DIGITAL **MALVERTISING** 11.05.16

So gefährlich ist die dunkle Seite der Online-Werbung

Für Google und Facebook ist sie das Lebenselixier: Online-Werbung. Die lukrative Reklame wird tausendfach auf Rechnern ausgespielt. Deshalb kann sie zum perfekten Einfallstor für Hacker werden.

Von Benedikt Fuest
Korrespondent für Innovation, Netzwelt und IT

Manchmal sehen komplizierte Hackerangriffe einfach aus: Thorsten Schröder drückt auf seiner Laptop-Tastatur F5, im Fenster des Internetbrowsers wird eine Seite mit bunten Werbebannern geladen – und plötzlich öffnet sich auf dem Windows -Desktop ein Taschenrechner-Programm. Der Taschenrechner ist harmlos – doch an seiner Statt hätten die Hacker auch eine Schadsoftware starten können, um einen fremden Rechner zu übernehmen.

Foto: AP

Google-Sitz in Mountain View in Silicon Valley. Das Geschäftsmodell des Konzerns basiert zum großen Teil auf Online-Werbung

Dass der Taschenrechner wie von Zauberhand startet, obwohl doch eigentlich nur der Firefox-Browser geöffnet war, zeigt: Hier geht etwas nicht mit rechten Dingen zu. Schuld daran ist das Werbebanner auf der Internetseite, die Schröder aufgerufen hat.

Schröder und sein Freund Frank Rieger sind bekannte Hacker und Sicherheitsberater, die beiden zeigten auf der Internetkonferenz Re:publica, wie sich Internetwerbung dazu ausnutzen lässt, Hackerangriffe auf wildfremde Rechner zu starten. Diese Angriffe heißen "Malvertising" – sie sind extrem gefährlich, da die Hacker nicht auf einen Fehler der Nutzer setzen müssen.

Weder muss der Besitzer eines PCs auf einen verdächtigen Download-Link klicken noch eine infizierte E-Mail öffnen. Stattdessen nutzen die Hacker Internet-Werbenetzwerke zur automatischen Verbreitung ihrer Schadsoftware.

US-Football-Liga betroffen

Diese Netzwerke nehmen Werbeaufträge von Marketingagenturen an und mieten den Platz dafür auf Tausenden Webseiten gleichzeitig an. Wird eine Webseite mit Werbung darauf geladen, lädt der Internetbrowser die Werbebanner vom Server des Werbenetzwerks. Zu den weltweit größten

MEISTGELESENE ARTIKEL


Präsident Erdogan
Das ist die große Schwäche des "Königs von Europa"


Austritt nach 26 Jahren
Sein Facebook-Post entlarvt das ganze Problem der SPD


Talk bei Maischberger
"Ich wollte unbedingt eine Frau haben"

MEISTGELESEN AUF Computer

1. Assassin's Creed: Erster Trailer zum Film ist da!

Netzwerk-Anbietern gehören die US-Internetgiganten Facebook und Google.

Bei einem solchen Netzwerk haben auch Schröder und Rieger – rein aus Demonstrationszwecken – ihre Anzeige geschaltet. Die manipulierten Werbebanner können überall dort im Netz auftauchen, wo Internetwerbung zur Finanzierung von Onlineangeboten genutzt wird. Sobald die Nutzer eine Seite ansurfen, die die Hackerwerbung anzeigt, verlieren sie die Kontrolle über ihren Rechner.

In der Vergangenheit zeigten vor allem Internetseiten aus den schäbigeren Ecken des Internets Malvertising – Opfer der Angriffe waren oft Nutzer von Pornoseiten oder Downloadportalen. Doch inzwischen haben die Täter besser gelernt, ihren Schadcode in der Werbung zu verbergen – und schaffen es deswegen, dass auch renommierte Werbenetzwerke ihre manipulierten Banner annehmen und auf den Webseiten ihrer Kunden ausliefern.

ZUR STARTSEITE

Datenschutz
So verhindern Sie den Missbrauch ihrer Daten im Internet

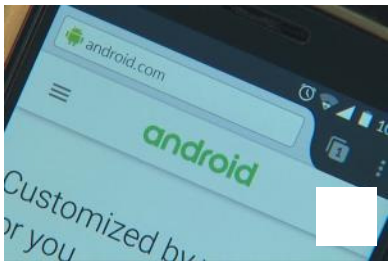
Mitte März bemerkten Sicherheitsforscher des US-Antivirus-Anbieters Malwarebytes, dass die internationale Webseite des britischen Fernsehsenders BBC ihren Lesern Werbebanner mit Schadcode anzeigte – die Seite kommt auf knapp 300 Millionen Besucher pro Monat. Die BBC-Seite war nicht als einzige betroffen: Auch die Internetauftritte von AOL, der "New York Times" sowie der US-Football-Liga NFL zeigten gefährliche Werbebanner.

1000 Angestellte für ein Problem

Über diese infizierten unbekannte Täter die Rechner der Nutzer mit Erpressungs-Trojanern. Ausgeliefert wurden die manipulierten Anzeigen laut der Malwarebytes-Analyse unter anderem über die Plattform Googlesyndication.com, über die das Google-Werbenetzwerk seine Anzeigen ausliefert.

Google erklärte auf Anfrage, dass der Konzern das Problem Malvertising sehr ernst nimmt: Über 1000 Angestellte arbeiten demnach daran, unerwünschte Werbung rechtzeitig zu erkennen. Die von ihnen programmierten Filtersysteme blockierten 2015 über 17 Millionen betrügerische Anzeigen. Ähnliche Filter bietet der Antivirus-Anbieter Symantec unter dem Namen Advantage auch kleineren Werbeunternehmen an.

Dennoch schaffen es versierte Hacker wie Schröder und Rieger, ihre manipulierten Anzeigen an den Filtern vorbeizuschleusen. "Für die Werbenetzwerke ist es teils extrem schwierig, die Schadsoftware zu erkennen", erklärt Sicherheitsforscher Candid Wüest von Symantec.



EU-Kommission
Google missbrauche mit Android Marktbeherrschung

"Internetwerbung ist heute nicht mehr nur ein statisches Banner. Stattdessen können Inhalte auch dynamisch von Drittservern nachgeladen werden. Dann tauschen die Hacker den Inhalt des Banners aus, nachdem es den Filter passiert hat. Alternativ können die Täter ihren Schadcode auch so programmieren, dass er erst verzögert aktiv wird."

Risiko von Schadenersatzklagen

In der Vergangenheit infizierten Hacker die Rechner der Nutzer vor allem mit Spam-Software oder spionierten Mail-Passwörter aus. Doch mittlerweile ist das Hacking-Geschäft lukrativer geworden – mittels sogenannter Crypto-Trojaner verschlüsseln die Hacker die Dateien der Nutzer und erpressen diese dann direkt. Entsprechend höher ist der

2. FIFA 17: Erste Hinweise auf kommende Neuerungen
3. Xiaomi Mi Max: 6,44-Zoll-Smartphone vorgestellt
4. Zuse Z3: Ur-Computer feiert 75. Geburtstag
5. Die besten Programme für iOS und Android

Aufwand, den die Täter treiben, erklärt Wüest.

"Sie investieren für ihre Attacken Tausende Dollar, damit ihre Werbung möglichst häufig auf beliebten Internetseiten angezeigt wird, und nutzen dabei Schwachstellen aus, die teils bereits länger bekannt sind. Die Attacken funktionieren trotzdem, da viele Nutzer ihre Browser nicht regelmäßig updaten." Aktuell, so schätzt Wüest, wird täglich eine neue Schwachstelle pro Browser bekannt – und die Angreifer aktualisieren ihre Schadsoftware meist schneller als die Nutzer ihre Browser.

ZUR STARTSEITE

Ausgerechnet die Mechanismen der Internetwerbung helfen den Tätern dabei, ihre Opfer zu finden. Die Werbenetzwerke bieten ihren Kunden an, die Bannerwerbung gezielt an bestimmte Zielgruppen auszuliefern. Dieses Angebot nutzen auch die Hacker – und schließen etwa die Server der Antivirus-Anbieter als Ziel aus, damit ihre Attacke möglichst lange unentdeckt bleibt. "Die Täter spezifizieren teils auch bestimmte Länder als Ziel und programmieren den Erpressungstext ihrer Crypto-Trojaner in der passenden Sprache", weiß Wüest.

Die beiden Sicherheitsforscher Schröder und Rieger warnten in ihrem Vortrag nicht nur die Nutzer, sondern auch die Webseiten-Betreiber: Wird ein Nutzer beim Besuch eines Angebots mit Schadsoftware infiziert, wird er anschließend so schnell nicht wiederkommen. Dass die Anzeige mit dem Schadcode darin nicht von dem Server des Webseitenbetreibers selbst kam, sondern über ein Werbenetzwerk eingespielt wurde, dürfte den Nutzern dabei egal sein – das Potenzial für Reputationsverluste oder sogar Schadensersatzklagen ist enorm hoch.

MEHR ZUM THEMA

W SUBTILER EINFLUSS
W gitale Daten Wähler
n ılieren können

DIGITAL WETTBEWERBSHÜTER
EU nimmt Google jetzt auf dem Smartphone ins Visier

ZUR STARTSEITE

THEMEN

Google

DIE FAVORITEN UNSERES HOMEPAGE-TEAMS

Peter Behrens †
Dem traurigen Trio-Clown war ziemlich viel ziemlich egal

Platt-Paradoxon
Das Rätsel um den quadratischen A380-Reifen

NEUES AUS UNSEREM NETZWERK

LESERKOMMENTARE

6 Kommentare

Leserkommentare sind ausgeblendet.

Kommentare einblenden

ZUR STARTSEITE