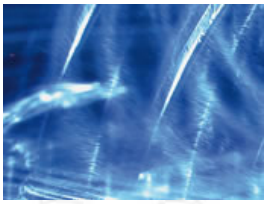

Spyware

Forscher des IT-Security-Unternehmens Bitdefende haben eine Android-Spyware entdeckt, die ihnen zufolge mindestens vier Jahre lang im Google Play Store unbemerkt geblieben ist. Die laut Bitdefender "unglaublich ausgereifte" Malware hat sich dabei als Bitcoin-Wallet oder Banking-App ausgegeben und konnte letztlich volle Kontrolle über ein Gerät und die darauf befindlichen Daten erlangen. Der Schädling war aber wählerisch und hat nur relativ wenige Ziele voll befallen - wohl auch, um eben lange unbemerkt zu bleiben.

Stufenweise zum Erfolg

Die Cyber-Kriminellen hinter Mandrake nutzten verschiedene Entwickler-Accounts, um ihre Malware als verschiedenste vermeintliche legitime Apps getarnt zu vertrieben, beispielsweise als Crypto-Wallet Coinbase, Chrome-Browser, PayPal oder als Banking-App australischer und deutscher Banken. Dabei gaben sich die Hintermänner große Mühe, die falschen Apps legitim aussehen zu lassen und brachten beispielsweise in manchen Fällen Wartungs-Updates heraus, um von Nutzern gemeldete Probleme zu beheben. Manche Apps hatten sogar eigene kleine Webseiten oder Social-Media-Präsenzen.

Die falschen Apps waren dabei noch nicht der eigentliche Schädling, sondern konnten einen Loader nachladen, der dann den eigentlichen Mandrake-Kern herunterlädt. Diese zwei weiteren Schritte geschahen aber offenbar nur, wenn die Cyber-Kriminellen der Malware den Befehl dazu gaben. Das geschah wohl nur bei aus ihrer Sicht lohnenden Zielen mit einem eher geringen Risiko, entdeckt zu werden. Daher dürften nur relativ wenige Geräte wirklich eine vollwertige Mandrake-Infektion haben. "Wir vermuten, dass die Zahl der Opfer in den Zehntausenden liegt", meint Bitdefender-Sicherheitsexperte Bogdan Botezatu gegenüber "TheRegister".

Selbstmord-Malware

Bei voll befallenen Geräten konnten die Angreifer sämtliche Daten wie beispielsweise Zugangsdaten für diverse Accounts oder das Online-Banking stehlen und den Bildschirminhalt aufnehmen. Mandrake ermöglichte auch, den Nutzerstandort zu verfolgen. Wohl um einer möglichen Entdeckung möglichst lange zu entgehen, kam der Schädling auch mit einer Art Selbstzerstörungsfunktion: Indem Mandrake ein Zurücksetzen des Geräts auf Werkseinstellungen auslöste, konnte sich die Malware wieder spurlos entfernen.

Die Apps am Anfang der Infektionskette hatten laut Bitdefender teils auch Mechanismen, um zu erkennen, ob sie auf einer virtuellen Maschine oder in einem Emulator laufen. Dies diente dazu, eine tiefgehende Analyse insbesondere der weiteren Komponenten durch Experten zu vermeiden. All das hat dazu geführt, dass Mandrake-Varianten zumindest seit 2016 unbemerkt im Google Play Store zu finden waren. Inzwischen wurden die entsprechenden Apps aber aus dem offiziellen Android-Marktplatz entfernt.