Neuartiger Android-Schädling manipuliert Finanztransaktionen - Nutzer von Kryptowährungen Bitcoin und Ethereum betroffen

Forscher des europäischen Security-Spezialisten ESET haben die erste sogenannte Clipper-Malware im Google Play Store entdeckt. Dieser Schädling ist für Besitzer der Kryptowährungen Bitcoin und Ethereum besonders gefährlich: Er kann den Inhalt der Zwischenablage auf den genutzten Android-Geräten verändern und Transaktionen umleiten. Statt in das Wallet des Finanzpartners, wandern die digitalen Währungen in die Geldbeutel der Kriminellen.
"Clipper-Malware ist nicht mehr länger nur ein Problem von Windows-Anwendern oder dubiosen Android-Foren. Jetzt betrifft das Problem auch den durchschnittlichen Android-Anwender", sagt ESET-Malware-Forscher Lukás Stefanko.

Android/Clipper.C nutzt Bequemlichkeit aus

Der von ESET als Android/Clipper.C erkannte neue Schädling nutzt die Bequemlichkeit der Benutzer von Kryptowährungen aus. Diese geben für Währungstransfers selten manuell die komplexen Wallet-Adressen ein, sondern kopieren diese häufig. Dadurch werden sie kurzzeitig in der Zwischenablage des Betriebssystems abgelegt. Die Malware kann dort die Adresse einfach austauschen.

Clipper-Malware tauchte das ersten Mal 2017 auf Windows-Betriebssystemen auf. ESET-Forscher konnten bereits im letzten Jahr nachweisen, dass es drei solcher Schädlinge bis zu download.cnet.com geschafft hatten - einer der beliebtesten Download-Plattformen weltweit. Im August 2018 wurde der erste Android Clipper überhaupt in Untergrundforen entdeckt. Seitdem tauchte diese Art Malware in mehreren zweifelhaften App-Stores auf.

ESET liess Clipper aus Google Play Store löschen

Android-Nutzer, die ihre Downloads ausschliesslich aus dem Google Play Store beziehen, schienen bis 2019 davor sicher. Dies ändert sich nun, nachdem ESET-Forscher die Schadsoftware in Googles offiziellem Store nachweisen konnten. "Zum Glück haben wir den Clipper bereits kurz nach seinem Upload in den Store entdeckt. Wir haben den Sachverhalt dem Google Play Security Team gemeldet, welches kurz daraufhin die App entfernte", sagt Lukás Stefanko.
Die jetzt entdeckte Malware ahmt einen legitimen Dienst namens MetaMask nach. Dieser ermöglicht es, dezentrale Ethereum-Anwendungen im Browser auszuführen. Dazu ist es nicht notwendig einen vollen Ethereum Knoten zu betreiben. Der Dienst wird dazu als Add-On für Chrome und Firefox angeboten. Eine mobile App existiert nicht. "Es scheint eine rege Nachfrage nach einer mobilen Version von MetaMask zu geben. Das nutzen Cyberkriminelle aus, indem sie ihren Schadcode entsprechend verkleiden", warnt Lukás Stefanko.

Simples Formular überlistet Kryptowährungsbesitzer

Die gefundene Malware hat es auf die Bitcoin- und Ethereum-Werte seiner Opfer abgesehen. Dazu blendet sie lediglich ein gefälschtes Formular ein. In dieses soll der Anwender seine Wallet-Adresse eingeben und somit den Angreifern zugänglich machen. "Mit einem installierten Clipper könnte es gar nicht leichter sein, digitale Werte zu stehlen. Es sind die Opfer selbst, die diese den Angreifern unfreiwillig zuschicken", erklärt Lukás Stefanko.

Diese erste Entdeckung von Clipper-Malware im Google Play Store verdeutlicht einmal mehr die Notwendigkeit, dass Android Nutzer sich mit den Security-Grundregeln beschäftigen sollten. Um sich vor Clipper und anderer Malware zu schützen, raten Experten:
- Android immer aktuell halten und eine vertrauenswürdige Schutz-App installieren!
- Apps nur aus dem Google Play Store laden, aber vorher sicherheitshalber die Webseite des App-Anbieters überprüfen, die in der Beschreibung der App verlinkt sein sollte. Existiert keine Webseite, sollten Sie das Angebot meiden.
- Jeden Schritt bei der Ãœbertragung von sensiblen Informationen und Werten überprüfen. Beim Verwenden der Zwischenablage sollte gecheckt werden, ob die ausgefüllten Daten auch den gewollten entsprechen.
Indikatoren einer Infektion und technische Details finden sich im Blogeintrag auf WeLiveSecurity: