Lookout-Entdeckung: eSurvAgent

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

Hintergrund und Ablauf der Entdeckung

Anfang 2018 stieß Lookout auf eSurvAgent, eine raffinierte Android-Surveillanceware, die mit einem italienischen Unternehmen namens eSurv, vormals Connexxa, in Verbindung gebracht wird. Die Malware, die auch unter dem Namen Exodus bekannt ist, wurde anscheinend über einen Zeitraum von mindestens fünf Jahren entwickelt und umfasst drei Stufen: Am Anfang steht ein Dropper, der der zweiten Stufe, einer großen Payload-Anwendung, den Weg bahnt und schließlich erfolgt der Root-Zugriff auf das Gerät. Lookout-Experten entdeckten kürzlich das iOS-Pendant dieser Bedrohung, das sich Anwender auf Phishing-Webseiten einfingen, die Kundensupport-Webseiten nachempfunden waren. Darüber hinaus machten sich mit dem eSurv-Agenten befallene Anwendungen das Apple Provisioning System für Unternehmen zunutze, indem sie sich mit vertrauenswürdigen Apple-Zertifikaten tarnten.

Das Wichtigste in Kürze

1. Zielt anscheinend auf legale Überwachungsmechanismen ab
2. Macht sich Schwächen im App Provision System für Unternehmen von Apple zunutze
3. Funktionen werden über Push-Payloads gesteuert, sodass Angreifer selbst festlegen können, welche Daten ausgeschleust werden

Funktionen und betroffene Gruppen

Die iOS-Variante verfügte über weniger Funktionen als die Android-Versionen und war daher nicht in der Lage, Geräte vollständig auszulesen. Dennoch gelang es ihr, den Zertifizierungsprozess von Apple so auszunutzen, dass sie den Anschein eines legitimen Zertifikats vortäuschte und folgende Datentypen auf iOS-Geräten ausschleusen konnte:

Kontakte | Fotos | GPS-Standort | Audioaufnahmen | Videos | Geräteinformationen

Entdeckt wurde die Malware auf Phishing-Websites, die die Onlineauftritte italienischer und turkmenischer Mobilfunkanbieter imitierten, sowie im italienischen Google Play Store. Mittlerweile wurde sie aus Google Play entfernt, und Apple hat die betroffenen Zertifikate widerrufen.

Wie erkennt Lookout eSurvAgent-ähnliche Bedrohungen und schützt davor?

Zum Schutz und zur Beratung unserer Kunden erkennen und untersuchen die Lookout Security Intelligence Teams kontinuierlich neue Bedrohungen. Dazu kombinieren sie statische und dynamische Analysemethoden mit unserer Machine Learning Engine. Sobald der eSurvAgent HTTPS-Pinning, asymmetrische Verschlüsselungsmethoden für C2-Datenverkehr über HTTPS sowie Globally Unique Identifiers (GUIDs) für sämtliche Bestandteile von API-Endpunkt-URLs und Verzeichnispfade nutzte, wurde die Malware von uns als Surveillanceware erkannt und klassifiziert. Auf Geräten mit Lookout-Schutz wird eSurvAgent seit März 2018 erkannt und angezeigt. Daneben schützt Lookout auch vor anderer, ähnlich ausgeklügelter Surveillanceware, die sonst unter Umständen unentdeckt bliebe.

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.