+++++++AKTUELL+++++AKTUELL+++++AKTUELL+++

Mord und Intrigen in der Welt der Chip Technologien

Eben noch hat Marc Jansen an seinem Schreibtisch in Hamburg eine Marktanalyse für Netzwerkchips erstellt, jetzt findet sich der Spezialist für Halbleitertechnologie plötzlich in einem undurchsichtigen Strudel aus Mord, Korruption und Intrigen wieder. Nach dem mysteriösen Tod eines renommierten amerikanischen Quanteninformatikers in Thailand sollen er und seine Partnerin Lana de Vries im Auftrag eines internationalen Konsortiums herausfinden, was es mit einer neuen Generation von Chips auf sich hat - der ermordete Wissenschaftler arbeitete angeblich an deren Herstellung. Noch ahnt Jansen nicht, auf was er sich da eingelassen hat.

Spionagesoftware der Superlative entdeckt

Sie versteckt sich unlöschbar auf Festplatten und spioniert hochrangige Ziele aus: Antivirenspezialisten entdecken extrem ausgefeilte Malware mit Parallelen zu Stuxnet.

Spionagesoftware, die seit vielen Jahren gezielt Computer von Regierungen, Militärs und anderen hochrangigen Zielen angreift. Die sich unlöschbar auf Festplatten bekannter Hersteller einnistet, die sensible Informationen selbst aus vom Internet getrennten Rechnern abschöpft und mit extrem aufwendigen Methoden alle Schutzvorkehrungen umgeht: Der Fund der russischen Antivirenspezialisten von Kaspersky Lab strotzt vor Superlativen. Kaspersky nennt die Entwickler dieser Familie von Spionagewerkzeugen in einem Bericht "wahrscheinlich eine der raffiniertesten Cyberangriffsgruppen der Welt und die am weitesten entwickelte Bedrohung, die wir je gesehen haben." Illustriert ist der Bericht mit einer stilisierten Darstellung des Todessterns aus Krieg der Sterne. Wer hinter der Software steckt, sagen die Russen nicht. Aber sie legen eine Reihe von Indizien vor, die auf die NSA hinweisen.

So beherrscht die Malware der Gruppe, die Kaspersky die Equation Group getauft hat, mehrere Tricks, die zu den Kernfunktionen der NSA-Mitentwicklungen Stuxnet und Regin gehören. Mitunter basieren sie sogar auf denselben sogenannten Zero-Day-Angriffen, also Attacken auf bis dahin unbekannte Sicherheitslücken. Die Spuren, die Kaspersky fand, lassen sich allerdings bis 2001 und möglicherweise sogar noch weiter zurückverfolgen. Damit wären die Programme der Equation Group die Vorläufer von Stuxnet und Regin. Den einzelnen Angriffsplattformen der Gruppe hat Kaspersky die Namen Fanny, Grayfish, Doublefantasy und Triplefantasy oder auch Equationlaser und Equationdrug verpasst.

Doublefantasy nistet sich auf einem Rechner ein und stellt fest, ob dieser für die Angreifer von Interesse ist. Wenn das der Fall ist, ermöglicht Doublefantasy das Nachladen weiterer Malware wie

Equationdrug oder Grayfish. Die beiden befallen praktisch alle Windows-Betriebssysteme, die neuere Plattform Grayfish macht auch vor Windows 8 nicht halt.

Grayfish steuert anschließend den kompletten Rechner, und wenn das aus irgendeinem Grund nicht mehr funktioniert, zerstört sich die Malware selbst. Vor einer Entdeckung schützt sie sich, indem sie alle ihre Komponenten sowie abgefangene Daten verschlüsselt in der Registry ablegt. Im Dateisystem dagegen tauchen keinerlei ausführbare Module auf, für Antivirensoftware ist Grayfish unsichtbar. Das Ganze ist so komplex, dass Kaspersky "Entwickler von höchstem Kaliber" dahinter vermutet.

Die 2008 entwickelte Software Fanny wiederum nutzt zwei Zero-Days für ihre Spionagetätigkeit, die später auch Teil von Stuxnet waren, und zwar auf vergleichbare Art und Weise. Kaspersky schließt daraus, dass die Entwickler von Fanny die gleichen waren wie die von Stuxnet oder zumindest eng zusammenarbeiteten. Fanny versteckt sich auf USB-Sticks und soll vor allem Computer auskundschaften, die vom Internet getrennt sind. Das heißt aber, dass jemand den infizierten Stick in den Zielcomputer stecken muss. Andere Infektionswege für die verschiedenen Werkzeuge der Equation Group waren präparierte CD-ROMS und Websites.

Zwölf Festplattenhersteller betroffen

Am meisten beeindruckt hat Kaspersky die Fähigkeit der Equation-Gruppe, die Firmware von handelsüblichen Festplatten umzuschreiben. Das ermöglicht die Einrichtung versteckter Speicherplätze, die auch eine Formatierung und eine Neuinstallation des Betriebssystems überstehen, und funktioniert auf Festplatten von Samsung, Toshiba, Seagate, Western Digital Technologies und mindestens acht weiteren Herstellern.

Etwas Vergleichbares hatten die Kaspersky-Spezialisten nie zuvor gesehen. Um die Firmware umprogrammieren zu können, braucht ein Angreifer eigentlich den Quellcode. Diesen zu beschaffen, ist für staatliche Akteure zwar durchaus möglich, aber sehr aufwendig. Der tatsächliche Einsatz dieser Spionagemethode sei Kaspersky zufolge deshalb extrem selten. Nur sehr wertvolle Ziele seien betroffen.

Angriffe auf Forschungseinrichtungen und Aktivisten

Was spricht abgesehen von den Zero-Day-Angriffen von Fanny für eine Beteiligung der NSA? Es sind Indizien wie Codenamen, Schlüsselwörter und Abkürzungen, die im Code auftauchen, weil sie nicht richtig verschleiert wurden. Sie deuten auf schon bekannte NSA-Werkzeuge hin, deren Existenz der Spiegel enthüllt hat. Fünf Opfer der Equation Group aus dem Iran wurden später auch von Stuxnet befallen. Die meisten der insgesamt rund 500 infizierten Computer befinden sich laut Kaspersky im Iran, allerdings auch einige in den USA und Großbritannien sowie in Russland, Pakistan, Afghanistan, Belgien und Deutschland.

Das Ziel der Spionageangriffe waren Wired zufolge neben Regierungen und Militärs auch Atomforschungseinrichtungen, Telekommunikationsunternehmen, Medien, islamische Gelehrte und Aktivisten sowie Experten für Nanotechnologie und Verschlüsselung. Zwei anonyme ehemalige US-Geheimdienstmitarbeiter haben Reuters zudem versichert, dass die Analyse von Kaspersky korrekt ist. Dass ein Antivirenspezialist wie Kaspersky Lab derart hochentwickelte Malware entdeckt und analysiert, obwohl sie sein Kerngeschäft kaum berührt, ist heute nichts Besonderes mehr. Auch Stuxnet wurde vor allem durch die Arbeit einer solchen Firma öffentlich: Symantec. Die stellte anfangs drei ihrer Analysten ab, um die rätselhafte Spionagesoftware zu untersuchen, obwohl Symantec-Kunden kaum davon betroffen waren, wie die Wired-Journalistin Kim Zetter in ihrem Buch Countdown to Zero Day schreibt. Spätestens seit Beginn der Snowden-Enthüllungen gelten solche

Funde als Trophäen, die werbewirksam veröffentlicht werden können. Kaspersky will auf die ersten Spuren der Equation Group aufmerksam geworden sein, als seine Antivirensoftware auf den Versuch einer unbekannten Schadsoftware reagierte, sich mit einem seit 2005 bekannten Trick ins Windows-Betriebssystem einzunisten. Nach und nach fand das russische Unternehmen schließlich weitere Puzzlestücke sowie rund 300 sogenannte Command-and-Control-Server, die Daten aus den befallenen Rechnern empfingen.

Die NSA wollte den Bericht auf Anfrage verschiedener US-Medien nicht direkt kommentieren.

von Patrick Beuth 17. Februar 2015 10:05 Uhr Patrick Beuth