Dissecting Android Spyware

Fachgebiet: IT-Security und Mobile Computing
Betreuer: Dr. Endre Bangerter, Dominic Fischer
Experte: Dr. Igor Metz (Glue Software Engineering AG)

Die Anzahl mobiler Endgeräte wie Smartphones und Tablets nimmt stetig zu. Gleichzeitig wächst auch die Zahl der Schadsoftware für diese Geräte. Eine Form davon sind Rootkits, welche ihre böswilligen Aktionen unbemerkt vom Benutzer ausführen. Spionagesoftware, wie sie im privaten und geschäftlichen Umfeld eingesetzt wird, hat dieselben Bedürfnisse nach Unsichtbarkeit. Es stellt sich die Frage wie diese Spionagesoftware funktioniert, ob Ähnlichkeiten mit Schadsoftware bestehen und wie sie die Android Sicherheitsmechanismen Umgehen.

Unsere Arbeit hatte zum Ziel, Spionagesoftware, wie sie im privaten und geschäftlichen Umfeld zur Überwachung von Familienangehörigen oder Mitarbeitenden eingesetzt wird, auf dem Android Betriebssystem zu analysieren. Dabei sollte die technische Funktionsweise und Umsetzung aber auch eventuelle Ähnlichkeiten mit Schadsoftware aufgezeigt werden.

Unsere Recherchen zeigten, dass der Markt für solche Anwendungen sehr gross ist. Viele Hersteller versuchen über Schreckensszenarien, wie das Fremdgehen des Ehepartners oder Belästigung der eigenen Kinder, ihre Produkte zu verkaufen. Dabei konnten zwei Typen unterschieden werden: Anwendungen für die Langzeitprotokollierung des Verhaltens des Beobachteten und Anti-Diebstahllösungen. Letztere unterschieden sich dadurch, dass Informationen nur in Echtzeit abgefragt werden konnten.

Für die technische Analyse wählten wir vier Produkte mit ähnlichem Funktionsumfang und unterschiedlichem Preisniveau aus. Die Spanne reichte von 3 Euro bis 349.– US Dollar. Funktionen, wie das Protokollieren von SMS, Telefonaten, WhatsApp-Nachrichten sowie die Benachrichtigung bei einem Wechsel der SIM-Karte, wurden von fast allen Produkten unterstützt. Spezialitäten, wie die das Mithören und Aufzeichnen von laufenden Telefonaten oder eine Art Echtzeitüberwachung, für welche die Bildschirmanzeige zum Spion übermittelt wurde, boten nur wenige an. Diese Zusatzdienste liessen sich die Hersteller meistens zusätzlich bezahlen.

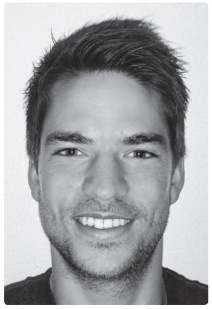
Es zeigte sich, dass die meisten Funktionen mit Methoden realisiert wurden, welche Android den Entwicklern standardmässig zur Verfügung stellt. Dies hatte zur Folge, dass fast alle Anwendungen durch den Beobachteten einfach entdeckt und deinstalliert, oder zumindest deaktiviert werden konnten. Es gab zwei Methoden, mit der versucht wurde, sich vor einer Deinstallation zu schützen: Eine Installation der Anwendung in die Systempartition bot zwar den Vorteil, beim Zurücksetzen des Geräts nicht gelöscht zu werden; eine Deaktivierung war jedoch weiterhin möglich. Das andere Produkt nutzte die Möglichkeiten, welche das Native Development Kit (NDK) bot, um sich als native Prozesse, losgelöst von Android, zu installieren. Dadurch konnte diese Anwendung, als Einzige, über die Benutzeroberfläche von Android weder entdeckt, deaktiviert oder deinstalliert werden.

Erschreckendes zeigte sich bei der Kommunikation. Lediglich ein Produkt verschlüsselte den Kommunikationskanal zum Anwendungsserver und bot somit einen Schutz der übertragenen Daten. Allerdings wurde die Verschlüsselung der Einfachheit halber unsicher implementiert und dadurch anfällig für eine «Man-in-the-middle-Attacke». Bei allen Produkten gelang es uns, sensible Benutzerinformationen wie Benutzernamen und Passwort vom Beobachteten und vom Spion mitzulesen. In zwei Fällen wäre es sogar möglich gewesen, Informationen über fremde Benutzer von den Anwendungsservern abzufragen. In einem Fall konnten wir unseren kompletten Datensatz einschliesslich Benutzernamen und Passwort für das Adminportal im Klartext abfragen. Es wäre ein Leichtes gewesen, sich dieselben Informationen fremder Konten zu besorgen!

Gewisse Ähnlichkeiten mit Schadsoftware zeigten sich bei einigen Produkten in der Art, wie Befehle an das überwachte Gerät gesendet werden. Ein Produkt nutzte ein Chatsystem und eines den Cloud 2 Device Messaging Dienst von Google, um Instruktionen an das Gerät zu übermitteln. Erstgenanntes wurde früher häufig von Botnetzbetreibern eingesetzt, um ihre befallenen Systeme zu steuern. Andere Analogien zu Schadsoftware, wie die Integration in legitime Prozesse oder das Verändern der Ausgabe mittels Hooking, fanden wir nicht.

Das Fazit ist ernüchternd: Alle Produkte bieten so gut wie keine Verschlüsselung der Kommunikation und machen es neugierigen Dritten leicht, die Informationen mitzulesen oder zu verändern. Nur ein Produkt schaffte es, sich ordentlich im System zu verstecken und lediglich ein weiteres konnte sich vor einer Deinstallation schützen.

Patrick Ravi-Pinto$
patrick.ravi-pinto@itravix.ch



Stefan Zahnd
stefan@zahndsolutions.ch