



ESET: Vorsicht vor gefälschten Banking-Apps - Mit simplen, aber effizienten Methoden ziehen Betrüger ihren Opfern das Geld aus der Tasche

In der aktuellen Studie "Android Banking Malware: Sophisticated trojans vs. fake banking apps " warnen die Sicherheitsexperten von ESET davor, die Gefahr durch betrügerische Banking-Apps zu unterschätzen. Diese geben sich als legitime Onlinebanking-Anwendungen aus und erbeuten Geld oder Zugangsdaten. Während Banking-Trojaner seit langem als ernsthafte Bedrohung für Android-Nutzer gelten, werden Finanz-Fake-Apps aufgrund ihrer begrenzten Möglichkeiten gerne übersehen. Obwohl technisch weniger komplex, erzielen sie ähnliche Ergebnisse wie die ausgeklügelten und kostspieligen Trojaner-Varianten.

"Unsere Analyse dieser beiden Malware-Typen, die es leider auch immer wieder in den offiziellen Google Play Store schaffen, zeigt vor allem eines: Gerade die geringe Komplexität der gefälschten Banking-Apps ist für die Angreifer ein entscheidender Vorteil gegenüber den gefürchteten Banking-Trojanern", erläutert Lukás Stefanko, ESET Malware Researcher.

Anwendervertrauen wird ausgenutzt

Stefanko zufolge sind die Anwendungen vor allem deshalb so effektiv, weil sie sich auf das Nachahmen legitimer Apps beschränken. Ist die erste Hürde genommen und hat der Nutzer die vermeintlich legitime App installiert, wird er mit grosser Wahrscheinlichkeit auch das weitere Verhalten der Software für gerechtfertigt halten. Entsprechend gibt er bereitwillig Zugangsdaten preis. Anders als Banking-Trojaner fordern die gefälschten Banking-Apps keine weiteren Zugriffsrechte auf das Gerät und erregen so keinen Verdacht. Auch sind sie im Gegensatz zu Trojanern nicht auf Methoden angewiesen, die sie für Anti-Malware-Lösungen leicht erkennbar machen würden.

Vier Tipps gegen Fake-Banking-Apps

Um nicht Opfer eines betrügerischen Banking-App zu werden, sollten mobile Anwender einige Tipps befolgen:

- * Halten Sie ihr Android-Gerät auf dem aktuellsten Stand und nutzen Sie eine zuverlässige mobile Sicherheitslösung.
- * Vermeiden Sie inoffizielle App-Stores. Wenn möglich, deaktivieren Sie die "Installation aus unbekanntem Quellen" dauerhaft.
- * Bevor Sie eine App aus dem Google Play Store installieren, werfen Sie einen Blick auf Bewertungen, Nutzerkommentare, Anzahl von Installationen und benötigte Zugriffsrechte. Behalten Sie das Verhalten der App auch nach Installation im Auge.
- * Installieren Sie ausschliesslich Banking- und Zahlungs-Apps, die von ihrer Bank oder ihrem Finanzdienstleister bereitgestellt werden. Nutzen Sie die Verlinkungen auf deren offizieller Webseite, um zum App-Store zu gelangen.