Erster Malware-Star 2018: SkyGoFree spioniert Android-Smartphones im großen Stil aus

Noch nicht mal drei Wochen ist das neue Jahr alt, da kristallisiert sich mit der Spyware SkyGoFree bereits der erste Anwärter für die Schadsoftware 2018 heraus. Die Sophos Security-Spezialisten haben entdeckt, dass die Malware vorgibt, ein System-Update zu sein. Die gute Nachricht: man kann sich schützen.

Wiesbaden, 23. Januar 2018. SkyGoFree – der neue Shootingstar am Malware-Himmel. Auf den ersten Blick denkt man an ein kostenloses, mobiles Produkt des bekannten Bezahl-TV-Senders. Doch weit gefehlt: SkyGoFree ist Spyware vom Feinsten und hat es auf Android-Smartphones abgesehen.

Was macht SkyGoFree auf den Geräten?
Ein Blick auf den Java Code offenbart viel Heimtückisches, inklusive einer Funktion, die StartReverse heißt: sie verbindet das Handy mit einem Server der Kriminellen, um diesen einen Kommandozeileninterpreter zu geben. Normalerweise benötigt man dafür eine initiale Verbindung zu einem Gerät, und damit Durchgang durch Firewalls und die Übersetzung der Netzwerk-Adressen, die dazwischen sind. Viele mobile Netzwerke und nahezu alle Wi-Fi-Netzwerke lassen abgehende Verbindungen zu anderen Personen zu, verhindern aber Eingehende. Man muss schon ein Client, also ein Datennutzer, auf dem Netzwerk sein, kein Datenproduzent (Server). Hacker umgehen dieses Prinzip mit einer Reverse Shell, einem üblichen Trick, der den Log-on Prozess auf den Kopf stellt: das verwendete Gerät ermöglicht die Verbindung zu den Hackern nach außen, aber nur um die Verbindung aufzubauen. Danach verhält sich das Gerät wie ein Server, auf dem die Kriminellen sich als Clients zuschalten. Eingelogged mit direkter Kontrolle über das Gerät.

SkyGoFree hat noch ein weiteres Merkmal: es erlaubt den Kriminellen Daten von zahlreichen anderen Applikationen auf dem Gerät zu sammeln. SkyGoFree hat zudem eine Komponente, die weitere Schadsoftware downloaden und installieren kann – eine Art Plug-In-System für Malware. Schadsoftware wird oft so programmiert, dass es sich selbst aktualisieren oder erweitern kann. Ein ernsthaftes Problem, denn niemand kann sicher sein, was die Kriminellen mit den infizierten Geräten vorhaben.

Die gute Nachricht: auf einem regulären AndroidSmartphonekönnen Apps untereinander nicht blind irgendwelche Daten lesen. Es sei denn, das Gerät ist sehr alt und ohne aktuelle Updates, wodurch eineSicherheitslücke ausgenutzt werden kann, die es Malware erlaubt, automatisch Root-Rechte zu bekommen und verborgen im Hintergrund zu arbeiten.

Wie erkennt man SkyGoFree auf seinem Gerät?
Die Sophos Security-Spezialisten haben entdeckt, dass die Malware vorgibt, ein System-Update zu sein. Dazu nutzt es ein grünes Android-Symbol. Wenn ein Nutzer nun die App startet, läuft sie im Hintergrund los und lässt das eigene Icon nahezu sofort verschwinden, so dass der User den Eindruck gewinnt, das Update ist fertig. Zumindest verbleibt die App auf der Einstellungsseite, auf der alle Apps aufgelistet sind. Nutzer können sie hier stoppen und deinstallieren.

Tipps zum Schutz vor SkyGoFree:
„Malware betrifft heutzutage jeden, der Computer oder Mobilgeräte mit Internetanbindung nutzt, es gibt keine Ausnahme. Allerdings kann man sich auf unterschiedlichste Art und Weise

schützen. Gute Security-Software hilft und lässt sich leicht sowohl auf Mobilgeräte als auch auf Computer installieren. Mindestens so wichtig ist auch der vorsichtige Umgang mit den Geräten. Ein genauer Blick auf Nachrichten oder angebotene Software beziehungsweise Updates lassen oft erkennen, dass der Ursprung zweifelhaft ist“, so Michael Veit, IT-Sicherheitsexperte bei Sophos. Er gibt folgende Tipps:

- Keine Apps aus ungesicherten Quellen wählen. SkyGoFree zum Beispiel ist nicht in Google Play. Um infiziert zu werden, muss der Nutzer also unter „Einstellungen/Sicherheit“ die Nicht-Standard Einstellung aktiv einschalten, um App-Installationen von unbekannten Quellen zu erlaubten. Google Play ist sicher nicht das virenfreie Paradies, aber die sicherere Wahl, statt alternative Märkte, unregulierte Android-Foren oder Links, die von Bekannten zugeschickt werden.
- Finger weg von System-Updates, die von Dritten angeboten werden. Gern werden diese mit Zusatz-Features beworben, die offiziell nicht erhältlich sind. Aus gutem Grund.
- Ein Android Anti-Virus Programm verwenden. Die Sophos Mobile Security for Android blockiert Malware und warnt den User vor unsicheren Einstellungen auf dem Gerät. Kostenlos hier erhältlich: Sophos Mobile Security for Android

Über Sophos
Sophos ist führender Anbieter von Endpoint- und Network-Security-Lösungen der nächsten Generation. Als Pionier der Synchronized Security entwickelt Sophos sein innovatives Portfolio an Endpoint-, Netzwerk-, Verschlüsselungs-, Web-, E-Mail- und mobilen Security-Lösungen, die miteinander kommunizieren. Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Lösungen von Sophos mit hervorragendem Schutz vor anspruchsvollen Bedrohungen und Datenverlust. Sophos Produkte sind exklusiv über den weltweiten Channel mit mehr als 26.000 registrierten Partnern erhältlich. Sophos hat seinen Hauptsitz in Oxford, Großbritannien, und wird an der Londoner Börse unter dem Symbol "SOPH" öffentlich gehandelt. 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 +172 4536839
sophos@tc-communications.de