Selbstverteidigung

Android-Schädlinge erkennen und loswerden

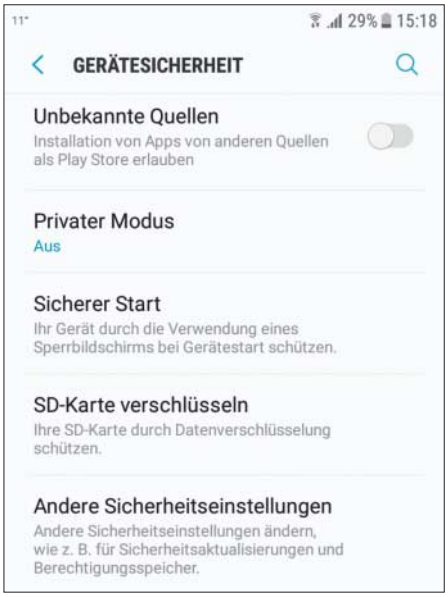
Die Patches für Meltdown und Spectre sind noch nicht überall angekommen, da tauchen bereits die nächsten angeblichen Android-Bedrohungen auf: AdultSwine, Skygofree, Dark Caracal. Es ist weder nötig, übervorsichtig das Handy in den Sondermüll zu geben, noch ratsam, einfach nichts zu tun.

Von Jörg Wirtgen

Da kann einem schon etwas mulmig werden – ständig tauchen Sicherheitslücken in Android selbst, in den Prozessoren und in Apps auf. Am berüchtigtsten sind zurzeit Meltdown und Spectre: Die raffinierten Angriffe gegen Smartphone- und Tablet-Prozessoren lassen sich nur durch Firmware-Updates von den Geräteherstellern (der Security-Patch vom Januar ist erforderlich) und durch App-Updates abwehren – vor allem Browser sind gefährdet (siehe S. 16). Noch wurden allerdings keine echten Schädlinge beobachtet, die diese Angriffe ausführen.

Aber es gibt noch viel mehr Bedrohungen: AdultSwine ist eine Malware, die vor allem Pornowerbung nachlädt, überteuerte Abodienste anbietet und zur Installation dubioser Security-Apps auffordert. Eine ähnliche Malware lauert im SDK „Ya Ya Yun“, das offenbar viele App-Entwickler nutzen. Damit erstellte Programme öffnen heimlich im Hintergrund Webseiten und klicken die Werbebanner an. Beide Malwares sind Google beim Virencheck durchgerutscht und stecken laut Sicherheitsforschern in über 100 Apps. Inzwischen hat Google die betroffenen Apps aus dem Store geworfen, aber Android deinstalliert sie nicht automatisch. Anwender müssen sie selbst herunterwerfen – da vor allem Spiele betroffen sind, sollten Eltern auch die Smartphones ihrer Kinder überprüfen. Eine Liste mit den betroffenen Apps finden Sie über ct.de/y3nn.

Skygofree und Dark Caracal sind ausgefeilte Spionage-Kits, die infizierte Handys nicht nur nach persönlichen Daten wie Adressbüchern und Chat-Inhalten durchsuchen, sondern auch in Wanzen verwandeln, also Mikrofon und Kamera aktivieren und die Aufnahmen an die Angreifer verschicken können. Möglicherweise verschaffen sie sich sogar Root-Zugang (siehe S. 100). Nach bisherigem Kenntnisstand fängt man sich beide Spionage-Kits nicht im Google Store ein, sondern höchstens über manipulierte Apps aus dubiosen Kanälen. Möglicherweise muss der Angreifer sie auch direkt auf dem Handy installieren, wenn der Besitzer es eine Zeitlang unbeaufsichtigt lässt; man muss sich also persönlichen Angriffen etwa durch Behörden ausgesetzt sehen. Sicherheitsforscher vermuten zumindest hinter Skygofree einen italienischen Staatstrojaner. Details zu den Lücken finden Sie auf ct.de/y3nn.



Eine einfache, aber wichtige Schutzmaßnahme: die App-Installation aus anderen Quellen als dem Play Store blockieren.

Schutzmaßnahmen

Diese anscheinende Häufung von Sicherheitslücken zeigt zwei Trends: Erstens stehen Smartphones zunehmend im Ziel von direkten Angriffen; doch wenn ein Angreifer physischen Zugriff auf Handy oder PC hat, stehen ihm sowieso nahezu unbegrenzte Möglichkeiten offen. Zweitens werden die Grenzen der Store-Virenscanner von Google, Apple und Microsoft deutlich: Sie entdecken nur Bekanntes. So lange die Gefährlichkeit eines Werbe-SDKs unerkannt bleibt oder kein Spectre-Schädling existiert, finden sie nichts.

Auch die Virenscanner auf dem Smartphone helfen nur eingeschränkt weiter, vor allem, weil sie unter Android auf wenig mehr achten können als bekannte Schädlingssignaturen. Eine verhaltensbasierte Erkennung ist aufgrund der Sicherheitsstruktur von Android nicht möglich – aus diesem Grund sind immerhin Schädlinge wie Verschlüsselungstrojaner nur eingeschränkt möglich. Besser helfen andere Vorsichtsmaßnahmen:

- Installieren Sie Apps nur aus vertrauenswürdigen Stores etwa von Google, Amazon oder F-Droid; meiden Sie Apps mit wenigen dutzend Bewertungen.
- Deaktivieren Sie das Installieren von Apps aus unbekannten Quellen.
- Klicken Sie (wie auch am PC) nicht auf Links in dubiosen Mails oder Social-Media-Beiträgen. Ignorieren Sie an ungewohnten Stellen auftauchende Aufforderungen, Apps zu installieren oder Sicherheitsmaßnahmen zu ergreifen – vor allem im Browser oder beim Spielen.
- Gönnen Sie bei viel genutzten Apps lieber dem Entwickler ein paar Euro, statt sich dem Generve und Risiko von Werbeeinblendungen auszusetzen.
- Aktivieren Sie die Displaysperre per PIN, Passwort oder Biometrie. Falls das Gerät im Entwicklermodus ist: Schalten Sie das USB-Debugging aus. So erschweren Sie nicht nur Dieben den Zugriff auf Ihre Daten, sondern machen es Angreifern ungleich schwerer, die in Ihrer Abwesenheit Schädlinge installieren möchten.

Ist mein Handy mit Schadcode infiziert?

Folgendes kann auf eine Infizierung hinweisen:
- unbekannte Posten auf Handy-/Kreditkartenrechnungen
- erhöhtes Datenvolumen
- erhöhter Akkuverbrauch und erhöhte Wärmeentwicklung
- viele Werbeeinblendungen
- lahme Reaktionen
- neue App-Icons
- ungewollte Reboots
- unbekannte Geräteadministratoren

Ein beliebter Ratschlag ist, auf die angeforderten Rechte einer App zu schauen, bevor man sie installiert. Doch dabei muss man sich mit so vielen Fehlalarmen beispielsweise aufgrund der Werbe-SDKs der werbefinanzierten Apps herumschlagen, dass echte Schädlinge einem möglicherweise entgehen.

Aktuelle Android-Geräte fragen nochmals nach, wenn eine App Rechte etwa zur Standortverfolgung und Zugriff auf die Kontakte anfordert. Sie können dann immer noch ablehnen, wodurch einige Apps allerdings nicht mehr funktionieren.

Gegenmaßnahmen

Wenn Sie ein ungewöhnliches Verhalten Ihres Smartphones bemerken, könnte es befallen sein (siehe Kasten); einzelne Vorkommnisse dieser Liste haben allerdings meist andere Gründe. Überprüfen Sie zuerst in den Einstellungen die Gerätemanager oder Geräteadministratoren. Hier dürften im Allgemeinen nur Googles „Mein Gerät finden“ und Ihnen bekannte Apps stehen, etwa Ihre Mail-App. Löschen Sie fragwürdige Einträge.

Wenn eine App sich seltsam benimmt oder in einer Liste von infizierten Apps auftaucht, deinstallieren Sie die App sofort. Die einfachen Schädlinge haben Sie dadurch abgewehrt. Komplizierter wirds, wenn der Schädling einen Rooting-Angriff durchgeführt hat: In vielen Fällen dürfte das eine der Root-Checker-Apps entdecken, ein guter Schädling mag sich aber erfolgreich vor ihnen verstecken. Weitere Tipps dazu in [1].

Wenn Sie einen Schädling entdeckt haben oder vermuten, könnte der schon sein Unwesen getrieben haben. Überprüfen Sie also Ihre Kreditkarten- und Telefon-Abrechnungen, auch in den nächsten Wochen.

Vor allem bei Rooting- und Gerätemanager-Angriffen sowie einem Schädling in der Tastatur-App: Ändern Sie – und zwar unbedingt an einem anderen Gerät – alle Passwörter, die der Schädling mitgeschnitten haben könnte. Eine gute Maßnahme bei dieser Gelegenheit wäre, eine Zwei-Faktor-Authentifizierung überall dort zu aktivieren, wo es möglich ist.

Sofern ein Gerätemanager- oder Rooting-Angriff stattgefunden hat, sollten Sie das Handy unbedingt auf Werkseinstellungen zurücksetzen und sämtliche Apps neu installieren – nicht ohne vorher ein Backup Ihrer wichtigen Daten und Fotos anzulegen. *(jow@ct.de)* c't

Literatur

[1] Michael Spreitzenbarth, Prävention, Diagnose, Behandlung, Schädlinge unter Android: Wie man sie aufspürt und los wird, c’t 17/2016, S. 70

Infos zu den Schädlingen: ***ct.de/y3nn***