Equation-Group: "Höchstentwickelte Hacker der Welt" infizieren u.a. Festplatten-Firmware

Seit Jahren, wenn nicht sogar Jahrzehnten treibt eine Gruppe von Cyberangreifern weltweit ihr Unwesen und setzt auf äußerst hochentwickelte Technik, behauptet Kaspersky. Details bereits bekannter Malware impliziert Verbindungen zum US-Geheimdienst NSA.

Die russische IT-Sicherheitsfirma Kaspersky Lab hat Details zu einer Equation Group getauften Hackergruppe veröffentlicht, die mit ausgefeilten Methoden Regierungen und Unternehmen in mehr als 30 Ländern angegriffen haben soll. Auch wenn sie nicht direkt genannt wird, gibt es Hinweise, das die NSA oder ein anderer US-Geheimdienst dahinter steckt. Als besonders intensive Angriffsmethode hebt Kaspersky die Fähigkeit der Gruppe hervor, die Firmware von Festplatten bekannter Hersteller zu manipulieren. Die entsprechende Malware habe man in zwei Festplatten gefunden. Dass die NSA intern erklärt, dazu in der Lage zu sein, hatten bereits Jacob Appelbaum und *Der Spiegel* anlässlich des 30C3 in Hamburg öffentlich gemacht.

Verbindung zu US-Geheimdiensten

Kaspersky bringt die Equation Group zwar nicht direkt mit US-Behörden wie der NSA in Verbindung, erklärt aber, dass es "solide Hinweise" dafür gebe, dass mit den Erschaffern von Stuxnet und Flame zusammengearbeitet wurde. So hätten die Entwickler Zero-Day-Lücken ausgetauscht, die in einigen Fällen von der Equation Group genutzt worden seien, bevor sie bei Stuxnet oder Flame eingesetzt wurden. Als Verantwortliche hinter diesen beiden äußerst hochentwickelten Malware-Programmen waren bereits US-Geheimdienste wie die NSA und die CIA ausgemacht worden.

Angegriffen wurden dem ausführlichen Bericht zufolge Ziele in mehr als 30 Ländern, darunter auch Deutschland, Frankreich, Großbritannien und in den USA. Zu den Opfern gehörten Regierungen und diplomatische Institutionen, Rüstungskonzerne, Forschungseinrichtungen, Massenmedien sowie Kryptographieentwickler. Während in Deutschland Telekommunikationsunternehmen betroffen seien, habe man in Großbritannien und den USA islamische Gelehrte und Aktivisten als Ziele ausgemacht. Diese Länder seien aber weniger stark betroffen, besonders viele Infektionen gebe es dagegen etwa im Iran und in Russland.

Hochentwickelte Angriffsmethoden

Die Gruppe nutzt demnach ein mächtiges Arsenal an Trojanern. Die Infizierung der Firmware von Festplatten sei darunter nur eine, wenn auch die intensivste Angriffsmethode. Diese Malware überlebt eine Formatierung der Festplatte oder Neuinstallation des Betriebssystems und sei nicht zu entdecken. Gleichzeitig werde sie genutzt, um einen versteckten Bereich auf der Festplatte zu schaffen, auf dem Daten gesichert werden, um sie später abgreifen zu können. Die einzige Methode, die Malware loszuwerden, sei die physische Zerstörung der Festplatte, twitterte Kaspersky-Forscher Fabio Assolini.
(mho)

Erschienen am 17.02.2015 um 10:06 Uhr auf heise.de

Permalink: http://heise.de/-2550779