IT-Sicherheit: Kaspersky entdeckt Spionagesoftware für Android

Kelkheim, 25. Januar 2018

Flickr: John Mosbaugh CC Lizenz

Das Softwareunternehmen Kaspersky hat eine Spionagesoftware für das Handy-Betriebssystem Android entdeckt: Skygofree, wie KasFpersky die Software nennt, ist vermutlich eine Überwachungssoftware speziell für staatliche Ermittler. Denn die Software ist nicht dazu ausgelegt, breite Bevölkerungsschichten auszuspionieren, sondern dient der gezielten Überwachung. Gefunden wurde das Programm überwiegend in Italien; entwickelt wahrscheinlich auch von einem italienischen Unternehmen. Verbreitet wird der Trojaner über infizierte Websites, die denen der Mobilfunkanbieter nachgebaut wurden. Die Handy-Nutzer werden dort aufgefordert, ihr Gerät zu aktualisieren bzw. neu zu konfigurieren – so wird die Software heimlich installiert.

„Skygofree" gibt es vermutlich seit 2014 und wird immer weiterentwickelt. Der Trojaner nutzt eine Schnittstelle namens Accessibility Services, die eigentlich dazu gedacht ist, barrierefreie Apps zu entwickeln. Apps also, die zum Beispiel den Inhalt einer Whatsapp-Konversation vorlesen. Skygofree nutzt dieses Tor und leitet die Nachricht an die Ermittler weiter. Die Verschlüsselung von WhatsApp wird also nicht geknackt, sondern umgangen.

Doch nicht nur Whatsapp ist das Ziel. Skygofree kann insgesamt 48 verschiedene Funktionen aktivieren. Darunter das Mikrofon des infizierten Geräts, um den Beobachteten heimlich

abzuhören. Zudem kann die Kamera angeschaltet und unbemerkt Bilder und Videos gemacht werden. Sogar eine WLAN-Verbindung kann Skygofree herstellen und so Daten versenden, darunter zum Beispiel Standortdaten, SMS, Kalendereinträge und vieles weitere aus dem Speicher des Handys. Auch wenn einige der Funktionen, die Skygofree heimlich einschalten kann, noch nicht im realen Leben beobachtet wurden – möglich ist es.

Die Software ist in den vergangenen Jahren so weiterentwickelt worden, dass sie mehrere Root-Exploits mitbringt und auf verschiedenen Geräten einsatzfähig ist. Die Malware kann über HTTP, XMPP, Binär-SMS oder Firebase Cloudmessaging kontrolliert werden. Neben Android soll die Schadsoftware auch Windows-Nutzer im Visier haben. Darauf deuten einige Module hin, die Kaspersky gefunden hat. Infizierte Computer wurden bis jetzt allerdings noch nicht entdeckt.

Über die gb.online gmbh

Die gb.online gmbh hat sich auf die berufliche Absicherung von Freelancern spezialisiert und bietet mit www.easy-insure.eu das umfangreichste Online-Versicherungsportal für freie und beratende Berufe in Deutschland. Seit 2011 können Selbstständige und Unternehmen bis 1 Million Euro Umsatz pro Jahr hier ihre beruflichen Risiken versichern.

Steigt der Umsatz, und wird eine individuelle Lösung benötigt, so steht mit dem Schwesterunternehmen groot bramel versicherungsmakler gmbh ein verlässlicher Partner zur Seite, der seit über 25 Jahren Gewerbetreibende und industriellen Unternehmen in Versicherungsfragen vertritt. Die groot bramel versicherungsmakler gmbh ist in 18 Ländern vertreten und begleitet sie, wohin auch immer sich ihr Geschäftsfeld entwickelt.

Kontaktdaten

gb.online gmbh
Frankfurter Straße 93
65779 Kelkheim

Ansprechpartner: Lutz-Hendrik Groot Bramel, Geschäftsführer

Folgen Sie uns auch auf	