Unerkanntes Absaugen

Google deckt Attacken auf iOS über bisher unbekannte Lücken auf

Die Meldung schlug verzögert ein, aber dennoch wie eine Bombe: Google-Mitarbeiter haben Ende August veröffentlicht, dass iOS-Geräte offenbar jahrelang unerkannt ausspioniert werden konnten. Jeder, der bestimmte Webseiten aufsuchte, wurde zum Opfer.

Von Dušan Živadinović

Ob für PC, Laptop, Tablet oder Smartphone – praktisch alle Betriebssysteme weisen gravierende, aber öffentlich nicht bekannte Sicherheitslücken auf (Zero-Day). Besonders die unbekannten Lücken von Smartphones sind für Angreifer interessant, weil sie Passwörter oder andere für Strafverfolger und Spione interessante Daten enthalten.

Im Februar 2019 haben Mitarbeiter von Googles Security-Abteilung Project Zero einer vermutlich staatlich organisierten Angreifertruppe einen Strich durch die Rechnung gemacht: Sie entdeckten zahlreiche aktiv genutzte und bis dahin nicht bekannte Zero-Day-Angriffspunkte in iOS.

Alle Attacken führten bestimmte Websites offenbar ohne Kenntnis ihrer Administratoren oder Besitzer aus. Offen ist, auf welche Weise die Websites gehackt wurden und welche Werkzeuge die Angreifer darauf deponierten, um iOS-Geräte anzugreifen.

Es dürfte sich aber um eine ganze Reihe von Werkzeugen handeln, denn sie haben nicht nur 14 Lücken ausgenutzt, sondern damit auch insgesamt fünf verschiedene Angriffsroutinen für iOS 10, 11 und 12 gebaut (Exploit-Chains).

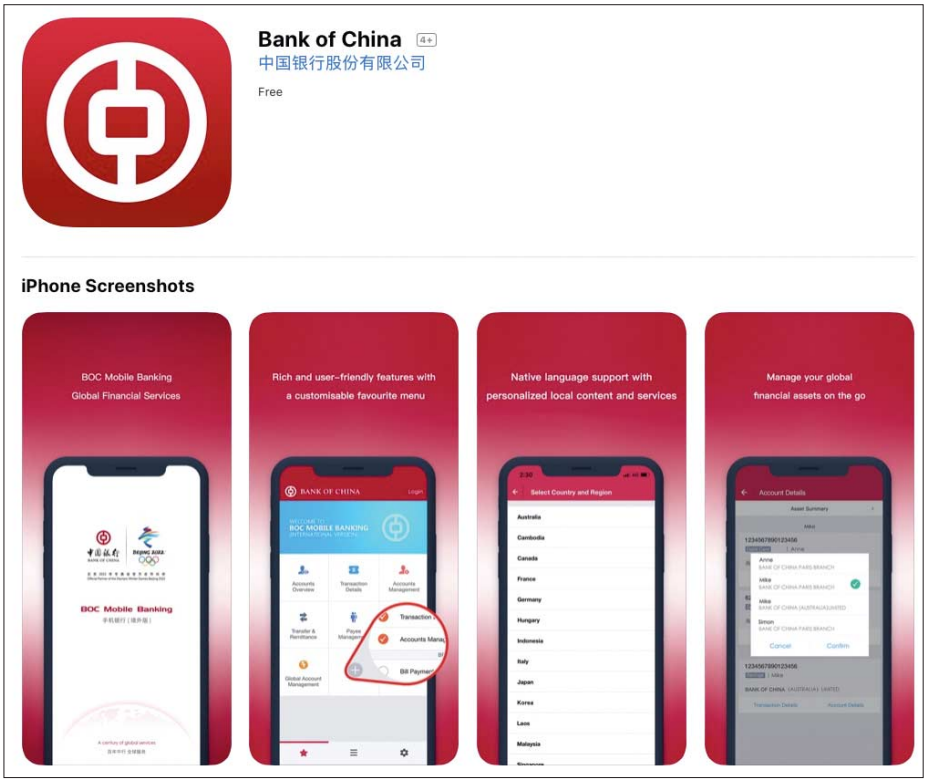
Googles Sicherheitsforscher Ian Beer schreibt dazu: „Schon der Besuch der Website genügte, um das Gerät anzugreifen und ein Abhörimplantat zu installieren“.

War das iPhone erstmal geknackt, ließ sich weitere Schadsoftware unerkannt nachladen. Auch konnten die Angreifer die iOS-Keychain mitsamt sämtlichen darin gespeicherten Passwörtern auslesen. Je nach Gewohnheiten oder Vorlieben der Nutzer stecken in der Keychain Zugangsdaten für Mail- und Websites oder auch für Online-Banken. Außerdem ließen sich Foto-, Kontakt- und Messaging-Datenbanken sowie der aktuelle Standort auslesen und versenden. Dazu nahm die Spionagesoftware alle 60 Sekunden Kontakt mit einem Kontrollserver auf.

Das Sicherheitsgefühl der Angreifer

Für die Programmierung dieser Kommunikation wandten die Angreifer anscheinend nur wenig Mühe auf – möglicherweise, weil sie sich sicher vor Entdeckung wähnten. Die iPhone-Daten wurden im Klartext, also ohne HTTPS-Verschlüsselung übertragen und die IP-Adressen der Zielserver waren fest kodiert.

Insgesamt gelten die Angriffe aber als hochkomplex und daher selten. Eine ähnlich komplexe, mehrstufige Angriffstechnik hat beispielsweise Cisco beschrieben. Damit wurden Mail- und VPN-Passwörter von Institutionen und Firmen in zwölf Ländern abgegriffen. Experten mutma-



Heikel: Strafverfolger und Sicherheitsbehörden behalten Sicherheitslücken für sich. Solange sie aber ungepatcht sind, können sie auch kriminellen Angreifern in die Hände fallen. Dann sind prinzipiell auch Online-Banking-Zugänge gefährdet.

ßen, dass die Angriffe von staatlich organisierten iranischen Gruppen ausgingen.

Die Attacken auf iOS-Geräte schreiben Fachleute ebenfalls staatlichen Akteuren zu. Ungewohnt ist jedoch, dass die Angreifer mit den wertvollen Zero-Day-Lücken eine nur diffus definierte Gruppe an Nutzern attackierten. Bisher setzte man solche Lücken nur gezielt für Angriffe auf einzelne Personen oder kleine Gruppen ein.

Das Project Zero von Google machte weder Angaben über die präparierten Websites, noch über die Herkunft der Angriffe. Laut dem IT-Blog TechCrunch und dem Wirtschaftsmagazin Forbes soll der Ausgangspunkt in China liegen. Ziel seien uigurische Muslime gewesen, die in der chinesischen Provinz Xinjiang leben.

Zwar wurde eine Handy-Überwachung in Xinjiang mittels Schadcode schon beschrieben. Sie richtete sich jedoch vor allem gegen Android-Nutzer. Chinesische Zollbeamte sollen beim Grenzübertritt Malware auf Geräte aufgespielt haben. Zudem gab es Durchsuchungen von iPhones mit spezieller Hardware. iOS-Angriffe per Drive-by-Download sind hingegen neu und gerade deshalb bedenklich – denn weltweit jedes iPhone, das eine solche Website öffnete, wurde geknackt und ließ sich auslesen.

Gegenmaßnahmen

Das Auslesen lässt sich immerhin leicht stoppen: Die aktuellen Implantate sind nach einem Neustart des iPhones aus dem Arbeitsspeicher getilgt; auf dem Festspeicher lassen sie sich laut Google nicht nieder. Über die zuvor abgesaugten Daten hat man natürlich keine Kontrolle mehr. Deshalb empfiehlt es sich, möglichst alle Passwörter zu ändern.

Im Februar gab Apple mit der Version 12.1.4 ein iOS-Update heraus, das die bis dahin von Project Zero aufgedeckten Lücken schließt. Sollten Sie das noch nicht eingespielt haben: Tun Sie es umgehend.

So weit bisher bekannt, starteten alle Angriffe mit einer Attacke auf Apples Safari-Browser. Diese waren so spezifisch auf Safari zugeschnitten, dass Firefox- oder Brave-Nutzer ungeschoren davonkamen. Allerdings gründen auch diese Browser auf dem iOS-Webkit und sind daher prinzipiell anfällig. Die Angreifer könnten das künftig für ihre Zwecke nutzen.

In Mails oder Messaging-Apps eingebetteten Links sollte man nicht per Antippen folgen, weil sie in der iOS-Werkseinstellung per Safari-Browser geöffnet werden. Um das zu verhindern, müsste man entweder Copy-and-paste verwenden oder die Standard-Browsereinstellung umkonfigurieren.

Auch sind iPhones mit A12- oder A12X-CPUs nicht betroffen, also etwa die Modelle XS und XR. Angesichts des geballten Know-hows der Angreifer sollte man sich aber nicht darauf verlassen, dass das so bleiben wird.

Derweil melden die umstrittenen Sicherheitslückenhändler Crowdfense und Zerodium, dass der Markt neuerdings von Angeboten „überflutet“ sei.

Handel mit Exploits

Laut Chaouki Bekrar, Gründer von Zerodium, betreffen die zuletzt angebotenen Exploits vor allem Safari und Apples verschlüsselten Kommunikationsdienst iMessage. Der Grund für das erhöhte Angebot sei, dass sich viele Forscher der iOS-Analyse inzwischen in Vollzeit widmeten. Bekrar gab gegenüber dem IT-Blog Motherboard an, es gebe „so viele iOS-Exploits, dass wir begonnen haben, einige zurückweisen“.

Außerdem hat seine Firma die Preise für Exploits gesenkt. Eine Chain, mit der sich iOS-Geräte vollständig übernehmen lassen, ohne dass Nutzer einen Finger rühren, ist „nur“ 2 Millionen US-Dollar wert. Für 1-Click-iOS-Chains müssen Angreifer das Opfer dazu bringen, einen Klick durchzuführen, um sich zu infizieren. Dafür zahlt der Exploit-Broker 1 Million US-Dollar. Zuvor waren es 1,5 Millionen US-Dollar.

Auf Android schränken die zahlreichen Betriebssystemvarianten die Zahl an weitläufig einsetzbaren Exploits ein, meint Bekrar. Für eine Exploit-Chain, mit der sich Android-Geräte ohne Nutzerinteraktion übernehmen lassen, will Zerodium nun 2,5 Millionen US-Dollar zahlen.

(dz@ct.de) c't

Analyse von Project Zero: ***ct.de/y7ps***