Neuer Android-Schädling geht auf Einkaufstour

MMarketPay.A bestellt automatisch kostenpflichtige Apps

(ddp direct) Die Experten der G Data SecurityLabs haben einen neuen Android-Schädling entdeckt, der unbemerkt vom Smartphone- oder Tablet-Besitzer kostenpflichtige Apps herunterlädt. Der Schädling befindet sich in gefälschten GO Weather, Travel Sky oder E-Strong File Explorer Apps und wird über diverse chinesische Webseiten und Drittanbieter App-Marktplätze verbreitet. Aktuell haben es die Täter auf die Kunden des weltweit größten Mobilfunkanbieters China Mobile abgesehen. Der Trojaner verschafft sich einen Zugang zum App-Store des Mobilfunkanbieters und kann so weitere Schadcode- oder kostenpflichtige Apps herunterladen und installieren. Nach Einschätzung der G Data SecurityLabs ist eine Verbreitung in Europa nicht auszuschließen.

Mit dem Android-Schädling MMarketPay.A haben Online-Kriminellen einen weiteren E-Crime-Geschäftszweig für sich erschlossen. Hatten es die Schadcode-Schreiber bisher auf den Diebstahl persönlicher Daten, Spionageangriffe oder den Versand von kostenpflichtigen Premium-SMS abgesehen, es ist ihnen jetzt erstmals gelungen, sich Zugang zum App-Markt eines Mobilfunkanbieters zu verschaffen. Hierzu verändert das Schadprogramm den sogenannten APN-Verbindungspunkt des Mobilgeräts und verbindet sich mit China Mobile. APN-Punkte auf Tablets und Smartphones werden im Regelfall von den Mobilfunkanbietern genutzt um z.B. Systemupdates bereit zu stellen. Der Trojaner fängt hierzu auch die Bestätigungs-Nachricht ab und stellt über einen speziellen Server eine Antwort bereit.

Der Schädling ist so in der Lage, ohne Anmeldung jederzeit auf den App-Store von China Mobile zu zugreifen und beliebige Apps auf Kosten des Opfers einzukaufen und zu installieren.

Wir beobachten hier die Entwicklung eines neuen und lukrativen Geschäftsmodells von Cyber-Kriminellen. Mit MMarketPay.A ist eine neue Dimension von schädlichen Apps aufgetaucht, die es auf das Ergaunern von Geld abgesehen haben, erklärt Ralf Benzmüller, Leiter der G Data SecurityLabs. Daher ist es aus unserer Sicht auch gut vorstellbar, dass eine abgeänderte Variante dieser Schad-App auch in Europa auftaucht und Kunden europäischer Mobilfunk-Anbieter ins Visier nimmt.

Sicherheitstipps für Android-Nutzer:
- Setzen Sie eine effektive und umfassende Sicherheitslösung ein, die das Mobilgerät umfassend absichert.
- Halten Sie Ihr Betriebssystem, die verwendeten Programme und Applikationen mit Updates immer auf dem aktuellsten Stand. So werden Sicherheitslücken geschlossen, die Cyber-Kriminelle ansonsten für Angriffe ausnutzen könnten.
- Beziehen Sie Apps nur aus vertrauenswürdigen Quellen, z.B. aus Google Play bei Android-Geräten und von Hersteller-Seiten. Beachten Sie bei der Auswahl der Applikationen, wie oft diese schon heruntergeladen wurden je höher die Zahl, desto vertrauenswürdiger ist die Anwendung. Zusätzlich sollten Sie überprüfen, welche Berechtigungen die Apps haben. Seien Sie vorsichtig bei Applikationen, die z.B. Anrufe initiieren oder SMS-Nachrichten verschicken können. Generell sollten Sie nur Apps installieren, die sich wirklich brauchen.
- Ignorieren Sie Mitteilungen auf ihrem Smartphone oder Tablet, dessen Ursprung sie nicht nachvollziehen können. Nutzer, die auf Nummer sicher gehen wollen, können diese online auf ihre Richtigkeit hin überprüfen oder den Kunden-Service ihres Providers kontaktieren.
- Kontrollieren Sie Ihre Telefon-Rechnung, wenn dort Dienste abgerechnet wurden, die Sie nicht genutzt haben, könnten Sie ein Opfer von Betrügern geworden sein.

Weitere Informationen stehen im G Data SecurityBlog zur Verfügung: http://blog.gdatasoftware.com/blog/article/new-android-malware-goes-on-a-shopping-spree-at-your-expense.html

Shortlink zu dieser Pressemitteilung:
http://shortpr.com/vw7thv

Permanentlink zu dieser Pressemitteilung:
http://www.themenportal.de/wirtschaft/neuer-android-schaedling-geht-auf-einkaufstour-22721

=== G Data: MMarketPay.A bestellt automatisch kostenpflichtige Apps (Bild) ===

Die Experten der G Data SecurityLabs haben einen neuen Android-Schädling entdeckt, der unbemerkt vom Smartphone- oder Tablet- Besitzer kostenpflichtige Apps herunterlädt. Der Schädling befindet sich in gefälschten GO Weather, Travel Sky oder E-Strong File Explorer Apps und wird über diverse chinesische Webseiten und Drittanbieter App-Marktplätze verbreitet. Aktuell haben es die Täter auf die Kunden des weltweit größten Mobilfunkanbieters China Mobile abgesehen. Der Trojaner verschafft sich einen Zugang zum App-Store des Mobilfunkanbieters und kann so weitere Schadcode- oder kostenpflichtige Apps herunterladen und installieren. Nach Einschätzung der G Data SecurityLabs ist eine Verbreitung in Europa nicht auszuschließen.

Shortlink:
http://shortpr.com/mdaz58

Permanentlink:
http://www.themenportal.de/bilder/g-data-mmarketpay-a-bestellt-automatisch-kostenpflichtige-apps

=== Screenshot: Diese gefälschte GO Weather App wurde von den Tätern mit MMarketPay.A infiziert und geht unbemerkt vom Anwender auf Einkaufstour. (Bild) ===

Mit dem Android-Schädling MMarketPay.A haben Online-Kriminellen einen weiteren E-Crime-Geschäftszweig für sich erschlossen. Hatten es die Schadcode-Schreiber bisher auf den Diebstahl persönlicher Daten, Spionageangriffe oder den Versand von kostenpflichtigen Premium-SMS abgesehen, es ist ihnen jetzt erstmals gelungen, sich Zugang zum App-Markt eines Mobilfunkanbieters zu verschaffen. Hierzu verändert das Schadprogramm den sogenannten APN-Verbindungspunkt des Mobilgeräts und verbindet sich mit China Mobile. APN-Punkte auf Tablets und Smartphones werden im Regelfall von den Mobilfunkanbietern genutzt um z.B. Systemupdates bereit zu stellen. Der Trojaner fängt hierzu auch die Bestätigungs-Nachricht ab und

stellt über einen speziellen Server eine Antwort bereit.

Shortlink:
http://shortpr.com/2h06ub

Permanentlink:
http://www.themenportal.de/bilder/screenshot-diese-gefaelschte-go-weather-app-wurde-von-den-taetern-mit-mmarketpay-a-infiziert-und-geht-unbemerkt-vom-anwender-auf-einkaufstour

Pressekontakt

G Data Software AG

Frau Kathrin Beckert
Königsallee b 178
44799 Bochum

presse@gdata.de

Firmenkontakt

G Data Software AG

Frau Kathrin Beckert
Königsallee b 178
44799 Bochum

gdata.de
presse@gdata.de

Die G Data Software AG, mit Unternehmenssitz in Bochum, ist ein innovatives und schnell expandierendes Softwarehaus mit Schwerpunkt auf IT-Sicherheitslösungen. Als Spezialist für Internetsicherheit und Pionier im Bereich Virenschutz entwickelte das 1985 in Bochum gegründete Unternehmen bereits vor mehr als 20 Jahren das erste Antiviren-Programm.G Data ist damit eines der ältesten Securitysoftware-Unternehmen der Welt.

Das Produktportfolio umfasst Sicherheitslösungen für Endkunden, den Mittelstand und für Großunternehmen. G Data Security-Lösungen sind in weltweit mehr als 90 Ländern erhältlich.

Weitere Informationen zum Unternehmen und zu G Data Security-Lösungen finden Sie unter www.gdata.de

Anlage: Bild