Staatstrojaner schaden der Sicherheit

28. Juli 2015

Nach dem grossen Datenklau bei «Hacking Team» Anfang Juli 2015 wurde gemunkelt, dass Zero-Day-Lücken im Darknet gehandelt würden und dass eine Schwachstelle in einer Software locker 1 Million Dollar kosten würde. Eine Analyse der Emails von «Hacking Team» hat aber ergeben, dass Programm-Fehler, welche zur Installation von Trojanern ausgenutzt werden können, an offiziellen internationalen «Sicherheits»-Konferenzen gehandelt werden, und dass systemübergreifende Exploits, z. B. für Adobe Flash, schon für 35,000 US Dollar zu haben sind.

«Hacking Team» befasste sich ab dem Jahre 2009 ernsthaft mit Schwachstellen. Als Einstieg begann «Hacking Team» mit Brokern zu geschäften, welche als Mittler zwischen Anbietern und Interessenten von Exploits fungieren. So wurden Exploit-Pakete von «D2Sec» und «VUPEN» gekauft, welche aber lediglich alte, bereits gepatchte oder minderwertige Exploits enthielten.

Dennoch konnten mit diesen Schwachstellen via soziale Netzwerke Benutzer mit ungepatchten Systemen gehackt werden, z. B. mit einem präparierten Word-Dokument auf Mamfakinch.com, um marokkanische Aktivisten zu überwachen, oder mit einem Android-Installations-Paket, welches die Saudi-Arabische Nachrichten-App von «Qatif Today» (?????? ?????) mit Malware von «Hacking Team» bündelte und mit welcher die Shia-Gemeinde in Saudi-Arabien ausspioniert wurde. Auch wenn das «Remote Controlled System» über eine schwache Sicherheitslücke eingeschleust wird, ist nach der erfolgreichen Installation die gesamte Funktionalität uneingeschränkt verfügbar.

Ein weiterer Broker ist «Netragard». Obwohl «Netragard» angeblich ausschliesslich an US-Kunden liefert, konnte «Hacking Team» dort einkaufen. «Netragard» hat seinen Handel mit Exploits nach der Veröffentlichung der Emails von «Hacking Team» und der daraus resultierenden negativen Presse am 20. Juli 2015 eingestellt.

Aktive Suche nach Sicherheitslücken

Als Citizen Lab ab dem Jahr 2012 seine Reporte über das «Remote Controlled System» und die Bespitzelung von Medienschaffenden und Aktivisten in Marokko, den Vereinigten Arabischen Emiraten, Saudi-Arabien und weiteren Ländern veröffentlichte und «Hacking Team» dadurch in die negativen Schlagzeilen geriet, brachte dies «Hacking Team» in direkten Kontakt zu Exploit-Entwicklern.

«Hacking Team» nahm in der Folge auch Entwickler unter Vertrag, z. B. Eugene Ching aus Singapur oder Rosario Valotta aus Rom. Eugene Ching erhielt für einen Ein-Jahres-Vertrag 60,000 US$ sowie 20,000 US$ Bonus für einen Exploit, welcher Windows 32-Bit und 64-Bit-Systeme angriff. Rosario Valotta erhielt 3,500 € pro Monat, hat aber keinen Exploit zur Produktionsreife gebracht.

Die beste Zusammenarbeit entstand jedoch mit dem 33-jährigen Vitaliy Toropov aus Moskau. Bis Oktober 2013 meldete Vitaliy Toropov viele Schwachstellen an Softwarehersteller, welche

sie dadurch beheben konnten. Ab diesem Zeitpunkt begann er, seine Exploits zu verkaufen, unter anderem an «Hacking Team». Exploits waren bei Vitaliy Toropov ab 35,000 US Dollar zu haben, inklusive Gratisersatz, falls die Schwachstelle innerhalb von 2 Monaten entdeckt und gepatcht wurde.

Mit diesen guten, noch unbekannten Exploits von Vitaliy Toropov und Konsorten konnte «Hacking Team» jeden Benutzer unabhängig von der verwendeten Hard- und Software spezifisch und erfolgreich angreifen.

«Staatstrojaner» fördern Handel mit Exploits

Besonders das Beispiel Vitaliy Toropov zeigt, dass mit der staatlichen Beschaffung von Spionagesoftware die weltweite Internetsicherheit gefährdet wird, weil Entdecker von Schwachstellen mit hohen Prämien dazu animiert werden, ihre Exploits zu verkaufen statt ohne Entschädigung an die Hersteller zu melden. Die Steuerzahler von Zürich haben mit den 500,000 Franken, welche an «Hacking Team» bezahlt wurden, keinen Beitrag an die Sicherheit geleistet, im Gegenteil, sie ermöglichten das Hacken von vielen Benutzern. Mit einem Nein zum BÜPF und zum NDG kann das Sicherheitsproblem «Staatstrojaner» zumindest in der Schweiz verhindert werden.

Diese Zusammenstellung wurde basierend auf der Analyse «Hacking Team: a zero-day market case study» von Vlad Tsyrklevich verfasst.

Spionagesoftware: Der Handel des Hacking Teams mit Zero-Days

«Hacking Team: a zero-day market case study»