SOPHOS
Cybersecurity made simple.

Android-Adware bei Google Play

App-Entwickler betten seit Jahren Ad-Codes in ihre Apps ein, um die Entwicklungskosten zu decken. Einige Entwickler nutzen ihre Apps aber einfach als Plattform, um Anzeigen auf mobile Geräte zu schalten. Die SophosLabs haben kürzlich 15 Apps bei Google Play entdeckt, die sich mit solchen Praktiken beschäftigen. Die Apps erzeugen dabei häufig auftretende, große und aufdringliche Anzeigen. Dabei verstecken sie ihre App-Icons im Launcher, um es Anwendern schwer zu machen, sie zu finden und zu entfernen. Einige von ihnen gehen sogar noch einen Schritt weiter, indem sie sich auf der App-Einstellungsseite des Telefons tarnen. Mittlerweile haben weltweit mehr als 1,3 Millionen Geräte mindestens eine dieser aufdringlichen Apps installiert.

Die Entwickler nutzen dabei unterschiedliche Ansätze. So bedient sich die App free.calls.messages (Flash On Calls & Messages - auch bekannt als Free Calls & Messages) einiger cleverer Tricks, um zu verhindern, dass Benutzer die App deinstallieren. Beim ersten Start zeigt die App eine Meldung mit der Aufschrift „Diese App ist mit Ihrem Gerät nicht kompatibel" an. Anwender könnten denken, dass die App abgestürzt ist, denn nach diesem „Absturz" öffnet die App den Play Store und navigiert zur Google Maps-Seite. Der Anwender meint dann irrtümlich, dass die Maps App die Ursache des Problems ist. Das ist sie aber nicht. Die App verbirgt ihr eigenes Symbol, so dass sie nicht in der App-Tray des Launchers erscheint.

Die SophosLabs haben auch beobachtet, dass Name und Symbole der Anwendung, die auf der Einstellungsseite der Apps auf dem Smartphone zu sehen sind, oftmals nicht mit der Funktion übereinstimmen. Neun von 15 Apps verwendeten irreführende Applikationssymbole und -namen, von denen die meisten ausgewählt zu sein scheinen, weil sie plausibel einer harmlosen System-App ähneln könnten. Indem bei diesen Apps das Launcher-Symbol ausgeblendet ist und ein Anwendungssymbol und ein Name verwendet wird, der einer Systemanwendung ähnelt, liefern diese Anwendungen dem Anwender ein überzeugendes Argument dafür, dass auf dem Telefon nichts Ungewöhnliches installiert ist.

Andere Apps verwenden eine Bibliothek namens koolib, die einen Dienst installiert, um das Symbol nach einer bestimmten Zeit nach der Installation der App auszublenden. Die meisten dieser Apps wurden dem Benutzer als eine oder andere Art von Utility-App präsentiert. QR-Codeleser, Bildbearbeiter, Backup-Dienstprogramme oder ein Telefonfinder. Die Apps tarnen sich außerdem mit einem Namen, der eine harmlose App darstellt, wie z.B. Google Play Store, Update, Backup oder Time Zone Service. Diese Namen werden nur in den Einstellungen des Telefons angezeigt.

All diese Apps erschienen in diesem Jahr. Die älteste von ihnen, free.calls.messages, wurde im Januar veröffentlicht; zwei Monate nach ihrem Erscheinen hatte sie mehr als eine Million Installationen. Obwohl diese Apps von verschiedenen Publisher-Accounts hochgeladen wurden, teilten viele eine ähnliche Code-Struktur, Benutzeroberfläche, Paketnamen und Verhalten – zu viele, als dass es ein Zufall sein könnte. So enthielt beispielsweise die App com.cc.image.editor einen Verweis auf eine andere App, com.bb.image.editor, innerhalb ihres Codes. Die beiden Apps wurden trotz ihrer ähnlichen Namen von völlig unterschiedlichen Unternehmen veröffentlicht. Dies deutet darauf hin, dass erstere von letzteren abgeleitet sein könnten – dennoch kann man nicht definitiv sagen, dass derselbe Autor beide Apps entwickelt hat

„Durch die Nutzung immer innovativerer Techniken können solche Anwendungen innerhalb weniger Wochen nach ihrer Veröffentlichung eine Vielzahl von Opfern schnell infizieren“, so Michael Veit, Security-Experte bei Sophos. „Smartphone-Nutzer sollten vor der Installation von Apps aus Google Play genau auf die Bewertungen der Benutzer achten. Zudem sollten sie nicht die erste Person sein, die eine brandneue App ausprobiert.“

Die SophosLabs haben Google im Juli über diese Apps informiert und soweit bekannt, wurden sie entfernt. Diese Apps werden von Sophos Mobile Security als Andr/Hiddad-AB und Andr/Hiddad-AC erkannt.

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de