Google gibt zu, dass „andere“ auf die Kameras von Samsung- und Android-Smartphones zugreifen können + Gesichtserkennung ~ Simon Parkes

transinformation.net/google-gibt-zu-dass-andere-auf-die-kameras-von-samsung-und-android-

Alkione

December 13, 2019

am 23. November 2019 von Alanna Ketler auf Collective Evolution veröffentlicht, übersetzt von Alkione

In Kürze

Die Fakten:

Hacker konnten erfolgreich – ohne Zustimmung des Benutzers und unabhängig davon, ob das Telefon entsperrt wurde oder nicht – auf die Frontkameras von Google- und Samsung-Handys zugreifen. Sie konnten Fotos machen und Videos aufnehmen.

Zum Nachdenken:

Warum sollte dir das was ausmachen? Dies ist eine regelrechte Verletzung unseres Rechts auf Privatsphäre. Wenn wir weiterhin bereitwillig auf alle unsere Rechte verzichten, werden wir bald keine mehr haben.

So praktisch wie sie sind, unsere Smartphones sind buchstäblich tragbare Ortungsgeräte. Ausgestattet mit GPS-Technologie, können Menschen leicht lokalisiert werden und für die meisten Android-Nutzer wird, seit sie ihre schicken Telefone haben, online eine

Aufzeichnung darüber gespeichert, wo sie jeden Tag gewesen sind. Falls das nicht schon beängstigend genug ist – die Mikrofone unserer Telefone sind auch in der Lage, unsere Gespräche aufzuzeichnen, weil sie zuhören, auch wenn wir nicht glauben, dass sie es tun. Und zu guter Letzt – du kennst diese praktischen Frontkameras, die oft verwendet werden, um das perfekte Selfie aufzunehmen? Vor kurzem haben Forscher gezeigt, wie man mit dieser Kamera Benutzer ausspionieren kann. Wer hätte das gedacht?

Das Sicherheitsforschungsteam von Checkmarx hat eine grosse Schwachstelle aufgedeckt, die Google- und Samsung-Smartphones betrifft und die Hunderte von Millionen Android-Nutzer auf der ganzen Welt betreffen könnte. Anscheinend ist es jetzt behoben, doch die Forscher haben einen Weg für Hacker entdeckt, die Kontrolle über die nach vorne gerichtete Kamera zu übernehmen und aus der Ferne Fotos zu machen, Videos aufzunehmen, deine Gespräche zu belauschen und mehr. Alles geschieht unbemerkt im Hintergrund ohne dein Wissen.

Und auch wenn es wichtig ist zu beachten, dass das Folgende nur Spekulation ist: Wenn Hacker die Fähigkeit haben, dies zu tun, dann solltest du besser glauben, dass die NSA und andere hochrangige Regierungsbehörden in der Lage sind, dasselbe zu tun. Das ist nichts Neues. Edward Snowden, NSA-Whistleblower, und viele andere wie er haben darüber gesprochen und erklärt, wie unsere Telefone tatsächlich benutzt werden, um uns auszuspionieren.

Was hat das Sicherheitsforschungsteam von Checkmarx herausgefunden?

Ihre Forschung begann mit der Google-Kamera-App auf den Smartphones Pixel 2XL und Pixel3. Sie fanden einige Schwachstellen, die dadurch entstanden, dass sie einem Angreifer erlaubten, Benutzerrechte aus der Ferne zu umgehen. Anscheinend sind Gesichtserkennung-, Fingerabdruck- und Passwortsicherheit nicht so sicher, wie uns weisgemacht wurde.

> „Unser Team hat einen Weg gefunden, bestimmte Aktionen und Vorhaben zu manipulieren“, sagte Erez Yalon, Leiter der Sicherheitsforschung bei Checkmarx, „der es jeder Applikation ermöglicht, ohne besondere Berechtigungen die Google-Kamera-App zu steuern. Dieselbe Technik galt auch für Samsungs Kamera-App.“

Davey Winder von Forbes.com erklärt, wie ein Angreifer in der Lage ist, die Schwachstellen der Google-Kamera-App zu nutzen:

> Checkmarx schuf einen Machbarkeitsnachweis (PoC), indem es eine Malware-App entwickelte, eine Wetter-App, wie sie seit jeher im Google Play Store beliebt ist. Diese App erforderte keine besonderen Berechtigungen ausser dem einfachen Speicherzugriff. Wenn man nur diese einzige, alltägliche Erlaubnis verlangt, ist es unwahrscheinlich, dass die App die Alarmglocken des Benutzers auslöst. Schliesslich sind wir darauf eingestellt, unnötige und umfangreiche Berechtigungsanforderungen in Frage zu stellen und nicht nur eine einzige, gängige. Diese App war jedoch keineswegs harmlos. Sie bestand aus zwei Teilen, der Client-App, die auf dem Smartphone läuft und einem Befehls- und Steuerungsserver, mit dem sie sich verbindet, um das Ansinnen des Angreifers zu erfüllen. Sobald die App installiert und gestartet ist, baut sie eine dauerhafte Verbindung zu diesem Befehls- und Steuerungsserver auf und wartet dann auf Anweisungen. Das Schliessen der App hat diese Serververbindung nicht beendet. Welche Anweisungen könnte der Angreifer senden, die zu welchen Aktionen führen?

Ich hoffe, dass du dich hingesetzt hast, denn es ist eine lange und besorgniserregende Liste.

- Ein Foto mit der Smartphone-Kamera aufnehmen und auf den Kommandoserver hochladen
- Ein Video mit der Smartphone-Kamera aufnehmen und auf den Befehlsserver hochladen
- Warten, bis ein Sprachanruf gestartet wird, indem der Annäherungssensor des Smartphones überwacht wird, um festzustellen, wann das Telefon am Ohr gehalten wird, und den Ton aus beiden Seiten des Gesprächs aufzunehmen
- Während dieser überwachten Anrufe konnte der Angreifer auch Videos des Benutzers aufnehmen und gleichzeitig Audio aufnehmen.
- Erfassen von GPS-Tags aus allen aufgenommenen Fotos und so den Besitzer auf einer Weltkarte lokalisieren
- Auf die gespeicherten Foto- und Videoinformationen sowie die während eines Angriffs aufgenommenen Bilder zugreifen und diese kopieren
- Heimlich arbeiten, indem das Smartphone beim Fotografieren und Aufnehmen von Videos zum Schweigen gebracht wird, so dass kein Auslöser der Kamera ertönt, der den Benutzer warnt
- Die Foto- und Videoaufzeichnung konnte unabhängig davon, ob das Smartphone entsperrt war, eingeleitet werden.

Natürlich schien Google, als sie mit diesem alarmierenden Problem konfrontiert wurden, froh zu sein, davon zu hören, damit sie das Problem beheben konnten – so sagten sie es Winder, nachdem er sich gemeldet hatte:

> „Wir schätzen es, dass Checkmarx uns darauf aufmerksam macht und mit Google- und Android-Partnern zusammenarbeitet, um die Bekanntgabe zu koordinieren. Das Problem wurde auf betroffenen Google-Geräten über ein Play Store Update der Google-Kamera-App im Juli 2019 behoben. Ein Patch wurde auch allen Partnern zur Verfügung gestellt.“

Warum sollte es dich kümmern?

Während es grossartig ist, dass sie ihre Sicherheit erhöhen, besteht für mich kein Zweifel daran, dass Hacker einen Weg finden können, um die neue Sicherheit zu umgehen. Und was meiner Meinung nach noch beunruhigender ist als Hacker, ist, dass Regierungsbehörden die Möglichkeit haben, wann immer sie wollen ohne deine Erlaubnis oder dein Wissen deine Kamera einzuschalten und sich einzuloggen.

Kommt dir das bekannt vor?

Das ist im wahrsten Sinne des Wortes Orwells 1984, das zum Leben erwacht! Wenn du mit diesem Buch nicht vertraut bist, empfehle ich es dir erstens sehr, und zweitens prognostiziert es im Grunde genommen eine totalitäre Regierung, die als „Big Brother" bezeichnet wird, die ständig zusieht und ausspioniert, um sicherzustellen, dass die Bürger sich an die vom Staat festgelegten Regeln halten.

Wie Orwell schreibt:

> „Der Bildschirm empfing und übertrug gleichzeitig. Jeder Klang, den Winston machte, der über der Ebene eines sehr leisen Flüsterns lag, wurde von ihm aufgenommen; ausserdem konnte er, solange er sich im Sichtfeld befand, das die Metalltafel vorschrieb, sowohl gesehen als auch gehört werden. Es gab natürlich keine Möglichkeit zu wissen, ob man zu irgendeinem Zeitpunkt beobachtet wurde. Wie oft oder über welches System die Gedankenpolizei an einen einzelnen Draht angeschlossen war, war reine Vermutung. Es war sogar denkbar, dass sie alle die ganze Zeit zusahen. Aber auf jeden Fall konnten sie dein Kabel einstecken, wann immer sie wollten. Du musstest leben – lebtest, aus Gewohnheit, die zum Instinkt wurde – in der Annahme, dass jeder Ton, den du gemacht hast, gehört wurde, und, ausser in der Dunkelheit, jede Bewegung auf Herz und Nieren geprüft wurde."

und ...

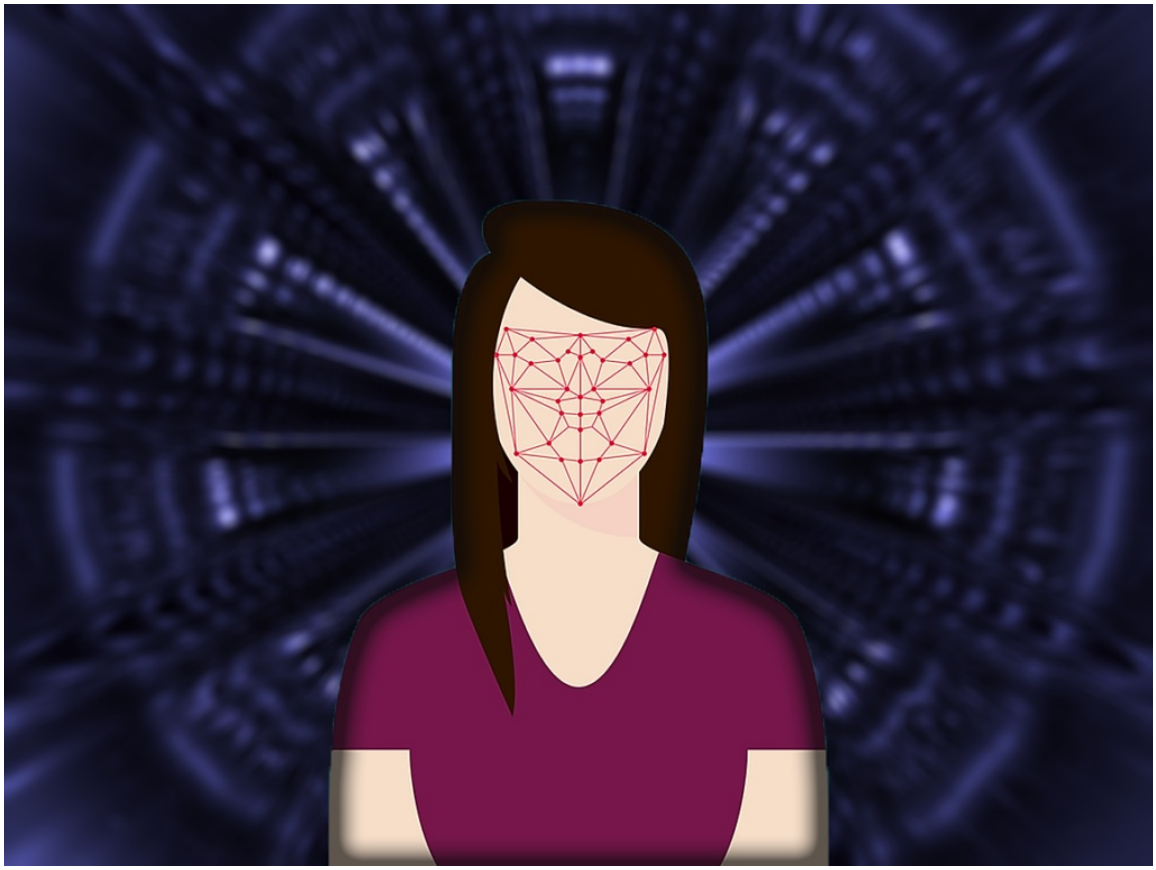
> „Er dachte an den Fernseher mit seinem niemals schlafenden Ohr. Sie konnten dich Tag und Nacht ausspionieren, aber wenn du die Ruhe bewahren würdest, könntest du sie immer noch überlisten. Mit all ihrer Geschicklichkeit hatten sie nie das Geheimnis gemeistert, herauszufinden, was ein anderer Mensch dachte. … Fakten konnten unter keinen Umständen verborgen bleiben. Sie konnten auf Anfrage aufgespürt werden, sie konnten durch Folter aus dir herausgeholt werden. Aber wenn das Ziel nicht darin bestand, am Leben zu bleiben, sondern menschlich zu bleiben, welchen Unterschied machte es dann letztendlich? Sie konnten deine Gefühle nicht ändern; in der Tat konntest du selbst sie nicht ändern, auch wenn du es wolltest. Sie konnten alles, was du getan oder gesagt oder gedacht hast, bis ins kleinste Detail enthüllen; aber das innere Herz, dessen Funktionsweise selbst für dich persönlich geheimnisvoll war, blieb unbezwingbar."

Was können wir also tun?

Ich bin sicher, es gibt eine grosse Anzahl von euch da draussen, die denken, *ich habe nichts zu verbergen, also wen interessiert das?* Dies ist eine sehr passive Haltung, und es geht nicht darum, ob du an illegalen Aktivitäten teilnimmst oder nicht, und/oder ob du Angst hast, ins Gefängnis gesteckt oder von Behörden erwischt zu werden. Es geht um unser Recht auf Privatsphäre. Wie der Informant Edward Snowden sagte, ist es nicht anders, zu argumentieren, dass du dich nicht um das Recht auf Privatsphäre kümmerst, weil du nichts zu verbergen hast, als zu sagen, dass du dich nicht um die freie Meinungsäusserung sorgst, weil du nichts zu sagen hast.

Aber jedem das Seine. Einige Massnahmen, die du ergreifen kannst, um deine Privatsphäre zu schützen:

- Überklebe die nach vorne gerichtete Kamera auf deinem Gerät, wenn du sie nicht benutzt.
- Du kannst etwas über das Mikrofon kleben, wenn du es nicht benutzt.
- Schalte dein Handy aus, wenn es nicht benutzt wird.
- Nutze dein Handy einfach weniger, und wenn es nicht benutzt wird, leg es in einen anderen Raum.
- Du magst besonders vorsichtig sein wollen, wenn du vorhast, deine Regierung umzuwandeln oder zu stürzen.
- Du kannst wirklich raffinierte kleine Schiebeabdeckungen kaufen, um deine Kamera für dein Handy und deinen Computer zu blockieren.
- Ich persönlich spiele mit der Idee, zum guten alten, einfachen Flip-Telefon zurückzukehren … nicht nur aus Gründen der Sicherheit und des Datenschutzes, sondern um nicht so viel Zeit zu verschwenden.



Passend zu dem obenstehenden Artikel hat Simon Parkes am 1. Dezember folgenden Beitrag veröffentlicht.

Gesichtserkennung

China verlangt jetzt von jedem, der ein neues Handy kauft, dass sein Gesicht fotografiert, abgeglichen und in die chinesische Datenbank zur Gesichtserkennung aufgenommen wird.

Wenn jetzt jemand ein Handy benutzt, um Anti-Regierungsbeiträge zu schreiben, kann er identifiziert und bestraft werden. Die Ausrede, dass jemand anderes dein Telefon benutzt hat, fällt damit weg.

https://www.bbc.co.uk/news/world-asia-china-50587098