

G DATA Mobile Malware Report: Kriminelle halten das Tempo bei Android-Malware hoch

Alle elf Sekunden erscheint eine neue schädliche App für Android-Smartphones

Bochum (Deutschland), 20. Oktober 2021

Die Zahl der schadhaften Android-Apps ist im ersten Halbjahr 2021 auf rund 1,3 Millionen Malware-Samples gesunken. Das zeigt eine aktuelle Analyse von G DATA CyberDefense. Trotz des Rückgangs bleibt das Tempo der Cyberkriminellen allerdings hoch..

Smartphones mit Android-Betriebssystem bleiben bei Cyberkriminellen ein beliebtes Angriffsziel. Der aktuelle Mobile Malware Report von G DATA CyberDefense zeigt, dass in der ersten sechs Monaten des Jahres mehr als 1,3 Millionen neue schädliche Apps für Smartphones mit Android-Betriebssystem im Umlauf waren. Gegenüber dem Vergleichszeitraum des Vorjahres ist die Zahl um 34,5 Prozent zurückgegangen. Allerdings halten die Angreifer das Tempo der Attacken weiterhin hoch: Immer noch erscheint alle elf Sekunden eine neue App mit Schadsoftware. Die Gesamtzahl der bekannten Android-Malware-Samples liegt seit der Entdeckung der ersten schädlichen App vor über zehn Jahren bei rund 23,4 Millionen.

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



„Trotz des markanten Rückgangs kann von Entspannung keine Rede sein. Im ersten Halbjahr 2020 haben sich Cyberkriminelle den Beginn der Corona-Pandemie zu Nutze gemacht und waren sehr aktiv, beispielsweise mit gefälschten Corona-Tracker-Apps. Mittlerweile nutzen die Angreifer auch andere Wege, um Smartphones mit Schadsoftware so schädigen, wie etwa mit gefälschten Links, die sie via SMS versenden“, sagt Stefan Decker, Sicherheitsforscher im Mobile Team bei G DATA CyberDefense AG.

Flubot – Der Angriff via SMS

Wie Cyberkriminelle ihre Methoden angesichts der andauernden Corona-Pandemie angepasst haben, zeigt Flubot. Dabei haben die Angreifer den anhaltenden Online-Shopping-Boom und das damit hohe Aufkommen von Paketen ausgenutzt. Via SMS erhielten sehr viele Nutzer*innen eine Nachricht, beispielsweise: „Ihr Paket wurde verschickt. Bitte überprüfen und akzeptieren Sie es.“, „Ihr Paket kommt an, verfolgen Sie es hier.“ oder „Paketzustellung Ihrer Lieferung nicht möglich. Mehr Info:“. Alle Nachrichten erhalten einen Link, der allerdings nicht zu der Webseite eines Paketdienstes führt, sondern den Download des Banking-Trojaners Flubot initiiert und so

das Smartphone mit Schadsoftware infiziert. Ist die Malware einmal installiert, kopiert sie vertrauliche Informationen wie Bank- oder Kontaktdaten und leitet Kreditkarteninformationen aus. Die Kontaktinformationen nutzen die Angreifer dann, um weitere gefälschte SMSen zu versenden.

Luca – Pannen ohne Ende

Wie wichtig Datenschutz und Datensicherheit bei mobilen Endgeräten sind, haben im ersten Halbjahr 2021 zwei Themen gezeigt: Die immer noch andauernde Diskussion um die Luca-App sowie das Gesetz zur Telekommunikationsüberwachung. Die Luca-App wurde zur Dokumentationspflicht in der Corona-Pandemie für Veranstalter oder Gastronomen genutzt. Allerdings konnten IT-Sicherheitsfachleute den Entwicklern mehrfach Fehler nachweisen. So hätten Cyberkriminellen aufgrund einer Schwachstelle Nutzerdaten ausleiten und Schadsoftware bei Gesundheitsämtern einschleusen können. *„Die Fehlerliste von Luca ist lang und Nutzende entdecken regelmäßig neue Probleme mit der App“*, sagt Stefan Decker. *„Fehler beim Auschecken, Fake-Checkins oder das Erstellen falscher Identitäten zeigen, dass das entwickelnde Unternehmen Sicherheitsstandards einfach außer Acht gelassen hat. Gerade in der aktuellen Situation sind aber zuverlässige Daten für die Kontaktnachverfolgung unablässig. Ich empfehle stattdessen auf die Funktion der offiziellen Corona-Warn-App umzusteigen, da diese sich in Sicherheitsaspekten bewiesen hat.“*

Staatstrojaner - staatlich verordnete Sicherheitslücke

Und auch die Regierung hat mit einer Entscheidung die Sicherheit digitaler Dienste maßgeblich geschwächt: Durch eine Änderung des Gesetzes zur Telekommunikationsüberwachung können die Bundespolizei sowie alle 19 Nachrichtendienste in Deutschland Computer und Smartphones von Verdächtigen hacken. Mit einer entsprechenden Überwachungssoftware, auch Staatstrojaner genannt, können Ermittlungsbehörden die verschlüsselte Kommunikation von Verdächtigen wie Chats oder Anrufe mitlesen oder mithören. *„Diese geplante, massive Einschränkung der verschlüsselten Kommunikation schadet der gesamten Sicherheitswirtschaft in Deutschland und Europa und ist ein gravierender Einschnitt in die sichere Kommunikation der Menschen“*, sagt Ralf Benzmüller, Executive Speaker G DATA Security Labs.

Verantwortung übernehmen, Sicherheit schaffen

Die Sicherheitslage für Smartphones und Tablets bleibt weiterhin angespannt. *„Das letzte Halbjahr hat eindrucksvoll gezeigt, dass gerade manche Unternehmen keine Verantwortung übernehmen und so dem Vertrauen in Datenschutz nachhaltig Schaden zufügen“*, sagt Stefan Decker. *„Dabei vertrauen immer mehr Nutzende ihrem Smartphone viele persönliche Daten an, die einen besonderen Schutz bedürfen.“* Bereits seit einigen Jahren investiert Google wesentlich mehr Arbeit, um den Play Store sowie das Android-Betriebssystem abzusichern. Dazu gehört auch, dass Google die Zugriffsrechte von Apps stärker kontrolliert und so die Zahl schädlicher Apps im Play Store weiter zurückgegangen ist.

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