SPIEGEL ONLINE
06. Dezember 2010, 08:48 Uhr

**IT-Forscher**

# So leicht können Kriminelle Websurfer aushorchen

Von Konrad Lischka

**Ob Pornoseiten, Extremistenforen oder Selbsthilfeportale - über eine Browser-Sicherheitslücke können Seitenbetreiber ausspähen, wo sich ihre Besucher sonst noch im Netz herumtreiben. Dass das geschieht, haben US-Forscher nachgewiesen. Experten sind alarmiert.**

Irgendwann wird diesen Witz wohl keiner mehr verstehen: "Im Internet weiß niemand, dass du ein Hund bist", stand 1993 unter einem Cartoon des US-Magazins "New Yorker". Zu sehen war ein Vierbeiner vor einem Rechner, der die Vorzüge der Anonymität im Netz lobt. Heute müsste das Tier wohl sagen: "Das Internet weiß, dass jemand hier ständig Hundefotos aufruft. Aber wer rechnet schon mit einem Hund?" Denn so langsam schwindet die Anonymität im Web. Eine Reihe technischer Entwicklungen macht es möglich, mit etwas Aufwand das Surf-Verhalten einzelner Web-Nutzer zu verfolgen und womöglich sogar mit Namen oder zumindest Profilen in sozialen Netzwerken zu verknüpfen.

Mit solchen serverseitigen Analysemethoden beschäftigt sich die US-Verbraucherschutzbehörde FTC. In einem nun veröffentlichten Datenschutzbericht schlägt die FTC vor, dass Software-Hersteller und Online-Dienstleister einen universellen "Nicht-Verfolgungsmechanismus" ("do not track mechanism") entwickeln. Über diese Funktion sollen Internetnutzer mit einem Mausklick sämtlichen Analysen ihres Surf-Verhaltens widersprechen können. Bis Ende Januar sammelt die FTC Stellungnahmen zu der Idee.

Was das FTC-Papier recht abstrakt als "Verfolgungsmechanismen" beschreibt, ist eine Vielzahl unterschiedlicher Methoden, mit denen man das Surf-Verhalten an bestimmten Computern auswerten und mit Aufwand zum Teil auch einzelnen Personen zuordnen kann.

**Surf-Verhalten abgreifen, Rechner identifizieren, den Profilen Klarnamen zuordnen - SPIEGEL ONLINE beschreibt, wie Angreifer Web-Nutzer Schritt für Schritt enttarnen könnten.**

**1. Schritt - So analysieren Pornoseiten die Surf-Vergangenheit der Besucher**

Eine lange bekannte, aber noch immer in Browsern wie dem Internet Explorer und Firefox klaffende Sicherheitslücke ermöglicht es Seitenbetreibern, das bisherige Surf-Verhalten ihrer Besucher auszuhorchen. Hintergrund: Um Websurfern einmal besuchte Links in einer anderen Farbe anzuzeigen, können Websites auf das Protokoll der aufgerufenen Seiten im Browser zugreifen.

Ein Forscherteam der University of California dokumentiert in einer Studie, dass 46 der 50.000 meistbesuchten Seiten im Web (laut dem Statistikdienst Alex) mit dieser "History Hijacking" genannten Methode das Surf-Verhalten ihrer Nutzer aushorchen. So schnüffelt den Forschern zufolge zum Beispiel ein solcher Mechanismus beim US-Porno-Portal Youporn aus, welche Seiten die Besucher sonst noch aufrufen.

**Dritte schleusen Ausspäh-Code auf Web-Seiten ein**

Ein bedenklicher Aspekt beim History Hijacking: Es muss keineswegs immer der Betreiber einer Web-Seite sein, der diese Informationen abgreift. Auch Dritte können den entsprechenden Code auf Seiten platzieren. So etwas haben die US-Forscher bei ihrer Untersuchung zum History Hijacking beobachtet. Ihnen war zum Beispiel die Web-Seite des Finanzinformationsdienstes Morningstar als Browser-Verlaufsschnüffler aufgefallen. Eine Sprecherin des Unternehmens erklärte dem Wirtschaftsmagazin "Forbes", ein Werbenetzwerk habe den Code auf den Morningstar-Seiten ohne Wissen des Anbieters eingesetzt.

Mit dieser Methode können Dritte im großen Stil Informationen im Netz sammeln, erklärt Sicherheitsforscher Gilbert Wondracek von der Technischen Universität Wien. Er hält diese Szenarien für plausibel: "Angreifer schleusen entweder über Werbung oder über Angriffe einen Code zum History Stealing auf vielen Angeboten im Web ein, sie werfen ein Netz aus und sammeln an vielen Stellen im Netz Informationen. Denkbar ist auch, dass Angreifer den Code in Stilvorlagen für Seiten einschleusen, die Anwender herunterladen und bei eigenen Web-Auftritten verwenden."

**2. Schritt - Rechner per Cookie oder Browser-Fingerabdruck identifizieren**

Bei einfachen Angriffen mit der History-Hijacking-Methode erhalten die Datenklauber keine Auskunft darüber, wessen Surf-Geschichte sie nun eigentlich ausgelesen haben. Sie erfahren eine IP-Adresse und alle anderen Details, die ein Browser beim Aufrufen einer Web-Seite an den Anbieter übermittelt. Für viele Anbieter dürfte es auch gar nicht so interessant sein, herauszufinden, wie ihre Besucher denn nun heißen. Sie wollen nur erfahren, wie ihre Besucher das Web nutzen, zum Beispiel, um ihr Publikum in Interessengruppen einzuteilen und ihnen zielgerichtet Werbung anzuzeigen.

Dafür genügt es, Rechner bei wiederholten Besuchen zu identifizieren. Das ist mit relativ geringem Aufwand möglich. Mit einem Cookie (kleine Textdateien, die der Browser ablegt) kann ein Seitenbetreiber einen Rechner einigermaßen zuverlässig markieren, mit sogenannten Flash-Cookies geht das auch unabhängig vom Browser.

Für die meisten Surfer ist das ein Schock: Auch wo Sie sich in der Zeit seit der letzten Flash-Cookie-Löschung Videos angesehen haben, weiß das Plug-in und meldet es nicht nur dem betreffenden Web-Seiten-Anbieter, sondern im Extremfall auch allen seinen Kooperationspartnern. Im Extremfall lassen sich so Profile eines persönlichen Netz-Nutzungsverhaltens erstellen. Wer das nicht glaubt, schaue sich die Flash-Cookie-History des eigenen Browsers an:

Die hier verlinkte Seite ist zugleich die Schnittstelle, über die sich diese Dokumentation der eigenen Video-Nutzung löschen lässt.

Allerdings könnten anhand der von Browsern übermittelten Informationen durchaus Rechner identifiziert und mit etwas Aufwand vielleicht auch Namen zugeordnet werden. Das hängt davon ab, wie viele Analysemethoden die Betreiber kombinieren und ob die ausgehorchten Surfer irgendwo im Netz mit ihrem Klarnamen aktiv sind. Rechner lassen sich auch ohne den Einsatz von Cookies ausschließlich serverseitig identifizieren. Entsprechende Datenbanken bieten viele Unternehmen an.

**Browser-Konfiguration als Fingerabdruck**

Der Ansatz ist raffiniert: Rechner erhalten auf Basis der Konfiguration eine ID. Um Rechner voneinander zu unterscheiden, genügen in vielen Fällen die vom Browser übermittelten Informationen. Der Informatiker Wondracek erklärt: "Vergleicht man die verfügbaren Informationen über installierte Schriftarten und Browser-Plug-ins, Betriebsystem und Browser, installierte Software und Bildschirmauflösung, sind Rechner gut voneinander zu unterscheiden."

*Diese Geräte-Profile lassen sich auch serverseitig speichern, diese Information kann der Nutzer nicht durch das Löschen von Cookies aus der Welt schaffen. Bei einem Experiment mit 470.000 Datensätzen demonstrierte die US-Organisation EFF (Electronic Frontier Foundation) im Frühjahr, wie gut dieser Browser-Fingerabdruck Rechner auseinanderhält: 83,6 Prozent der aufrufenden Computer hatten ein eindeutiges Profil.*

*Sollte sich jemand die Mühe machen, die Möglichkeiten der Rechneridentifikation mit dem History Hijacking zu verknüpfen, sind sehr zielgerichtete Angriffe auf Web-Nutzer denkbar. Ein denkbares Beispiel: Ein Angreifer schleust auf diversen Seiten über Werbung oder Angriffe einen Code ein, der analysiert, welche Rechner Browser mit bestimmten Sicherheitslücken verwenden, welche Sprache die Nutzer sprechen und ob sie zum Beispiel oft Motorradseiten aufrufen.*

*Mit diesen Informationen können Angreifer dann im nächsten Schritt auf die einzelnen Zielgruppen abgestimmte Lockangebote auf den Seiten einschleusen, die Opfer auf Web-Seiten mit Phishing- oder Schadsoftware lockt. In dem hypothetischen Fall könnte der Angreifer zum Beispiel einfach allen Mopedfreunden eine Anzeige für ein neues Motorradportal zeigen.*

**3. Schritt - Websurfer enttarnen und erpressen**

*Noch einen Schritt weiter können Angreifer gehen, die ihr Wissen über das Surf-Verhalten mit anderen Methoden zu Geld machen wollen als den bekannten Schadsoftware-Tricks. Wenn man Rechner identifiziert und ihnen bestimmte Seitenaufrufe zugeordnet hat, wäre es bei besonders kompromittierenden Seiten (Raubkopien, Pornografie, extreme politische Ansichten) interessant, die Namen der Surfer herauszufinden, um sie mit dem gesammelten Wissen zu erpressen.*

*Dass sich Internetsurfer, die soziale Netzwerke unter Klarnamen nutzen, mit einem einfachen Trick identifizieren lassen, haben die Informatiker Thorsten Holz, Gilbert Wondracek, Engin Kirda und Christopher Kruegel im Frühjahr demonstriert. Diese Analysemethode könnten Angreifer sehr gut mit dem History Hijacking und dem Identifizieren von Rechner kombinieren. Informatiker Wondracek hält diese Attacke für machbar: "Die Angreifer schauen sich um, bei welchen Foren oder sozialen Netzwerken sie Klarnamen in Verbindung mit Informationen über die verwendeten Rechner abgreifen können. Haben sie diese Informationen, suchen sie auf Web-Seiten mit potentiell kompromittierendem Material nach Aufrufen dieser Rechner."*

*Sprich: Wer ruft bestimmte Pornoangebote auf? Wer lästert in Foren anonym über seinen Arbeitgeber? Wer veröffentlicht in Foren freizügige Fotos? Solche Querverbindungen lassen sich mit den beschriebenen Methoden finden. Informatiker Wondracek: "Es ist natürlich aufwendig, aber sollte es für Angreifer lukrativer sein als andere Missbrauchsmethoden, wird es mit Sicherheit jemand machen."*

**URL:**

*http://www.spiegel.de/netzwelt/web/0,1518,732566,00.html*

**MEHR AUF SPIEGEL ONLINE:**

*Sicherheitslücke: IT-Forscher enttarnen Internetsurfer (02.02.2010)*
*http://www.spiegel.de/netzwelt/web/0,1518,675395,00.html*
*Von wegen diskret: Der Porno-Modus funktioniert nicht (09.08.2010)*
*http://www.spiegel.de/netzwelt/web/0,1518,710837,00.html*

**MEHR IM INTERNET**

*Wissenschaftler analyisieren History Hijacking*
*http://cseweb.ucsd.edu/~d1jang/papers/ccs10.pdf*
*Privacy Report der FTC*
*http://www.ftc.gov/os/2010/12/101201privacyreport.pdf*
*Peter Steiners berühmter Cartoon: "Im Internet weiß niemand, ob Du ein Hund bist"*
*http://www.unc.edu/depts/jomc/academics/dri/idog.html*
*"Forbes" über History Hijacking*
*http://blogs.forbes.com/kashmirhill/2010/11/30/history-sniffing-how-youporn-checks-what-other-porn-sites-youve-visited-and-ad-networks-test-the-quality-of-their-data/*
*EFF-Projekt Panopticlick*
*https://panopticlick.eff.org*
*Flash-Cookies bei Macromedia löschen*
*http://www.macromedia.com/support/documentation/de/flashplayer/help/settings_manager07.html*
*SPIEGEL ONLINE ist nicht verantwortlich für die Inhalte externer Internetseiten.*