Kurioser Fotoklau vom iPhone und Tipps zum Schutz

Schwachstellen gibt es immer und überall. Und nicht jede lässt sich mühelos ausnutzen. Aber: mit genügend Zeit und Biss wird auch das Absurdeste möglich, wie das Ausspionieren von iPhone-Daten aus einem Nachbarraum. Welche Fähigkeiten dafür nötig sind und wie man sich mit simplen Methoden schützt, verrät Sophos in diesem Worst-Case-Szenario.

Taschendiebstahl ist eine bekannte und gegenwärtige Lästigkeit. Dass man aber seiner Bilder und Daten auf seinem iPhone durch einen Hacker im Nebenzimmer beraubt wird, klingt für viele erst einmal unwahrscheinlich. Ist aber möglich, wie Ian Beer, ein renommierter Google-Project-Zero-Forscher, kürzlich zeigte. Er entdeckte eine Exploit-Sequenz, die es einem Angreifer tatsächlich ermöglicht, in ein nahegelegenes iPhone einzubrechen und persönliche Daten zu stehlen – und zwar ausschließlich via Drahtlos-Verbindungen, ohne Zutun von Benutzerklicks und ohne dass das unschuldige Opfer etwas davon mitbekommt.

Mit folgendem Versuchsaufbau wurde das Szenario in nebeneinander gelegenen Räumen nachgestellt:

- Im Versuch fotografierte eine Person ein "geheimes Dokument" mit dem iPhone in einem Raum.
- Und der Benutzer des Telefons musste sich ein YouTube-Video ansehen.
- Nebenan im anderen Raum startete eine Person einen Angriff auf das Smartphone in Raum 1, der einen Kernel-Fehler des Telefons ausnutzt.
- Der Exploit lud heimlich eine Malware auf das Telefon, gewährte sich Zugriff auf das Datenverzeichnis der Photo-App, las das "geheime Dokument“ und lud es unbemerkt auf einen Laptop herunter.
- Das angegriffene Telefon funktionierte während des gesamten Vorgangs normal weiter, ohne Warnungen, Pop-ups oder andere Hinweise, die den Benutzer auf den Hack aufmerksam machen könnten.

Soweit, so schlecht.

Fehler gibt es immer – viele bleiben aber unter dem Radar der Hacker.
Die gute Nachricht ist allerdings, dass die zentrale Schwachstelle, auf die sich Beer verließ, eine Schwachstelle ist, die er selbst gefunden und Apple gemeldet hat und die bereits behoben wurde. Wer also sein iPhone in den letzten Monaten aktualisiert hat, sollte vor diesem speziellen Angriff sicher sein.
Außerdem kostetet es ihn rund sechs Monate detaillierter und engagierter Arbeit, herauszufinden, wie er diese Schwachstelle ausnutzen konnte. Das zeigt, dass es mit genügend Ehrgeiz und Entschlossenheit zwar möglich ist, ein iPhone in unmittelbarer Nähe zu kompromittieren, diese Art der Übergriffe aber auch sehr unwahrscheinlich sind.

Hacker-Skills auf hohem Level
Um derartige Schwachstellen zu finden und um diese auch ausnutzen zu können, muss ein Hacker über sehr umfangreiche Fähigkeiten verfügen. Die Expertise, die Beer in diesem Versuch zum Einsatz brachte, liegt hauptsächlich in folgenden Bereichen:

- Das Aufspüren eines Kernel-Variablennamens, der riskant erscheint.
- Das Finden eines Fehlers im TLV-Datenverarbeitungscode.

- Aufbau eines Apple Wireless Direct Link (AWDL)-Netzwerktreiber-Stacks zur Erzeugung bösartiger Pakete.
- Einen Weg finden, wie Pakete, die den Puffer sprengen, an Sicherheitsprüfungen vorbeikommen.
- Lernen, wie man den Pufferüberlauf in eine kontrollierbare Heap-Korruption verwandelt.
- Das Testen von in diesem Fall insgesamt 13 verschiedenen Wi-Fi-Adaptern, um einen Weg zu finden, den Angriff zu starten.

Zu diesem Zeitpunkt hatte Beer bereits ein Proof-of-Concept-Ergebnis erreicht, bei dem die meisten triumphierend aufgehört hätten. Er war jedoch entschlossen, einen Zero-Click-Angriff zu kreieren, bei dem das Opfer nichts Konkreteres zu tun braucht, als einfach sein Telefon zu benutzen – ganz ohne verräterische Zeichen, anhand derer das Opfer gewarnt wäre. Beer hat sich dafür folgende Strategie zurechtgelegt:

- Vorgeben ein nahegelegenes Gerät zu sein, das Dateien zur gemeinsamen Nutzung über AirDrop anbietet. Wenn das anvisierte Smartphone aufgrund der Daten, das es via Bluetooth überträgt, glaubt, dass das Gerät in der Nähe einem seiner Kontakte gehören könnte, startet es vorübergehend AWDL um zu sehen, wer es ist. Wenn es sich nicht um einen der eigenen Kontakte handelt, sieht man kein Popup oder eine andere Warnung, aber der ausnutzbare AWDL-Fehler wird über das automatisch aktivierte AWDL-Subsystem kurzzeitig aufgedeckt.

- Den Angriff ausweiten, um mehr zu erreichen als nur eine bestehende Anwendung wie „Calc“ aufzurufen. Beer hat herausgefunden, wie er seinen anfänglichen Exploit in einer detaillierten Angriffskette einsetzen kann, um auf beliebige Dateien auf dem Gerät zuzugreifen und diese zu stehlen.

In der Simulation übernahm der Angriff mit YouTube eine Anwendung, die bereits lief. Er nutzte sie, um auf das DCIM-Verzeichnis (Kamera) zuzugreifen, das zur „#Fotos“-Anwendung gehört. Dann stahl er die letzte Bilddatei (das "geheime Dokument") und exfiltrierte sie über eine harmlos erscheinende TCP-Verbindung.

Sophos rät: Mehr Patches, weniger aktive Verbindungen
Auch wenn diese Art des Angriffs natürlich kaum massentauglich ist, zeigt er auf, dass bei entsprechender Hartnäckigkeit kaum Grenzen gesetzt werden. Allerdings können Nutzer sich auch vor solch ausgefuchsten Angriffen recht einfach schützen, wenn folgende Tipps beherzigt werden:

Tipp 1: Sicherheitsfixes auf dem neuesten Stand halten. Denn der Fehler, der das Herzstück von Beers Angriffskette bildet, wurde von ihm überhaupt erst gefunden und offengelegt, so dass er bereits gepatcht wurde.

Tipp 2: Abschalten von Datenverbindungen, wenn diese nicht benötigt werden. Beers Angriff ist eine gute Erinnerung daran, dass "weniger mehr ist", weil er Bluetooth benötigte, um einen echten Zero-Click-Angriff zu erzeugen.

Tipp 3: Man sollte sich nie ganz in Sicherheit wiegen, nur weil es wie in diesem Fall sehr schwierig sein kann, eine bestimmte Schwachstelle auszunutzen. Denn das ist kein Freifahrschein für sorgloses Verhalten mit dem Smartphone. Mit genügend Zeit und Engagement lässt sich nahezu alles kompromittieren.

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de