Android Malware Analyse: Hook

Studiengang: BSc in Informatik | Vertiefung: IT Security
Betreuer*in: Prof. Dr. Benjamin Fehrensen
Experte: Ivan Bütler (Compass Security)

Android ist das weltweit am weitesten verbreitete Betriebssystem für Mobiltelefone. In den letzten Jahren hat aber nicht nur die Anzahl Apps im Play Store rapide zugenommen, sondern auch die Anzahl Malware-Apps wächst stetig. Am 12. Januar dieses Jahres wurde der Bankentrojaner Hook in einem russischen Untergrundforum vorgestellt. Unsere Analyse dieses Trojaners trägt massgeblich zum Verständnis und zur Verteidigung gegen aktuelle Android-Bankentrojaner bei.

Einleitung

Da sich Android vor allem durch seine Offenheit auszeichnet, ist die Plattform ein attraktives Ziel für Malware-Entwickler geworden. Malware wie Trojaner, Ransomware, Spyware und Adware werden immer häufiger entdeckt. Unsere Analyse nimmt den russischen Bankentrojaner Hook genauer unter die Lupe und trägt so dazu bei, dass Anwender und Entwickler zugleich die Gefahren, die von aktuellen Android-Bankentrojaner ausgehen, kennen und sich vor ihnen schützen können.

Ziele

Diese Bachelorthesis soll zeigen, wie der Bankentrojaner Hook auf Android-Geräte gelangt, welche Persistenzmechanismen er besitzt, welche Banken betroffen sind und welche Fähigkeiten er aufweist. Zu diesen Fähigkeiten gehören das Imitieren legitimer Apps, das Stehlen von Login- und Kreditkartendaten, die Fernsteuerung des Geräts, das Abfangen von SMS-Nachrichten und das Verschlüsseln des Gerätes. Ausserdem soll die Kommunikation zwischen dem Bankentrojaner und den Command-and-Control-Servern entschlüsselt und analysiert werden. Diese Ziele sollen mit Hilfe statischer und dynamischer Analyse, einer automatisierten Analyseumgebung und Emulatoren des Trojaners und der Command-and-Control-Server erreicht werden.

Ergebnisse

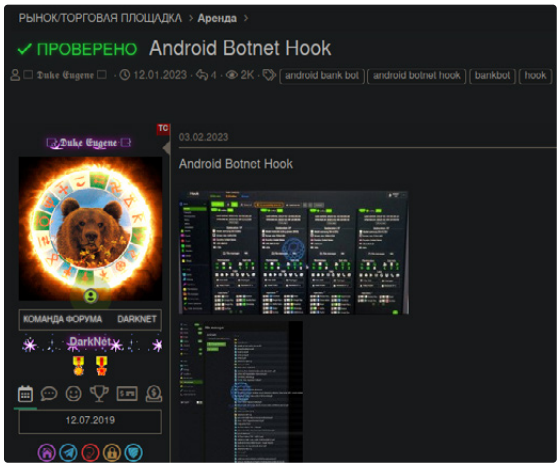
Es wurden über 60 Proben von Hook untersucht. Der Trojaner nutzt die Bedienungshilfen von Android um funktionsfähig zu sein. Wenn diese vom Anwender aktiviert werden, ist das Gerät infiziert und kann vom Angreifer gesteuert werden. Während unserer Analyse konnten Webinjects für mehr als 700 Android-Apps gesammelt. Diese werden verwendet, um sogenannte Overlay-Angriffe auszuführen. Dabei wird beim Start einer betroffenen App diese vom Trojaner sofort mit einer Phishing-Seite überlagert, um so Login- und Kreditkartendaten zu stehlen. Der grösste Anteil der gesammelten Webinjects ist für Banken-Apps, gefolgt von Krypto-Wallets. Ausserdem identifizierten wir Fähigkeiten wie

- Fernzugriff (Remote Access Trojan)
- Abfangen und Versenden von SMS-Nachrichten
- Lesen von Kontakten, E-Mails und Multi-Faktor-Authentifikations-Codes
- Keylogging

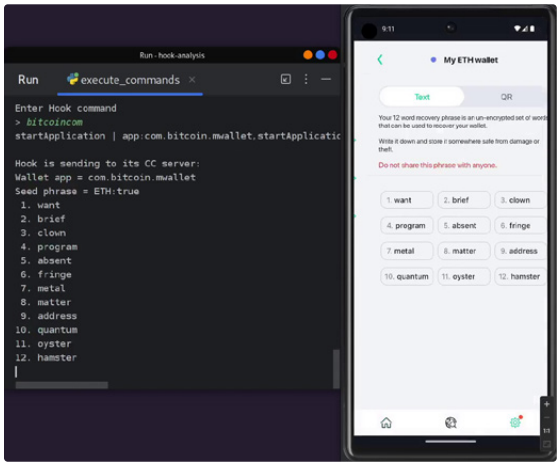
und viele mehr. Neben den über 60 Proben wurden 12 Command-and-Control-Server gefunden und untersucht.

Robin Martin Rapp
rmrapp@pm.me

Dominic Schmutz
dominic.schmutz@yahoo.com



Beitrag, im Untergrundforum, in dem Hook vorgestellt wurde



Automatisiertes Stehlen der Wiederherstellungsphrase