

16.06.2014 - 09:52 Uhr

Android-Smartphone von Werk aus mit Spionageprogramm ausgestattet / G DATA entdeckt gefährlichen Computerschädling in Firmware von Android-Gerät

Bochum (ots) -

- Querverweis: Bildmaterial ist abrufbar unter
<http://www.presseportal.de/galerie.htx?type=obs> -

Die Experten des deutschen Sicherheitsherstellers G DATA haben erstmalig ein Smartphone entdeckt, das bereits ab Werk mit einem umfassenden Spionageprogramm ausgeliefert wird. Die Malware ist als Google Play Store-Dienst getarnt und Teil der vorinstallierten Geräte-Software. Das Spionageprogramm arbeitet im Hintergrund und ist für Nutzer nicht zu entdecken. Unbemerkt vom Anwender sendet das Smartphone persönliche Daten an einen in China befindlichen Server und ist in der Lage, heimlich weitere Anwendungen verdeckt zu installieren. So können persönliche Daten abgerufen, Gespräche belauscht, Online-Banking Daten, E-Mails und SMS gelesen oder Kamera und Mikrofon ferngesteuert werden. Der chinesische Hersteller Star fertigt das betroffene Modell "N9500", das in seinem Aussehen an das Smartphone eines namhaften Herstellers erinnert. Eine Deinstallation der manipulierten App und des Spionageprogramms ist nicht möglich, da diese in die Firmware des Geräts integriert ist. Das Android-Gerät ist bei großen Online-Händlern zu Preisen zwischen 130 und 165 Euro erhältlich und wird europaweit vertrieben.

"Die Möglichkeiten mit diesem Spionageprogramm sind nahezu unbegrenzt. Online-Kriminelle erhalten den vollen Zugriff auf das Smartphone", weiß Christian Geschkat, Produktmanager Mobile Solutions. "G DATA Kunden hatten eine Erkennung durch unsere Sicherheitslösung gemeldet und uns dadurch auf die Spur dieser kriminellen Masche gebracht."

++ Testkauf führte zu beunruhigenden Ergebnissen

Die G DATA Sicherheitsexperten haben nach den Hinweisen durch Kunden das Gerät gekauft und analysiert. So wurde festgestellt, dass in der Firmware ein Fake Google Play Store-Dienst mit dem Trojaner Android.Trojan.Uupay.D versehen wurde. Die Spionagefunktion ist für den Besitzer unsichtbar und kann nicht deaktiviert werden. Dadurch haben Online-Kriminelle vollen Zugriff auf das Smartphone und alle persönlichen Daten. Protokolle, die einen Zugriff für Anwender ersichtlich machen könnten, werden direkt gelöscht. Auch das Einspielen von Sicherheits-Updates wird durch das Programm blockiert.

"Lediglich in den laufenden Prozessen des Smartphones können Anwender eine App mit dem Icon des Google Play Stores sehen, ansonsten maskiert sich die Anwendung", berichtet Christian Geschkat, G DATA Produktmanager Mobile Solutions. "Eine Deinstallation des Trojaners ist leider nicht möglich, da dieser Teil der Geräte-Firmware ist und hierzu zählende Apps können nicht gelöscht werden. Hierzu zählt auch die gefälschte Google Play Store App des N9500." Ob das eigene Gerät betroffen ist, können Besitzer mit Hilfe der G DATA Internet Security für Android feststellen, die den Schädling unter Android.Trojan.Uupay.D entdeckt. Betroffenen Käufern rät der Experte zur umgehenden Kontaktaufnahme mit dem jeweiligen Verkäufer.

++ Gefahr für Anwender

Für Anwender stellt das Smartphone eine große Gefahr dar. Über das Spionageprogramm können Kriminelle heimlich Apps installieren, wodurch das gesamte Spektrum an Missbrauch möglich ist: Ortung, Abhören & Aufzeichnen, Einkäufe, Bank-Betrug wie mTan-Diebstahl, Versand von Premium-SMS.

Wohin die Daten übermittelt werden ist nicht feststellbar. "Die abgegriffenen Daten werden an einen anonymen Server in China geschickt", so Christian Geschkat. "Wer die Daten schlussendlich erhält und verwendet, lässt sich nicht nachvollziehen."

++ Preis des Mobilgeräts soll Anwender anlocken

Es überrascht der günstige Preis zwischen 130 und 165 Euro, obwohl das Gerät technisch hochwertig ausgestattet ist. Das Quad-Core Smartphone wird mit umfangreichem Zubehör, wie zweitem Akku, KFZ-Ladeadapter und zweiter Schale, ausgeliefert. Vergleichbare Geräte von namhaften Herstellern kosten fast das Dreifache. Die Sicherheitsexperten von G DATA vermuten, dass der günstige Preis des Mobilgeräts durch den späteren Verkauf von gestohlenen Datensätzen der Smartphone-Besitzer erreicht wird. "Besonders günstige Angebote im Internet, die verlockend klingen, sollten Käufer generell stutzig machen. Niemand hat etwas zu verschenken", rät Christian Geschkat.

++ Smartphones und Tablets im Visier von Kriminellen

Die gestiegenen Verkaufszahlen von Smartphones und Tablets sind nicht unbemerkt an Online-Kriminellen vorbeigegangen. Allein in Deutschland nutzen laut comScore rund 40 Millionen Bürger ein Smartphone. Im vergangenen Jahr sind mehr als 1,2 Millionen neue Schadprogramme für Android aufgetaucht - die Tendenz zeigt steil nach oben. Anwender sollten daher eine umfassende Sicherheitslösung für die mobilen Alleskönner einsetzen.

Kontakt:

Thorsten Urbanski
Public Relations Manager
Phone: +49 (0) 234 - 9762 239
E-Mail: thorsten.urbanski@gdata.de

Vera Schmidt
Pressereferentin
Phone: +49 (0) 234 - 9762 376
E-Mail: vera.schmidt@gdata.de

Königsallee 178b
44799 Bochum, Deutschland

Diese Meldung kann unter <https://www.presseportal.ch/de/pm/100011910/100757636> abgerufen werden.