SPIEGEL ONLINE
17. Februar 2015, 11:29 Uhr

Equation Group

Sicherheitsforscher entdecken mutmaßliche NSA-Schadprogramme

Vor einem Jahr haben SPIEGEL und SPIEGEL ONLINE über geheime NSA-Schadsoftware berichtet, die sich in der Firmware von Festplatten einnistet. Jetzt haben Experten solche Programme auf Hunderten Rechnern gefunden.

Auf über 500 Rechnern rund um den Globus haben die Sicherheitsexperten von Kaspersky Lab brandneue Schadsoftware entdeckt. Die Virenforscher sprechen von bislang ungeahnter Komplexität und Qualität, vom "Todesstern der Malware-Galaxie". Die Superspähprogramme stammen vermutlich von der NSA.

Den acht Schadprogrammen, die Kaspersky Lab in einem Bericht (PDF) vorstellt, haben die Virenforscher selbst Namen wie Fanny oder Grayfish gegeben. Sie sollen alle aus einer Hand stammen: Die Experten nennen sie die Equation-Gruppe. Equation, Gleichung, wegen ihrer Vorliebe für "ausgefeilte Verschlüsselungsmethoden".

Wahrscheinlich seit 2001, vielleicht schon seit 1996 wurden dem Bericht zufolge von der Equation-Gruppe Tausende bis Zehntausende Computer infiltriert, vor allem in Regierungen, Telekomunternehmen, der Luftfahrt- und Energiebranche, dem Militär und von muslimischen Aktivisten und Gelehrten. Die meisten Infektionen fand Kaspersky in Iran, Russland, Pakistan, Afghanistan, Indien, China, Syrien und Mali. Aber auch Telekommunikationsinfrastruktur in Deutschland sei betroffen.

Verbreitet wurden die Programme auf zum Teil originelle Weise. Ein Wissenschaftler beispielsweise habe eine CD mit Fotos von einer Konferenz in den USA geschickt bekommen, an der er teilgenommen hatte, so Kaspersky. Auf dem Datenträger verbarg sich aber auch eine Spähsoftware von einer "nahezu allmächtigen Cyberspionage-Organisation", so die Virenforscher.

Festplatten-Firmware infiziert

Die Schadprogramme sind ausgefeilt: Zwei von ihnen nisten sich in der Steuersoftware (Firmware) von Festplatten ein und können so auch Festplatten-Löschungen und -Neuinstallationen überstehen. "Das übertrifft selbst Regin an Raffinesse. Dass die Firmware einer Festplatte infiziert wird, haben wir nie zuvor gesehen", so die Kaspersky-Forscher. Regin ist eine Schadsoftware, die ebenfalls der NSA und ihren Verbündeten zugeordnet wird.

Dass der US-Geheimdienst NSA über genau solche Werkzeuge verfügt, ist schon seit Dezember 2013 bekannt: Damals veröffentlichten SPIEGEL und SPIEGEL ONLINE einen Katalog mit Hard- und Softwareimplantaten einer NSA-Abteilung namens ANT, was vermutlich für Advanced Network Technologies steht. Der Katalog enthält beispielsweise ein "Produkt" namens Iratemonk, das dazu dient "Desktop-Rechner und Laptops mit überdauernden Softwareanwendungen auszustatten, indem es die Festplatten-Firmware implantiert". Geeignet ist Iratemonk demnach für "eine Vielzahl von Festplatten von Western Digital, Seagate, Maxtor und Samsung".

Die Firmware-Modifikation, die Kaspersky entdeckte, ist dem Bericht zufolge in der Lage, "über ein Dutzend unterschiedliche Festplattenmarken" zu infizieren, darunter "Seagate, Western Digital, Toshiba, Maxtor und IBM". Das zitierte Dokument über die Festplatten-Malware namens Iratemonk stammt aus dem Jahr 2008. Die Festplatten-Malware, die Kaspersky beschreibt und nur "nls_933w.dll" nennt, ist neuer, sie stammt dem Bericht zufolge aus dem Jahr 2010.

Weitere Parallelen zu NSA-Werkzeugen

Beschrieben wird auch ein Software-Implantat, das speziell dazu gemacht ist, über infizierte USB-Sticks auch von solchen Rechnern Daten abzuzweigen, die gar nicht ans Internet angeschlossen sind (air gap). Auch solche Technik findet sich im ANT-Katalog. Die von Kaspersky beschriebene Software nutzte zwei Schwachstellen in Windows-Computersystemen aus, um auch Computer ohne Internetanschluss infizieren zu können. Diese zwei Lücken kannten die Experten schon: Sie hatten sie bereits im Stuxnet-Wurm entdeckt, mit dem die USA und Israel mutmaßlich iranische Uran-Anreicherungsanlagen sabotierten.

Der Bericht der russischen Anti-Virus-Firma lässt wenig Zweifel daran, ohne explizit darauf hinzuweisen: Hinter den Angriffen steckt der amerikanische Geheimdienst NSA. Die Liste der Ziele, das technische Know-how und der Ressourcen-Aufwand für die Entwicklung der Schadsoftware deuten darauf hin.

Aber es gibt noch weitere handfeste Hinweise: So taucht der Codename Grok in von Edward Snowden verfügbar gemachten NSA-Dokumenten auf, als NSA-Werkzeug zur unentdeckten Aufzeichnung von Tastaturanschlägen. Auch der Equation-Grok ist so ein Keylogger. Es gibt eine ganze Reihe weiterer Querverbindungen, darunter die von den Viren-Autoren selbst verwendeten Namen für ihre Schöpfungen. Dort taucht zum Beispiel das Kürzel UR auf, das für Unitedrake stehen könnte, eine aus dem ANT-Katalog bekannte NSA-Software, außerdem mehrere Programme mit dem Adjektiv Straight- im Namen - sie könnten zur Familie der Straightbizarre-Softwareplattform der NSA gehören.

Es könnte auch sein, schreiben die Experten, dass der Stuxnet-Angriff mit einem der jetzt präsentierten Schadprogramme eingeleitet wurde. In den nächsten Tagen wird Kaspersky Labs die bislang gesammelten technischen Informationen veröffentlichen. Schon jetzt haben sich andere Sicherheitsexperten zu Wort gemeldet und eine NSA-Autorenschaft bekräftigt.

Die NSA selbst reagierte mit einer Stellungnahme, nachzulesen etwa bei "Forbes". Der Geheimdienst sei "über den kürzlich veröffentlichten Bericht informiert", werde aber "keine der Behauptungen des Berichts öffentlich kommentieren oder Details daraus diskutieren". Danach folgt ein Absatz, in dem der Geheimdienst auf eine spionagefreundliche Anordnung des US-Präsidenten verweist, und darauf, dass die US-Geheimdienste die USA und ihre Bürger vor Terroranschlägen, Massenvernichtungswaffen, "ausländischer Aggression gegen uns selbst und unsere Verbündeten" und vor "internationalen kriminellen Organisationen" schützen müssten.

fko/cis

URL:

http://www.spiegel.de/netzwelt/web/equation-group-kaspersky-warnt-vor-manipulierter-festplatten-firmware-a-1018852.html