ne Tracker auf den Webseiten eines einzigen Anbieters aktiv und sammeln Daten. Für Verbraucher können dadurch unerwartete Nachteile entstehen, etwa schlechtere Konditionen bei Krankenversicherungen oder Benachteiligungen beim Online-Shopping. Die Studie liefert einen umfangreichen Überblick über die aktuelle Praxis, Risiken und Schutzmöglichkeiten. Sie ist im Internet kostenlos unter *www.sit.fraunhofer.de/wtr* herunterladbar.

Auf vielen Webseiten wird das Surf-Verhalten der Nutzer überwacht. Was viele nicht wissen: Oft sammeln nicht nur die Betreiber der Web-Angebote Informationen, sondern im Hintergrund überwachen auch fremde Tracker das Online-Verhalten. Auf einzelnen Seiten fanden die Fraunhofer-Forscher Spitzenwerte mit über 100 dieser Datensammler. Sind diese Tracker bei mehreren Web-Angeboten aktiv, können sie sich ein sehr umfangreiches Bild von einzelnen Seitenbesuchern machen. So lassen sich mitunter Bezüge zum realen Namen und Wohnort herstellen. „Bestimmte Tracker waren über den Analysezeitraum auf mehr als 70 Prozent der von uns beobachteten Seiten aktiv", sagt Dr. Markus Schneider, stellvertretender Leiter des Fraunhofer SIT und Hauptautor des Berichts, „dadurch können diese Tracker sich ein umfassendes Bild über einzelne Verbraucher und ihre Vorlieben machen, ohne dass dies den Besuchern der Webseiten bewusst ist."

Die Wissenschaftler des Fraunhofer SIT haben recherchiert, was weltweit über die Verwendung von Tracking-Daten bisher bekannt geworden ist, und weisen auf weitere risikoreiche Verwertungsmöglichkeiten hin. „Auch wenn die Daten heute vorrangig für zielgerichtete Werbung gesammelt werden, so ist die Verwertung der Daten nicht auf diesen Zweck beschränkt", sagt Schneider. So lassen sich die Daten zum Beispiel nutzen, um Risikofaktoren aus dem Internetverhalten abzuleiten, Kreditwürdigkeit von Verbrauchern oder Gesundheitsrisiken von Krankenversicherten abzuschätzen. Da Tracker in vielen Fällen die gesammelten Daten mit der echten Identität eines Verbrauchers in Verbindung bringen können, sind auch Verwertungen außerhalb der Online-Welt denkbar. „Die gesammelten Daten sind eine Art Rohstoff, der über zielgerichtete Werbung hinaus viele weitere Geschäftsmodelle ermöglicht", sagt Schneider. „Verbraucher können sich vor Tracking-Aktivitäten schützen, indem sie entsprechende Werkzeuge verwenden." Ein Beispiel ist die Tracking-Protection-Liste des Fraunhofer SIT. Die Liste wird regelmäßig aktualisiert und Verbraucher können sie sich im Internet unter *www.sit.fraunhofer.de/tpl* kostenlos herunterladen. Die unabhängige Studie wurde von Microsoft finanziell unterstützt.

Kaspersky Lab: Cyberkriminelle nutzen aktive Online-Ressourcen in Tor

Kaspersky Lab beobachtet derzeit im so genannten „Darknet" verstärkte Aktivitäten der Cyberkriminellen über das Tor-Netzwerk. Obwohl die Infrastruktur und die cyberkriminellen Ressourcen des alternativen Netzwerks nicht dieselben Standards wie das klassische Internet bieten, kennt Kaspersky Lab aktuell etwa 900 versteckte Online-Services im Tor-Netzwerk.

Nutzer des Tor-Netzwerks können wie im „normalen" Internet Seiten besuchen, sich über Foren austauschen oder über Instant-Messaging-Dienste kommunizieren. Der große Unterschied besteht darin, dass Nutzer bei Tor während ihrer Netzaktivität anonym bleiben. Es ist unmöglich, IP-Adressen zu identifizieren und Rückschlüsse auf den Anwender zu ziehen. Darüber hinaus nutzen bestimmte Darknet-Ressourcen so genannte Pseudo-Domains. Diese machen es unmöglich, persönliche Informationen des Betreibers zu erhalten.

Tor als anonyme Infrastruktur für Malware beliebt

Cyberkriminelle nutzen Tor, um ihre Infrastruktur zu hosten. Kaspersky Lab hat Tor-Funktionalitäten beim Banking-Trojaner „Zeus", beim Keylogger-Trojaner „ChewBacca" sowie bei einem kürzlich aufgetauchten Tor-Trojaner für Android entdeckt. Netzwerkressourcen innerhalb von Tor werden beispielsweise für C&C (Command-and-Control)-Server oder Admin-Panels in Kombination mit Malware eingesetzt.

Erster Tor-Trojaner für Android

Kaspersky Lab hat Ende Februar 2014 einen Android-Trojaner entdeckt, der eine Domain in der so genannten Onion-Pseudo-Zone – also im anonymen Tor-Netzwerk – als C&C-Server nutzt. Der mobile Schädling namens „Backdoor.AndroidOS.Torec.a" nutzt Funktionalitäten des Tor-Clients „Orbot". Durch die Nutzung von Tor verschleiert der Trojaner seine Kommandozentrale, also seinen C&C-Server. Auf Android-Geräten ist der Trojaner in der Lage, eingehende SMS-Nachrichten abzufangen und ausgehende zu stehlen, SMS-Nachrichten an bestimmte Nummern zu senden, USSD-Anfragen durchzuführen sowie Telefondaten und Informationen zu installierten Apps an den C&C-Server zu senden.

Rezensionen

Veranstaltungen

23. RSA Conference, 24.02. – 28.02.2014 in San Francisco, USA

Die weltgrößte IT-Sicherheitskonferenz fand auch diesmal wieder im Moscone Center in San Francisco statt. Die RSA Konferenz ist nach wie vor die Welt-Leit-Messe für IT-Security mit starker internationaler Beteiligung und ist weiter gewachsen: mit etwa 27.000 Besuchern und rund 400 Ausstellern hat diese Veranstaltung die Grenzen der Kapazitäten des Moscone Centers North und South überschritten. Mitgenutzt wird nun auch das Moscone Center West. Dadurch standen nun in North und South zwei Messehallen zur Verfügung. Die insgesamt 78 Sponsoren wurden in North platziert, die übrigen 322 Ausstellern verblieben in South. Diese räumliche Teilung der Messeflächen hat keinen erkennbaren Einfluss auf die Besucherfrequenz an den einzelnen Ständen bewirkt.

Für die Präsentation von ‚IT Security Made in Germany' – zum 14. Mal in ununterbrochener Folge – standen für die vom Bundesministerium für Wirtschaft und Technologie (BMWi) und vom Ausstellungs- und Messe-Ausschuss der deutschen Wirtschaft e.V. (AUMA)