EUROPEAN-NEWS-AGENCY.COM

EUROPEAN NEWS AGENCY

International Press Service

Ressort: Internet und Technik

Kaspersky entdeckt Spionage-Trojaner in App Stores

Ingolstadt, 06.07.2025 [ENA]

Kaspersky hat einen neuen Spionage-Trojaner namens SparkKitty entdeckt, der Smartphones sowohl unter iOS als auch Android betrifft. SparkKitty sendet Bilder von einem infizierten Telefon und Informationen über das Gerät an die Angreifer. Die Store-Betreiber sind bereits informiert.

Die Spionage-Software SparkKitty greift gezielt Smartphones mit iOS- und Android-Betriebssystemen an, um Informationen abzugreifen. Bestimmte technische Details deuten darauf hin, dass die Malware-Kampagne mit dem SparkCat-Trojaner in Verbindung steht. SparkCat zielt ebenfalls sowohl auf iOS als auch Android ab und hat es auf Passwörter und Recovery Phrases für Krypto-Wallets abgesehen, die sie über OCR aus Screenshots von Nutzern extrahiert. SparkKitty ist nach SparkCat bereits die zweite Malware innerhalb eines Jahres, die Kaspersky-Experten in offiziellen Appstores entdeckt haben.

Verbreitungswege in iOS

„Einer der Verbreitungswege des Trojaners waren gefälschte Websites, auf denen die Angreifer versuchten, iPhones zu infizieren“, erklärt Sergey Puzan, Malware-Experte bei Kaspersky. „iOS bietet mehrere legitime Möglichkeiten, Programme zu installieren, die nicht aus dem App Store stammen. In dieser Malware-Kampagne nutzten die Angreifer eine davon – spezielle Entwicklertools zur Verbreitung von Unternehmensanwendungen. In der gefälschten TikTok-Version stahl die Malware während der Autorisierung nicht nur Fotos vom Gerät, sondern bettete auch Links zu einem verdächtigen Shop in das Profilfenster der betroffenen Person ein. Dieser Shop akzeptiert ausschließlich Kryptowährungen, was unsere Bedenken verstärkt.“

Verbreitungswege in Android

Auch bei den Angriffen gegen Android schlugen die Cyberkriminellen unterschiedliche Wege ein. Die Angreifer zielten sowohl auf Nutzer von Drittanbieter-Websites als auch auf Google Play ab und gaben die Malware als verschiedene Krypto-Apps aus. Die infizierte Anwendung SOEX wurde über 10000x aus dem offiziellen Appstore heruntergeladen. Die Kaspersky-Experten fanden außerdem infizierte APK-Dateien auf Drittanbieter-Websites. Diese Dateien können direkt auf Android-Smartphones installiert werden, ohne den Umweg über offizielle Stores. Die betreffenden Websites stehen vermutlich in Verbindung mit der erkannten Schadkampagne und wurden unter anderem über YouTube beworben.

Redaktioneller Programmdienst:
European News Agency

Annette-Kolb-Str. 16
D-85055 Ingolstadt
Telefon: +49 (0) 841-951. 99.660
Telefax: +49 (0) 841-951. 99.661
Email: contact@european-news-agency.com
Internet: european-news-agency.com

„Nach der Installation funktionierten die Apps wie versprochen“, so Dmitry Kalinin, Malware-Experte bei Kaspersky. „Gleichzeitig wurden jedoch Fotos aus der Smartphone-Galerie an die Angreifer gesendet. Diese könnten später versuchen, in den Bildern vertrauliche Daten zu finden, wie beispielsweise Wiederherstellungsphrasen für Krypto-Wallets, um auf die Vermögenswerte der Opfer zuzugreifen. Denn es gibt indirekte Hinweise darauf, dass die Cyberkriminellen genau an solchen interessiert sind: Viele der infizierten Apps hatten einen Bezug zu Kryptowährungen, und die trojanisierte TikTok-App verfügte zudem über einen integrierten Store, der Zahlungen für Waren nur in Kryptowährungen akzeptierte.“

Tipps zum Schutz

Keine Screenshots mit sensiblen Informationen, einschließlich Wiederherstellungsphrasen für Krypto-Wallets erstellen und speichern. Passwörter wie auch Wiederherstellungsphrasen für Krypto-Wallets in dedizierten Passwort Managern wie Kaspersky Password Manager speichern. Alle Geräte mit einer robusten mobilen Sicherheitssoftware wie Kaspersky Premium schützen. Aufgrund der architektonischen Besonderheiten des Apple-Betriebssystems zeigt die Kaspersky-Lösung für iOS eine Warnung an, wenn ein Versuch festgestellt wird, Daten an den Command-Server des Angreifers zu übertragen, und blockiert die Übertragung dieser Daten.

App-Berechtigungen stets überprüfen; bittet eine App um Erlaubnis, auf die Fotobibliothek des Geräts zuzugreifen, sollte geprüft werden, ob der Zugriff wirklich erforderlich ist. Die betroffenen Apps nicht mehr nutzen und sofort vom Smartphone löschen. Und zur Verfügung stehende Sicherheitsupdates des Betriebssystems zeitnah installieren sowie auf einen aktuellen Virenschutz achten.

Bericht online lesen:
https://schulz.en-a.de/internet_und_technik/kaspersky_entdeckt_spionage_trojaner_in_app_stores-91748/

Redaktion und Verantwortlichkeit:
V.i.S.d.P. und gem. § 6 MDStV: Heiko Schulz

Redaktioneller Programmdienst:
European News Agency

Annette-Kolb-Str. 16
D-85055 Ingolstadt
Telefon: +49 (0) 841-951. 99.660
Telefax: +49 (0) 841-951. 99.661
Email: contact@european-news-agency.com
Internet: european-news-agency.com