Lookout-Entdeckung: Monokle

Zum Schutz und zur Beratung unserer Kunden erkennt und untersucht Lookout kontinuierlich neue Bedrohungen.

Hintergrund und Ablauf der Entdeckung

2018 kam Lookout zufällig einer ersten Variante von Monokle auf die Spur. Seitdem wird die Android-Surveillanceware genauestens untersucht. Hierbei erkannte das Lookout-Team, dass die Überwachungssoftware in der Android-Virenschutzlösung Defender einen gemeinsamen App-Signer hat. Dieser wird vom russischen Auftragnehmer Special Technology Centre (STC) entwickelt. STC ist eines von drei in Russland ansässigen Unternehmen, die von der US-amerikanischen Regierung unter Barack Obama sanktioniert wurden, als ihre Verbindung zum russischen Geheimdienst GRU bekannt wurde: Sie sollen ihm Material für Eingriffe in den US-Präsidentenwahlkampf 2016 geliefert haben.

СПЕЦИАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР

Das Wichtigste in Kürze

1. Fortschrittliche Surveillanceware von STC, einem von der US-Regierung sanktionierten Unternehmen
2. Kann als Remote-Access-Trojaner (RAT) auftreten. Verfügt über hochentwickelte Funktionen für Datendiebstahl und Zertifikatinstallation.
3. Verbirgt seine manipulativen Absichten hinter der Fassade legitimer Anwendungen.

Funktionen und betroffene Stellen

Monokle zeigt sich nur in einigen wenigen Anwendungen. Dies lässt darauf schließen, dass Angriffe mithilfe dieser Surveillanceware speziell auf bestimmte Personen zugeschnitten sind. Die Anwendungen erscheinen legitim, sodass der Anwender keinen trojanischen Angriff darüber vermutet. Diese Vorgehensweise kennen wir von anderen mit Trojanern infizierten Anwendungen, allerdings verfügt Monokle über einige Funktionen, die unsere Lookout-Experten noch nicht kannten.

Als Remote-Access-Trojaner (RAT) setzt Monokle hochentwickelte Techniken zum Diebstahl von Daten ein und kann auf dem infizierten Gerät ein angriffsspezifisches Zertifikat im Verzeichnis vertrauenswürdiger Zertifikate installieren, um Man-in-the-Middle-Angriffe zu vereinfachen. Mit der Malware ist es auch möglich, Daten aus fremden Apps abzugreifen, ohne dass dazu ein Root-Zugang zum Gerät erforderlich wäre. Darüber hinaus kann Monokle mittels Wortvorschlägen Einblick in die Interessen des Nutzers gewinnen, die dann für gezieltere Angriffe genutzt werden. Und schließlich kann Monokle auch die Passcode-Eingabe am Gerät aufzeichnen, um die Sperre zu umgehen.

Monokle-Erkennung und -Schutz durch Lookout

Zum Schutz vor Monokle können Lookout-Kunden anwendungsbasierte Richtlinien in der Lookout-Plattform erstellen, durch die sie auf mit dem Trojaner infizierte Anwendungen aufmerksam gemacht werden, sodass sie Gegenmaßnahmen ergreifen können. Mit Lookout versehene Geräte sind seit Anfang 2018 vor Monokle geschützt. Da es jedoch Anzeichen für die Weiterentwicklung der Malware für Android und sogar für die Ausweitung auf iOS gibt, wird Lookout sie weiter untersuchen und diesbezügliche Ergebnisse veröffentlichen.

Lookout Threat Advisory Service

So dynamisch, wie die Welt der mobilen Sicherheit nun einmal ist, verliert man schnell den Überblick. Der Lookout-Dienst Threat Advisory nutzt deshalb den enormen Datensatz aus dem globalen, Millionen Geräte umfassenden Lookout-Sensorennetzwerk und verknüpft ihn mit den Erkenntnissen seiner Top-Sicherheitsexperten, damit Sie alle nötigen Informationen bekommen, um angemessen auf die neuesten mobilen Bedrohungen und Risiken zu reagieren.