INTERNET

Krank durch Surfen

Eine neue Bedrohung geistert durchs Netz: Computerviren, die Rechner schon beim Aufrufen ganz normaler Web-Seiten infizieren.

Fast wirkt es, als hätte der unheimliche Erreger eine Art bösen Blick, der dem Opfer schon durchs Anschauen Unheil bringt. Und das geht so: Nichtsahnend ruft der Nutzer im Internet eine äußerlich unauffällige Web-Seite auf – schon wird sein Rechner mit einem Schadprogramm infiziert, das unbemerkt im Hintergrund nach Kontodaten sucht oder unerwünschte Werbung verschickt.

Nach diesem Prinzip funktioniert „Mpack“: ein neuartiger Computervirus, der sich im Code von ganz normalen Internet-Seiten versteckt. Über 300 000 Seiten sind bereits verseucht, schätzt Panda Software, ein Hersteller von Antivirensoftware aus Madrid. Die Betreiber wissen von der verheerenden Wirkung ihrer Websites ebenso wenig wie die Nutzer, die beim Betrachten der Seiten ungewollt ihre eigenen Rechner anstecken. Über eine Million Computer haben sich den „Mpack“-Virus in den vergangenen zwei Wochen angeblich schon eingefangen.

Der bunte Mutantenzoo aus digitalen Viren und Würmern ist damit um eine exotische Gattung reicher. Herkömmliche Vorsichtsregeln greifen meist nicht. Bislang verbreiteten sich digitale Schädlinge vor allem per E-Mail. Oft war es dabei notwendig, dass das Opfer aus Neugier einen mitgeschickten Dateianhang per Mausklick öffnet.

Bei dem aktuellen Infektionsweg reicht es bereits aus, eine verseuchte Internet-Seite einfach nur aufzurufen – schon wird binnen Sekunden im Hintergrund automatisch eine zweite Verbindung aufgebaut, die unbemerkt eine kleine Schadsoftware herunterlädt; diese wiederum installiert eine heimliche Hintertür im Rechner, durch die nun Kriminelle nach und nach weitere versteckte Programme einschmuggeln können (siehe Grafik).

Die neue Gefahr im Internet wird paradoxerweise dadurch gefördert, dass die Betriebssysteme sicherer geworden sind. Windows zum Beispiel galt lange als legendär einbruchsgefährdet; das neue „Vista“ hingegen macht es mit vielen Tricks und Kniffen Angreifern sehr viel schwerer, die Kontrolle über den Rechner zu gewinnen.

Die Cyberkriminellen reagieren auf die verbesserte Sicherheit der Betriebssysteme wie gewöhnliche Einbrecher: Je besser die Eingangstür verrammelt ist, desto eher steigen sie durchs Fenster ein – im Falle des Internet eben durch das Browserfenster. Denn während der Kernbereich der Rechner zur Datenfestung umgebaut wurde, gleicht die Surfsoftware eher einem chaotischen Abenteuerspielplatz.

Anfangs waren Browser nur schlichte Anzeigefenster für Texte und Bilder; doch um Nutzer anzulocken, haben die Programmierer daraus wahre Alleskönner gemacht.

Schließlich geht es um viel: Wer den Browsermarkt beherrscht, der kontrolliert den Zugang zur Online-Welt. So tobt derzeit der „Zweite Browserkrieg“ – im „Ersten Browserkrieg“ hatte sich Microsoft mit seinem „Internet Explorer“ um die Jahrtausendwende gegen den „Navigator“ von Netscape durchgesetzt.

Doch das Quasimonopol wankt. Im derzeitigen Browserkrieg konnte der Herausforderer „Firefox“ dem Platzhirschen von Microsoft immerhin schon über zehn Prozent Marktanteil abjagen. Und Mitte Juni gab auch Apple bekannt, in den globalen Wettkampf einzusteigen mit seiner eigenen Software namens „Safari“, die vorher nur für Apple-Computer verfügbar war.

Im Kampf um die Vorherrschaft versuchen sich die Browserhersteller mit immer neuen Sonderfunktionen gegenseitig zu übertrumpfen. Alles was Nutzer heute brauchen, ist ein Rechner mit Internet-Zugang – schon können sie mit den kostenlos verfügbaren Browsern Texte schreiben, Tabellen erstellen, Computergames spielen oder Fotos bearbeiten; die Anschaffung teurer Spezialprogramme ist nicht mehr erforderlich. „Browser sind vom Funktionsumfang her schon fast so etwas wie eigene kleine Betriebssysteme“, sagt Jeff Jones vom Sicherheitsteam bei Microsoft.

Zudem versprechen einige Browser wie „Firefox“ oder „Opera“ den Brückenschlag zwischen den oft getrennten Systeminseln Windows, Apple und Linux. Sogar Handys lassen sich so in die Welt der Netzwerkrechner eingemeinden. Die Kehrseite dieser Vereinheitlichung: Wenn Datenkriminelle Sicherheitslücken in einem Browser finden, halten sie damit möglicherweise einen wirksamen Universaldietrich in Händen, der weiter reichend als je zuvor den Einbruch in Notebooks, Server, Handys und Navigationsgeräte ermöglicht.

Wie ein guter Dietrich hinterlässt auch „Mpack“ kaum Einbruchsspuren, und diese Unauffälligkeit macht es gefährlich: Das Einschmuggeln der Hintertür bringt den Rechner nicht zum Absturz. Eine solche unbemerkte Infektion ist weitaus gefährlicher als der altbekannte Virenvandalismus, weil die Eindringlinge über lange Zeit ihr Unwesen treiben können.

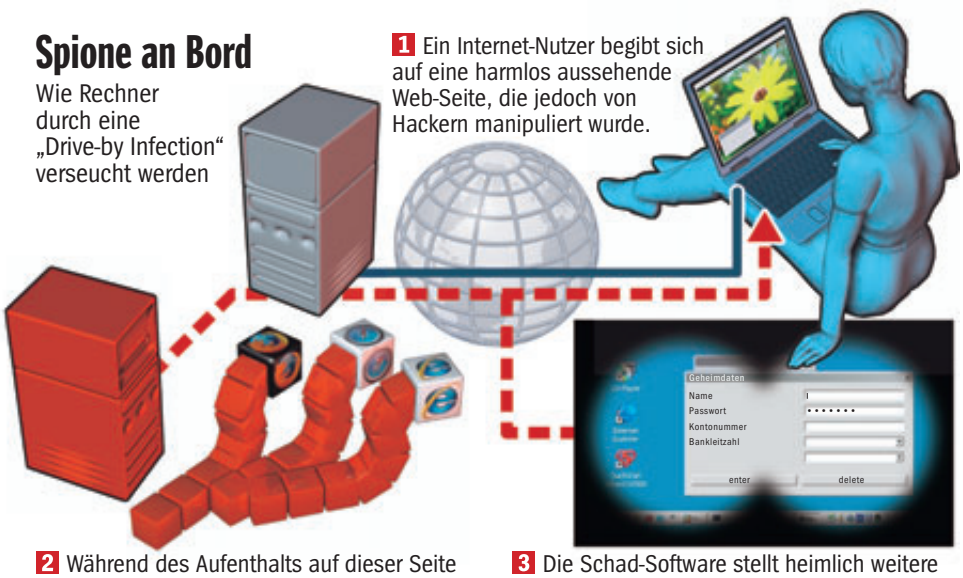
Die Browserbanditen agieren ohnehin immer professioneller. Über acht Updates sind bereits von „Mpack“ im Umlauf, offensichtlich programmiert von einer russischsprachigen Gang. Vor der Auslieferung an kriminelle Kunden wird „Mpack“ angeblich einer ausgiebigen Qualitätskontrolle unterzogen und stößt auf reges Interesse bei den kriminellen Käufern.

Der Schwarzmarktpreis des Virus zog mit jedem Update in den vergangenen Wochen deutlich an, von rund 700 auf derzeit etwa 1000 Euro.

HILMAR SCHMUNDT

Spione an Bord

Wie Rechner durch eine „Drive-by Infection“ verseucht werden



1 Ein Internet-Nutzer begibt sich auf eine harmlos aussehende Web-Seite, die jedoch von Hackern manipuliert wurde.

2 Während des Aufenthalts auf dieser Seite wird heimlich Kontakt zu einem weiteren Server hergestellt, der u. a. analysiert, welchen Browser der Surfer benutzt (z. B. „Internet Explorer“, „Safari“, „Firefox“). Die jeweils passende Schad-Software wird anschließend unbemerkt auf den Nutzerrechner überspielt.

3 Die Schad-Software stellt heimlich weitere Serververbindungen her, über die u. a. Spy-Software installiert werden kann. Unbemerkt protokollieren diese Schnüffelprogramme dann beispielsweise jede Tastatureingabe, suchen nach Bankdaten und Passwörtern und verschicken diese automatisch an die Hacker.

DER SPIEGEL