Staatstrojaner überwacht WhatsApp:
Forscher entdecken geheimes Spionageprogramm

Veröffentlicht am 20.01.2018 von chip.de

von Dominik Hayon

Sicherheitsforscher haben einen neuen Staatstrojaner entdeckt, der unter anderem in der Lage ist, WhatsApp-Nachrichten abzuhören. Auch darüber hinaus umfasst die Android-Spyware etliche Abhörmethoden.

Zum Anschauen des Videos auf das Bild klicken (chip.de)

Sicherheitsforscher von Kaspersky haben ein Spionageprogramm für Android entdeckt, das offenbar schon seit Ende 2014 eingesetzt wird und unter anderem in der Lage ist, WhatsApp-Nachrichten auszulesen. Verteilt wurde und wird die Software über gefälschte Webseiten, die den Seiten von Mobilfunkprovidern nachempfunden sind.

Die von ihren Entdeckern Skygofree getaufte Spyware ist ersten Erkenntnissen nach das Produkt eines italienischen Unternehmens, das sich auf die Entwicklung professioneller Überwachungsprogramm spezialisiert hat. Die Käufer dieser Programme sind in der Regel staatliche Behörden.

Kaspersky zufolge ist die Android-Version von Skygofree "*eines der mächtigsten Spionageprogramme, das wir auf dieser Plattform jemals gesehen haben*". Indem sich das Programm in die erweiterten Bedienungshilfen (die *Accessibility Services*) einklinkt, kann es praktisch sämtliche auf dem Gerät dargestellten Inhalte auslesen. Diese Fähigkeit macht sich die Software unter anderem zunutze, um WhatsApp-Nachrichten abzufangen, die ansonsten von einer starken Verschlüsselung geschützt sind.

Zum Anschauen des Videos auf das Bild klicken (chip.de)

Ferner ist die Spyware aber auch in der Lage, über das eingebaute Mikrofon die Umgebung des Smartphones abzuhören. Das kann zum Beispiel automatisiert immer dann passieren, wenn sich Gerät und Besitzer an einem bestimmten Ort befinden. Ebenso unbemerkt kann das Programm Fotos und Videos aufnehmen. Daten auf dem Gerät sind im vollen Zugriff der Angreifer: Kurznachrichten lassen sich also ebenso auslesen wie Standortdaten.

Um überhaupt auf die Geräte zu kommen, ist *Skygofree* beim Download gleich mit einer ganzen Batterie an Exploits ausgestattet, die es erlauben, unterschiedliche bekannte Sicherheitslücken von Android auszunutzen, um auf dem Gerät Admin-Rechte zu erlangen.

Nach bisherigen Erkenntnissen ist *Skygofree* als Staatstrojaner in erster Linie für gezielte Angriffe auf einzelne Personen zum Einsatz gekommen, eine massenhafte Verbreitung ist unwahrscheinlich. Geräte, auf denen *Kaspersky* eine *Skygofree*-Infektion feststellen konnte, fanden sich ausschließlich in Italien. Da die Spyware nun bekannt ist - nebst Hinweisen, mit denen sich die Infektion entdecken lässt - werden die meisten Antivirenprogramme für Android in Kürze in der Lage sein, die Schadsoftware zu erkennen.