

# Das Geschäft der Kennwortdiebe: Wer ist an Identitätsdiebstahl beteiligt, und wie funktioniert er?

Dennis Elser und Micha Pekrul, McAfee® Avert® Labs

## Inhalt

|  |    |
|--|----|
| Auftreten und Verbreitungsmethoden   | 3  |
| Katz und Maus: Banksysteme entwickeln sich weiter, doch die Angreifer holen auf                                  | 5  |
| Sinowal und StealthMBR: Der derzeit hinterhältigste Kennwortdieb und das am schwierigsten zu entdeckende Rootkit | 7  |
| Die neue „Masche“ von Sinowal  | 8  |
| Eine einzige Infektion bringt das gesamte Immunsystem aus dem Gleichgewicht                                      | 10 |
| Zbot: Die nächste Keylogger-Generation   | 11 |
| Steam Stealer und der illegale Markt für Spieler-Daten   | 13 |
| Fazit: Internetkriminelle nutzen die Wirtschaftskrise aus  | 15 |
| Danksagung   | 17 |
| Informationen zu den Autoren   | 17 |

## Forschungsbericht Das Geschäft der Kennwortdiebe: Wer ist an Identitätsdiebstahl beteiligt, und wie funktioniert er?

Durch die immer stärker zunehmende Abwicklung von Einkäufen und Banktransaktionen über das Internet ist Kennwortdiebstahl zu einem typischen Verbrechen geworden. Egal welche Angriffsmethode eingesetzt wird – in vielen Fällen findet Kennwortdiebstahl-Malware ihren Weg auf den Computer des Opfers.

Die kriminellen Organisationen, die hinter der Verbreitung böswilliger Malware stecken, arbeiten häufig von Ländern wie Russland, China oder Brasilien aus. Ihr einziges Ziel besteht darin, Benutzerdaten zu ergattern und diese in Geld zu verwandeln. In Zeiten wirtschaftlicher Unsicherheit werden gestohlene Anmeldedaten sogar noch wertvoller, sodass der Schutz Ihrer Daten und Identität höchste Priorität hat.

In diesem Bericht werden aktuelle Angriffsmethoden beschrieben, die in den am weitesten entwickelten und verbreiteten Kennwortdiebstahl-Malware-Familien verwendet werden. Außerdem werden die Tricks (z. B. Bildschirmstastaturen) erklärt, mit denen die neuesten Banksicherheitsfunktionen angegriffen werden. Und schließlich werden neue Ziele für Kennwortdiebstähle analysiert – Massive Multiplayer Online Role-Playing Games (MMORPG).

### Auftreten und Verbreitungsmethoden

Zwischen 2007 und 2008 konnte McAfee Avert Labs beobachten, dass die Anzahl der Kennwortdiebstahl-Malware-Varianten um fast 400 Prozent anstieg.

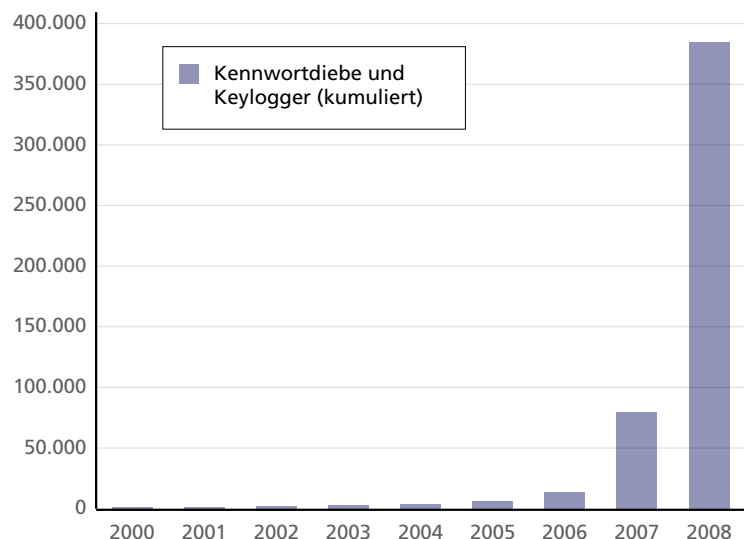


Abbildung 1: Zunahme der Kennwortdiebstahl-Malware. (Quelle für alle Grafiken (sofern nichts anderes angegeben): McAfee Avert Labs)

Nachdem Infektionen mit Kennwortdiebstahl-Malware, die speziell auf Spiele abzielen, zunächst eher selten auftraten, stiegen die Infektionen in den Jahren 2006 und 2007 auch in dieser Unterkategorie.<sup>1</sup> In dieser Zeit schossen Untergrundfirmen aus dem Boden, die den Handel mit virtuellen Spieleobjekten wie Schwertern, Helmen und Erfahrungspunkten betreiben. Diese virtuellen Objekte werden in echtes Geld umgewandelt, indem sie an andere Spieler verkauft werden, die ihre Charaktere verbessern wollen, ohne dazu endlose Stunden im Spiel zu verbringen. Die Spieler, die diese Objekte erspielen, werden als „Goldfarmer“ bezeichnet. In einigen Ländern (z. B. China) bestreiten Tausende auf diese Weise ihren Lebensunterhalt: Sie erspielen so viele virtuelle Werte wie möglich und verkaufen diese anschließend an wohlhabendere Spieler aus aller Welt.

1. Dr. Muttik, Igor: „Securing Virtual Worlds Against Real Attacks–The challenges of online game development“ (Absichern virtueller Welten vor echten Angriffen – Die Herausforderungen bei der Entwicklung von Online-Spielen). McAfee Avert Labs. [www.mcafee.com/us/local\\_content/white\\_papers/threat\\_center/wp\\_online\\_gaming.pdf](http://www.mcafee.com/us/local_content/white_papers/threat_center/wp_online_gaming.pdf)

**Forschungsbericht** Das Geschäft der Kennwortdiebe:  
Wer ist an Identitätsdiebstahl beteiligt, und wie funktioniert er?

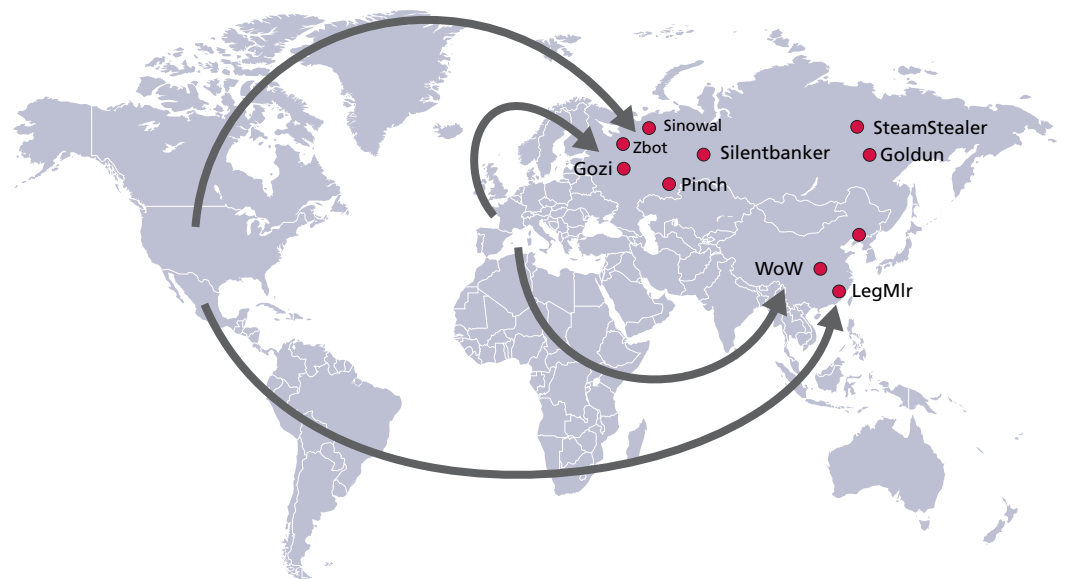


Abbildung 2: Zielländer, in die Malware derzeit gestohlene Identitäten überträgt; nach Malware-Familie.

Benutzer werden auf verschiedene Weise mit Datendiebstahl konfrontiert. Dabei handelt es sich nicht immer um Malware. Eine Form von virtuellem Diebstahl ist Phishing. Hierbei werden die gleichen Ziele verfolgt (die Anmeldedaten des Opfers), jedoch ohne Verwendung von böswilligem Code. Stattdessen setzt diese Angriffsform ausschließlich auf Social-Engineering-Techniken, um den ahnungslosen Benutzer dazu zu bringen, seine Kennwörter herauszurücken. Die gefälschten Webseiten, die für die Phishing-Angriffe verwendet werden, sehen oft täuschend echt aus.

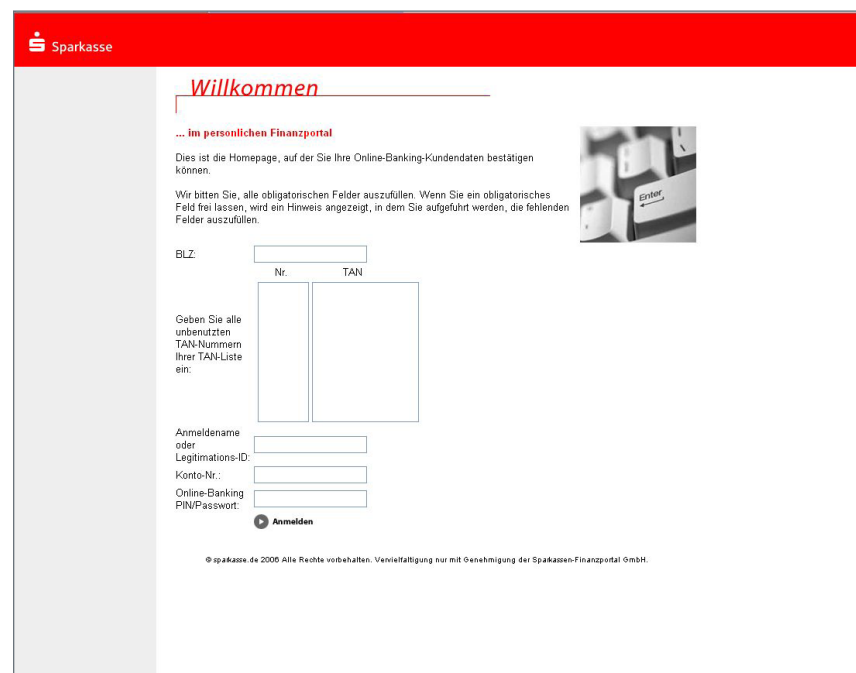


Abbildung 3: Diese Phishing-Webseite fordert den Benutzer auf, alle noch nicht verwendeten TANs und den Index einzugeben. Dadurch können Angreifer auch die fortschrittlicheren iTAN-Systeme austricksen.

Spam ist eine der häufigsten Methoden zur Verbreitung von Kennwortdieben. Durch Massen-Mailings wie gefälschte Rechnungen oder UPS-Benachrichtigungen werden Benutzer dazu verleitet, angeblich legitime PDF-Anlagen zu öffnen. Dabei handelt es sich jedoch um ausführbare Dateien, die ihre Systeme kompromittieren. Die Betreffszeilen der Spam-E-Mail sind meist auf die Zielgruppe abgestimmt und beziehen sich dabei auf Trends, politische Nachrichten oder landesspezifische Themen.

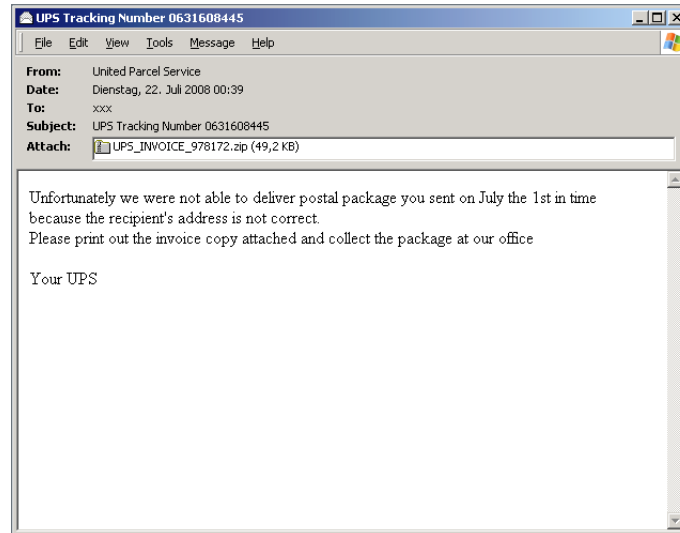


Abbildung 4: Eine typische Spam-E-Mail, die die Zbot-Malware verbreitet.

Neben Phishing, Spam und anderen verbreiteten Social-Engineering-Tricks wird eine weitere Methode zur Infizierung von Benutzer-PCs zunehmend beliebt und effizient: Browserbasierte Angriffe.<sup>2</sup> Angreifer hacken automatisiert Tausende von legitimen und vertrauenswürdigen Webseiten und missbrauchen sie, um mithilfe von „Drive-by-Infektionen“ böswilligen Code zu verbreiten. Hacker stützen sich auf Suchmaschinen, um potenziell anfällige Webseiten zu finden. Meist wird ein Skript oder ein iframe-Element injiziert, um das Opfer auf den böswilligen Code zu verweisen, der entweder auf dem Home-Server des Angreifers oder direkt auf der kompromittierten Webseite gehostet wird. Benutzer, die diese kompromittierten Webseiten besuchen, fordern unwissentlich böswilligen Code an und führen ihn aus.

### **Katz und Maus: Banksysteme entwickeln sich weiter, doch die Angreifer holen auf**

Die Evolution der Kennwortdiebstahl-Malware ist eng mit den Fortschritten bei digitalen Sicherheitsgeräten und -maßnahmen verbunden. Einfache Authentifizierungsfaktoren, die lediglich auf einer Kombination von Benutzername und Kennwort basieren, werden recht schnell durch einfach Keylogger außer Kraft gesetzt. Sobald die Sicherheitsmaßnahmen verbessert werden (z. B. durch Hinzufügen „externer“ Authentifizierungsmethoden), sind Keylogger nicht mehr erfolgreich. Ein „einprägsames Wort“ könnte ein solcher zusätzlicher Faktor sein. Online-Banking-Systeme fordern den Benutzer auf, nur Teile eines zuvor festgelegten Wortes anzugeben. Dieses Wort kann ein Keylogger-Trojaner schon prinzipbedingt nicht komplett erkennen. Heute sehen sich Angreifer Systemen gegenüber, die durch mehrere Authentifizierungssysteme geschützt werden. Zur Mehrfachfaktor-Authentifizierung werden in Europa häufig TANs (Transaction Authentication Numbers) eingesetzt. Diese werden von der Bank bereitgestellt. Dabei handelt es sich um eine lange Liste einmalig verwendbarer Kennwörter, wobei der Benutzer bei jeder Transaktion eine TAN zur Authentifizierung auswählen muss. Der nächste Schritt zur verbesserten Sicherheit stellen indizierte TANs (iTANs) dar – eine TAN mit zugehöriger Indexnummer. Das Online-Banking-System gibt für jede Transaktion einen zufällig gewählten Index vor (der zu einer bestimmten TAN gehört).



Abbildung 5: Token für einmalig verwendbare Kennwörter von Blizzard. (Quelle: Blizzard Entertainment)

2. Alme, Christoph: „Web-Browser: Eine neue Plattform wird angegriffen“, McAfee Avert Labs. [www.mcafee.com/us/local\\_content/white\\_papers/wp\\_webw\\_browsers\\_w\\_de.pdf](http://www.mcafee.com/us/local_content/white_papers/wp_webw_browsers_w_de.pdf)

**Forschungsbericht** Das Geschäft der Kennwortdiebe:  
Wer ist an Identitätsdiebstahl beteiligt, und wie funktioniert er?

Andere starke oder Mehrfachfaktor-Authentifizierungssysteme verwenden Verschlüsselungsgeräte, die ein einmalig verwendbares Kennwort generieren, das nur eine Minute lang gilt. Diese Sicherheits-Token werden häufig in Unternehmensnetzwerken eingesetzt. Auch Blizzard, der Hersteller des beliebten Online-Spiels *World of Warcraft*, hat Sicherheits-Tokens zur Authentifizierung eingeführt.<sup>3</sup> Moderne Sicherheitssysteme setzen Geräte zur TAN-Generierung ein, für die zusätzlich die Bankkarte des Kunden sowie der erfolgreiche Abschluss eines Frage-Antwort-Prozesses erforderlich sind.

Für jedes neue Hindernis gibt es auch bei den Kennwortdieben ein Gegenstück. So führten Banken beispielsweise virtuelle Tastaturen ein, bei denen der Benutzer auf entsprechende Ziffern klickte, statt sie einzugeben. Die Malware-Autoren reagierten darauf mit Bildschirmaufzeichnungsfunktionen. Eine weitere verbreitete Methode ist die Web-Injektion. Hierbei fügt die Malware den Webseiten der Bank weitere Formularfelder für zusätzliche Daten wie PIN-Nummern, ein vollständiges „einprägsames Wort“ oder andere personenbezogene Informationen hinzu. Diese „injizierten“ Elemente sind für den Benutzer nur sehr schwer zu erkennen, da sie legitim aussehen und keinen Verdacht erregen.

Es ist wenig überraschend, dass Malware-Autoren nicht nur versuchen, auf dem aktuellen Stand zu bleiben, sondern sogar einen Schritt voraus zu sein. Um die Kennwörterfassungsformulare nicht an die Sicherheitsmaßnahmen und das Layout der Zielbank-Webseite anpassen zu müssen, leiten die Angreifer die DNS-Server oder Hostdateien so um, dass sie auf ihre eigenen Server verweisen. Ein infizierter Benutzer, der eine Verbindung zur Webseite der Bank of America herstellen möchte, würde zu einer genauso aussehenden Webseite geleitet, die auf einem anderen Server gehostet wird und – natürlich – den Angreifern gehört. Eine andere Form beinhaltet DNS-Hijacking, bei dem der Angreifer remote als „Man in the Middle“ auftritt: Der Angreifer hört den Netzwerkverkehr ab und leitet dann den (geänderten) Datenverkehr an das tatsächliche Ziel weiter und umgekehrt.

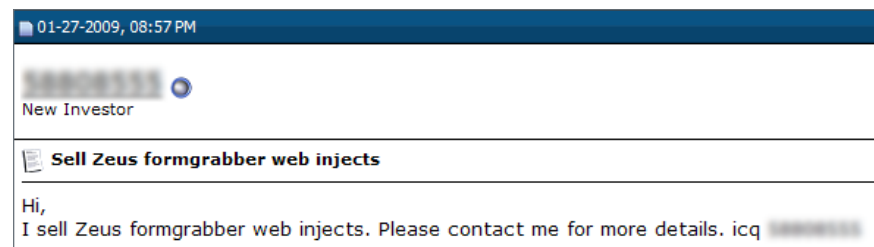


Abbildung 6: „Web-Injektionen“, die auf das angepasste Layout der Zielwebseite zugeschnitten sind, werden auf dem Untergrundmarkt für Malware verkauft.

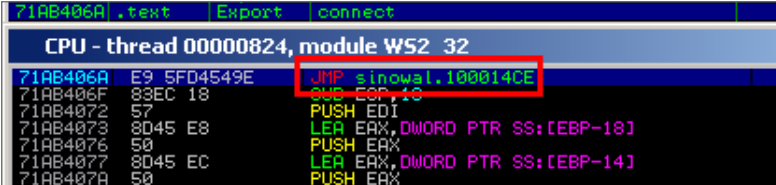
Hijacking-Angriffe, die lokal durchgeführt werden, sind nicht auf bestimmte Protokolle wie DNS angewiesen. Bei Verwendung nicht vorhersehbarer TANs wartet die Malware auf infizierten Systemen stattdessen darauf, dass der Benutzer die gesuchten Anmeldedaten eingibt. Und da es sich hier um einmal verwendbare Kennwörter handelt, wird die TAN von der Malware abgefangen und gespeichert, und dem Benutzer wird eine gefälschte Fehlermeldung über die angeblich falsche TAN angezeigt. Dies erfolgt auf passivem Wege, indem die aufgebauten Verbindungen abgehört und die Authentifizierungsnummer mit Datenmüll überschrieben wird, oder auf aktivem Wege, indem dem Benutzer eine selbst erstellte gefälschte Pop-Up-Meldung angezeigt wird.

Wir gehen in diesem Whitepaper noch an anderer Stelle auf Kennwortdiebstahl-Trojaner mit solchem Verhalten ein.

### Sinowal und StealthMBR: Der derzeit hinterhältigste Kennwortdieb und das am schwierigsten zu entdeckende Rootkit

Sinowal ist ein weit verbreiteter Trojaner, der Kennwörter stiehlt und mit einem der derzeit raffiniertesten und am schwersten zu entdeckenden Rootkits auf den Computer gelangt – dem StealthMBR, auch bekannt unter dem Namen „Mebroot“. Das StealthMBR-Rootkit infiziert den Master Boot Record (MBR) der Festplatte, um bereits vor dem Hochfahren des Betriebssystems die Kontrolle über das System zu erlangen, und gräbt sich tief in die internen Microsoft Windows-Strukturen ein. Das Rootkit lädt bei jedem Systemneustart weitere Komponenten für den Kennwortdiebstahl herunter. Statt den Trojaner auf der Festplatte zu speichern, sorgt das Rootkit dafür, dass dieser sich direkt über die Windows-API-Funktion (Application Program Interface) „SetWindowsHookEx()“ in beliebige laufende Prozesse injiziert.

Zusätzlich zum Rootkit-Stealth nutzt der neu heruntergeladene Trojaner noch weitere verdeckte Mechanismen. Neben Zeichenfolgen mit XOR-Verschlüsselung wie Hostnamen erkennen frühe Sinowal-Varianten abgeschottete Sandbox-Umgebungen und zeigen keine Auffälligkeiten, wenn sie sich beobachtet fühlen. Auf echten Computersystemen werden jedoch bestimmte Windows-API-Funktionen auf eigens dafür entwickelte Funktionen umgelenkt, die zum Code des Trojaners gehören. Dahinter steckt die kriminelle Absicht, vertrauliche Daten zu stehlen, die von diesen Funktionen verarbeitet werden. Bei dem hier vom Trojaner angewendeten „API-Hooking“ (Einklinken in API-Funktionen) werden Sprungbefehle in den zunächst normalen Betriebssystem-Code eingefügt (siehe Abbildung 7), um den Kontrollfluss zu böswilligem Code umzuleiten, bevor der echte Code ausgeführt werden kann.



```
71AB406A .text | Export | connect
CPU - thread 00000824, module WS2_32
71AB406A E9 5FD4549E JMP sinowal.100014CE
71AB406F 83EC 18 SUB ESP,18
71AB4072 57 PUSH EDI
71AB4073 8D45 E8 LEA EAX,DWORD PTR SS:[EBP-18]
71AB4076 50 PUSH EAX
71AB4077 8D45 EC LEA EAX,DWORD PTR SS:[EBP-14]
71AB407A 50 PUSH EAX
```

Abbildung 7: Umleitung von der „connect()“-API der ws2\_32-Programmbibliothek zum Sinowal-Code.

Mithilfe von Sicherheitssoftware können diese API-Hook-Formen erkannt (und entfernt) werden. Dazu wird der Code der Programmbibliothek im Speicher auf Umleitungen geprüft und das Ziel nachverfolgt. Diese Technik nutzt Sinowal tatsächlich ebenfalls und sogar zum eigenen Vorteil: Der Trojaner umgeht damit API-Hooks, die von Sicherheitssoftware wie Personal Firewalls oder Systemen zum hostbasierten Schutz vor Eindringlingen (Host Intrusion Prevention Systems, HIPS) eingearbeitet wurden. Wenn der Sinowal-Trojaner eine per Hooking veränderte API-Funktion erkennt, versucht er, die Sprung- und Aufrufbefehle zu entschlüsseln und die „echte“ Adresse der API zu finden, damit der Code des Sicherheitsprodukts erst gar nicht aufgerufen wird. Der Benutzer erhält dadurch keine Informationen über das verdächtige Verhalten der Malware.

| Address  | Hex dump                | ASCII    |
|----------|-------------------------|----------|
| 001D8440 | 52 65 66 65 72 65 72 3A | Referer: |
| 001D8448 | 20 68 74 74 70 73 3A 2F | https:// |
| 001D8450 | 2F 77 77 77 2E 62 61 6E | /www.ban |
| 001D8458 | 6B 6F 66 61 6D 65 72 69 | kofameri |
| 001D8460 | 63 61 2E 63 6F 6D 2F 69 | ca.com/i |
| 001D8468 | 6E 64 65 78 2E 6A 73 70 | ndex.jsp |

Abbildung 8: Darstellung des vom Browser gesetzten Referrers für die „HttpSendRequestA()“-API.

Es überrascht nicht, dass es sich bei den umgelenkten Funktionen genau um diejenigen handelt, die häufig von Anwendungen genutzt werden, die über das Internet kommunizieren. Ist der Trojaner aktiv, überwacht er Webbrowser, E-Mail- und FTP-Clients und andere Anwendungen, die Funktionen nutzen, die aus den Bibliotheken „ws2\_32.dll“, „wininet.dll“, „nspr4.dll“ (Firefox), „crypt32.dll“ und „advapi32.dll“ exportiert werden und der Verarbeitung vertraulicher Daten dienen. So klinkt Sinowal sich beispielsweise in die API-Funktion „HttpSendRequestA()“ ein, wenn sie im Kontext von Internet Explorer ausgeführt wird. Bevor die Code-Ausführung ihr vorgesehenes Ziel (die Originalfunktion „wininet::HttpSendRequestA“) erreichen kann, übernimmt die Umleitung die Kontrolle. Sie verarbeitet dann das „IpszHeaders“-Argument der Funktion für Referrer, die vom Browser immer

**Forschungsbericht** Das Geschäft der Kennwortdiebe:  
Wer ist an Identitätsdiebstahl beteiligt, und wie funktioniert er?

dann gesetzt werden, wenn der Benutzer beim Browsen im Internet auf einen Hyperlink klickt. (Der HTTP-„Referrer“-Header enthält die URL der vorherigen Webseite, die auf die neue Ressource verweist, die jetzt angefordert wird.) Je nach Referrer sorgt Sinowal nun dafür, dass im Internet Explorer ein kontextsensitives Pop-Up-Fenster mit dem Titel „Advanced Card Verification“ (Erweiterte Kreditkartenprüfung) angezeigt wird, in dem der Benutzer zur Angabe seiner Kreditkartendaten aufgefordert wird. Das böswillige Pop-Up gelangt über eine COM-Schnittstelle in den Internet Explorer.

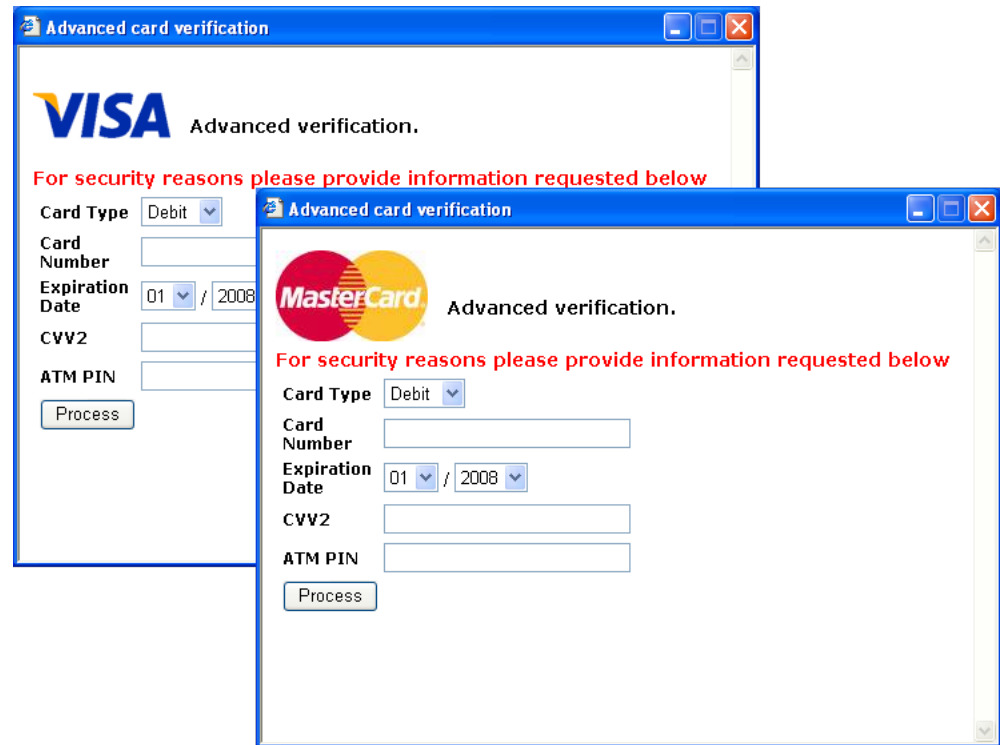


Abbildung 9: Vom Sinowal-Trojaner infizierte Pop-Ups fangen die Anmeldedaten des Benutzers ab.

Je nachdem, welche Zahlungsmethode der Benutzer auf einer eCommerce-Webseite auswählt, sieht er entweder ein gefälschtes VISA- oder ein MasterCard-Pop-Up-Fenster (siehe Abbildung 9). Der Benutzer kann das Pop-Up nicht einmal „aus Versehen“ wegklicken, da Sinowal die Funktion „SetForegroundWindow()“ nutzt, um das Pop-Up in einer Endlosschleife über andere Fenster zu legen. Die vom Trojaner gestohlenen Informationen werden zunächst verschlüsselt und dann an eine kriminelle Organisation gesendet, die früher unter dem Namen „Russian Business Network“ bekannt war und deren IP-Adressen fest in den Code des Trojaners einprogrammiert wurden. Man könnte nun annehmen, dass die Verschlüsselung, die in die HTTPS- und SSH-Protokolle eingebunden ist, ausreichenden Schutz bietet. Die Malware erfasst jedoch alle Daten, bevor sie verschlüsselt werden bzw. gleich nachdem sie entschlüsselt worden sind.

#### Die neue „Masche“ von Sinowal

Bei den neuesten Generationen der Sinowal-Familie wurden Strategie und Code wesentlich verändert: Die Trojaner sammeln global weniger Daten (z. B. auf Betriebssystemebene, wobei weniger API-Funktionen per Hooking verändert werden), sondern stehlen Daten erfolgreich durch direkte Angriffe auf bestimmte Anwendungen. Dies bietet den Angreifern verschiedene Vorteile gegenüber den vorherigen Generationen des Sinowal-Trojaners:

- Das Daten- und Datenverkehrsaufkommen wird reduziert.
- Der Trojaner kann nicht durch die API-Hooks erkannt werden, die er im Speicher hinterlässt.
- Sinowal ist kompatibler. Ältere Sinowal-Generationen waren an bestimmte Internet Explorer-Versionen gebunden. Die neueren Generationen funktionieren auf den verschiedenen Versionen unabhängiger und universeller.

**Forschungsbericht** Das Geschäft der Kennwortdiebe:  
Wer ist an Identitätsdiebstahl beteiligt, und wie funktioniert er?

Die neuen Generationen suchen jetzt Anmeldedaten direkt auf der Festplatte, nachdem sie der Windows-Registrierung deren exakte Speicherorte entnommen haben. Der Feind des Trojaners – die lokale Sicherheitssoftware – wird direkt angegriffen und mit Patches auf der Festplatte außer Gefecht gesetzt. Die Domännennamen der Angreifer sind nicht nur fest einprogrammiert, sondern werden auch mit einem Algorithmus berechnet, der auf dem aktuellen Datum basiert. Ältere Generationen des Trojaners verfügten über leistungsstarke Funktionen für den Datendiebstahl. Sie wurden möglicherweise in einer Data-Mining-Vorbereitungsphase für die Zusammenstellung böswilliger Informationen genutzt, die dann verwendet wurden, um die nächsten Generationen so zu verbessern, dass sie optimale Ergebnisse erzielen.

Benutzernamen- und Kennwortkombinationen, die automatisch vom Internet Explorer gespeichert wurden, werden mit den API-Funktionen „FindFirst/FindNextUrlCacheEntry()“ ausgelesen. Automatisch gespeicherte Anmeldeinformationen des Firefox-Browsers werden durch Auslesen und Verarbeiten der Dateien „signons.txt“, „signons2.txt“ und „signons3.txt“ abgerufen. Dies sind genau die Dateien, die alle privaten Informationen des Benutzers enthalten. Die Liste der Anwendungen, die auf ähnliche Weise angegriffen werden, ist lang: Microsoft Outlook, Eudora, Mozilla Thunderbird, VanDyke SecureCRT, WinSCP und PuTTY – um nur einige zu nennen. Kennwörter, PINs (Personal Identification Numbers) und TANs, die ein Benutzer in ein Dialogfeld eingibt, werden mit einer Technik gestohlen, die im Vergleich zu den älteren Hooking-Funktionen weniger Misstrauen erweckt: Ein Thread, der im Hintergrund arbeitet, durchläuft die Fenster auf dem Desktop und sucht nach speziellen Fensterbeschriftungen und -klassen, die darauf hinweisen, dass beliebige Kennwortdialoge oder aber Dialoge verwendet werden, die zu bestimmten Finanzanwendungen gehören, die der Trojaner explizit unterstützt. Kennwörter, TANs oder PINs werden abgerufen, indem eine „WM\_GETTEXT“-Fenstermeldung an den Dialog gesendet wird. Das funktioniert auch dann, wenn das Kennwort nur als Folge von Sternchen (\*) angezeigt wird, da der Trojaner diese visuelle Schutzmaßnahme aufhebt, bevor er das Kennwort ausliest. Danach aktiviert er sie mit der Meldung „WM\_SETPASSWORDCHAR“ erneut. Dies alles läuft so schnell ab, dass der Benutzer die Veränderung überhaupt nicht bemerkt.

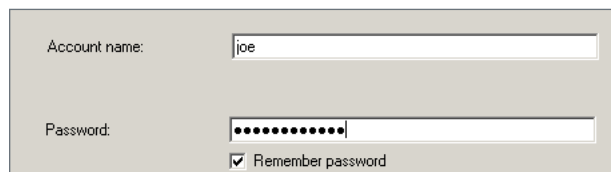


Abbildung 10: Herkömmlicher Kennwortdialog.

Durch die Infektion an sich werden nicht nur die Sicherheit und die Vertraulichkeit der infizierten Systeme gefährdet, sondern in mehrfacher Hinsicht auch die Vertrauenswürdigkeit der Seite. Software, die für zusätzliche Sicherheit sorgen soll, wie etwa Browser-Plug-Ins (die auch als Browserhilfsobjekte oder BHO bezeichnet werden), zeigen mit visuellen Signalen wie etwa einem Ampelsymbol an, wenn sichere Verbindungen zu einer Online-Banking-Webseite aufgebaut wurden. Diese Plug-Ins werden durch die Malware auf der Festplatte so gepatcht, dass sie ihr Verhalten ändern. Auf diese Weise wird vorgetäuscht, dass eine sichere Verbindung besteht, obwohl dies ganz und gar nicht der Fall ist. Da die Malware nach bestimmten zu patchenden Byte-Mustern im Code sucht, haben Malware-Autoren einen weiteren Grund, Sicherheitsprodukte per Reverse Engineering zurückzuentwickeln. Selbst verschlüsselte oder per Hashing geschützte Kennwörter werden mit brachialen Methoden geknackt. Hierfür werden kommerzielle Bibliotheken Dritter missbräuchlich verwendet, die für die Sicherung der Kommunikation gedacht sind. Ein noch gefährlicheres Merkmal aktueller Sinowal-Varianten ist deren Fähigkeit, aus einem infizierten Benutzercomputer einen Proxy zu machen, der für die ganze Welt geöffnet ist. Dafür bringt Sinowal seinen Proxyserver-Code in den Prozess „services.exe“ ein. Diese Anwendung wird mit Systemberechtigungen ausgeführt. Nach der Einbindung des Codes nimmt der nun infizierte Prozess fortlaufend alle eingehenden HTTP-, SOCKS4- und SOCKS5-Proxyverbindungen an. Der Angreifer kann dann die zweite Phase seines Angriffs starten und den geografischen Standort sowie das Ansehen des infizierten Hosts für seine kriminellen Zwecke nutzen.

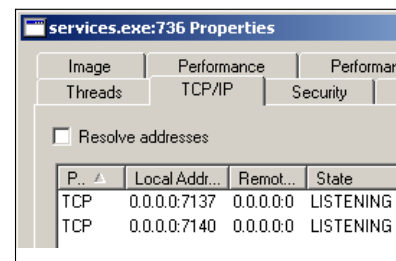


Abbildung 11: Proxyserver, die innerhalb eines Prozesses mit Systemrechten ausgeführt werden.

**Eine einzige Infektion bringt das gesamte Immunsystem aus dem Gleichgewicht**

Und als ob die Infektion und der Identitätsdiebstahl durch eine Malware nicht schon ausreichen würden, reißt der HTTP-Proxycode noch ein weiteres Loch in den infizierten Computer. Da es den Angreifern egal ist, ob sie sicheren Code produzieren, wird der Computer durch Fehler im Sinowal-Proxy (und ebenso in anderen bedeutenden Malware-Familien) anfällig für weitere Angriffe durch Remotecodeausführung.

```

copy_buffer_to_stack:
inc     esi
mov     cl, [esi]
mov     [eax], cl
inc     eax
dec     [ebp+1en]
mov     [eax], bl
cmp     [esi], dl
jnz    short copy_buffer_to_stack
    
```

Abbildung 12: Fehlerhafter HTTP-Proxycode.

Eine einzige Malware-Infektion kann eine endlose Zahl weiterer Infektionen über die folgenden Angriffswege nach sich ziehen:

- Die Angreifer geben dem infizierten Computer den Befehl, eine weitere Malware-Komponente herunterzuladen.
- Der Angreifer ist ein „Bot Herder“ und leiht den infizierten Computer an andere Angreifer aus, die andere Malware auf den Computer des Opfers herunterladen und darauf ausführen.
- Ein anderer Hacker sucht nach Systemen, die mit einer bestimmten Malware infiziert sind, und nutzt dann per Fernzugriff die „Schwachstellen“ der Malware aus.

Wie bereits erläutert, entwickeln Malware-Autoren Sicherheitssoftware mittels Reverse Engineering zurück, warum sollten sie also nicht die Malware ihrer Konkurrenz ebenso zurückentwickeln, um sich einen größeren „Marktanteil“ zu verschaffen? Ein aktuelles Beispiel für eine böswillige Software, die ihre Kontrahenten auf unkonventionelle Weise aus dem Weg räumt, ist das Rootkit Tigger.<sup>4</sup> Es nutzt eine lokale Schwachstelle (MS08-066) im Windows-Code und erhält dadurch Systemberechtigungen, die es zum Deaktivieren von Sicherheitsprodukten und Löschen konkurrierender Malware nutzt.

Wie in Abbildung 12 dargestellt, ist eine der Schwachstellen des HTTP-Proxycodes von Sinowal ein Loop (Schleife), der Daten aus einem vom Benutzer übermittelten Puffer aus dem Internet in einen begrenzten Stack-Buffer kopiert, bis ein bestimmtes Zeichen in dem vom Benutzer übermittelten Puffer gefunden wird. Durch die Bereitstellung fehlerhafter Eingabedaten würde der entsprechende Puffer über seine Grenzen hinaus mit Daten gefüllt werden. Dadurch hätte ein anderer Angreifer die Möglichkeit, auf dem bereits infizierten Computer des Opfers willkürlich anderen böswilligen Code auszuführen. Dies ermöglicht es wiederum anderen potenziellen Angreifern, durch Überschreiben kritischer Daten wie etwa dem SEH (Structured Exception Handler), Heap-Strukturen und der Rücksprungadresse der Funktion zum Stack, die Kontrolle zu übernehmen. Zwar verfügt Windows über integrierte Sicherheitsmechanismen zum Schutz vor der Ausführung von Code in Speicherbereichen mit Daten und vor dem Überschreiben des SEH<sup>5</sup>, jedoch erweisen sich diese Mechanismen als ineffizient, da jede Anwendung selbst entscheiden kann, ob diese Maßnahmen bei einem bestimmten Anwendungsprozess zum Tragen kommen sollen.

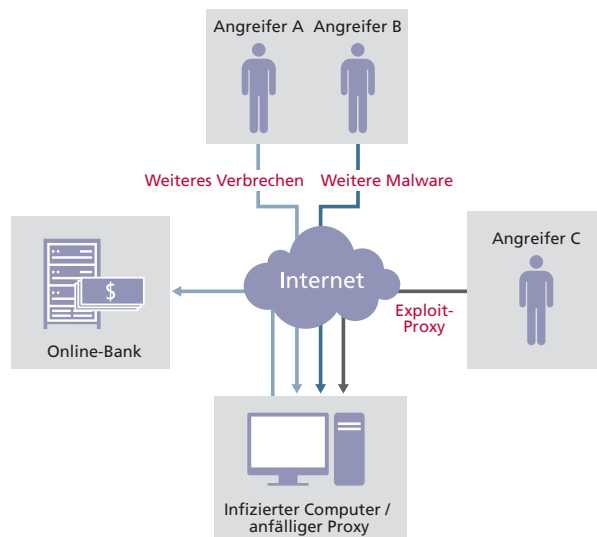


Abbildung 13: Verschiedene Angriffsszenarien.

4. <http://mmin.blogspot.com/2009/02/why-i-enjoyed-tiggersyzor.html>.  
5. <http://blogs.technet.com/swil/archive/2009/02/02/preventing-the-exploitation-of-seh-overwrites-with-sehop.aspx>.

## Forschungsbericht Das Geschäft der Kennwortdiebe: Wer ist an Identitätsdiebstahl beteiligt, und wie funktioniert er?

Es ist davon auszugehen, dass Malware-Autoren ihre Produkte eher nicht mit /GS oder /NXCOMPAT kompilieren. Es handelt sich hierbei um Flags, die einen Compiler anweisen, sichereren Code zu erstellen.

Da in Sinowal ein Stack-Buffer Overflow möglich ist, können alle „übrigen“ Felder (die gleich nach dem Puffer folgen) und, was am wichtigsten ist, die Zeiger, die für eine willkürliche Codeausführung verantwortlich sind, per Fernzugriff überschrieben werden. Schwerwiegende bekannte Bedrohungen sind heute „nur“ einige Wochen wirksam, denn durch die Kooperation von Sicherheitsunternehmen und die Strafverfolgung werden die Command-and-Control-Server schließlich aus dem Netz genommen. In diesem Fall kann die Kennwörter stehlende Malware die gestohlenen Anmeldedaten nicht mehr „nach Hause“ übermitteln. Allerdings ist der infizierte Computer aufgrund des defekten Proxyservers, der zusammen mit einem Prozess mit umfangreichen Berechtigungen ausgeführt wird, ungeschützt weiteren Angriffen ausgesetzt. Dass dieser Proxycode und die damit zusammenhängenden Fehler existieren, scheint im Untergrund schon seit 2006 bekannt zu sein.

### Zbot: Die nächste Keylogger-Generation

Zbot ist eine weitere finanziell motivierte Datendiebstahl-Malware-Familie, die es auf Bank-PINs und ganz besonders auf TANs abgesehen hat. Der Zbot-Trojaner geht ähnlich wie die ersten Sinowal-Generationen vor: Er klinkt sich in einige Benutzermodus-API-Funktionen ein, um die Anmeldedaten während der Weiterleitung abzufangen. Ein Unterschied besteht darin, dass Zbot sich mit Hooks für Benutzermodus-APIs begnügt – im Gegensatz zu Sinowal, der die Kernel-Mode-Hooks benötigt, die sein zugehöriges Rootkit benötigt. Bei Umgehung der ntdll.dll-Funktion „NtQueryDirectoryFile()“, bei der es sich um die native API handelt, die von den API-Funktionen „FindFirst/FindNextFile()“ aufgerufen wird, werden mehrere Verzeichnisnamen und Dateien gefiltert, die dann für den Benutzer unsichtbar sind.

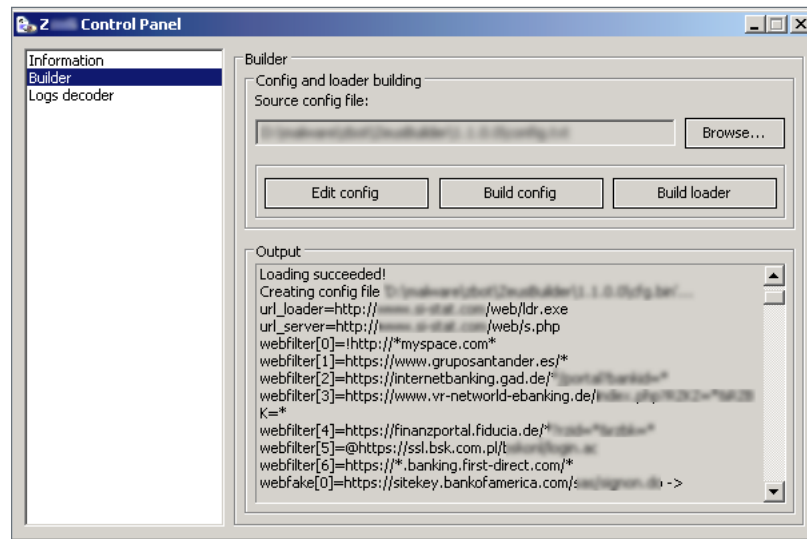


Abbildung 14: Mit dem Zbot-Konstruktionskit können mit einem einfachen Mausklick neue Varianten erstellt werden.

Verschiedene weitere Hooks für native API-Funktionen wie „NtCreateThread()“, „LdrLoadDll()“ und „LdrGetProcedureAddress()“ werden verwendet, um böswilligen Code in neu erstellte Prozesse und Threads einzufügen und sicherzustellen, dass die eigenen API-Hooks auch weiterhin funktionieren. Genau wie Sinowal stiehlt der Zbot-Trojaner Anmeldedaten während der Übertragung, indem er sich in Code einklinkt, der zu den Netzwerk-APIs gehört. Diese Hooks stellen den lokalen Man-in-the-Middle-Angriff dar: Die Kommunikation auf dem Client wird abgehört, bevor sie das Netzwerk erreicht. Der Trojaner kann so konfiguriert werden, dass nur Sitzungen auf einem bestimmten Host (z. B. die Webseite einer großen Bank) abgehört werden, er kann aber auch sämtliche Anmeldedaten und Hostnamen erfassen. So sucht der Hook „InternetReadFile()“ nach typischen HTML-Tags; die umgeleitete ws2\_32.dll-Funktion „send()“ sucht hingegen in Puffern alles, was ein FTP-Protokoll sein könnte. Die Schlüsselwörter und Verben „User“, „pass“, „feat“, „pasv“, „list“, „nbsp“, „br“ oder „script“ können die Protokollierungs- oder Änderungsfunktion des Trojaners auslösen.

**Forschungsbericht** Das Geschäft der Kennwortdiebe:  
Wer ist an Identitätsdiebstahl beteiligt, und wie funktioniert er?



Abbildung 15: Derzeit aktive Command-and-Control-Server der Zbot-Malware-Familie. (Quelle: abuse.ch)

Eine der raffiniertesten Zbot-Umleitungen nutzt die Windows-Funktion „TranslateMessage()“, die virtuelle Tastencodes in lesbare Zeichen konvertiert. Hier fügt sich der Trojaner selbst ein und agiert als konventioneller Keylogger, indem er WM\_KEYDOWN-Meldungen abgehört und alle Zeichen wie zum Beispiel Anmeldedaten protokolliert. Der trickreichste Teil besteht jedoch aus der Umleitung, die WM\_LBUTTONDOWN-Windows-Meldungen abhört, die Klicks auf die linke Maustaste signalisieren. Bei jedem Klick (beschränkt auf maximal 20) wird ein quadratischer Screenshot mit dem Mauscursor als Mittelpunkt erstellt und dazu verwendet, Anmeldedaten, die der Benutzer mit einer virtuellen oder Bildschirmtastatur eingibt, grafisch einzufangen. Die Reaktion der Kriminellen, einen „grafischen Keylogger“ dieser Art zu entwickeln, ist mehr als natürlich. Dieses typische Katz-und-Maus-Spiel entwickelte sich, nachdem die Online-Bankinstitute von traditioneller tastaturbasierter Authentifizierung zu proprietären Authentifizierungsmechanismen wechselten, die auf virtuellen Tastaturen basieren.

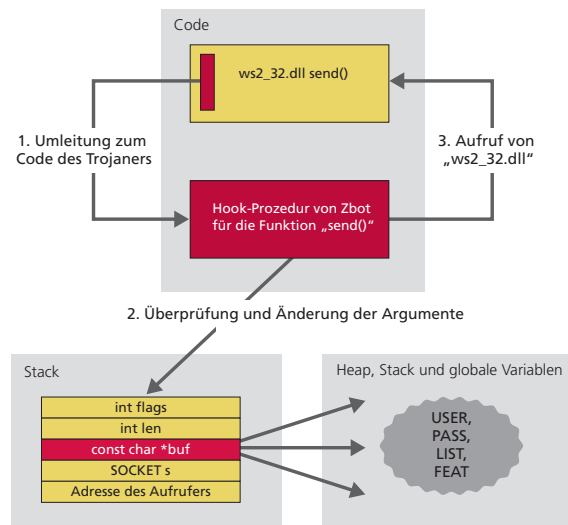


Abbildung 16: API-Hook „send()“ des Trojaners Zbot.

**Forschungsbericht** Das Geschäft der Kennwortdiebe:  
Wer ist an Identitätsdiebstahl beteiligt, und wie funktioniert er?

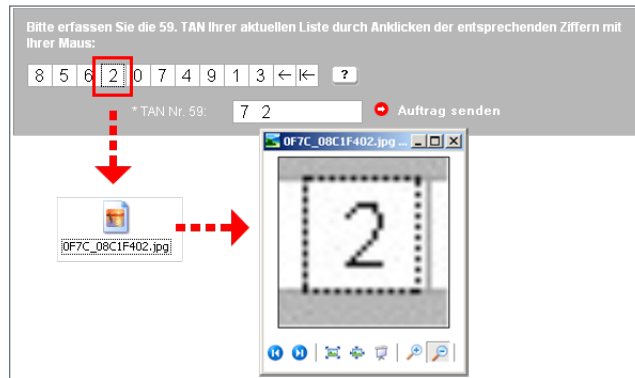


Abbildung 17: Keylogger der nächsten Generation stiehlt Daten von virtuellen Tastaturen.

Die Screenshots werden als JPEG-Dateien im Unterverzeichnis namens „screens“ gespeichert. Dieses wird mithilfe der Rootkit-Funktion des Trojaners ausgeblendet – der Benutzer kann sie also nicht zufällig entdecken. Alle Dateinamen werden aus verschiedenen Komponenten zusammengesetzt, z. B. eine Kennung für den derzeit ausgeführten Prozess, ein Unterstrich und die genaue Uhrzeit. Mithilfe dieser Informationen kann die chronologische Reihenfolge der angeklickten Ziffern leicht zu vollständigen TANs zusammengesetzt werden.

Eine weitere gemeinsame „Funktion“ von Sinowal und Zbot ist der SOCKS-Proxy. Zbot integriert darin eine Backdoor, die zufällig gewählte TCP-Ports (Transmission Control Protocol) abhört. Zu den von dieser Backdoor unterstützten Befehlen gehören Funktionen zum Erstellen und Senden von Screenshots mithilfe eines proprietären Protokolls. Je nach Bandbreite des Opfers kann der Angreifer das passende Format auswählen (z. B. GIF, JPEG oder BMP). Mit noch verheerenderen Konsequenzen ist jedoch beim Ausführen eines Backdoor-Befehls zu rechnen, der alle Unterschlüssel in der Registrierung löscht, die mit den Root-Schlüsseln „KEY\_CURRENT\_USER\Software“, „HKEY\_LOCAL\_MACHINE\Software“, und „HKEY\_LOCAL\_MACHINE\System“ beginnen, da das betroffene System dadurch völlig unbrauchbar wird. Die Angreifer können auf diese Weise das kompromittierte System remote zerstören, um nach dem Durchführen eines Angriffs und Missbrauch der Host-IP-Adresse als Angriffsquelle ihre Spuren zu entfernen.

**Steam Stealer und der illegale Markt für Spieler-Daten**

Steam Stealer, ein anderer Kennwortdieb, ist weniger bekannt als die beiden professionell betriebenen Kennwortdiebe Sinowal und Zbot. Er ist modular aufgebaut, was darauf hindeutet, dass er mit einem Toolkit zum Erstellen von Malware oder durch Zusammenfügen verschiedener Malware-Codeteile erstellt wurde. Letzteres ist die wahrscheinlichere Erklärung, da die Malware mithilfe einer Ressource konfiguriert wird, die in die ausführbare Datei eingebettet ist. Dadurch ist kein separates Erstellungs-Toolkit notwendig. Glücklicherweise hat der Code zahlreiche Unzulänglichkeiten (z. B. werden veraltete Bibliotheksfunktionen verwendet), weshalb die Malware kein Muster an Stabilität ist. Steam Stealer missbraucht Tools von Drittanbietern, um auf diese Weise die gesammelten Anmeldeinformationen zu entschlüsseln. Zusammenfassend kann gesagt werden, dass dieser Trojaner ein Sammelsurium von Codeteilen und Fremd-Binärdateien ist, die in den verschiedenen Untergrundforen zu finden sind.

|    | A  |
|----|--|
| 1  | Counter-Strike (Retail)                      |
| 2  | The Gladiators                               |
| 3  | Gunman Chronicles                            |
| 4  | Half-Life                                    |
| 5  | Industry Giant 2                             |
| 6  | Legends of Might and Magic                   |
| 7  | Soldiers Of Anarchy                          |
| 8  | Unreal Tournament 2003                       |
| 9  | Unreal Tournament 2004                       |
| 10 | IGI 2: Covert Strike                         |
| 11 | Freedom Force                                |
| 12 | Call of Duty 2                               |
| 13 | Call of Duty 4                               |
| 14 | Microsoft Windows Product ID and CD Key      |
| 15 | Battlefield 1942                             |
| 16 | Battlefield Vietnam                          |
| 17 | Need for Speed Most Wanted                   |
| 18 | Black and White                              |
| 19 | Empire Earth II                              |
| 20 | Medal of Honor Airborne                      |
| 21 | Battlefield 1942 (Road To Rome)              |
| 22 | Battlefield 1942 (Secret Weapons of WWII)    |
| 23 | Command & Conquer 3 Tiberium Wars            |
| 24 | Command and Conquer 3 Kanes Wrath            |
| 25 | Command & Conquer Generals (Zero Hour)       |
| 26 | Crysis                                       |
| 27 | James Bond 007: Nightfire                    |
| 28 | Command & Conquer Generals                   |
| 29 | Global Operations                            |
| 30 | Shogun: Total War: Warlord Edition           |
| 31 | Medal of Honor: Allied Assault               |
| 32 | Medal of Honor: Allied Assault: Breakthrough |
| 33 | Medal of Honor: Allied Assault: Spearhead    |
| 34 | Need For Speed Hot Pursuit 2                 |

Abbildung 18: Eine Liste von Spielen, die von Steam Stealer angegriffen werden.

**Forschungsbericht** Das Geschäft der Kennwortdiebe:  
Wer ist an Identitätsdiebstahl beteiligt, und wie funktioniert er?

Bevor Steam Stealer nach dem Schätzen eines Spielers greift, nutzt die Malware verschiedene bekannte Methoden für die Entdeckung virtueller Maschinen. Die einfachsten greifen auf die API-Funktion „GetCurrentUser()“ zu und vergleichen die Ergebnisse mit einer Liste von Benutzernamen, die von bestimmten Sandbox-Programmen verwendet werden. Andere Methoden versuchen, virtuelle Betriebssysteme zu erkennen, indem sie nach bestimmten Hardware-Registerwerten suchen. Das Byte-Muster, das von dieser x86-Assemblycode-Sequenz gebildet wird, ist recht einmalig; genau genommen so einmalig, dass es von vielen Anti-Malware-Produkten einfach entdeckt und gekennzeichnet werden kann. Als Reaktion darauf begannen die Malware-Programmierer, das Muster zu verbergen, indem sein Code (der nur aus wenigen Zeilen besteht) dynamisch einen Stack erstellt, bevor die Malware darauf zugreift. Code, der den Stack ausführen möchte, wird von Microsoft DEP (Data Execution Prevention) erkannt, das mit Windows XP SP2 eingeführt wurde. Wenn DEP für alle Prozesse aktiviert wäre (was bei einigen Windows-Plattformen nicht standardmäßig der Fall ist), würde die Malware abstürzen, ohne weiteren Schaden anzurichten. Andere von Steam Stealer verwendete Erkennungsmethoden (z. B. die Suche nach verschiedenen Sicherheitsprodukten) beschränken sich auf einfache Vorgehensweisen wie das Öffnen bestimmter Schlüssel in der Windows-Registrierung oder das Aufnehmen von Prozessen und geladenen Bibliotheken anhand ihres Namens in die schwarze Liste.

Dennoch gibt es einen kommerziellen Markt für Steam Stealer: Die Malware wird von ihren Autoren für 60 Euro pro Kopie verkauft und an die Bedürfnisse des Kunden angepasst. Zusätzlich zur eigentlichen Malware können die Kunden für 40 Euro noch ein Packprogramm für ausführbare Dateien kaufen, das die Malware vollständig „FUD“ machen soll – im Hacker-Jargon steht das für „komplett verborgen“ (engl.: fully undetectable). Diese Packprogramme für ausführbare Dateien (bzw. Crypter) werden auch als Binder bezeichnet, da sie wie konventionelle Installationsprogramme funktionieren. Sie laden gebündelte und verschlüsselte Binärdateien herunter und führen sie aus. Dies kann vollständig im Arbeitsspeicher geschehen, damit On-Access-Scanner die heruntergeladenen Dateien nicht untersuchen. Mithilfe öffentlich verfügbarer Dienste wie VirusTotal.com oder mit „Offline“-Befehlszeilenscannern können Internetkriminelle ihre neu erstellten Varianten mit Bindern scannen und verändern, bis diese nicht mehr erkannt werden.

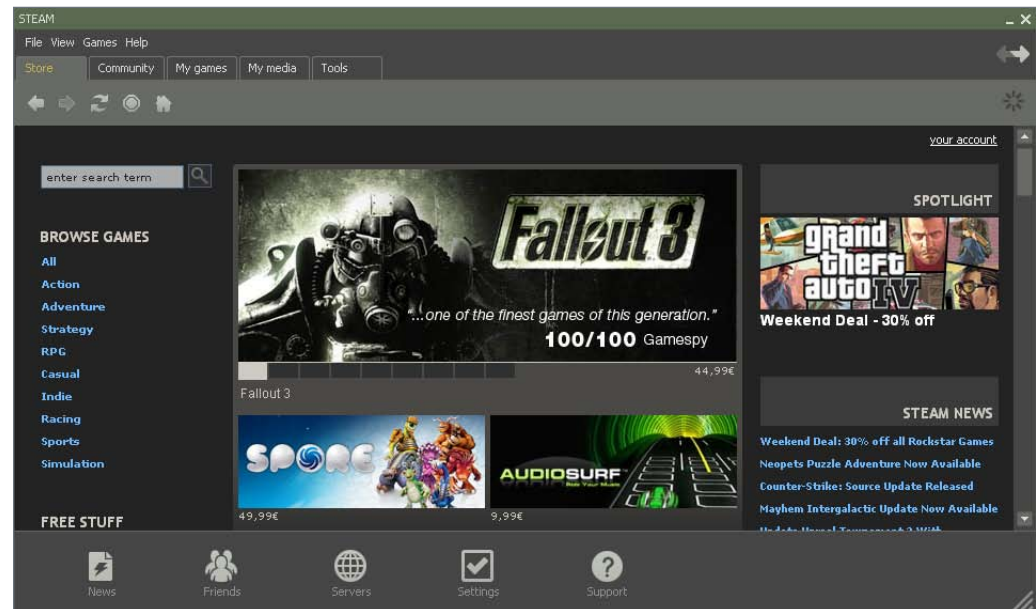


Abbildung 19: Steam-Onlineshop.

```
if ( get_steam_install_path() && get_steam_installed_apps() )
{
  get_string_from_reg_key("SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\", v0, HKEY_LOCAL_MACHINE, "ProductId");
  get_string_from_reg_key("SOFTWARE\\Microsoft\\Cryptography\\", v7, HKEY_LOCAL_MACHINE, "MachineGuid");
  get_string_from_reg_key("SOFTWARE\\Valve\\Half-Life\\Settings\\", v8, HKEY_CURRENT_USER, "io");
  lstrcpyA(&string1, "\n\n\n *****\n\n\n");
  lstrcatA(&string1, "\n\n *****STEAM PASS STEALER*****\n\n");
}
```

Abbildung 20: Ausschnitt des dekomilierten Pseudocodes von Steam Stealer.

Sobald Steam Stealer ausgeführt wird, lädt die Software mehrere Module, die gespeicherte Firefox-Kennwörter, CD-Schlüssel und Produkt-IDs sehr vieler beliebter Spiele und Microsoft-Produkte sammelt. Steam Stealer arbeitet eine vordefinierte Liste der Registrierungspfade von Produkten ab und liest deren Werte mit den unverschlüsselten Anmeldeinformationen aus, hinter denen die Angreifer her sind. Eine Komponente, die explizit nach Steam-Anmeldeinformationen sucht, liest und dekodiert eine Datei mit dem Benutzernamen und dem Kennwort für Steam. Diese Datei (ClientRegistry.blob) befindet sich im Installationsverzeichnis von Steam. Die Liste der gestohlenen Anmeldeinformationen wird zu einer Stack-Variablen assembliert und an einem getrennten Speicherort auf der Festplatte gespeichert. Dort wartet sie darauf, ihre wertvolle Ladung an den Angreifer zu übertragen.

Abhängig von der in Steam Stealer eingebetteten Konfiguration kann die Malware auch die Anmeldeinformationen von Instant Messengern, E-Mail-, LAN- und FTP-Konten stehlen. Leider werden nicht alle Anmeldeinformationen von ihren Anwendungen verschlüsselt, bevor sie gespeichert werden. Doch auch dieses Problem können die Malware-Autoren umgehen, indem sie kostenlose Software zum Wiederherstellen von Kennwörtern dazu verwenden, verschlüsselte Anmeldeinformationen zu cracken. Steam Stealer kann so konfiguriert werden, dass die Malware alle erdenklichen Daten sammelt und per E-Mail an den Besitzer der Malware (mit einer separaten SMTP-Komponente) verschickt oder diese Daten auf einen FTP-Server hochlädt.

### **Fazit: Internetkriminelle nutzen die Wirtschaftskrise aus**

Anfang Februar 2009 gab das FBI eine Pressemeldung heraus<sup>6</sup>, die die Öffentlichkeit über das aktuelle Problem der Heimarbeitsplatz-Betrugsnachrichten informierte. Verzweifelte Menschen, die aufgrund der Wirtschaftskrise unerwartet ihren Arbeitsplatz verloren haben, suchen nach neuen Verdienstmöglichkeiten und werden womöglich alle sich bietenden Gelegenheiten nutzen – und manchmal geraten sie dabei an Internetkriminelle. Sie könnten sich dafür entscheiden, als Geldwäsche-Kuriere zu arbeiten, indem sie im Auftrag der Kriminellen illegal durch Kennwortdiebe erbeutetes Geld weiterleiten. Diese Verzweifelten stehen unter starkem finanziellem Druck und wissen häufig gar nicht, dass hinter dieser Geldwäsche kriminelle Aktivitäten stecken – oder sie interessieren sich nicht dafür. Sie sind jedoch in ein riskantes Geschäft verwickelt: die von ihnen getätigten Banküberweisungen können rückabgewickelt werden und daher ein Loch im Konto des Kuriers hinterlassen. Zudem befinden sie sich im Visier der Ermittler von Internetkriminalität.

Glücklicherweise gelten in vielen Banken Beschränkungen dazu, wie viel Geld ins Ausland überwiesen werden dürfen. Durch die Hilfe der Geldkuriere gehen diese Überweisungen jedoch als inländische Überweisungen durch und entgehen auf diese Weise meist der Aufmerksamkeit der Strafverfolgungsbehörden. Die meist sichtbarer Geldwäscher werden hingegen entdeckt und verurteilt, während die wahren Kriminellen im Hintergrund verborgen bleiben. Kunden wird geraten, die Augen offen zu halten und nicht auf Jobangebote hereinzufallen, die zu gut klingen um wahr sein zu können – andernfalls könnten sie unabsichtlich in kriminelle Aktivitäten hineingezogen werden.

In der virtuellen Welt verstecken die Angreifer sich hinter dem infizierten Host eines anderen Benutzers, da die Proxys heute nicht mehr als eigenständige Software ausgeführt sein müssen – sie sind ganz einfach Teil der Malware. Ähnlich wie beim Echtweltszenario des Geldwäschers wird die IP-Adresse des „übernommenen“ Hosts dazu verwendet, anonym Internetverbrechen zu begehen. Und für die Opfer gibt es sogar noch einen Doppelschlag – als wenn die Infektion mit einem Kennwortdieb nicht schon ärgerlich genug wäre! Da die Opfer als Quelle für das Malware-Exploit identifiziert werden, müssen sie zudem rechtliche Konsequenzen aufgrund der scheinbar von ihnen verübten Internetverbrechen befürchten. Da die Angreifer in der Lage sind, das infizierte System per Fernzugriff zu zerstören, können sie wie in einem einfachen Computerspiel ihre Spuren entfernen. Das Opfer erhält dadurch nicht einmal die Chance, einen Forensiker zu bitten, die Quelle der Malware nachzuverfolgen.

**Forschungsbericht** Das Geschäft der Kennwortdiebe:  
Wer ist an Identitätsdiebstahl beteiligt, und wie funktioniert er?

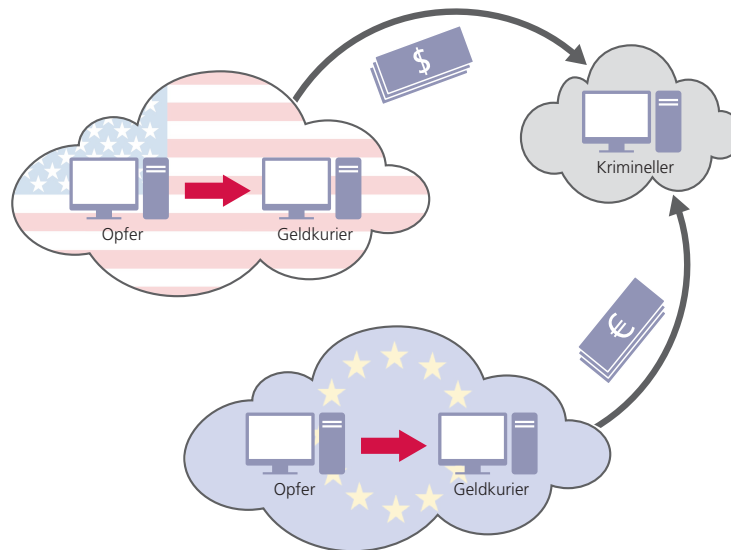


Abbildung 21: So begehen Geldkuriere (die Geldwäsche betreiben) und Opfer von Heimarbeitsplatz-Betrug ihre Verbrechen.

Wie bereits in diesem Whitepaper beschrieben, wird die Evolution der Kennwortdiebstahl-Malware vom Räuber-und-Gendarmen-Spiel zwischen Internetkriminellen und Online-Bankinstituten voran getrieben. Doch die Einführung von noch mehr Sicherheit führt nicht unbedingt zu besserer Bedienbarkeit. Das Gegenteil ist meist der Fall, da die Einführung einer weiteren Sicherheitsfunktion meist dazu führt, dass die Bedienung durch die Benutzer komplizierter wird. Dies kann schließlich dazu führen, dass sie den Dienst zukünftig meiden. Wie viel Komplexität sind die Kunden bereit zu tolerieren? Das Ziel wird nicht dadurch erreicht, dass die Kunden einen neuen „Geheimcode“ eingeben oder ihn sich merken müssen. Die Kreditinstitute müssen einen besseren Kompromiss zwischen Sicherheit und Bedienbarkeit finden. Einige Kunden notieren sogar ihre Geldkarten-PIN und bewahren diese Notiz zusammen ihren Bankkarten in der Brieftasche auf, da es ihnen zu schwer fällt, sich so viele Codes und Kennwörter zu merken. Zweifellos sind bei solchem Verhalten alle Sicherheitsbemühungen zum Scheitern verurteilt. Einmal verwendbare Kennwort-Token sind ein guter Anfang, doch die Kosten für diese Geräte werden an den Kunden weitergereicht. Wie viele Kunden werden bereit sein, für zusätzliche Banksicherheit zu zahlen, die ihrer Meinung nach kostenfrei sein sollte?

Und noch eines ist sicher: Die Kennwortdiebe werden in absehbarer Zeit nicht verschwinden. Aufgrund der Tatsache, dass jeder mithilfe einfach bedienbarer Erstellungskits angepasste Trojaner erstellen kann, sind Infektionen mit noch raffinierterer Kennwortdiebstahl-Malware traurige Realität. Da der Online-Diebstahl von Anmeldedaten so viel Profit verspricht, werden die Bemühungen der Kriminellen nicht nachlassen, sondern vielmehr ihre Zielgruppe über Bankkunden und Online-Spieler hinaus zu erweitern. Skimming-Angriffe, mit denen die Betriebssysteme und die Software von Bankautomaten kompromittiert werden, sind ein Beispiel für neue Techniken, die unter Internetkriminellen beliebt werden könnten. Aufgrund der ausgeklügelten Mechanismen moderner Malware zur Umgehung von Sicherheitslösungen und Vermeidung der Entdeckung ist es zunehmend wichtig, vorhandene Infektionen in einem Netzwerk nicht nur aufzudecken und zu isolieren, sondern auch von vornherein zu vermeiden. Ungewöhnliches Verhalten wie die Zunahme des konstanten Netzwerkverkehrs oder verschlüsselte HTTP POST-Anforderungen (Power-On Self-Test) sind ein sicheres Zeichen für eine Infektion und können mithilfe des Benachrichtigungs-Netzwerk-Gateways schnell entdeckt werden. Das Risiko, das ein einziger Benutzer das gesamte Unternehmensnetzwerk infizieren kann, ist überraschend hoch. Dazu muss ein Mitarbeiter lediglich einen infizierten Laptop oder ein infiziertes Massenspeichergerät am Arbeitsplatz an das Unternehmensnetzwerk anschließen.

In wirtschaftlich schwierigen Zeiten neigen Regierungen zu Protektionismus und Beschränkungen des internationalen Handels. Aufgrund der zukünftigen grenzüberschreitenden Bedrohungen – bei denen ein Verbrechen in einem Land begangen wird, der Verdächtige sich jedoch in einem anderen Land befindet – müssen Regierungen der Internetkriminalität mehr Aufmerksamkeit widmen und auf internationaler Ebene kooperieren, um die Übeltäter fassen zu können.

**Forschungsbericht** Das Geschäft der Kennwortdiebe:  
Wer ist an Identitätsdiebstahl beteiligt, und wie funktioniert er?

### Danksagung

Wir danken unserem Kollegen François Paget für die unschätzbare Hilfe bei den statistischen Daten.

### Informationen zu den Autoren



**Dennis Elser** ist Senior Engineer des McAfee-Forschungs- und Entwicklungsteams für Gateway-Anti-Malware-Lösungen. Zu seinen Schwerpunkten gehören die Schwachstellenforschung und die Entwicklung proaktiver Exploit-Erkennungstechniken. Elser veröffentlicht regelmäßig Artikel im McAfee Avert Labs-Blog. Außerdem ist er Autor mehrerer Artikel im *Virus Bulletin*. Die Bandbreite der Artikel reicht von Windows-Schwachstellen bis zu multimediasbasierter Malware.



**Micha Pekrul** ist Senior Engineer des McAfee-Forschungs- und Entwicklungsteams für Gateway-Anti-Malware-Lösungen. Zu seinen Schwerpunkten gehören die Forschung zu böswilligen Webinhalten und die Entwicklung entsprechender Erkennungsmechanismen, die in McAfee Web Anti-Malware, Gateway Edition eingesetzt werden. Pekrul veröffentlicht seine Erkenntnisse zu den neuesten Bedrohungen regelmäßig im Avert Labs-Blog. Außerdem ist er Autor mehrerer *Virus Bulletin*-Artikel.

**McAfee®**

McAfee GmbH  
Ohmstr. 1  
85716 Unterschleißheim  
Deutschland  
+49 (0)89 3707  
www.mcafee.com/de

McAfee und/oder weitere hier enthaltene McAfee-bezogene Produkte sind eingetragene Marken oder Marken von McAfee, Inc., und/oder der Tochterunternehmen in den USA und/oder anderen Ländern. Die Farbe Rot in Verbindung mit Sicherheit ist ein Merkmal der McAfee-Produkte. Alle anderen nicht zu McAfee gehörenden Produkte sowie eingetragene und/oder nicht eingetragene Marken in diesem Dokument werden nur als Referenz genannt und sind alleiniges Eigentum der jeweiligen Besitzer. © 2009 McAfee, Inc. Alle Rechte vorbehalten.  
6622wp\_password-stealers\_0709\_ETMG