Dubiose Deals und teure Trojaner

7. Juli 2015

von Eike Kühl, Zeit online

Mehr und mehr Details über das Geschäftsmodell und die Dienste von Hacking Team kommen ans Licht. Zu den Kunden der Firma zählten das FBI und die Deutsche Bank.

48 Stunden nach dem umfassenden Hack des italienischen Unternehmens Hacking Team ergibt sich ein immer klareres Bild der Firma, ihrer Kunden und Dienstleistungen. Am Sonntag hatten Unbekannte mehr als 400 Gigabyte Daten von den Servern entwendet und im Internet veröffentlicht. Hacking Team entwickelt und verkauft IT-Überwachungstechnik, immer wieder warfen Bürgerrechtsorganisationen der Firma vor, mit repressiven Regierungen und Geheimdiensten zusammenzuarbeiten.

Diese Vermutung bestätigen zahlreiche Dokumente, die jetzt nach und nach ans Tageslicht kommen. Der oder die Unbekannten konnten interne E-Mails, Kundenlisten und Rechnungen entwenden, in den sich Hinweise auf Kunden aus Ländern wie Ägypten, Äthiopien, Saudi-Arabien, Kasachstan und Sudan befinden - allesamt Länder, in denen Oppositionelle überwacht und verfolgt werden. Gerade im Fall des Sudan könnte Hacking Team nach den jetzigen Erkenntnissen wissentlich das bestehende Handelsembargo gebrochen haben.

Deutsche Bank zahlte für Sicherheitsaudit

Auch Behörden investierten grosszügig in die Software. Fast 700,000 Euro soll allein das FBI seit dem Jahr 2011 an die Italiener gezahlt haben, in erster Linie für die Software Remote Controlled System (RCS) und Lizenzgebühren. Offenbar hat das FBI die Software allerdings nur zur Ergänzung der eigenen Lösungen eingesetzt. Immerhin 35 namentlich nicht erwähnte Ziele werden in den Dokumenten erwähnt. Auch die US-Drogenvollzugsbehörde DEA gehörte zu den Kunden, was aber bereits seit April bekannt ist. Nicht bekannt war, dass die Kantonspolizei Zürich bereits 2014 Trojaner bestellte. Erst vor Kurzem wurde in der Schweiz ein neues Überwachungsgesetz auf den Weg gebracht.

Die Dienste von Hacking Team waren auch in der Finanzbranche gefragt, wenn auch nicht zur Überwachung, sondern offenbar vor allem zum Schutz vor Angriffen von aussen. So hat Barclays einer Rechnung zufolge 74,000 Euro für eine interne Sicherheitsanalyse bezahlt. 2004 nahm die Deutsche Bank solche Dienste in Anspruch. Unabhängige Analysen, sogenannte Sicherheitsaudits, sind nicht ungewöhnlich in der Branche.

Angebliche Angriffe auf das Tor-Netzwerk

Schon länger ist bekannt, dass RCS zu den beliebtesten Produkten der Firma zählt. Hacking Team pries die Software in der Vergangenheit mit dem Slogan "Internetüberwachung leicht gemacht" an und bot die Möglichkeit, die Rechner von anderen Nutzern zu überwachen, Tastaturbefehle, Kamera- und Mikrofonaufnahmen mitzuschneiden und WLANs zu überwachen. Vergangenes Jahr zeigte ein geleaktes Nutzerhandbuch bereits, welche

Funktionen RCS seinen Käufern bietet.

Zudem haben die Entwickler von Hacking Team auch versucht, verschlüsselte Verbindungen auszuhebeln. In einer Dokumentation mit dem Titel Project X geht es um die gesicherte HTTPS-Verbindung und das Tor-Netzwerk sowie um mutmassliche Wege, deren Verschlüsselungs- und Verschleierungstechnik zu umgehen. "Unsere Lösung ist zurzeit der einzige Weg, um den Datenverkehr im Tor-Netzwerk abzugreifen" heisst es unter "Stärken". Die Tor-Entwickler reagierten mittlerweile auf Twitter und liessen verlauten, dass es keine Hinweise für einen erfolgreichen Hack des Tor-Netzwerks gebe. Es sei aber nicht überraschend, wenn Hacking Team wie viele andere auch versuchten, es zu infiltrieren.

Malware für Android kostet 40,000 Euro

Einige der Hacking-Team-Lösungen zielen zudem auf mobile Geräte. Ein Android-Modul für die RCS-Software etwa kostet einer Preisliste zufolge 40,000 Euro, für iOS sind es noch einmal 10,000 mehr. Einigen Dokumenten zufolge sind die Entwickler aber offenbar bei der Installation der Malware auf diverse Probleme gestossen. Zumindest Apple-Geräte müssen zudem bereits mit einem sogenannten Jailbreak versehen sein, heisst es. Ohne den ist es nicht möglich, inoffizielle Software wie etwa die Trojaner, zu installieren. Justin Case vom Blog AndroidPolice weist darauf hin, dass in den Unterlagen von Hacking Team bekannte Jailbreaks und Exploits als mögliche Angriffsstelle erwähnt werden.

Generell zeigen die geleakten Informationen, dass Hacking Team sich an bereits bestehender Malware orientiert oder sogenannte Zero-Day-Lücken, etwa im Flash-Player, zu seinen Gunsten verwendet hat. Zero-Days heissen bisher unbekannte Sicherheitslücken, gegen die es folglich noch keinen Schutz gibt. Sie werden in Hacker-Kreisen für teilweise viel Geld gehandelt. Dass Hacking Team mit bekannter Malware und neuen Sicherheitslücken arbeitet, ist nicht überraschend. Aber es zeigt, dass die als fortschrittlich angepriesene Überwachungssoftware nicht unbedingt das alleinige Werk der Italiener ist.

Die Hacker melden sich

Inzwischen haben sich erstmals auch der oder die mutmasslichen Täter zu Wort gemeldet. Motherboard ist es gelungen, über den gekaperten Twitter-Account von Hacking Team mit einem von ihnen in Kontakt zu treten. Dieser hinterliess nach der Aufforderung des Motherboard-Journalisten eine Nachricht auf dem Parodie-Account GammaGroupPR. Den hatten Unbekannte vergangenes Jahr eingerichtet, als das ebenfalls auf Spähsoftware spezialisierte deutsch-britische Unternehmen Gamma gehackt wurde. Damit liegt die Vermutung nahe, dass hinter den Hacks auf Gamma und Hacking Team die gleichen Personen stehen. Weitere Fragen wollten die Hacker nicht beantworten, allerdings haben sie angekündigt, demnächst noch weitere Details zu veröffentlichen.

Die Verantwortlichen von Hacking Team antworten weiterhin nicht auf Anfragen von ZEIT ONLINE, eine erste Stellungnahme hat aber Firmensprecher Eric Rabe im Gespräch mit IB Times UK abgegeben: "Wir glauben nicht, dass es in diesen 400 Gigabyte Beweise dafür gibt, dass wir Gesetze übertreten haben. Ich würde sogar behaupten, es gibt keine Beweise, dass wir jemals unethisch gehandelt haben."

Zuvor hat das Unternehmen offenbar eine Rundmail an die Käufer von RCS, Codename Galileo, verschickt. Darin heisst es, dass sie die Software nicht mehr nutzen sollen. Wie aus geleakten Dokumenten hervorgeht, ist offenbar jede Instanz der Software mit einer einmaligen ID-Nummer versehen, die Dritte nun möglicherweise dazu nutzen könnten, um Angriffe

zurückzuverfolgen.

Der Entwickler Christian Pozzi, über dessen unsichere Passwörter die Hacker möglicherweise Zugriff auf die Infrastruktur von Hacking Team bekamen, drohte in mittlerweile gelöschten Nachrichten auf Twitter mit der Polizei, rechtfertigte das Geschäftsmodell von Hacking Team und warnte, dass die veröffentlichten Datensätze einen Virus enthalten. Darauf gibt es allerdings keine Hinweise. Ein anderer Mitarbeiter sagte Motherboard, dass er schon mal seinen Lebenslauf überarbeitet - möglicherweise wird er sich demnächst einen neuen Arbeitgeber suchen müssen.