Analysiert: Spioniert die undokumentierte WhatsApp-Umstellung?

Hintergrund 16.08.2016 00:07 Uhr – Jürgen Schmidt

In der Anzeige von WhatsApp tauchen plötzlich Namen auf, die aus dem privaten Adressbuch stammen. Spioniert die neue Version etwa im Auftrag des Konzerns in den Kontakten der Anwender? heise Security ging dem Verdacht eines Lesers nach und stieß auf spannende WhatsApp-Interna.

Manche Informationen von Lesern schaffen es nicht in die News. So auch diese Geschichte rund um WhatsApp, die sich als nicht nachrichtenwürdig entpuppte, in deren Lauf wir aber einiges über die Funktionsweise von iOS und WhatsApp lernten. Deshalb dokumentieren wir die Recherchen hier im Rahmen unserer heisec-Serie Analysiert -- ein Blick hinter die Kulissen.

Zweifelhafte Adressbuchzugriffe

Mit der vor wenigen Tagen veröffentlichten aktuellen WhatsApp-Version 2.16.8 für iOS änderte sich der angezeigte Absendername von Nachrichten in den Pop-ups. Statt wie bisher den vom Absender eingestellten WhatsApp-Namen präsentieren die Pop-ups jetzt den im Adressbuch des Empfängers gespeicherten. In den Informationen zur neuen Version fand sich kein Hinweis auf diese Änderung. Kein Wunder also, dass Sicherheitsberater Holger Ahrend misstrauisch wurde und vermutete, dass die Adressbuchdaten seit der Umstellung bei WhatsApp landen.

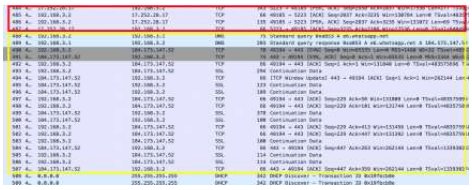
Zum Hintergrund: Laut der Informationen zum Datenschutz lädt WhatsApp zum Bereitstellen der verfügbaren WhatsApp-Kontakte eines Nutzers lediglich die Telefonummern seines Adressbuchs auf den WhatsApp-Server hoch; E-Mail-Adressen und Namen hingegen nicht. Sollte WhatsApp gegen die eigenen Datenschutz-Versprechen verstoßen, wäre das ein ziemlich heftiger Vertrauensmissbrauch.

heise Security konnte schon mal die von Ahrend beschriebene, undokumentierte Verhaltensänderung nachvollziehen. Doch bei der Anzeige des Namens hatten wir einen anderen Verdacht; also forschten wir weiter. Als erstes führten wir folgenden Test durch:

1. WhatsApp via SwipeUp in der Prozessübersicht beendet, Flugmodus eingeschaltet
2. Adressbucheintrag von "Heinz" geändert auf "Heinz (XXX)"

3. WhatsApp gestartet, Adressbuch lokal aktualisiert, "Favoriten" zeigt jetzt lokal "Heinz(XXX)" an, der Server kennt den Namen noch nicht (immer noch im Flugmodus)
4. WhatsApp via SwipeUp beendet
5. Flugmodus aus
6. Heinz schickt uns eine WA-Nachricht

Das sollte sicherstellen, dass WhatsApp zwar die Möglichkeit hatte, sich lokal mit dem Adressbuch abzugleichen, diese Informationen jedoch nicht auf den Server schieben konnte. Als Resultat erschien trotzdem eine Push-Nachricht mit: "Heinz (XXX): ..."



Die Push-Nachricht kommt von einem Apple-Server (roter Kasten). Anschließend startet WhatsApp und baut eine Verbindung zum Server auf (gelb). (Bild: Holger Ahrend)

Die logische Schlussfolgerung daraus: Der Abgleich zwischen Telefonnummer und Adressbuch erfolgt lediglich lokal zur Anzeige des richtigen Namens. Bei einem zweiten Test dieser Art bestätigte Ahrend auch noch, dass nach dem Beenden des Flugmodus bis zum Eintreffen der Nachricht keine Kommunikation mit einem WhatsApp-Server statt fand. Der angezeigte, neue Name konnte also nicht aus WhatsApps Datenbanken stammen.

WhatsApp und Silent Notifications

Doch wie kann WhatsApp Namen aus dem Adressbuch in die vom System angezeigten Push-Nachrichten einbauen? Dazu müsste sich die App in den Empfang der von Apple verschickten Push-Notifications einklinken und sie vor deren Anzeige ändern. Klingt nach einem klassischen Notification-Hook.

Doch wie uns iOS-Experte Klaus Rodewig auf Nachfragen erklärte, erfolgt bis inklusive iOS 9 die Darstellung von Push-Nachrichten unabhängig von der App. Das Betriebssystem zeigt diese an, ohne dass die App auf den Inhalt einwirken kann. Echte Hooks kommen erst mit iOS 10. Unsere erste Theorie war damit also schon mal hinfällig.

Allerdings gibt es sogenannte Silent Notifications, erklärte Rodewig weiter. Die zeigt iOS nicht an, sondern reicht sie an die App durch. Es wäre also durchaus möglich, dass WhatsApp die Notification empfängt und dann als lokale Notification mit dem lokalen Adressbuchnamen anzeigt. Der Unterschied zu einer externen Push-Nachricht wäre für den Anwender nicht erkennbar.

Mit solchen Silent Notifications wäre das beobachtete Verhalten also durchaus zu realisieren. Und es würde neben dem Namen auch eine andere Merkwürdigkeit erklären. Nämlich dass die Push-Nachrichten bereits die Ende-zu-Ende-verschlüsselten Texte präsentieren können.

Das PushKit-Framework

Parallel dazu befragten wir den heise-Security-Autoren und iOS-Reverse-Engineering-Experten Adreas Kurtz, ob er bestätigen könne, dass WhatsApp die Push-Nachrichten lokal prozessiert. Und Kurtz wartete mit einer kleinen Überaschung auf. Ein schneller Blick auf den Code enthüllte, dass WhatsApp zwar keine Silent Notifications aber die sogenannten VoIP Notifications des recht neuen PushKit-Frameworks von iOS einsetzt.

Die Verarbeitung eingehender Nachrichten erfolgt dann letztendlich in der Klasse `WAMessageNotificationCenter`. Darin ist am Ende die Methode `presentLocalNotificationIfNeededForMessage:fromUser:withSoundEffect:` dafür zuständig, dem Anwender über den Eingang einer neuen Nachricht zu informieren. Der angezeigte Name ist dabei das Attribut `partnerName` aus der zugehörigen `WAChatSession`. Dies alles konnte Kurtz unter anderem mit dem Tool cycript verifizieren. Es erlaubte ihm unter anderem mit einem Befehl wie

Man-in-the-Middle-Angriff: Online-Zocker im Visier von Online-Kriminellen

Mit einem ungewohnt ausgefeilten Trojaner machen Online-Ganoven derzeit Jagd auf Gamer: Der Schädling installiert ein Root-Zertifikat und manipuliert damit TLS/SSL-Verbindungen. Er wird über YouTube verbreitet

Hintergrund

Neueste Forenbeiträge

Re: Da geht noch was.

Mario Schmidt schrieb am 08.10.2018 07:18: Das ist "advanced"! :-O

Forum: Lojax: Der Spion, der aus dem BIOS kam

von reichhart; vor 38 Minuten

Re: Ein paar technische Details

davor schrieb am 06.10.2018 16:48: Ich befasse mich u.a. mit Manipulationsschutz bei Geldverarbeitenden Systemen. Ohne zu sehr ins Detail…

Forum: Winzige Spionage-Chips aus China: Was da…

von Hightower; vor einer Stunde

Re: Aluhut

Ach so, Du bist also einer von der „Nichts zu verbergen“-Sorte. Schon klar.

Forum: Bericht: Winzige Chips spionierten in Cloud…

von ufo70; vor einer Stunde

```
cy# choose(WAChatSession)[1].partnerName = "Test Test“
```

einen beliebigen Absendernamen zu setzen.

WhatsApp entlastet

Damit war für uns klar, dass zumindest im Rahmen von Empfang und Anzeige der Push-Nachrichten keine Namen an den WhatsApp-Server gehen – und diese Geschichte kein Platz in unseren News verdient. Einen unumstößlichen Beweis, dass WhatsApp Namen und E-Mail-Adressen nicht doch bei passender Gelegenheit an die eigenen Server schickt, stellt das natürlich immer noch nicht dar. Den könnte höchstens ein umfassendes Komplett-Audit der App erbringen. (ju)

Analysiert: Die heise-Security-Serie für den Blick hinter die Kulissen.

Kommentare lesen (25 Beiträge)

Forum zum Thema: Desktopsicherheit

https://heise.de/-3295090 Drucken

Mehr zum Thema:

ANALYSIERT IOS VOIP WHATSAPP

News
7-Tage-News
News-Archiv
Hintergrund-Artikel
Alert-Meldungen

Newsletter
Tools
Foren
RSS
mobil

Security Consulter
Netzwerkcheck
Anti-Virus
Emailcheck
Browsercheck
Krypto-Kampagne