500.000 Downloads bei Google Play mit Rogue Malware – was war da los und was ist zu tun?

Die SophosLabs wiesen jüngst auf eine Malware-Familie auf Google Play hin, sie sich als eine Reihe praktischer Dienstprogramme präsentierte. Zu den infizierten Anwendungen zählten beispielsweise sechs QR-Code-Lese-Apps oder ein sogenannter "intelligenter Kompass". Schon der Name Andr/HiddnAd-AJ weist darauf hin, was die Rogue Apps eigentlich tun: eine intensive Bombardierung mit Werbung. Eines der Probleme bei dieser Malware ist, dass sie erst eine Weile im Hintergrund ruht um dem Anwender ein falsches Sicherheitsgefühl zu vermitteln. Nachdem Sophos die betroffenen Apps an Google gemeldet hat, wurden diese aus dem Play Store entfernt. Allerdings wurden zu diesem Zeitpunkt bereits über 500.000 Downloads registriert.

Malware situationsbedingt anpassbar
Zusätzlich zum Werbebombardement kann die Malware noch deutlich mehr: sie sendet beispielsweise Android-Benachrichtigungen, einschließlich anklickbarer Links. Das Ziel: noch mehr Werbeeinnahmen für die Kriminellen. Aber es kommt noch dicker: sobald die infizierte Anwendung zum ersten Mal ausgeführt wird, ruft sie „nach Hause“, um Konfigurationsinformationen an einen von den Gaunern kontrollierten Server zu senden. Diese Informationen werden von den Kriminellen genutzt, um das Verhalten der Malware jederzeit und remote anzupassen, ohne den Code selbst aktualisieren zu müssen. Dies schafft den Kriminellen hervorragende Möglichkeiten, die Effizienz ihrer Malware zu steigern.

Was kann man tun?
Zwar hat Google die Apps aus den Store genommen, doch von den rund 500.000 Downloads sind weltweit sicherlich viele aktiv. Es gilt also die Malware wieder los zu werden. Moderne Mobile Security Programme, wie das kostenlose Sophos Mobile Security for Android, erkennen die Malware und machen diese unschädlich. Zudem sollte man sich an die Anweisungen von Google halten. Der App-Überprüfungsprozess von Google ist zwar nicht perfekt, aber er führt zumindest einige Checks durch.

Mehr Details von Paul Ducklin zu diesem Thema stehen auf Sophos Naked Security unter: https://bit.ly/2GP5omU

Über Sophos
Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Sophos‘ Complete-Security-Lösungen als den besten Schutz vor komplexen IT-Bedrohungen und Datenverlust. Sophos bietet dafür preisgekrönte Verschlüsselungs-, Endpoint-Security-, Web-, Email-, Mobile- und Network Security-Lösungen an, die einfach zu verwalten, zu installieren und einzusetzen sind. Das Angebot wird von einem weltweiten Netzwerk eigener Analysezentren, den SophosLabs, unterstützt.
Sophos hat seinen Hauptsitz in Boston, USA, und Oxford, Großbritannien. In Deutschland hat das Unternehmen seinen Hauptsitz in Wiesbaden und ist in Österreich und der Schweiz je an einem Standort vertreten. Weitere Informationen unter www.sophos.de.

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