunahme von 900 Prozent im Vergleich zum Vorjahr verzeichnet.

Auch wenn demnächst eine neue Version von Windows (Vista) erwartet wird, darf ein damit einhergehender Rückgang an Malware-Aktivitäten (vergleichbar mit der "Kampfpause" bei der letzten Veröffentlichung von Windows 95) erst dann erwartet werden, wenn die neue Version eine weite Verbreitung gefunden hat. Somit kann angesichts der leichten Bereitstellung und zunehmenden Popularität von Rootkits unter Malware-Autoren vorausgesagt werden, dass Rootkits für die aktuelle Windows-Architektur in den nächsten zwei bis drei Jahren jährlich um mindestens 650 Prozent zunehmen werden und dass wahrscheinlich neue und noch weiter entwickelte Techniken eingesetzt werden. Im nächsten Dokument, "Rootkits Teil 2 von 3: Technische Grundlagen" werden die zukünftigen Stealth-Technologien detailliert analysiert und Prognosen zur Zukunft von Rootkits abgegeben. Im dritten und letzten Teil der Serie wird gezeigt, wie aktuelle und zukünftige Rootkits mit praktischen Sicherheitsstrategien bezwungen werden können.

Quellenverzeichnis

1. Brain, *http://vil.nai.com/vil/content/v_221.htm*
2. Lehigh, *http://vil.nai.com/vil/content/v_705.htm*
3. Tequila, *http://vil.nai.com/vil/content/v_98230.htm*
4. 1689 Stealth, *http://vil.nai.com/vil/content/v_98083.htm*
5. NTRootkit, *http://vil.nai.com/vil/content/v_99877.htm*
6. HackerDefender, *http://vil.nai.com/vil/content/v_100035.htm*
7. Greg Hoglund und James Butler, *Subverting the Windows Kernel: Rootkits*
8. Adware-SaveNow, *http://vil.mcafeesecurity.com/vil/content/v_100836.htm*
9. Adware-Isearch, *http://vil.nai.com/vil/content/v_133320.htm*
10. Apropos, *http://vil.nai.com/vil/content/v_137345.htm*
11. Qoolaid, *http://vil.nai.com/vil/content/v_126149.htm*
12. DigitalNames, *http://vil.nai.com/vil/content/v_135063.htm*
13. Greg Hoglund, "State of the Rootkit Address", *http://rootkit.com/blog.php?newsid=336*
14. *When's a Rootkit Not a Rootkit? In Search of Definitions, http://www.eweek.com/article2/0,1895,1913083,00.asp*
15. *Some Rootkits Are Worse Than Others, http://www.eweek.com/article2/0,1895,1910240,00.asp*
16. Backdoor-CEB, *http://vil.nai.com/vil/content/v_131340.htm*
17. W32/Brepibot, *http://vil.nai.com/vil/content/v_133091.htm*
18. XCP, *http://vil.nai.com/vil/content/v_136855.htm*
19. "Symantec Caught in Norton 'Rootkit' Flap" *http://www.eweek.com/article2/0,1895,1910077,00.asp*
20. "No Rootkit in Kaspersky Anti-Virus", *http://www.viruslist.com/en/weblog?weblogid=177727537*
21. Re: Sunbelt Software Distribution Inc. ("SunBelt"); Classification of iDownload.com's isearch Toolbar Product, *http://www.sunbelt-software.com/blog/sunbelt_idownload.pdf*
22. Backdoor-BAC.gen, *http://vil.nai.com/vil/content/v_138676.htm*
23. *Implementing and Detecting an ACPI BIOS Rootkit,* John Heasman
24. "Symantec, Kaspersky Criticized for Cloaking Software", *http://www.pcworld.com/news/article/0,aid,124365,00.asp*
25. Adclicker-BA, *http://vil.mcafeesecurity.com/vil/content/v_128301.htm*
26. AFXrootkit, *http://vil.nai.com/vil/content/v_102335.htm*
27. Adware-Elitebar, *http://vil.nai.com/vil/content/v_133782.htm*
28. Mark's Sysinternals Blog: Rootkits in Commercial Software, *http://www.sysinternals.com/blog/2006/01/rootkits-in-commercial-software.html*
29. W32/MyDoom.bb, *http://vil.nai.com/vil/content/v_131856.htm*
30. W32/MyDoom.bc, *http://vil.nai.com/vil/content/v_131860.htm*
31. W32/MyDoom.bd, *http://vil.nai.com/vil/content/v_131861.htm*
32. FURootkit, *http://vil.nai.com/vil/content/v_127131.htm*
33. FURootkit description, *http://rootkit.com/project.php?id=12*
34. SDBot, *http://vil.nai.com/vil/content/v_100454.htm*
35. Opanki.worm, *http://vil.nai.com/vil/content/v_133397.htm*
36. W32/Feebs, *http://vil.nai.com/vil/content/v_137971.htm*

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, USA, 888.847.8766, www.mcafee.com
McAfee und/oder weitere hier enthaltene Marken sind eingetragene Marken von McAfee, Inc. und/oder seinen Tochterunternehmen in den USA und/oder anderen Ländern. Die Farbe McAfee-Rot in Verbindung mit Sicherheit ist ein Merkmal der McAfee-Produkte. Alle anderen eingetragenen und nicht eingetragenen Marken in diesem Dokument sind alleiniges Eigentum ihrer jeweiligen Besitzer. © 2006 McAfee, Inc. Alle Rechte vorbehalten.

6-cor-root-001-0406