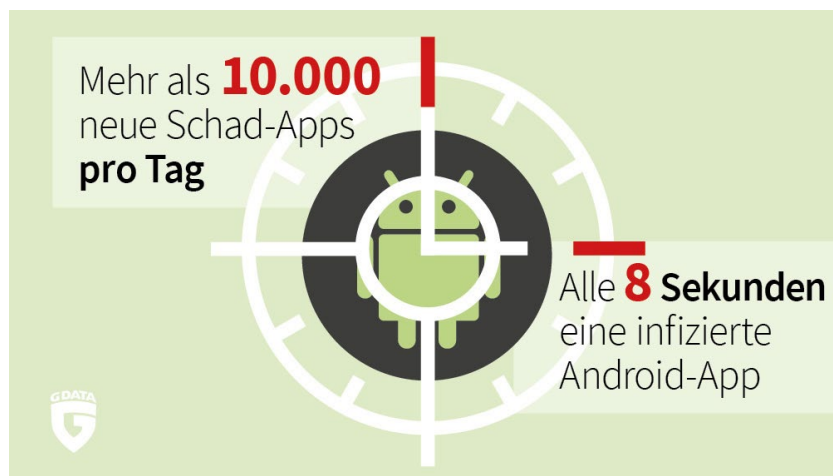


Mobile Malware Report: Keine Entspannung bei Android-Malware

Mehr als 10.000 neue Schad-Apps pro Tag zählten die G DATA Sicherheitsexperten im ersten Halbjahr 2019. Die Sicherheitslage im Mobile-Bereich bleibt weiterhin angespannt

Bochum (Deutschland), 30. Juli 2019

Kein neuer Rekord, aber auch keine Entspannung bei Android-Schadsoftware: Die Experten des Cyber Defense Spezialisten G DATA haben in den ersten sechs Monaten rund 1,9 Millionen neue schädliche Apps gezählt. Im Vergleich zum Vorjahr ein leichter Rückgang. Zur Einordnung: Durchschnittlich alle acht Sekunden veröffentlichen Kriminelle eine infizierte App für Android.



Die Zahl der neuen Schad-Apps für Android-Geräte ist im ersten Halbjahr 2019 etwas zurückgegangen. Entdeckten die Experten des Cyber Defense Spezialisten G DATA zwischen Januar und Juni 2018 noch über 2,04 Millionen infizierte Apps, waren es in diesem Jahr 1,85 Millionen – ein Rückgang von rund 9 Prozent. „Die Gefahr für Smartphones und andere mobile Geräte bleibt trotzdem weiterhin sehr groß“, sagt Alexander Burris, Lead Mobile Researcher bei G DATA. „Gerade weil Smartphones als ständiger Begleiter mittlerweile nahezu unentbehrlich sind, bilden sie für Cyberkriminelle ein attraktives Ziel. Besonders lukrativ sind Adware oder auch Ransomware, welche dem Nutzer direkt schadet.“ Die Zahl der insgesamt bekannten Schad-Apps nähert sich der 100-Millionen-Marke. Bis Ende Juni summierte sich die Zahl aller bekannten Apps mit Schadcode auf über 94,2 Millionen.

„Geräte mit alten Android-Versionen zu nutzen, ist wie ungeschützter Geschlechtsverkehr“, sagt Alexander Burris, Lead Mobile Researcher bei G DATA CyberDefense.

Zu viele Android-Versionen

Das weiterhin hohe Bedrohungspotenzial bei Android wird durch unterschiedlichste Faktoren begünstigt. Da ist zu einem die immer noch große Fragmentierung beim eingesetzten Betriebssystem. Denn aktuell ist nur bei jedem zehnten Gerät die aktuellste Android-Version 9 – Pie – installiert. Und Android 8 – Oreo – kommt bei 28 Prozent der Smartphones und Tablets zum Einsatz. Im Umkehrschluss bedeutet dies: 60 Prozent der Geräte nutzen immer noch veraltete Versionen, die vor August 2017 bereitgestellt wurden.

G DATA CyberDefense AG
Unternehmenskommunikation

G DATA CyberDefense AG
G DATA Campus
Königsallee 178
44799 Bochum

www.gdata.de

E-Mail: presse@gdata.de
Tel.: +49 (0) 234 9762-239
Fax: +49 (0) 234 9762-299

„Geräte mit alten Versionen zu nutzen, ist wie ungeschützter Geschlechtsverkehr“, warnt Burris. „Man sollte vorher sehr genau überlegen, was man macht.“ Allerdings haben Hersteller gerade bei älteren Geräten Anpassungen vorgenommen, die den Update-Prozess unnötig verlängern oder ganz blockieren. Googles Konzept „Android One“ mit garantierten Updates hat viel Schwung gebracht. Nutzer sollten sich im Falle einer Neuanschaffung schon im Vorfeld beim Hersteller informieren, ob Updates regelmäßig bereitgestellt werden.

Veraltete Geräte und billige China-Importe

Aber nicht nur veraltete Betriebssysteme, sondern auch veraltete Smartphones ohne aktuellen Patch machen es Hackern einfach, Malware auf dem Gerät zu installieren. Die Gründe dafür: Entweder existieren keine aktuellen Updates für das Gerät, oder Kunden haben diese nicht installiert.

Ein dritter Faktor: Immer noch sind Billiggeräte mit vorinstallierter Schadsoftware im Handel erhältlich. Die Malware ist für den Besitzer unsichtbar und lässt sich nicht deaktivieren. So haben Online-Kriminelle vollen Zugriff auf das Smartphone und alle persönlichen Daten. Nicht immer stellen die Anbieter virenfreie Updates für die Firmware bereit. Die Schadsoftware manuell zu entfernen, ist nicht möglich, weil sie tief in die Firmware integriert ist.

Google macht beim Thema Sicherheit ernst

Um Kosten zu sparen, vertreiben einige Anbieter ihre Apps über alternative Quellen. Sie sparen so die Lizenzgebühren für Google Play. Allerdings sind solche Alternativen ein beliebtes Einfallstor für Hacker. „Wer Apps nicht aus dem offiziellen Play-Store von Google installiert, setzt sich einer deutlich höheren Gefahr aus, eine infizierte App herunterzuladen“, warnt Alexander Burris.

Google hingegen widmet dem Thema Sicherheit deutlich mehr Aufmerksamkeit. Dazu hat das Unternehmen bereits im vergangenen Jahr Maßnahmen vorgestellt und umgesetzt. „Die von Google eingeleiteten Maßnahmen zeigen in die richtige Richtung“, sagt Burris. „Ob diese Schritte zu einem dauerhaften Rückgang der Malware-Zahlen führen, wird allerdings die Zukunft zeigen.“ Auch die aktuelle Ankündigung, für Android Q große Teile der Update-Infrastruktur umzustellen und die Systemkomponenten unabhängig von den OEM-Herstellern zu aktualisieren, lässt hoffen, das Problem der fehlenden Updates in den Griff zu bekommen.

Millionenfacher Schaden

SimBad“, „Operation Sheep“ und „Agent Smith“: Diese drei Beispiele verdeutlichen, wie erfolgreich Cyberkriminelle sind. Schätzungsweise 150 Millionen Nutzer haben eine Android-App mit der Malware „SimBad“ auf ihrem Handy installiert. Die zweite erfolgreiche Malware-Kampagne ist als „Operation Sheep“ bekannt. Mehr als 111 Millionen Mal wurden die infizierten Apps heruntergeladen. Sämtliche Apps finden sich insbesondere in den App-Stores von Drittanbietern. „Agent Smith“ heißt die dritte große Kampagne, die bereits 25 Millionen Smartphones in Asien befallen hat. Einmal installiert, ersetzt sie Applikationen durch infizierte Klone, sodass die Apps Werbung ausspielen. Nachdem die Schadsoftware zunächst nur über Drittanbieter-Stores in Umlauf kam, sind mittlerweile auch erste verseuchte Apps auf der Google-Plattform erschienen. Laut Experten ist der Infektionsweg sehr komplex, sodass künftig auch mit einem Einsatz als Spyware zu rechnen ist, um sensible Daten auszulesen.

G DATA CyberDefense AG

Unternehmenskommunikation

G DATA CyberDefense AG

G DATA Campus

Königsallee 178

44799 Bochum

www.gdata.de

E-Mail: presse@gdata.de

Tel.: +49 (0) 234 9762-239

Fax: +49 (0) 234 9762-299

Zusammenfassung und Ausblick

Die Sicherheitslage für Android bleibt angespannt. Auch wenn Google weitreichende Maßnahmen ergriffen hat, existieren immer noch zahlreiche Einfallstore für Kriminelle. Besorgniserregend ist der Trend, dass immer mehr Unternehmen aus Kostengründen Apps ausschließlich in alternativen Quellen anbieten. Dies stellt eine zentrale Sicherheitsmaßnahme in Frage: Den Verzicht auf die Installation von Apps aus unsicheren Quellen.

G DATA CyberDefense AG **Unternehmenskommunikation**

G DATA CyberDefense AG

G DATA Campus

Königsallee 178

44799 Bochum

www.gdata.de

E-Mail: presse@gdata.de

Tel.: +49 (0) 234 9762-239

Fax: +49 (0) 234 9762-299