Peinliche Blöße

Die „Vault 7“-Dokumente zeichnen ein intimes Bild vom digitalen Arsenal der CIA

Wikileaks hat eine riesige Datensammlung mit Hacks und internen Dokumenten der CIA-Hackerabteilung veröffentlicht. Eine konkrete Gefahr für die Allgemeinheit geht von der Veröffentlichung nicht aus. Nichtsdestotrotz schlagen die Wellen hoch: Verschwörungstheoretiker sehen in dem Leak einen Beweis für die Einmischung der CIA in die US-Wahl.

Von Jo Bager

Sie geben ihren Systemen schon mal spaßige Bezeichnungen wie „Fine Dinner“ und „geekige“ Projektbilder; sie stellen ausführliche Listen mit Unicode-Gesichtern zusammen – Nerd-Humor: Die Mitarbeiter im Center for Cyber Intelligence (CCI) der CIA haben offenbar Spaß im Job. Ihr Auftrag allerdings ist ernster Natur: Sie stellen die Mittel für Angriffe auf IT-Infrastrukturen aller Art bereit, von der Telefonanlage über Smartphones und PCs bis hin zu vernetzter Haustechnik.

Wikileaks hat unter dem Codenamen Vault 7 begonnen, interne CIA-Papiere zu veröffentlichen, die einen Einblick in die Arbeit der Hacker geben. In einem ersten Schwung hat die Whistleblower-Plattform 8761 Dokumente mit Programmier-Tipps aus den Jahren 2013 bis 2016 veröffentlicht. Das Center of Cyber Intelligence betreute rund 500 Projekte, nicht wenige davon am „Center for Cyber Intelligence Europe“ (CCIE) in Frankfurt am Main. Insgesamt haben wohl 5000 Programmierer beim CCI gearbeitet, zumindest hatte das CIA-Wiki auf der Basis von Atlassian Confluence über 5000 registrierte Nutzer.

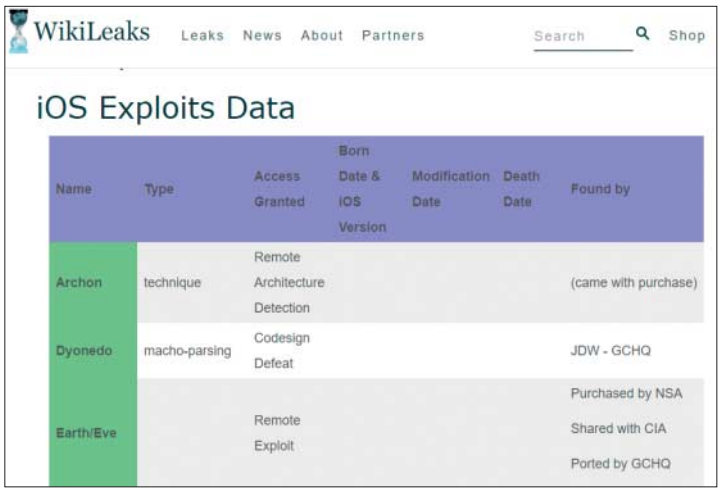
CIA not amused

Vault 7 soll nur der erste Teil einer größeren Dokumenten-Lieferung sein. Laut Wikileaks hat der Geheimdienst die Kontrolle über den Großteil seines Hacking-Arsenals verloren. Die Sammlung von insgesamt mehreren Hundert Millionen Code-Zeilen kursiere unter ehemaligen Hackern und Auftragnehmern der Agency, von denen einer Wikileaks mit einem Teil des Archivs versorgt habe.

Bislang hat die CIA die Echtheit der Sammlung nicht offiziell bestätigt. Sie ließ nur ganz allgemein verlauten: „Die amerikanische Öffentlichkeit sollte schwer besorgt sein“, wenn Wikileaks Veröffentlichungen vornehme, die dazu gedacht seien, die Leistungsfähigkeit der Geheimdienste beim Schutz Amerikas vor „Terroristen und anderen Gegnern“ zu beschädigen. Experten, die sich die Dokumente angesehen haben, sind von ihrer Echtheit überzeugt – wie Edward Snowden, der twitterte: „Looks authentic“.

Wikileaks hat bei seiner Veröffentlichung die Namen der CIA-Programmierer mit User-Nummern anonymisiert. Für Otto Normalanwender geht von den veröffentlichten Hacks scheinbar ebenfalls keine direkte Gefahr aus. Anders als einige Medien berichtet haben, können die CIA-Hacker etwa bewährte Verschlüsselungsverfahren wie die der Messenger WhatsApp oder Signal nicht knacken. Vault 7 enthält allerdings eine geballte Sammlung Wissen zum Thema Hacking. Wer sich über das Eindringen in fremde Systeme informieren will, findet in den Dokumenten einen guten Überblick.

Anders als bei den auf die massenhafte Überwachung ausgelegten NSA-Programmen geht es bei den CIA-Werkzeugen eher darum, die Systeme einzelner Zielpersonen zu infiltrieren. Dazu muss der Angreifer nicht selten physischen Zugang zu den Geräten haben.

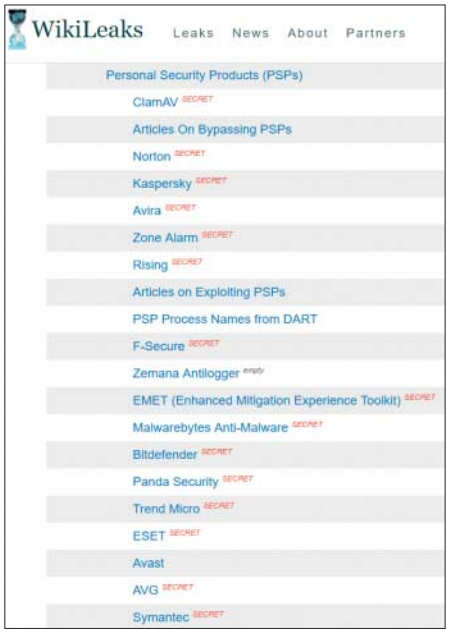


Die Vault-7-Dokumente listen detailliert auf, welche Exploits die CIA mit welchen befreundeten Diensten ausgetauscht hat.

Die Whistleblower-Plattform hat die in den Dokumenten beschriebenen Sicherheitslücken und Exploits, die noch missbraucht werden können, nicht veröffentlicht. Die Einzelheiten will Wikileaks zuerst den betroffenen Herstellern übergeben, damit diese ihre Lücken stopfen können. Einige Hersteller haben bereits Entwarnung gegeben, etwa Google. Apple will die wenigen Lücken, die noch offen stehen, schnell schließen.

Krude Theorien

Schnell wurden die Veröffentlichungen politisch verwertet. So enthalten die Dokumente Hinweise darauf, dass die CIA Techniken verwendet haben könnte, um ihre Spuren zu verwischen und wie das Werk russischer Hacker aussehen zu lassen. Vertreter der US-amerikanischen Alt-Right-Bewegung schließen daraus, dass die CIA russische Fake-Hacks produziere, um Trump zu schaden. Andere Beobachter sehen in der Veröffentlichung gar den Versuch von Wikileaks, sich bei Trump anzubiedern.



Die CIA-Sammlung enthält Werkzeuge, mit denen sich die verschiedensten Antivirenprogramme aushebeln lassen.

Egal, wie die Veröffentlichung politisch zu bewerten ist: Was bleibt, ist ein großer Schaden für die CIA. Ein solch riesiger Leak – noch dazu für jedermann abrufbar – ist die Höchststrafe für einen Geheimdienst. Es liegt nun mal in der Natur einer solchen Einrichtung, dass sich ihre Arbeit im Stillen vollziehen sollte und potenzielle Gegner im Unklaren über ihr Know-how bleiben.

Nach der Veröffentlichung aber kann sich jeder ein Bild davon machen, dass auch bei diesem Supergeheimdienst kein Hexenwerk betrieben wird. Selbst bei der CIA schlagen sich ganz normale Programmierer mit ganz normalen Programmierproblemen herum und lesen http://reddit.com/r/netsec, um auf dem Laufenden zu bleiben.

Mit den Vault-7-Dokumenten kann jeder genau nachvollziehen, dass die CIA zumindest zeitweise 22 Antivirenprogramme aushebeln konnte. Man kann einige wichtige Abteilungen des CCI identifizieren und man sieht gut aufgeschlüsselt, mit welchen befreundeten Geheimdiensten die CIA wann welche Zero-Day-Exploits ausgetauscht hat.

Es ist davon auszugehen, dass ein großer Teil der CIA-Tools mit der Veröffentlichung verbrannt ist; Antiviren-Software dürfte sie in Zukunft erkennen und blockieren. Das dürfte die Cyber-Fähigkeit der Agency um Jahre zurückwerfen.

(jo@ct.de) c't