Warnungen vor „Juicejacking“:
Wenn die öffentliche Ladestation hinter Ihrem Rücken mit Ihrem Smartphone interagiert

Wie gefährlich ist das Smartphone-Laden an öffentlichen Stationen?
Zuletzt warnten sogar FBI und FCC, das das Kriminelle öffentliche USB-Ports nutzen, um Malware und Überwachungssoftware auf Geräten einzuführen.
Sophos-Experte Paul Ducklin hat mit verschiedenen Smartphones die Probe aufs Exempel gemacht und gibt Tipps zur Sicherheit.

Wenn Sie das Cybersicherheits-Modewort „Juicejacking“ bisher noch nicht gehört haben, keine Panik. Der Begriff hatte Anfang der 2010er-Jahre für Aufmerksamkeit gesorgt, spielt aber auch heute noch eine Rolle im täglichen Smartphone-Leben – und hat aufgrund aktueller Warnhinweise, unter anderem vom FBI, kürzlich überraschend neue Popularität erlangt.

Beginnen wir zunächst mit einer kurzen Erklärung des Begriffs: Menschen, die unterwegs sind, insbesondere an Flughäfen, wo das eigene Telefonladegerät entweder tief im Handgepäck verstaut ist oder bereits im Frachtraum eines Flugzeugs steckt, werden oft von Ladeangst heimgesucht. Das Schreckgespenst vom leeren Akku, das uns seit dem Start mobiler Telefone heimsucht, geistert auch heute noch quietschfidel durch die Smartphone-Welt und führt trotz Powerbank & Co. dazu, dass gerade auf Reisen jede Möglichkeit genutzt wird, den Akku zu füllen – für den Fall, dass in naher Zukunft keine Möglichkeit mehr dazu besteht.

Was passiert da hinter Ihrem Rücken?
Und hier kommen die Juicehacking-Kriminellen ins Spiel. Smartphones werden allgemein über USB-Kabel aufgeladen, die speziell so konzipiert sind, dass sie sowohl Strom als auch Daten übertragen können. Was ist also, wenn sich am anderen Ende der Ladestation ein Computer befindet, der nicht nur 5 Volt Gleichstrom liefert, sondern zusätzlich hinter Ihrem Rücken versucht, mit Ihrem Telefon zu interagieren? Die einfache Antwort ist, dass Sie nicht sicher sein können. Genau aus diesem Grund haben sowohl Apple als auch Google schon seit Langem Standardeinstellungen eingeführt, die das Überraschungsmoment aus der Gleichung herausnehmen, indem beim Verbinden mit einem unbekannten Gerät eine Sicherheitsabfrage initiieren wird, ob der neuen Quelle vertraut werden soll. Abgesehen davon, dass Nutzer natürlich immer noch ausgetrickst oder überredet werden können, einem neuen Gerät zu vertrauen, kann also theoretisch kein Datenabruf mehr hinter dem Rücken des Besitzers stattfinden, ohne dass dieser selbst aktiv wird.

Etwas überraschend sind deshalb die aktuellen Warnungen von FBI und FCC davor, das Kriminelle öffentliche USB-Ports nutzen, um Malware und Überwachungssoftware auf Geräten einzuführen. Um Missverständnissen vorzubeugen: es ist auf jeden Fall angebracht, wann immer möglich, das eigene Ladegerät zu verwenden und sich nicht auf unbekannte USB-Stecker oder -Kabel zu verlassen. Nicht zuletzt, weil niemand wissen kann, wie sicher oder zuverlässig der Spannungswandler im Ladekreis ist.

Wie sicher sind die Daten?
Aber was ist mit dem Risiko, dass persönliche Daten heimlich von einem Ladegerät eingesogen werden, das auch als Host-Computer fungiert und versucht, ohne Erlaubnis die Kontrolle über das angeschlossene Gerät zu übernehmen? Haben die

Sicherheitsverbesserungen, die im Zuge des Mactans-Juicejacking-Tools im Jahr 2011 eingeführt wurden, immer noch Bestand? Sophos-Experte Paul Ducklin hat die Probe aufs Exempel gemacht und kommt basierend auf dem Anschließen eines iPhone (iOS 16) und eines Google Pixel (Android 13) an einen Mac (macOS 13 Ventura) und einen Windows 11-Laptop (2022H2-Build) zu dem Ergebnis: Ja, die Abfragen erfüllen weiterhin ihren Zweck. Erstens würde sich kein Telefon beim ersten Anschließen automatisch mit macOS oder Windows verbinden, egal ob gesperrt oder entsperrt. Zudem verweisen Genehmigungs-Popups deutlich darauf hin, dass ein fremdes Gerät zugreifen möchte – was aktiv bestätigt werden muss. Da aber bekanntlich der Teufel im Detail steckt, können Smartphone-Besitzer trotz dieser guten Sicherheitsbarrieren auf Nummer sicher gehen.

Auf folgende Dinge sollten Sie achten:

- Vermeiden Sie nach Möglichkeit unbekannte Ladestecker oder -kabel. Selbst eine in gutem Glauben eingerichtete Ladestation hat möglicherweise nicht die gewünschte elektrische Qualität und Spannungsregelung. Vermeiden Sie auch billige Netzladegeräte oder laden Sie vom eigenen Laptop aus auf.
- Sperren oder schalten Sie Ihr Telefon aus, bevor Sie es an ein öffentliches Ladegerät oder einen fremden Computer anschließen. Dadurch wird das Risiko minimiert, versehentlich Dateien für bösartige Aktivitäten offen zu legen. Zudem ist sichergestellt, dass das Gerät gesperrt ist, wenn es an einer Ladestation für mehrere Benutzer gestohlen wird.
- Falls Sie ein iPhone besitzen, können Sie erwägen, allen Geräten nicht zu vertrauen. Dadurch wird sichergestellt, dass keine ehemals vertrauenswürdigen Geräte vergessen werden, die Sie möglicherweise auf einer früheren Reise versehentlich eingerichtet haben.
- Erwägen Sie die Anschaffung eines Power-only-USB-Kabels oder einer Adapterbuchse. „Datenlose“ USB-A-Stecker sind leicht zu erkennen, da sie nur zwei metallische elektrische Anschlüsse in ihrem Gehäuse an den Außenkanten der Buchse haben, anstatt vier Anschlüsse über die Breite. Beachten Sie, dass die inneren Anschlüsse nicht immer sofort sichtbar sind, da sie nicht bis zum Rand der Buchse reichen – daher stellen die Stromanschlüsse zuerst Kontakt her.

Social Media von Sophos für die Presse

Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

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