SIMPLY SECURE

G DATA MOBILE MALWARE REPORT

GEFAHRENBERICHT: Q2/2015

Whitepaper Mobile Malware Report DE 07-2015 - 2313170815

SIMPLY SECURE

INHALTE

Whitepaper Mobile Malware Report DE 07-2015 • 2313170815

AUF EINEN BLICK

- Der weltweite Marktanteil von Android-Smartphones und -Tablets lag im zweiten Quartal 2015 bei fast 64 Prozent. Zum ersten Quartal bedeutet das einen Anstieg um drei Prozent. In Deutschland nutzten rund 68 Prozent der Anwender ein Mobilgerät mit Android-Betriebssystem, in Europa rund 64 Prozent.[1]
- Rasanter Anstieg der absoluten Schadcode-Zahlen für Android-Geräte: Im zweiten Quartal 2015 haben die G DATA Sicherheitsexperten 560.671 neue Malware-Samples analysiert. Im Vergleich zum ersten Quartal 2015 bedeutet das einen Anstieg neuer Schadprogramme um 27 Prozent.
- Neuer Rekord: Im Halbjahresvergleich wurde erstmals seit Veröffentlichung des Mobile Malware Reports die Millionen-Schallmauer an neuen Android-Schaddateien innerhalb eines Halbjahres durchbrochen. Im ersten Halbjahr 2015 entdeckten die G DATA Experten 1.000.938 neue Android-Schaddateien – zum zweiten Halbjahr 2014 bedeutet das einen Anstieg um 25 Prozent.
- Apps, die Funktionen verschleiern und Nutzer überwachen, blockiert G DATA in seinen Sicherheitslösungen. Aber welche Kriterien müssen erfüllt sein? Am Beispiel einer App mit versteckten Überwachungs-Funktionen erklären die Experten ihr Vorgehen.
- Das Smartphone Star N9500 hat mit seinen Spionagefunktionen im letzten Jahr für Furore gesorgt. Die G DATA Sicherheitsexperten haben Hinweise auf weit über 26 Geräten entdeckt, die solche Funktionen aufweisen. Die Experten vermuten dahinter Zwischenhändler, die die Firmware verändert haben, um möglicherweise Nutzerdaten zu stehlen und mit Werbung Geld zu verdienen.

PROGNOSEN UND TRENDS

ÜBER ZWEI MILLIONEN NEUE ANDROID-SCHÄDLINGE 2015

Für das Gesamtjahr 2015 rechnen die G DATA Sicherheitsexperten mit weit über zwei Millionen neuer Malware für das Android-Betriebssystem – ein neuer Rekord. Die Anzahl neuer Schädlinge hätte sich somit innerhalb von zwei Jahren verdoppelt.

QUALITÄT VON ANDROID MALWARE STEIGT

Die IT Firma Hacking Team programmiert umfangreiche Malware für Geheimdienste und Staaten. Durch einen Cyberangriff auf das Unternehmen wurde neben Firmendaten auch ein Quelltext für eine Android Malware veröffentlicht. Die G DATA Sicherheitsexperten erwarten, dass Cyberkriminelle diesen leicht zugänglichen Wissensfundus ausnutzen und ausgereiftere Android Malware in höherer Anzahl veröffentlichen wird.

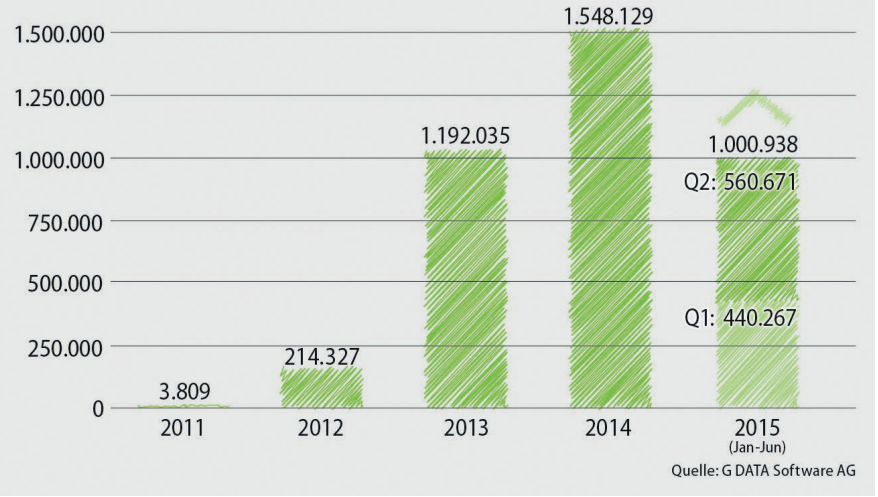
[1] Statcounter: http://gs.statcounter.com/

AKTUELLE LAGE: TÄGLICH 6.100 NEUE ANDROID-SCHADDATEIEN

Die Anzahl neuer Android-Malware ist weiter enorm gestiegen – die Prognose aus dem ersten Quartal hat sich bestätigt. Im zweiten Quartal 2015 analysierten die G DATA Sicherheitsexperten 560.671 neue Android-Schaddateien. Zum ersten Quartal 2015 (Q1/2015) bedeutet das einen Anstieg um über 27 Prozent. Durchschnittlich entdeckten die Experten in Q2/2015 pro Tag über 6.100 neue Android-Schaddateien, das sind täglich fast 1.200 mehr als in Q1/2015. Alle 14 Sekunden identifizieren die Analysten durchschnittlich einen neuen Schädling.

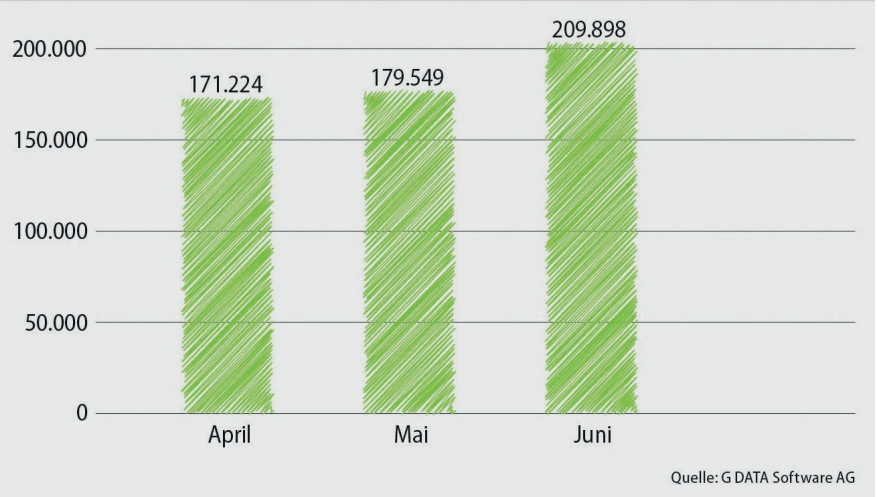
Der enorme Anstieg neuer Android-Schaddateien bedeutet für das erste Halbjahr 2015 einen neuen Rekord. Erstmals entdeckten die G DATA Sicherheitsexperten in einem Halbjahr über eine Millionen neuer Android-Schädlinge. Für das Gesamtjahr 2015 erwarten die Analysten insgesamt deutlich über zwei Millionen neue Android-Malware.

NEUE ANDROID SCHADDATEIEN



Die rückwirkenden Zahlen in diesem Bericht fallen höher aus, als die in den zuvor veröffentlichten Berichten. In einigen Fällen empfängt G DATA Datei-Sammlungen mit einer großen Anzahl neuer Schaddateien aus einem längeren Zeitraum und diese enthalten mitunter ältere Dateien, die dann dem entsprechenden Monat zugeordnet werden.

NEUE ANDROID SCHADDATEIEN 2015 / MONATLICH (Q2)



ÜBERWACHUNGS-APPS AUF DEM MOBILGERÄT

Im Mobile Malware Report aus dem ersten Quartal 2015 haben die G DATA Sicherheitsexperten gezeigt, was Adware auf Android-Mobilgeräten bedeutet. Neben Adware gibt es eine Vielzahl anderer Unterkategorien im Bereich PUP (Potentially Unwanted Programs). In diesem Bericht beleuchten wir den Bereich „Monitor". Diese Schaddateien sind keine Malware im klassischen Sinne. Sie dienen vielmehr zur versteckten Überwachung des Smartphone-Besitzers durch eine andere Person, die die gesammelten Daten erhält. Beispielsweise könnten Eltern ihren Nachwuchs überwachen und sehen, mit wem das Kind Kontakt hat oder wo es sich gerade befindet. Die Einsatzmöglichkeiten sind vielfältig.

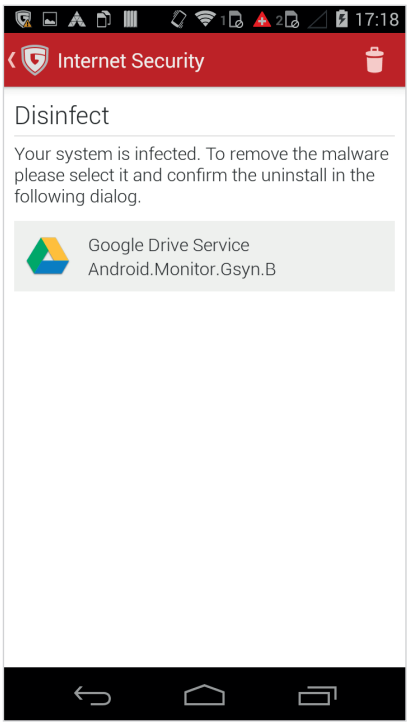
Monitor-Malware versteckt sich vor dem Anwender. Lediglich bei der Installation oder wenn der Anwender die App findet, besteht die Möglichkeit, die Berechtigungen zu sehen. Jedoch verlangen auch legitime Apps häufig Berechtigungen, die über die reine Tätigkeit der Anwendung hinausgehen. Dadurch ist es für Anwender nicht ersichtlich, dass sich eine App mit Überwachungs-Funktion auf dem Smartphone befindet. Aus diesem Grund stufen die G DATA Sicherheitsexperten diese Programme als PUP ein. G DATA Sicherheitslösungen erkennen die Anwendungen.

GETARNTE GOOGLE DRIVE-APP MIT ÜBERWACHUNGSFUNKTION

„Android.Monitor.Gsyn.B" ist eine als Monitor eingestufte App, welche sich bei Anwendern unter anderem als „Google Drive"-Anwendung ausgibt. Nutzer gehen davon aus, dass sie die originale Google Drive App besitzen, da das genutzte Icon und die Bezeichnung nah am legitimen Programm liegen. In diesem Fall beinhaltet die Anwendung aber nur Überwachungsfunktionen.

Die getarnte App kann laut Hersteller ohne das Wissen des Nutzers eine Vielzahl an Daten stehlen sowie Funktionen ausführen:

- Telefongespräche mitschneiden
- Kontakte einsehen und kopieren
- Standortdaten abfragen
- Bilder aufnehmen und kopieren
- Gespräche per Mikrofon aufnehmen
- SMS/MMS verschicken und lesen
- AV-Software und andere Apps ausschalten
- Chatverläufe von Messengern mitschneiden (WhatsApp, Skype, Viber, Facebook, Google+, etc.)
- Browserhistory auslesen



VORINSTALLIERTE MALWARE AUF DEM SMARTPHONE

Seit der Entdeckung eines vorinstallierten Schadcodes auf einem Smartphone im Frühjahr 2014 finden die G DATA Sicherheitsexperten immer mehr Modelle, bei denen Malware in der Firmware nachgewiesen werden kann. Doch woher kommen die Schadprogramme und wer installiert diese? Die G DATA Sicherheitsexperten sind sich sicher, dass in den meisten Fällen die Hersteller nicht die Täter sind. Renommierte Unternehmen werden ihren Ruf nicht für Malware in der Firmware riskieren.

Die G DATA Experten vermuten als Täter daher Zwischenhändler, die so neben dem Erlös, den der Weiterverkauf des Mobilgeräts einbringt, noch zusätzlich mit gestohlenen Nutzerdaten und aufgezwungener Werbung einen finanziellen Gewinn erwirtschaften wollen.

WIE VERSTECKT SICH DIE MALWARE?

In den analysierten Fällen versteckt sich das Schadprogramm in einer manipulierten App. Eine legitime Anwendung erhält ein Schadprogramm als Ergänzung. Neben den gewohnten Funktionen der App versteckt sich darin die Malware. Anwender bemerken von diesen Zusatz-Funktionen nichts, da die meisten Abläufe im Hintergrund stattfinden.

BEISPIEL: MANIPULIERTE FACEBOOK-APP

Ein beliebtes Vorgehen ist das Manipulieren einer legitimen und beliebten Anwendung, wie die Facebook-App. Bei der Manipulation sind alle gewohnten Facebook-Funktionen verfügbar. Anwender merken den Zugriff nicht. Durch das angehängte Schadprogramm erweitert sich der Funktionsumfang und ermöglicht Dritten Zugriff auf das gesamte Gerät, ohne das Wissen oder das Einverständnis des Nutzers. Die Rechte wurden bereits vor der Inbetriebnahme des Geräts durch den Besitzer frei gegeben. Somit merkt der Nutzer die schädliche Anwendung erst, wenn er eine Sicherheitslösung wie G DATA INTERNET SECURITY FÜR ANDROID einsetzt. Sobald die Security-Software installiert ist, schlägt sie sofort Alarm. In diesem Beispiel identifiziert die G DATA Sicherheitslösung den Schädling als „Android.Trojan.Andup.D“. Eine Deinstallation ist häufig nicht möglich, da die App zu den festinstallierten Anwendungen in der Firmware gehört.
Die G DATA Sicherheitsexperten raten betroffenen Anwendern, den Verkäufer des Mobilgeräts zu kontaktieren.

Die heimlichen Zusatzfunktionen sind weitreichend. Im vorliegenden Beispiel kann die App auf das Internet zugreifen, SMS lesen und senden, Anwendungen nachinstallieren,

Anrufdaten und Daten zum Smartphone einsehen, speichern und verändern, auf die Kontaktliste zugreifen, Standortdaten abrufen und App-Updates kontrollieren. Durch diese Rechte ist umfangreicher Missbrauch möglich: Ortung, Abhören & Aufzeichnen von Telefonaten oder Gesprächen, Einkäufe, Bank-Betrug oder der

Versand von Premium-SMS. Die Möglichkeiten sind beliebig erweiterbar.

In fast allen Varianten, die die G DATA Sicherheitsexperten analysierten, war die App schlecht programmiert und birgt ein enormes Sicherheitsrisiko. Sensible Daten werden zum Großteil unverschlüsselt verschickt oder lediglich mit einem festen Schlüssel versehen, der leicht entschlüsselt werden kann. So können Angreifer Daten stehlen oder die Kontrolle über die Malware übernehmen.

Dazu kommt, dass bisher keines der untersuchten Samples überprüft, ob es wirklich mit dem richtigen Server Daten austauscht. Auf diesem Weg könnten Man-in-the-Middle-Angriffe leicht umgesetzt werden.

```
<uses-permission android:name="android.permission.INTERNET" />
<uses-permission android:name="android.permission.READ_SMS" />
<uses-permission android:name="android.permission.RECEIVE_SMS" />
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.READ_PHONE_STATE" />
<uses-permission android:name="android.permission.SEND_SMS" />
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
<uses-permission android:name="android.permission.CHANGE_COMPONENT_ENABLED_STATE" />
<uses-permission android:name="android.permission.MODIFY_PHONE_STATE" />
<uses-permission android:name="android.permission.READ_CONTACTS" />
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
<uses-permission android:name="android.permission.ACCESS_MOCK_LOCATION" />
<uses-permission android:name="android.permission.CONTROL_LOCATION_UPDATES" />
<uses-permission android:name="android.permission.ACCESS_LOCATION_EXTRA_COMMANDS" />
```

Die App kann auf das Internet zugreifen, SMS lesen und senden, Anwendungen nachinstallieren, Anrufdaten und Daten zum Smartphone einsehen, speichern und verändern, auf die Kontaktliste zugreifen, Standortdaten abrufen und App-Updates kontrollieren.

WELCHE GERÄTE SIND BETROFFEN?

Eine manipulierte und vorinstallierte App konnten die Experten auf drei Mobilgeräten im Auslieferungszustand nachweisen. Neben dem Star N9500, welches bereits 2014 untersucht wurde, sind das Star N8000 und das ICE FOX Razor dazugekommen. Durch Rückmeldungen der G DATA INTERNET SECURITY FÜR ANDROID, Supportkontakt und Ergebnissen anderer Sicherheitsforscher haben die Experten noch weitere Fälle identifiziert, in denen der Verdacht nahe liegt, dass auch bei diesen Geräten vorinstallierte Malware nachzuweisen ist. In diesen Fällen vermuten die G DATA Sicherheitsexperten Mittelsmänner hinter der Manipulation, da nur einzelne Geräte betroffen sind wie das Huawei oder Lenovo Modell. Die Experten gehen von einer deutlich höheren Dunkelziffer aus.

INFIZIERTE MODELLE (AUSZUG)

- Xiaomi MI3
- Huawei G510
- Lenovo S860
- Alps A24
- Alps 809T
- Alps H9001
- Alps 2206
- Alps PrimuxZeta
- Alps N3
- Alps ZP100
- Alps 709
- Alps GQ2002
- Alps N9389
- Andorid P8
- ConCorde SmartPhone6500
- DJC touchtalk
- ITOUCH
- NoName S806i
- SESONN N9500
- SESONN P8
- Xido X1111

G DATA SIMPLY SECURE

Whitepaper Mobile Malware Report DE 07-2015 • 2313170815