# Android-Banker buhlt um Stimmen beim Fotowettbewerb

04.11.2015, 14:43 | IT, New Media & Software

Pressemitteilung von: *Doctor Web Deutschland GmbH*
Presseagentur: *Waggener Edstrom Communications*


Android.BankBot

Auf die wachsende Beliebtheit des mobilen Online-Bankings reagieren Cyber-Kriminelle mit neuen Trojanern, die es auf das Geld der Android-Benutzer abgesehen haben. Diesmal steht Android.BankBot im Zentrum der Aufmerksamkeit. Der von Virenanalysten entdeckte Trojaner Android.BankBot.80.origin ist als offizielle Anwendung einer russischen Bank getarnt. Wenn ein Trojaner installiert und gestartet wird, fragt er anschließend nach Administratorrechten. Nachdem das Opfer zugesagt hat, löscht Android.BankBot.80.origin die früher erstellte Desktopverbindung und startet seine Aktivitäten.
Der Schädling scannt das Adressbuch des Benutzers und versendet eine Kurznachricht mit einer Einladung, an einem angeblichen Fotowettbewerb teilzunehmen, an seine Kontakte. Sollte der Benutzer dem Link http://******konkurs.ru/ folgen, gelangt er auf eine Webseite, von welcher eine der Varianten von Android.BankBot.80.origin (u.a. Android.SmsBot.472.origin) automatisch auf sein Endgerät heruntergeladen wird. Darüber hinaus wird der Benutzer aufgefordert, bei einem Fotowettbewerb teilzunehmen. Die Tücke der Cyber-Kriminellen besteht darin, dass der Benutzer unabhängig von seiner Wahl genau auf den Trojaner für Android trifft.
Neben dem Versand von SMS-Spam baut Android.BankBot.80.origin eine Verbindung zum Verwaltungsserver auf und sendet eine Meldung über die erfolgreiche Infizierung des Android-Handys oder -Tablets. Der Schädling gibt u.a. folgende Daten an:
• Name des Mobilfunkanbieters;
• Modell;
• IMEI;
• Telefonnummer;
• Betriebssystemversion;
• Systemsprache.
Danach wartet Android.BankBot.80.origin auf einen Befehl von Cyber-Kriminellen und baut dazu regelmäßig eine neue Verbindung auf. Der Schädling kann folgende Anweisungen ausführen:
• call_number: Weiterleitung an die angegebene Nummer aktivieren;
• sms_grab: eingehende Kurznachrichten für einen definierten Zeitraum maskieren, indem Systemmeldungen gesperrt und Kurznachrichten gelöscht werden;
• sms_send: Kurznachrichten versenden;
• ussd: USSD-Anfrage starten;

• delivery: Kurznachrichten mit dem vorgegebenen Text an Kontakte aus dem Adressbuch versenden;
• new_url: Adresse des Verwaltungsservers anpassen.
Die Hauptaufgabe des Trojaners ist es, Geld der Benutzer von Online-Banking-Apps, Mobilfunkabonnenten sowie Benutzer von Bezahlungssystemen zu klauen. So wurde ein Versuch von Android.BankBot.80.origin festgestellt, Geld an Cyber-Kriminelle über die Kurznummern 7878 und 3116 zu klauen. Sollte ein Betrag auf dem Konto des Benutzers verfügbar sein, schickte er eine entsprechende Kurznachricht, um das Geld zu klauen oder versuchte, den Zugang zum Benutzerkonto des Abonnenten bzw. Visa-Kunden zu bekommen.
Die Analysten von Doctor Web haben folgende Telefonnummern und Bankkarten entdeckt, auf die Cyber-Kriminelle das gestohlene Geld überweisen wollten:
• Telefonnummern: 9612490525, 9605116893;
• Kreditkarten: VISA 4276880172933990, VISA 4276880101136772.
Die Virenschreiber haben für ihre App einen interessanten Algorithmus realisiert, der die Nutzungsdauer einer böswilligen App verlängern sollte. So versendet Android.BankBot.80.origin massenhaft Kurznachrichten an alle Kontakte aus dem Adressbuch des Benutzers. Wenn man eine solche Kurznachricht bekommt, ist ein kurzer Anruf bei der jeweiligen Person die effektivste Prüfungsmethode. Das haben Entwickler von Android.BankBot.80.origin berücksichtigt und eine Funktion integriert, die alle „gefährlichen“ Anrufe an die Nummer +79009999999 weiterleitet. Somit wird das Opfer sozusagen von der Außenwelt abgeschnitten.
Die Sicherheitsspezialisten von Doctor Web empfehlen Anwendern, keine Apps aus verdächtigen Quellen zu installieren und Kurznachrichten mit nicht vertrauenswürdigen Links zu ignorieren. Alle Varianten von Android.BankBot.80.origin werden von Dr.Web Antivirus für Android erfolgreich erkannt und neutralisiert und stellen deshalb für Dr.Web Anwender keine Bedrohung dar.

**Portrait**

Das russische Unternehmen Doctor Web Ltd. ist einer der führenden Hersteller von Anti-Virus- und Anti-Spam-Lösungen mit Hauptsitz in Moskau. Das Doctor Web Team entwickelt seit 1992 Anti-Malware-Lösungen und beschäftigt weltweit 400 Mitarbeiter, davon 200 im Research & Development. Doctor Web ist nicht nur Pionier, sondern auch einer der wenigen Anbieter, die ihre Lösungen vollständig innerbetrieblich entwickeln. Das Unternehmen legt großen Wert auf die effektive Beseitigung von Kundenproblemen und bietet schnelle Antworten auf akute Virengefahren. Die umfangreiche Produktpalette von Doctor Web umfasst effiziente Lösungen zur Absicherung von einzelnen Arbeitsplätzen bis hin zu komplexen Netzwerken. Im deutschsprachigen Raum werden die Produkte von der Doctor Web Deutschland GmbH in Frankfurt vertrieben. Zu den nationalen und internationalen Kunden zählen neben privaten Anwendern namhafte börsennotierte Unternehmen wie die Russische Zentralbank, JSC Russian Railways, Gazprom oder Arcelor Mittal sowie Bildungseinrichtungen und öffentliche Auftraggeber wie das Russische Verteidigungsministerium.

News-ID: 878019 • Views: 96 (Stand: 29.07.2026)

Link zur Pressemitteilung:
https://www.openpr.de/news/878019/Android-Banker-buhlt-um-Stimmen-beim-Fotowettbewerb.html