FinFisher & Co. machen harmlose Katzenvideos zur Waffe für Cyber-Attacken

Ein Forscher hat im Detail beschrieben, wie Angreifer mit Zugriff auf die Netzwerkinfrastruktur eines Internet-Providers Trojaner in den Traffic der Nutzer einschleusen können, ohne dass die Opfer etwas bemerken.

Normalerweise könnte man annehmen, dass das Surfen auf vertrauenswürdigen Internetseiten wie Googles YouTube und Microsofts Live.com relativ sicher ist. Ist man nicht auf zwielichtigen Seiten unterwegs und klickt blind auf verdächtige Links, sollte man davon ausgehen können, nicht gehackt zu werden. Steht man allerdings im Fokus von Ermittlungsbehörden oder Geheimdiensten, ist diese Annahme ein Trugschluss. Wie Morgan Marquis-Boire vom Citizen Lab der Universität von Toronto berichtet, kann einem in diesem Fall jede ungesicherte Internetverbindung zum Verhängnis werden – auch das süße Katzenvideo auf YouTube.

Gezielte Angriffe auf Internet-Nutzer

Marquis-Boire behandelt in seiner Forschungsarbeit sogenannte Network Injection Devices – diese Geräte werden von Firmen wie FinFisher oder Hacking Team verkauft und dann von deren Kunden im Netz von Internetanbietern installiert, um Angriffe auf die Rechner von einzelnen Zielpersonen auszuführen. Die Kosten für diese Art von Angriff liegen im siebenstelligen Bereich und Firmen wie FinFisher verkaufen ihre Dienste fast ausschließlich an Regierungen. Ist das Gerät installiert, wartet es, bis die Zielperson eine ungesicherte Verbindung aufbaut (etwa einen YouTube-Stream startet) und injiziert bösartige Pakete, die gezielt Schwachstellen auf dem System des Opfers missbrauchen und dieses unter die Kontrolle der Hacker bringen.

Der Forscher hat Marketing-Broschüren dieser Firmen untersucht, die von Hackern im Internet veröffentlicht wurden. Eine Sammlung von Wikileaks enthält Dokumente, die beschreiben sollen, wie FinFisher Software-Updates beliebter Programme – etwa des Flash Players von Adobe – on-the-fly infiziert. Hacking Team soll laut Informationen, die ein anonymer Informant dem Citizen Lab zur Verfügung gestellt hat, YouTube-Streams und unverschlüsselte Teile des Logins von Windows Live genutzt haben, um beim Opfer Trojaner zu installieren. Microsoft hat die Lücke mittlerweile geschlossen, YouTube will seine Webseite in naher Zukunft komplett auf TLS-Verschlüsselung umstellen.

Trojaner in vertrauenswürdigen Downloads

Angriffe dieser Art werden seit langem diskutiert und so gibt es zum Beispiel auch Open-Source-Tools wie The Backdoor Factory, die Downloads im Transit mit einem Trojaner infizieren können. Voraussetzung für den Einsatz solcher Tools ist, dass der Angreifer sich als Man-in-the-Middle positionieren kann – also der Internet-Traffic des Opfers bei ihm vorbei kommt. Das ist für die NSA offenbar kein Problem – normale Strafverfolger beziehungsweise Angreifer ohne die Ressourcen eines Geheimdienstes müssen da schon etwas Aufwand betreiben.

Denkbare Szenarien für einen solchen Angriff sind, wie angesprochen, Zugang beim Provider des Opfers (bei Strafverfolgungsbehörden ganz legal mit einer entsprechenden offiziellen Verfügung) oder Kontrolle über den WLAN-Hotspot, den das Opfer nutzt. Auch ist es denkbar, Tor-Nutzer zu kompromittieren, falls der Angreifer den Exit-Knoten betreibt, den das Opfer nutzt. Beim letzten Szenario ist es allerdings schwierig, gezielt einzelne Personen ins Visier zu nehmen. Abhilfe gegen jegliche Art dieser Angriffe lässt sich nur schaffen, wenn alle Verbindungen verschlüsselt sind. "Klartext muss sterben", sagt Marquis-Boire.
(fab)

Erschienen am 16.08.2014 um 16:44 Uhr auf heise.de

Permalink: http://heise.de/-2293549