Sicherheit

Bank-Bot nutzt die Schwachstelle Nutzer

Dass die Cyberkriminellen immer kreativer werden, wenn es darum geht, die Schwachstelle Kunde im elektronischen Datenverkehr auszutricksen. Das zeigt eine Meldung von Avast vom 20. November. Demzufolge hat ein Trojaner die Nutzeroberfläche der Apps von gleich fünf deutschen Banken gefälscht. Betroffen waren die Apps von Citibank, Comdirect, Commerzbank, DKB und Postbank

Eingeschlichen hat sich der Banking-Trojaner Bank-Bot bei Google Play als Taschenlampen-, Optimierungs- und Solitaire-Spiele-App, um die Benutzeroberfläche der genannten deutschen Banking-Apps zu manipulieren. Zusätzlich waren in der Schweiz Kunden der Raiffeisenbank und in Österreich Kunden der Bawag und der Sparda-Bank sowie weltweit insgesamt rund 160 Banken zum Angriffsziel der Cyberkriminellen geworden. Dies haben Sicherheitsforscher von Avast in Kooperation mit Forschern von Eset und Sfy-Labs herausgefunden.

Der Trojaner Bank-Bot ist eine Malware, die das Ziel hat, Geld von Mobile-Banking-Kunden zu stehlen. Die gefälschten Versionen der Mobile-Banking-Malware-Apps gaben sich zunächst als vermeintlich vertrauenswürdige Taschenlampen-Apps aus, danach als Solitaire-Spiele und als Cleaner-App, um die Nutzer zum Download zu verleiten.

Zu den schädlichen Aktivitäten gehörte anschließend die Installation einer gefälschten Benutzeroberfläche, die Bank-Bot beim Öffnen der Banking-App über deren Startseite legt. Sobald der Nutzer seine Bankverbindung eingibt, werden die Daten von Kriminellen gesammelt. Sie fangen so die SMS-Nachrichten mit der mobilen TAN ab und können dann Banküberweisungen im Namen des Nutzers durchführen.

Im Lauf des Jahres 2017 hat sich der Trojaner bereits mehrfach in den Google Play Store eingeschlichen. Google hatte zwar erst unlängst ältere Versionen des Bank-Bot aus dem Play Store entfernt; mehrere Versionen blieben jedoch bis zum 17. November 2017 aktiv. Dies genügte, um Tausende von Nutzern zu infizieren.

Auch die Scan- und Prüfmaßnahmen für alle Apps, die in den Play Store übermittelt werden, reichen offenbar nicht aus, um sicherzustellen, dass in Zukunft keine schädlichen Programme in den Play Store gelangen. Denn die Autoren von Mobile-Banking-Trojanern haben damit begonnen, spezielle Techniken anzuwenden, um diese automatischen Erkennungsdienste zu täuschen. So führt Bank-Bot beispielsweise bereits zwei Stunden, nachdem ein Nutzer der App Administratorrechte für das Gerät erteilt, schädliche Aktivitäten durch. Außerdem veröffentlichten die Cyberkriminellen die Apps unter verschiedenen Entwicklernamen, was eine gängige Taktik zur Umgehung der Überprüfung durch Google ist.

Die Schwachstelle bleibt also der Handynutzer selbst. Ihn gilt es noch stärker als bisher für die versteckten Gefahren zu sensibilisieren. Dabei geht es nicht nur um die Installation einer Sicherheits-App, sondern auch um Wachsamkeit bei der Verwendung der Banking-App und Obacht bei ungewöhnlichen Änderungen der Benutzeroberfläche. Hier müssen vielleicht auch die Banken in ihrer Kommunikation ansetzen und noch besser deutlich machen, wann sie welche Veränderungen an der App vornehmen. **Red.**