Gefährlicher Banking-Trojaner verbreitet sich auf Android-Geräten - Falsche Paket-Benachrichtigung birgt böse Überraschung

Android-Nutzer sollten eingehende SMS-Nachrichten derzeit besonders genau prüfen. Mit Hilfe einer vermeintlichen Sendungs-Benachrichtigung versuchen Kriminelle, Smartphones mit dem Banking-Trojaner FluBot zu infizieren. Als Absender werden die Namen großer Logistikunternehmen, wie DHL oder FedEx, missbraucht. In der SMS-Spam werden Empfänger dazu aufgefordert, auf einen Link zu klicken und eine App zu installieren, um so den Sendungsstatus des angeblichen Pakets einzusehen. Mit dieser Anwendung gelangt jedoch der Trojaner auf das Gerät. FluBot erlangt dabei wichtige Berechtigungen, wie das Einsehen von Benachrichtigungen, das Lesen und Schreiben von SMS-Nachrichten, das Abrufen der Kontaktliste sowie das Durchführen von Anrufen. ESET Mobile Security erkennt den Schädling und verhindert eine Infektion des Geräts.
"Der Banking-Trojaner FluBot verbreitet sich derzeit rasant in Deutschland und stellt ein ernsthaftes Sicherheitsproblem dar. Einmal auf dem Gerät, stiehlt das Schadprogramm Kontaktdaten und sensible Informationen", erklärt Lukas Stefanko, Malware Researcher bei ESET. "Anwender sollten mit vermeintlichen Zustellbenachrichtigungen derzeit sehr vorsichtig umgehen. Wir empfehlen dringend, diese Nachrichten genau zu prüfen und eine Sicherheitslösung zu installieren."

Malware-Kampagne verbreitet sich rasant

Seit Dezember treibt das Schadprogramm FluBot sein Unwesen. Die Aktivitäten waren bisher weitestgehend auf Spanien und Polen beschränkt. Mit ihrer aktuellen Kampagne zielen Cyberkriminelle jedoch auf Android-Nutzer in Deutschland ab. Durch die weitgehenden Rechte auf den Geräten verbreitet sich der Trojaner rasant.

So schützen Sie sich vor den dreisten Betrügern

- Im Zweifel die Nachricht löschen: Nachrichten von unbekannten Absendern, SMS oder E-Mails mit seltsamen Inhalten sollten im Zweifel gelöscht werden.

- Nicht auf Links klicken: Auf gar keinen Fall sollte in diesen dubiosen Nachrichten auf Links geklickt werden.

- Sicherheitslösung einsetzen: Anwender sollten eine Sicherheitslösung nutzen, die zuverlässig Schädlinge abwehrt und einen umfassenden Phishing-
Schutz bietet

- Immer auf dem neuesten Stand sein: Das Betriebssystem und die installierten Apps sollten stets auf dem neuesten Stand sein. Verfügbare Updates sollten umgehend eingespielt werden.

- Apps nur aus vertrauenswürdigen Quellen: Logistikunternehmen bieten Apps an, um den Sendungsstatus zu verfolgen. Anwender sollten die Verlinkungen auf deren offiziellen Webseiten verwenden, um zum App-Store zu gelangen und diese dort herunterladen.