All About SECURITY
www.all-about-security.de
Das unabhängige Security Portal

11.02.09

Von: Jan Valcke

Vasco

Keylogger im Sandkasten

Doktoranden von der Uni Mannheim schlugen Hacker mit ihren eigenen Waffen: Mit Hilfe eines ungeschützten, aber präparierten Rechners spionierten sie Spionageprogramme aus. Die Ergebnisse ihrer Studie zeigen einmal mehr, wie wichtig Strong Authentication ist.

Dass so genannte **Keylogger** ahnungslosen PC-Nutzern bei der Eingabe ihrer Passwörter über die Schulter schauen, ist keine neue Erkenntnis. Neu ist aber eine Studie, in der Thorsten Holz, Markus Engelberth und Felix Freiling vom Laboratory for Dependable Systems an der Universität Mannheim diese Schadprogramme und die von ihnen ausspionierten Daten wissenschaftlich analysierten. Zwei momentan sehr verbreitete Keylogger wurden dabei besonders genau betrachtet.

Malware unter Beobachtung

Die Malware-Familie Limbo/Nethell verbreitet sich üblicherweise über infizierte Web-Sites, auf die die Opfer zum Beispiel über fingierte DNS-Server umgeleitet werden (Drive by Pharming). Die Malware wird dann als Browser Helper Object (BHO) eingeschleust. BHOs reagieren als Plugin für Internet Explorer auf Browser-Events, zum Beispiel Navigation, Tastatureingaben oder Page Loads. Mit freundlicher Unterstützung des Microsoft Browsers kann Limbo auf das Document Object Model einer Internet-Seite zugreifen und so die Felder finden, in denen Account-Daten eingegeben werden. Diese Daten sendet Limbo dann an einen vom Hacker betriebenen Sammelpunkt, zu einer so genannten Dropzone.

Technisch versierter als Limbo ist die ZeuS/Zbot/Wsnpoem-Familie. Sie gelangt über verseuchte e-Mail-Anhänge in den Rechner. Die Träger-e-Mails werden wieder mit diversen Tricks als vertrauenswürdig getarnt (Spear Phishing). Auch hier ist der anfällige Internet-Explorer wieder der Angriffspunkt. Ist er erst einmal infiziert, fängt Zeus http POST Requests ab und ermittelt so sensible Daten. Registriert der digitale Schnüffler, dass man sich auf einer für Verbrecher interessanten Stelle befindet, macht er nach jedem Klick auf die linke Maustaste einen 50 x 50 Pixel großen Screenshot rund um die Cursorposition. Viele Banken bieten nämlich bereits die Eingabe von Passwörtern per Maus an. Das hilft gegen Limbo und Konsorten, nicht aber gegen Zeus. Auch Zeus liefert die gestohlenen Daten brav in der Dropzone ab.

Back to the Roots

Was die PC-Viren nicht ahnen konnten: Die Wissenschaftler der Uni Mannheim schauten ihnen aufmerksam bei der Arbeit zu. Sie ließen einen vermeintlich ungeschützten Rechner absichtlich infizieren. Auf diesem Testsystem war aber das Tool CWSandbox installiert, ebenfalls eine Entwicklung der Mannheimer Computerfreaks. CWSandbox lässt den Virus einige Zeit in einer geschützten Umgebung laufen und beobachtet genau sein Verhalten. So manche Malware wird allerdings erst nach typischen Anwendereingaben aktiv. Daher programmierten die Virusjäger ein Tool namens SimUser, das dem Spionageprogramm einen Dialog vorgaukelt.

Die auf diese Weise getäuschten Keylogger nahmen denn auch prompt Kontakt zur Dropzone auf und offenbarten so die Sammelpunkte des digitalen Diebesgutes. Und viele Kriminelle stehen ihren Opfern an Sorglosigkeit in nichts nach: Sie schützen ihre Drop-Zones nicht gegen „unbefugten“ Zugriff, so dass die Autoren der Studie mit relativ simplen Tricks an die hinterlegten Daten herankamen. Dazu reichte oft ein Zugang zum Standard-Server-Verzeichnis. „Wir haben nicht gedacht, dass das so einfach ist“, gibt sich Thorsten Holz gegenüber Spiegel Online schadenfroh.

Persönliche Daten auf dem Weg gen Osten

Dass so mancher Computerkriminelle das Pulver auch nicht gerade erfunden hat, ändert aber nichts an den prinzipiellen Schwächen in der immer noch gängigen Authentisierungspraxis. Denn was die Forscher aus zwielichtigen Dropzones zu Tage förderten, ist in der Tat besorgniserregend.

164.000 infizierte Rechner ermittelte die Studie allein bei Limbo. Der emsige Schädling hatte im Untersuchungszeitraum von April bis Oktober 28 GByte vertrauliche Daten eingesammelt. Als beliebtester Standort für die Dropzones erwies sich Estland, wo eine beobachtete Dropzone 133 Tage lang ungestört in Betrieb war. Rekordhalter bei den Limbo-Opfern war ein Rechner, auf dem der Virus mehr als 111 Tagelang anscheinend unbemerkt sein Unwesen trieb.

Paypal und Visa im Visier

Bevorzugtes Angriffsziel im Banking-Bereich war die Bezahlseite PayPal mit 2.263 gestohlenen Accounts, bei Kreditkarten lag Visa mit 3.764 abgegriffenen Nummern ganz oben auf der Hitliste der Schattenwirtschaft. Aber nicht nur Bankdaten sind für Limbo, Zeus und Konsorten von Interesse. Ganz nebenbei schnappten sie sich auch 66.540 Web-Mail-Accounts von Windows Live, dazu noch 14.698 Facebook-Zugänge.

Lohnend ist das für den Hacker auf jeden Fall. Nach Erhebungen von Sicherheitsfirmen werden auf dem Schwarzmarkt für einen gestohlenen Bank-Account 10 bis 1000 Dollar bezahlt – je nach Bonität des Opfers. Für Kreditkartendaten gibt es 40 Cent bis 20 Dollar, und Identitäten aus sozialen Netzwerken finden für 1 bis 15 Dollar ihre Abnehmer.

Nur die Spitze des Eisbergs

Wohl gemerkt: Die Mannheimer Ergebnisse zeigen nur die Spitze des Eisbergs, obwohl etwa 2000 Keylogger untersucht wurden. Die Dunkelziffer liegt natürlich weitaus höher. Eines zeigt aber diese Studie ganz deutlich. Herkömmliche statische Passwörter sind unsicher und sollten auch bei vermeintlich ungefährdeten Accounts nicht mehr eingesetzt werden – von Online-Banking ganz zu schweigen. Das Risiko, dass die persönlichen Daten in falsche Hände geraten, ist einfach zu groß, trotz ständiger Mahnung zur Vorsicht, trotz Virenscanner und Firewall.

Strong Authentication gegen den Datenklau

Dabei ließe sich den Keyloggern ihre digitale Ernte ganz einfach verhageln. Strong Authentication schützt zuverlässig vor Pishing und Account-Diebstahl. Unter diesem Fachbegriff werden Zugangssysteme zusammengefasst, die zur Identitätsprüfung mehrere Schritte verwenden. Am gängigsten sind dabei Zwei-Faktor-Authentisierungen. Wer sich einloggen will, muss etwas besitzen, zum Beispiel eine spezielle Hardware oder ein Software Token, und etwas wissen, also eine PIN. Beim Digipass-System von Vasco zum Beispiel gibt der Anwender seine PIN in ein spezielles Gerät ein. Dieses errechnet dann ein dynamisches Einmal-Passwort (One Time Passwort, OTP). Es ändert sich alle 36 Sekunden. Damit wird der Inhalte der Dropzone zum Datenmüll. Ausspionierte Passwörter bleiben nutzlos, denn bei jedem Login ist ja ein neues im Einsatz. Die Passwörter braucht der Anwender weder im Kopf zu behalten, noch muss er sie ständig selbst ändern.

Sicherheit nach Maß

Zwei-Faktor-Authentisierung und Einmal-Passwort basieren grundsätzlich auf einer Berechnung aus drei Faktoren:

- ein voreingestellter und geheim gehaltener Wert (Seed Value)
- ein Zeitsignal und/oder ein anderer Event
- ein öffentlicher Algorithmus.

Die Zeit- oder Event-Inputs für den Algorithmus werden intern generiert, um Manipulationen zu vermeiden. In die Berechnung des OTP können auch noch weitere Faktoren einbezogen werden, um die Sicherheit zu erhöhen.

Wie bei jeder Authentisierung gilt es auch bei der Zwei-Faktor-Methode einen sinnvollen Kompromiss zwischen Sicherheitsniveau und Benutzerfreundlichkeit zu schließen. Moderne Systeme wie Vasco Digipass bieten dafür eine ganze Reihe von Konzepten.

Wird nur ein relativ niedriges Sicherheitsniveau verlangt, zum Beispiel beim Abonnement von Online-Zeitungen, reicht ein rein Software-basiertes System. Dabei wird ein kleines Java-Applet auf Rechner, Handy oder PDA heruntergeladen. Es generiert dann das dynamische Passwort aus einem Cookie.

Bereits dieses Verfahren ist für viele Spionageprogramme ein unüberwindliches Hindernis, denn abgefangene Passwörter sind nach spätestens einer halben Minute wieder ungültig. Dennoch bleiben rein Software-basierte Systeme natürlich prinzipiell angreifbar.

Passwort auf Knopfdruck

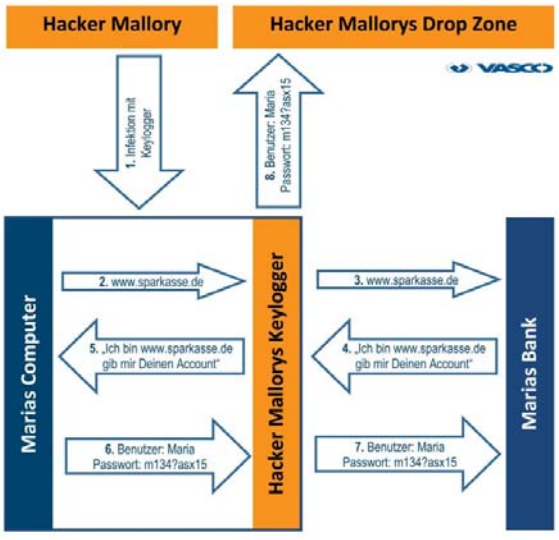
Deutlich sicherer wird die Zwei-Wege-Authentisierung, wenn man die Berechnung des OTP einem externen Gerät überlässt. Im einfachsten Fall ist das ein kaum daumengroßes, zehn Gramm leichtes Kästchen, das auf Knopfdruck ein Einmal-Passwort auf einem LCD anzeigt. Die Zusatz-Hardware hat keinerlei Schnittstellen, eine Manipulation ist ausgeschlossen. Anspruchsvollere Geräte sind noch mit einer Tastatur oder einem Kartenleser ausgerüstet. Dann ist die Eingabe einer PIN oder das Einstecken einer Smart Card erforderlich, um die Hardware zu aktivieren. Ein gestohlenes Gerät ist für den Dieb nutzlos.

Noch mehr Sicherheit bietet das so genannten Challenge-Response-Verfahren. Dabei liefert die Host-Applikation einen zusätzlichen Wert, die so genannte Challenge, den der Anwender zusätzlich zu PIN eingeben muss, um ein gültiges Einmal-Passwort zu generieren. Das Passwort wird dann wiederum vom Host überprüft. Diese Form der Zwei-Wege-Kommunikation stellt sicher, dass auch gefälschte Seiten kein gültiges Password beziehen können. Denn sie können ja nicht den richtigen Challenge-Wert liefern.

Die Mannheimer Ergebnisse sind alarmierend, aber simple Keylogger sind bei weitem nicht die einzige Gemeinheit der Digital-Langfinger. Spear Phishing, Drive-by-Pharming werden noch so manchem Online-Nutzer viel Geld kosten. Man-in-the-Middle-Angriffe gehören zwar in Deutschland noch nicht zu Standard-Repertoire der Hacker, es dürfte allerdings nur noch eine Frage der Zeit sein, bis auch Transaktionsverfälschungen durch unbemerkt zwischengeschaltete Malware an der Tagesordnung sind. Dagegen kann man sich nur mit einer digitalen Signatur schützen. Sie bezieht die Details einer Transaktion ebenfalls in die Authentisierung mit ein.
Wir sollten umdenken.

Jan Valcke, seit 2002 President und COO bei Vasco Data Security, Belgien

www.vasco.com



Bildupload

Schematische Darstellung einer Keylogger-Attacke: Hacker Mallory infiziert Marias Rechner mit einem Spionageprogramm. Dieses erkennt an Marias Eingaben ein lohnendes Ziel und protokolliert, von Maria unbemerkt, was sie eintippt, oder macht Screenshots von der Umgebung des Cursors. Die so gestohlenen Informationen sendet der Keylogger dann an einen zentralen Sammelpunkt, die so genannte Drop Zone. So wie Maria werden viele ahnungslose PC-Usern zu Mallorys Opfern, so dass sich in der Dropzone schnell Gigabytes von persönlichen Daten sammeln.
Grafik: Vasco

Digipass Go 7: Das kompakte Sicherheits-Token liefert ein Einmal-Passwort. Die Dropzone wird damit zur wertlosen Daten-Müllhalde.
(Foto: Vasco)