Banking-Trojaner

Mit Man-in-the-Middle-Angriffen manipulieren Trojaner heimlich Überweisungen und beklauen Bankkunden. Getarnte Banking-Trojaner können sich auf jedem PC verstecken.

Rund 43 Prozent aller Girokonten in Deutschland werden online geführt, berichtet der Bundesverband Deutscher Banken in einer aktuellen Studie. Das sind rund 40 Millionen Nutzer von Online-Banking oder – in den Augen der Internetmafia – 40 Millionen potenzielle Opfer, auf die sie mit Banking-Trojanern Jagd machen. In der Schweiz dürfte der Anteil ähnlich hoch sein.

Banking-Trojaner sind besonders heimtückische Schädlinge, die Zugangsdaten klauen und Überweisungen fälschen. Manche Banking-Trojaner kennen und manipulieren nach Angaben von Sicherheitsexperten mehrere Tausend Webseiten von Finanzdienstleistern. Besucht ein Surfer eine dieser Seiten mit einem verseuchten PC, tauscht der Schädling heimlich Teile der Seite aus. So klaut er Account-Daten und ändert Überweisungen.

Statt beispielsweise wie vom Nutzer beabsichtigt 100 Franken an Person A zu überweisen, erfolgt in Wirklichkeit eine verdeckte Zahlung von 1000 Franken an Person B.

Diese Methode bezeichnet man als Man-in-the-Middle-Angriff: Der Banking-Trojaner sitzt in der Mitte der Kommunikation, fängt die übertragenen Daten ab und verändert sie. Der Anwender bekommt dabei nur das zu sehen, was er sehen soll. Das Prinzip wird in der Grafik auf Seite 44 ausführlicher erläutert. Viele Banking-Verfahren, beispielsweise iTAN, sind nicht sicher gegen diese Angriffe.

Der Artikel zeigt, wie Sie Banking-Trojaner erkennen und entfernen. Ausserdem erfahren Sie, welche Verfahren sicher und welche unsicher sind.

Banking-Trojaner

Banking-Trojaner sind die Königsklasse der Trojaner, weil sie ihren Urhebern direkten Zugriff auf fremde Konten ermöglichen. In den folgenden Abschnitten lesen Sie, wie drei besonders gefährliche und weit verbreitete Banking-Trojaner funktionieren.

Kompakt

- *Banking-Trojaner nisten sich auf dem PC ein. Sie klauen heimlich Kontodaten und manipulieren Überweisungen.*
- *Anti-Malware 1.41, Anti-Rootkit 1.5 und Avira Antivir Rescue-System 3.6.9 entfernen Banking-Trojaner.*
- *Sichere Banking-Verfahren sind nur mTAN, HBCI, Smart TAN Plus, Flickercode sowie Secoder.*

Beispiel: Sinowal

Sinowal ist ein seit mehreren Jahren verbreiteter Banking-Trojaner. Er hat nach Erkenntnissen der Sicherheitsexperten von RSA Security und Kaspersky schon einige Hunderttausend Zugangsdaten zu Online-Konten geklaut. Der Schädling erkennt und manipuliert mehrere Hundert Webseiten aus dem Finanzsektor.

Das funktioniert so: Der Anwender ruft die Webseite seiner Bank auf, um sich dort einzuloggen. Sinowal pflanzt dabei eigenen Code in die Seite ein und klaut so Anmeldedaten und persönliche Informationen. Anschliessend sendet er sie über das Internet an seine Urheber.

Um auf dem PC nicht aufzufallen, verwendet Sinowal unter anderem Rootkit-Techniken. So macht er sich im Windows-Explorer und im Task-Manager komplett unsichtbar. Ausserdem schreibt er sich in den MBR (Master Boot Record) der Festplatte, um sich vor dem Zugriff durch Antivirenprogramme zu schützen.

Anfang 2009 gelang es amerikanischen Forschern, das Sinowal-Netz für zehn Tage zu unterwandern. In dieser Zeit klaute der Schädling 8'310 Kontodaten von 410 verschiedenen Finanzinstituten. Betroffen waren neben Paypal-Nutzern vor allem Kunden von Poste Italiane, Capital One und E-Trade. Dazu kamen mehrere Hunderttausend Zugangsdaten zu Webdiensten wie Gmail, Facebook und Myspace sowie zu Mail- und FTP-Konten.

Beispiel: Banker.ohq

Banker.ohq klaut nicht nur die Anmeldedaten des Banking-Nutzers, sondern manipuliert gleich die gesamte Transaktion: Der Banking-Trojaner tauscht die Originalseite gegen eine Kopie aus, auf der der Surfer seine Überweisung durchführt. Parallel dazu loggt sich der Schädling unsichtbar auf der Originalseite ein und verwendet die eingegebenen Daten, um eine eigene Überweisung durchzuführen.

Die folgenden TAN-Verfahren schützen nicht gegen diese Man-in-the-Middle-Angriffe: TAN, iTAN, eTAN und Smart TAN. Das Problem bei diesen Verfahren ist, dass dabei die angeforderte TAN nicht direkt mit der Transaktion verbunden ist. Selbst wenn die Bank gezielt eine bestimmte TAN anfordert, kann der Trojaner damit jedoch auch eine völlig andere Überweisung authentifizieren.

Nur mTAN, HBCI, Secoder oder Flickercode sind sicher gegen Trojaner, weil hier jede TAN nur eine ganz bestimmte Transaktion freigibt. Ändert der Trojaner heimlich den Betrag oder den Empfänger, ist die TAN nicht mehr gültig.

Beispiel: Urlzone

Der Banking-Trojaner Urlzone verwendet einen neuen Trick, um nicht aufzufallen: Er klaut nicht nur Zugangsdaten und macht Screenshots von Überweisungen, sondern er manipuliert auch die Anzeige des Kontostands im Browser. Damit verhindert der Schädling, dass ein aufmerksam gewordener Banking-Nutzer ihm auf die Schliche kommt.

Einzig ein Besuch bei der Bank vor Ort oder ein Kontoauszugsdrucker bringen den echten Kontostand zutage. Als zusätzliche Vorsichtsmassnahme klaut Urlzone nur niedrige Beträge und achtet darauf, dass das Konto nicht ins Minus gerät.

Aufgefallen ist der neue Banking-Trojaner zuerst in Deutschland. Der Sicherheitsanbieter Finjan hat berichtet, dass deutschen Kunden in nur 22 Tagen fast 300'000 Euro durch Urlzone geklaut wurden. Vermutlich ist dies jedoch nur die Spitze des Eisbergs.

Banking-Trojaner jagen mit Anti-Malware 1.41: Nur ein *Vollständiger Scan* bringt zutage, ob sich Trojaner auf dem Computer verbergen oder nicht (Bild A).

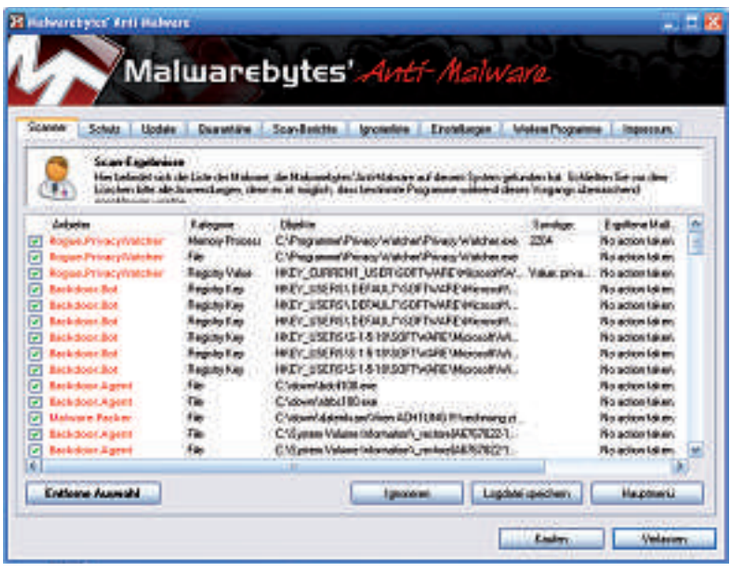
Banking-Trojaner entfernen

Banking-Trojaner verhalten sich extrem unauffällig, um möglichst lange im Verborgenen ihr schmutziges Handwerk zu verfolgen. Man kann sich deswegen nie hundertprozentig sicher sein, dass der eigene Rechner nicht doch verseucht ist. Kostenlose Spezial-Tools wie Anti-Malware 1.41 ▶

und Antivir Rescue-System 3.6.9 helfen bei der Suche nach Banking-Trojanern und entfernen diese auch gleich.

Anti-Malware 1.41

Anti-Malware 1.41 (kostenlos, **www.malwarebytes.org/mbam.php** und auf DVD) ist ein mächtiges Reinigungs-Tool, das viele Trojaner erkennt und zuverlässig entfernt. Die Freeware-Version sucht und löscht Schädlinge und hat keine Einschränkungen in den Kernfunktionen. Die Kaufversion für 30 Franken bietet zusätzlich einen Hintergrundschutz sowie die Möglichkeit, Zeitpläne für Aktualisierungen und für Suchvorgänge einzurichten.



Desinfektion mit Anti-Malware 1.41: Auf vielen mit Banking-Trojanern verseuchten PCs spürt das Sicherheits-Tool mehr als nur einen Schädling auf (Bild B).

So geht's: Starten Sie das Setup und klicken Sie auf *OK* sowie auf *Weiter*. Wählen Sie dann *Ich akzeptiere die Vereinbarung* und bestätigen Sie danach fünf Mal mit *Weiter* sowie zuletzt mit *Installieren*. Ein Klick auf *Fertigstellen* startet anschliessend das Schutzprogramm und aktualisiert auch gleich die Signaturen. Bestätigen Sie das kleine Infofenster mit *OK*, das die erfolgreiche Aktualisierung meldet. Das Tool ist nun einsatzbereit.

Markieren Sie auf dem Reiter *Scanner* die Option *Vollständigen Suchlauf durchführen* und klicken Sie auf *Scan*. Es öffnet sich ein kleines Fenster, in dem Sie vor jedes zu prüfende Laufwerk ein Häkchen setzen. Mit *Scan starten* beginnen Sie mit der Suche nach Banking-Trojanern auf Ihrem Computer (Bild A).

Bestätigen Sie das Ende des Suchlaufs mit *OK* und klicken Sie danach auf *Ergebnisse anzeigen*. Schliessen Sie jedoch zuerst alle geöffneten Anwendungen, bevor Sie mit *Entferne Auswahl* die gefundenen Schädlinge in Quarantäne verschieben. Es kommt sonst möglicherweise zu Problemen bei der Desinfektion Ihres PCs (Bild B).

Anti-Malware öffnet nach der Bereinigung automatisch ein Fenster mit einem Protokoll, welche Schädlinge gefunden und entfernt wurden. Sie finden diese Protokolldatei im TXT-Format auch im Unterordner *Logs* unterhalb des Installationsverzeichnisses von Anti-Malware.

Eventuell öffnet Anti-Malware ausserdem ein Hinweisfenster mit mehreren Einträgen, die erst mit einem Neustart des Computers entfernt werden können. Klicken Sie in diesem Fall auf *Ja*, um den PC neu zu starten und die Bereinigung abzuschliessen.

Anti-Rootkit 1.5

Viele Banking-Trojaner verstekken sich mit denselben Tricks wie Rootkits. Ein Rootkit manipuliert wichtige Systemtreiber und den Windows-Kernel, um sich so vor Virenscannern und im Windows-Explorer unsichtbar zu machen. Anti-Rootkit 1.5 (kostenlos, **www.sophos.de/products/free-tools/sophos-antirootkit.html** und auf DVD) von Sophos erkennt und entfernt auch unbekannte Rootkits.

So geht's: Installieren Sie das Tool und klicken Sie auf *Ja*, um das Programm direkt anschliessend zu starten. Mit *Start scan* beginnen Sie mit der Suche nach aktivierten Rootkits auf Ihrem PC. Das Sicherheits-Tool prüft die laufenden Prozesse und sucht in der Windows-Registry nach Hinweisen auf Schädlinge. Setzen Sie anschliessend je ein Häkchen vor jeden gefundenen Eintrag, den Sie entfernen wollen (Bild C).

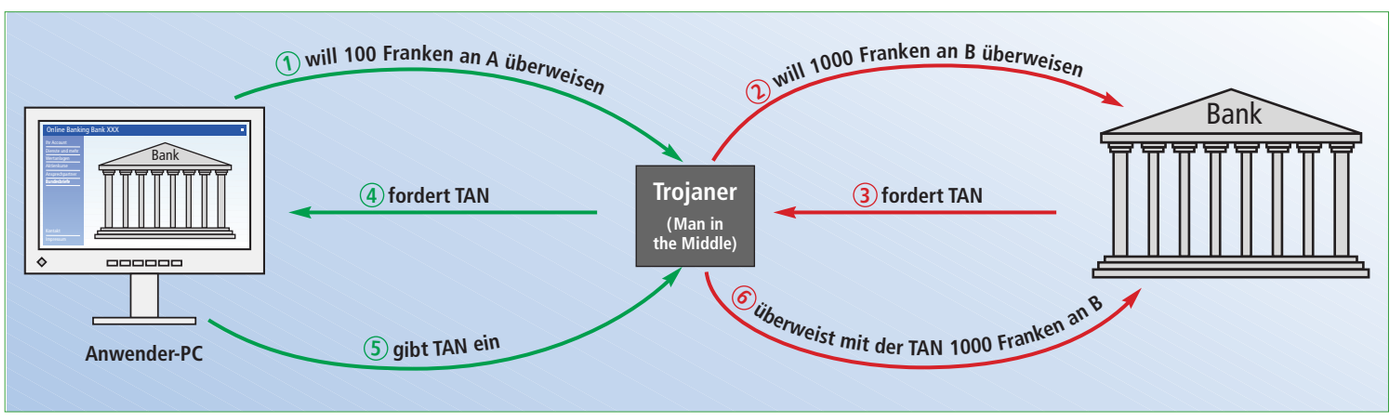
Manche Einträge wie laufende Prozesse lassen sich jedoch nicht bereinigen. Diese müssen Sie zuerst über den Task-Manager beenden und die Dateien dann im Windows-Explorer löschen. Mit *Clean up checked items* entfernen Sie gefundene Rootkits.

Antivir Rescue-System 3.6.9

Prüfen Sie Ihren PC zusätzlich mit dem Rescue System 3.6.9 von Avira (kostenlos, **www.free-av.de/de/tools/12/avira_antivir_rescue_system.html** und auf DVD). Dabei handelt es sich ▶

Man-in-the-Middle-Angriff: Das Prinzip

Ein Banking-Trojaner ändert die geplante Überweisung von 100 Franken an A heimlich in 1000 Franken an B. Während der Anwender glaubt, mit seiner TAN die Originalüberweisung freizugeben, verwendet der Schädling die TAN, um seine eigene Transaktion durchzuführen.



Community36 – die etwas andere Orbit

Die Zukunft verlangt nach neuen, kreativen Lösungen. Die Community36 bietet die Plattform dafür.

Community36 ist mehr als eine Plattform für die Präsentation von Waren, für die Darstellung von Dienstleistungen, für das Aufreihen von Neuheiten; mehr als ein Gefäss für Networking, als eine Austauschbasis von Informationen, als ein Durchlauferhitzer von Wissen; mehr als eine aktuelle Bühne für Branchen-Diskussionen mit anschliessendem Apéro-Smalltalk… **Community36 ist alles zusammen und darum viel mehr:**

Sie ist authentisches und aktuelles Kompetenzzentrum der ICT Schweiz mit Aktivitäten in allen Bereichen zur Förderung des persönlichen und institutionellen Fortschritts.

United Events of Switzerland

Das Konzept der Commuity36 ist von seiner Ausrichtung her geeignet, verschiedenste Events unter einem Dach zu vereinigen. Die Plattform bietet neuen und bestehenden Veranstaltungen Gelegenheit, sich mit ihrem eigenen Branding der Community36 anzuschliessen.

Der Main Event

Der Main Event eröffnet viele neue Möglichkeiten, die Angebote und Dienstleistungen zu präsentieren, Kunden zu pflegen und das Netzwerk auszubauen. Dieser Code hält einige Spielregeln fest, damit die Community36 erfolgreich funktioniert und das Neben- und Miteinander nicht aufregend, sondern möglichst anregend verläuft.

Community Code

Day Code

- Ihre **Stores** sind **alle** geöffnet und besetzt: Business as usual von 10 bis 17 Uhr.
- In den **Meeting Rooms** finden stundenweise Sitzungen statt.
- Die **Business Lounge** bietet freien Cateringbetrieb.
- In der **Members' Lounge** finden Besprechungen statt, oder man nutzt die Lounge zum Relaxen.
- Im **Presenters' Corner** haben alle Presenter die Möglichkeit, Firmenpräsentationen, Fachreferate, Marketing-Vorträge, Lancierungs-Shows oder ähnliche Veranstaltungen abzuhalten – für geladene Gäste oder bei freiem Eintritt.

Night Code

- Ab 17 Uhr wechselt die Community über zum Business Networking.
- Ihren **Store** können Sie so lange betreiben wie Sie es für sinnvoll halten.
- In den **Meeting Rooms** finden späte Sitzungen statt, man trifft sich zu einem Umtrunk oder zu Breakfast-Meetings im kleinen Kreis.
- Die **Business Lounge** bietet freien Cateringbetrieb und Animation (z.B. Sport-TV, Filme o.ä.).
- **Members' Lounge** und **Presenters' Corner** werden zusammen zur **Business Networking Zone**. Hier finden jetzt in Folge individuell durch Presenters oder Dritte organisierte Anlässe statt (z.B. Afterworkparty, Kunden-Event, Night Owls' Party, Chill Out, Breakfast Club).

Dieser Code will Ihrer Fantasie in keiner Weise Grenzen setzen.

Der Main Event – 6. und 7. Mai 2010

Messezentrum Zürich, Zürich-Oerlikon, CH, Schweiz

Community36 ist mehr als ein alljährlicher Marktplatz. Sie bietet ganzjährig geschäftliche Veranstaltungen, interessante Konferenzen, Networking-Plattformen sowie gesellschaftliche Anlässe wie eigene Lounges an begehrten Sport- und Kulturanlässen. Und vieles mehr...

Als Member werden Sie regelmässig mit den aktuellsten Infos versorgt. Ausserdem haben Sie zu allen Messen der Exhibit & More freien Zutritt. Infos: **www.community36.net**

Weitere Infos und Anmeldung: www.community36.ch

um eine bootfähige CD, die Ihren PC mit Antivir von Avira prüft, ohne dass Windows läuft. Das hat den Vorteil, dass sich ein Banking-Trojaner nicht aktivieren und verstecken kann.

So geht's: Klicken Sie doppelt auf die EXE-Datei des Rescue-Systems. Es öffnet sich ein integriertes Brennprogramm, mit dem Sie eine CD-ROM brennen. Legen Sie dazu einen CD-Rohling ein und klicken Sie danach auf *Brenne CD*.

Wenn Sie die CD lieber mit Ihrem Standard-Brennprogramm erstellen wollen, klicken Sie auf *Beenden* und bestätigen Sie die folgende Frage mit *Ja*. Danach geben Sie den Speicherort sowie einen Namen für die ISO-Datei an und brennen die CD.

Legen Sie danach die frisch gebrannte CD in Ihr CD-ROM-Laufwerk ein und starten Sie Ihren PC neu. Eventuell müssen Sie danach noch die Boot-Reihenfolge im BIOS ändern, wenn Ihr Computer nicht von der eingelegten CD startet.

Drücken Sie die Eingabetaste, sobald das Boot-Fenster des Rescue-Systems erscheint (Bild D). Danach startet das Live-System.

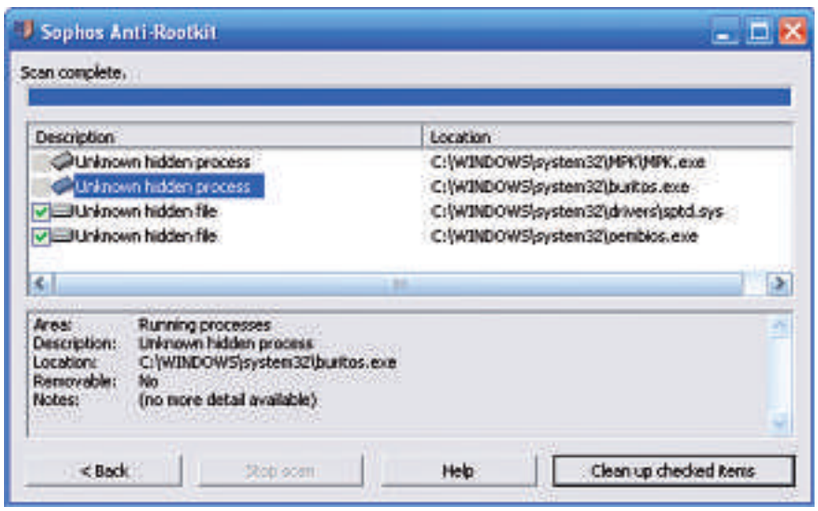
Bevor Sie anschliessend Ihren PC checken, sollten Sie zuerst noch den enthaltenen Virenscanner und die verwendeten Signaturen aktualisieren. Klicken Sie dazu auf *Update* und bestätigen Sie danach mit *Ja*. Sofern eine Online-Verbindung besteht, aktualisiert das Rescue-System sich nun über das Internet.

Wenn Sie einen DSL-Router mit integriertem DHCP-Server verwenden, klappt die Internetverbindung automatisch. Ansonsten müssen Sie sich jeweils ein neues Rescue-System herunterladen und auf CD brennen, um den Check immer mit einem aktuellen System durchzuführen.

Klicken Sie nun auf *Scanner starten*, um mit der Überprüfung des Computers zu beginnen. Rechts unten sehen Sie eine Übersicht der entdeckten Schädlinge. In der Standardeinstellung protokolliert das Rescue-System gefundene Schädlinge nur und löscht sie nicht.

Klicken Sie auf *Konfiguration* und wählen Sie anschliessend *Versuchen, infizierte Dateien zu reparieren* aus, um Schädlinge zu entfernen und gleichzeitig Datenverlust zu vermeiden. Setzen Sie zudem noch das Häkchen vor *Dateien umbenennen, wenn sie nicht repariert werden können?*.

Vorsicht: Wenn Sie die Option *Infizierte Dateien löschen* auswählen, werden wichtige Dateien eventuell unwiederbringlich gelöscht. Diese Auswahl sollten Sie deshalb nur in Ausnahmefällen nutzen.



Rootkits entfernen mit Anti-Rootkit 1.5: Das kostenlose Tool des Antiviren-Herstellers Sophos dringt tief ins System ein und spürt so Rootkits auf (Bild C).

Schutz vor Banking-Trojanern

Nur ein Teil der aktuell von den Banken angebotenen Verfahren ist sicher gegen Banking-Trojaner. Beim herkömmlichen TAN-Verfahren etwa fängt ein heimlich auf dem PC vorhandener Schädling problemlos jede TAN ab und verwendet sie für eigene Überweisungen.

Unsichere Banking-Verfahren

Keinen Schutz gegen Banking-Trojaner bieten die Verfahren TAN, iTAN, eTAN sowie Smart TAN.

Bei all diesen Verfahren sind die TANs unabhängig von der Transaktion einsetzbar. Ein Banking-Trojaner kann also die eingegebene Nummer dazu verwenden, eine ganz andere als die angezeigte Transaktion auszuführen. Dabei ist es nicht relevant, ob der Kunde die Transaktionsnummer von einer fixen Liste abliest oder ob er sie mit einem Generator wie beim Smart-TAN-Verfahren erstellt. Auch bei diesem technisch aufwendigeren Verfahren werden die TANs in einer vorgegebenen Reihenfolge erstellt und sind nicht abhängig von der aktuellen Transaktion.

Sichere Banking-Verfahren

Diese Verfahren sind sicher gegen Banking-Trojaner: mTAN, Smart TAN plus, Flickercode, HBCI und Secoder.

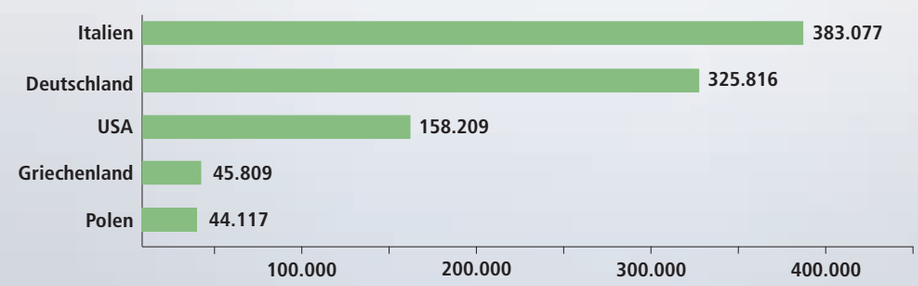
mTAN: Beim mTAN-Verfahren – das *m* steht für *mobil* – erhält der Bankkunde keine TAN-Liste mehr von seiner Bank. Stattdessen sendet ihm das Finanzinstitut für jede Transaktion eine TAN per SMS auf sein Handy (Bild E). Die per Mobilfunk übermittelte TAN muss der Kunde dann im Browser eingeben, um die aktuelle Transaktion freizugeben.

Weil die TAN nur für diese eine Transaktion gültig ist, hat ein Banking-Trojaner keine Chance, die Überweisung zu manipulieren. Vergewissern Sie sich allerdings zuerst bei Ihrer Bank, ob diese auch tatsächlich eine nur für eine bestimmte Transaktion gültige TAN erstellt oder ob sie wiederum nur mit einer Liste arbeitet, die statt bei Ihnen zu Hause im Rechenzentrum der Bank verwaltet wird. Im letzteren Fall bietet das Verfahren keinen Vorteil gegenüber einem klassischen TAN-Verfahren.

Smart TAN plus: Smart TAN plus beziehungsweise ChipTAN ist ein Zweischrittverfahren, das keine Manipulation einer Überweisung durch einen Banking-Trojaner mehr zulässt.

Verbreitung des Trojaners Sinowal

Der Banking-Trojaner Sinowal hat ein weltweites Bot-Netz aufgebaut. Forscher sind in dieses Netz eingedrungen und haben die Anzahl der IP-Adressen – siehe Grafik – der gekaperten PCs protokolliert. Die Grafik zeigt, in welchen Ländern Sinowal besonders aktiv ist.

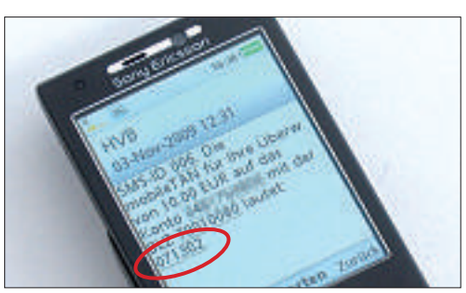


Quelle: University of California

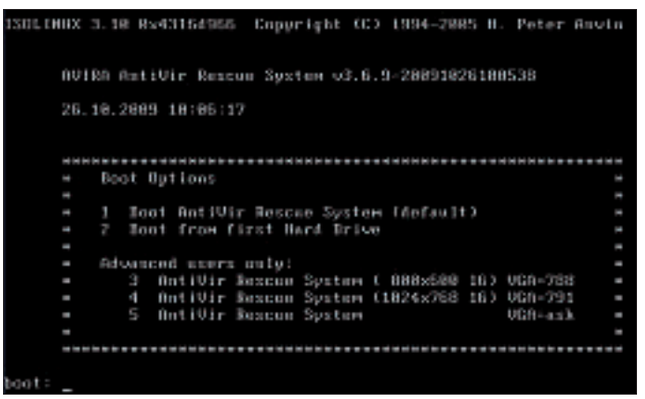
Um es zu nutzen, benötigt der Anwender einen speziellen TAN-Generator, in den er seine Kontokarte einsteckt. Danach füllt er das Überweisungsformular im Browser aus. Daraus errechnet die Bank einen Zifferncode, den der Kunde in seinen TAN-Generator zusammen mit den ersten sechs Ziffern der Kontonummer des Zielkontos eingibt. Das Gerät zeigt nun eine TAN an, die nur für diese eine Überweisung gilt und im Browser eingegeben werden muss, um die Transaktion freizugeben.

Flickercode: Der Flickercode ist eine Weiterentwicklung des Smart-TAN-plus-Verfahrens. Statt des Zifferncodes generiert die Bank hier eine animierte Grafik, die sie im Browser anzeigt.

Der Anwender benötigt einen speziellen TAN-Generator, den er vor den Bildschirm hält. Auf der Rückseite des Geräts befindet sich ein Rezeptor, der das Flackern (englisch: to flicker) der Animation entschlüsselt. Die übermittelten Informationen zeigt das Gerät dann zur Kontrolle im Display an. Anschliessend erstellt es eine an die Transaktion gebundene TAN, die der Bankkunde im Browser eingibt.



Keine Chance für Manipulationen: Die TAN in der SMS ist nur für die Überweisung gültig, die der Screenshot oben zeigt (Bild E).



Hier bootet das Antivir Rescue-System 3.6.9: Wenn der PC von dieser kostenlosen Live-CD und nicht mit Windows gestartet wird, kann sich ein Banking-Trojaner nicht aktivieren und schützen (Bild D).

HBCI und Secoder: Home Banking Computer Interface (HBCI) beziehungsweise FinTS (Financial Transaction Services) funktioniert ohne TANs. Stattdessen signiert der Kunde eine Transaktion mit der Eingabe seiner PIN und mit einem geheimen Schlüssel, der auf seiner Karte hinterlegt ist. Diese Signatur gilt ausschliesslich für diese eine Überweisung. Weil sie in der Karte erstellt wird, kann sie auch nicht klammheimlich von einem Banking-Trojaner ausgelesen werden.

Das Verfahren wird häufig zusammen mit Homebanking-Software eingesetzt. Problematisch ist, wenn die PIN mit der Tastatur des PCs eingegeben wird, da sie dort wiederum von einem Trojaner erlauscht werden kann. Eine Weiterentwicklung von HBCI ist das Secoder-Verfahren, bei dem der Kartenleser zusätzlich mit einem Display ausgestattet ist. ■

Andreas Th. Fischer