TRUST IN GERMAN SICHERHEIT

G DATA Mobile Malware Report

Gefahrenbericht: H1/ 2014

TRUST IN GERMAN SICHERHEIT

INHALT

Auf einen Blick

- In diesem Jahr rechnen Marktanalysten mit 1,2 Milliarden[1] neu verkauften Smartphones – davon wurden im ersten Halbjahr dieses Jahres 563 Millionen Mobilgeräte mit Android-Betriebssystem verkauft – 489 Millionen Smartphones[2] und 74 Millionen Tablets[3].
- Zerstückelte Android-Verteilung: 69,8 Prozent der Android-Nutzer haben im November 2014 eine veraltete Version des Betriebssystems installiert. 30,2 Prozent verwenden die Version 4.4 („KitKat“).[4]
- Absolute Schadcode-Zahlen für Android-Geräte: Die Anzahl neuer Mobile Malware-Samples ist im ersten Halbjahr 2014 im Vergleich zum Vorjahreszeitraum weiter angestiegen: 751.136 neue Schaddateien im ersten Halbjahr 2014 - im zweiten Halbjahr 2013 waren es 672.940.
- Steigerungsraten: 12 Prozent mehr neue Android-Schaddateien als im zweiten Halbjahr 2013- zum ersten Halbjahr 2013 ist das ein Anstieg von 43 Prozent.
- Verschlüsselung, Betrug, Erpressung: Ransomware gewinnt weiter an Bedeutung. Die Malware ist leicht zu entwickeln und bringt den Kriminellen schnell verdientes Geld.
- Dritt-Markets für Apps sind eine Hauptquelle für Schadcode.
- Einfallstor Custom-Firmware: Zahlreiche Nutzer greifen auf andere Software zurück, um ihr Android-Gerät auf den neuesten Stand zu bringen. Die Entwickler nutzen frei verfügbare Schlüssel zum Signieren der Software, dadurch öffnen sie ungewollt Angreifern eine Tür. Cyberkriminelle nutzen diesen Weg zum Verbreiten manipulierter Apps oder gefälschter Sicherheits-Updates.

Prognosen und Trends

- **Tickende Zeitbomben: Sicherheitslücken in Android-Betriebssystemen**
  Die langen Update-Intervalle vieler Smartphone- und Tablet-Hersteller werden perspektivisch zu einem großen Sicherheitsproblem heranwachsen und die effektive Absicherung der Endgeräte erschweren. Bis eine neue Android-Version Nutzer erreicht, können Wochen oder Monate vergehen. Ältere Geräte bleiben zudem meist unversorgt. Nicht geschlossene Sicherheitslücken mit veralteten und nicht gepatchten Android-Betriebssystemen werden zukünftig zu einem nicht kalkulierbaren Risiko für die Datensicherheit von Endanwendern und Unternehmen.

- **Digitaler Spion ab Werk „verbaut“**
  Erstmals konnte G DATA in diesem Jahr ein Spionageprogramm als Teil der Firmware nachweisen. Das betroffene Smartphone Star N9500 ist nach Einschätzung der Experten kein Einzelfall. Mit weiteren Entdeckungen ist zu rechnen, da Spionageprogramme innerhalb der Firmware nur schwer zu enttarnen sind.

[1] http://www.idc.com/getdoc.jsp?containerId=prUS24857114
[2] http://www.idc.com/getdoc.jsp?containerId=prUS25037214; http://www.idc.com/getdoc.jsp?containerId=prUS24823414; http://www.idc.com/prodserv/smartphone-os-market-share.jsp.
[3] http://www.prnewswire.co.uk/news-releases/tablet-shipments-rose-by-6-percent-year-on-year-in-q2-2014-says-strategy-analytics-268313362.html
[4] https://developer.android.com/about/dashboards/index.html

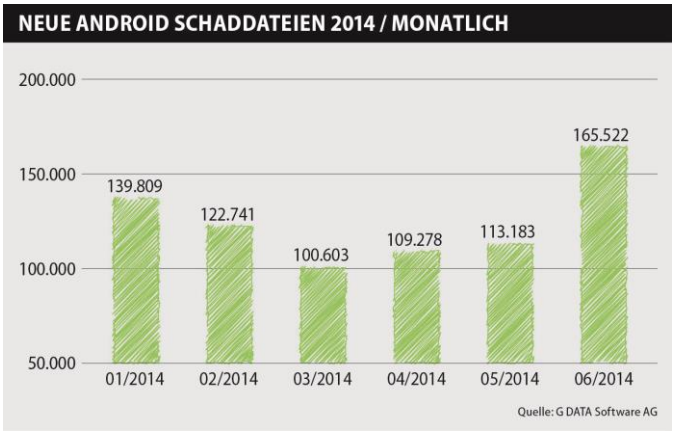
- **Do-It-Yourself Baukästen**
  Tools zur Entwicklung von Windows-Computerschädlingen sind seit Längerem Teil des Angebotsportfolios von Untergrundmärkten. Waren Malware-Baukästen zur Entwicklung schädlicher Android-Apps eher die Seltenheit, so tauchen diese 2014 immer häufiger auf kriminellen Handelsplattformen auf. G DATA rechnet in den kommenden 12 Monaten mit einer weiteren Zunahme dieser E-Crime-Tools und hieraus resultierend auch mit einer weiteren Zunahme von Schad-Apps.

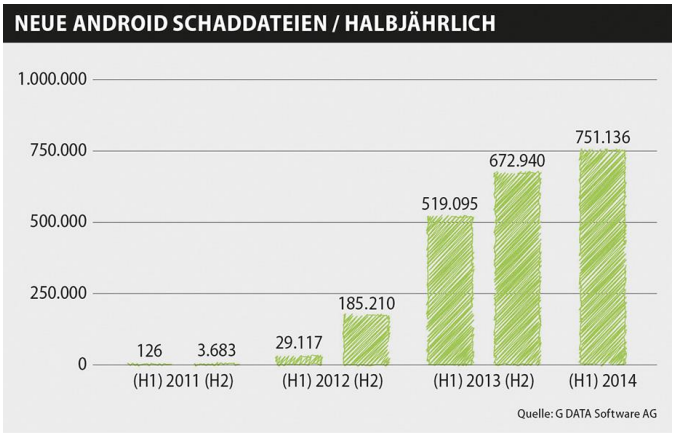
- **Infizieren – verschlüsseln – erpressen**
  Ransomware wird weiter an Bedeutung gewinnen. Es ist davon auszugehen, dass Angreifer noch durchdachtere Varianten der Malware verbreiten. Das Betriebssystem Android 5.0 könnte der weiteren Verbreitung einen Dämpfer verpassen, da alle Daten dort verschlüsselt werden.

- **Falsche Schutzprograme**
  Fake-AV, womit vermeintliche Sicherheits-Apps gemeint sind, die keinerlei Schutzfunktion besitzen oder sogar der Infektion des Geräts mit Schadcode dienen, tauchen stärker als zuvor auf. Bereits zu Beginn des Jahres haben zwei Maschen für Aufsehen gesorgt. Betrüger haben nutzlose Apps mit vermeintlichen Virenscannern verbreitet. Durch gekaufte Bewertungen haben tausende ahnungslose Nutzer die Apps gekauft und den Kriminellen große Gewinne beschert.

Aktuelle Lage: Täglich 4.200 neue Android-Schaddateien

In den ersten sechs Monaten des Jahres 2014 registrierten die G DATA Sicherheitsexperten 751.136 neue Schadprogrammtypen. Die Anzahl neuer Schadprogrammtypen ist somit um 12 Prozent im Vergleich zum zweiten Halbjahr 2013 (672.940) gestiegen. Durchschnittlich entdecken die Experten pro Tag 4.200 neue Android-Schaddateien.





Einteilung und Top 5

Die G DATA Sicherheitsexperten kategorisieren die Dateien anhand der Eigenschaften der Malware in bestimmte Familien. 195.923 der neuen Schadprogramme konnten zu Malware-Familien zugeordnet werden. Bei der Kategorisierung der variantenreichsten Android-Schädlinge dominieren Trojaner die Top 5 mit gleich vier Vertretern. Die hohe Anzahl von Varianten im Vergleich zum letzten Halbjahr liegt daran, dass bestimmte Malware-Typen leichter zu generieren sind.

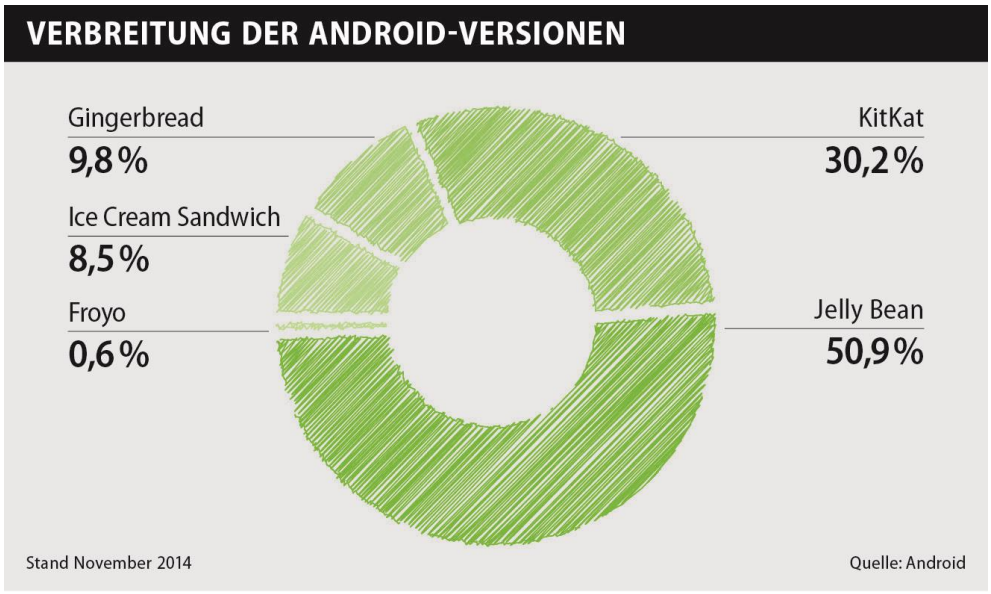
Die Malware-Familie „Backdoor.Gingermaster“ wird durch manipulierte Kopien von Apps aus Dritt-Stores verbreitet.[5] Gingermaster ist ein Schädling, der das Mobilgerät rooten kann und somit vollen Zugriff erhält. Die Schadsoftware stiehlt Gerätedaten, wie die „International Mobile Equipment Identity“ (IMEI)[6] oder „International Mobile Subscriber Identity“ (IMSI)[7].

[5] Weitere Information dazu, siehe Kapitel „Drittanbieter App Stores: Malware Gefahr“
[6] Die IMEI-Nummer ist eine 16-stellige Seriennummer, an der ein Mobilgerät identifiziert werden kann.
[7] Die IMSI-Nummer dient in GSM- und UMTS-Mobilfunknetzen zur Identifizierung des Mobilfunkteilnehmers.

Top 5 der Android Malware-Familien mit den meisten Varianten (H1 2014)

Familie	Varianten
Trojan.Agent	740
Trojan.SMSSend	322
Backdoor.GingerMaster	154
Trojan.SMSForward	78
Trojan.SMSAgent	74

Viele Android-Geräte sind tickende Zeitbomben: Die langen Update-Intervalle vieler Smartphone- und Tablet-Hersteller werden zu einem Sicherheitsproblem und somit zukünftig die effektive Absicherung der Endgeräte erschweren. Ältere Geräte bleiben häufig unversorgt. 69,8 Prozent der Geräte verwenden eine veraltete Android-Version. Lediglich 30,2 Prozent nutzen die Fassung 4.4 („Kitkat“)[8]. Die aktuelle Version 5.0 („Lollipop“) war im Erhebungszeitraum noch nicht verfügbar.



[8] Statistische Erhebung durch Google; November 2014
https://developer.android.com/about/dashboards/index.html

Ransomware: Wachsende Gefahr für Android

Abbildung 1: *Ransomware verschlüsselt Daten und erpresst Lösegeld. Zu sehen ist hier ein Sperrbildschirm für Großbritannien*

Ransomware sind Schadprogramme, mit deren Hilfe ein Eindringling Daten sowie das gesamte Gerät blockieren kann. Dabei werden die Inhalte auf dem Smartphone oder Tablet verschlüsselt oder der Zugriff verhindert. Der Schädling nistet sich tief ins System ein und gaukelt dem Anwender in den meisten Fällen vor, dass das Mobilgerät von staatlichen Behörden gesperrt wurde.

Um die Botschaft so realistisch wie möglich wirken zu lassen, ortet das Schadprogramm via GPS das Herkunftsland des Gerätebesitzers. So sehen beispielsweise betroffene Besitzer in Deutschland eine gefälschte Nachricht des Bundeskriminalamts (BKA) oder des Bundesamts für Sicherheit in der Informationstechnik (BSI). Ist die Ransomware aktiv, erscheint eine Nachricht auf dem Bildschirm des Mobilgeräts.

Dem Besitzer wird häufig vorgeworfen, pornografisches Material angeschaut zu haben. Die Betrüger behaupten, erst mit der Zahlung eines Lösegelds das Gerät wieder freizuschalten und die verschlüsselten Daten freizugeben. Die Zahlung soll über einen nicht verfolgbaren Bezahldienst, wie Paysafecard oder Ukash, erfolgen. Die Kriminellen setzen dabei gezielt darauf, dass die Vorwürfe den Besitzern peinlich sind und sie die Situation umgehend bereinigen möchten.

Wie kommt Ransomware auf das Android-Gerät?

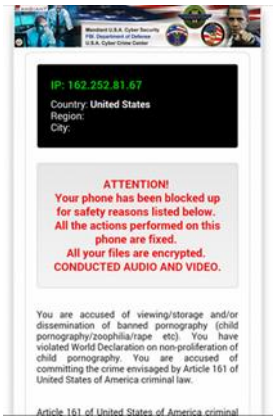


Abbildung 2: *Android-Nutzer in den USA sehen einen Text, der angeblich vom FBI stammt.*

Das Schadprogramm installiert sich nicht selbstständig, der Anwender muss eine APK-Datei selber aufspielen.

Im Play Store prüft Google Apps auf Schadprogramme, daher geht von dieser Quelle nur eine geringe Gefahr aus. Anders sieht es bei App-Stores von Drittanbietern aus.

Häufig werden hier eigentlich kostenpflichtige Apps vermeintlich gratis angeboten. Zusätzlich sind Anwendungen aufgelistet, die es im Playstore nicht gibt. Diese Programme sind oft mit Schadprogrammen wie Ransomware infiziert. Die Entwickler setzen auf die Neugier der potentiellen Opfer.

Drittanbieter App Stores: Potentielle Malware-Gefahr

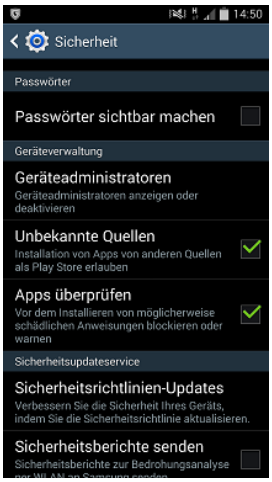


Abbildung 3: *Ist der Haken bei „Unbekannte Quellen" gesetzt, können Apps von Drittanbietern installiert werden.*

Es gibt viele Gründe, warum Anwender zu Dritt-App-Stores greifen. Kostenpflichtige Apps gibt es außerhalb des Google Play Stores deutlich günstiger oder sogar umsonst. Ebenfalls bieten Drittanbieter Apps an, die im Playstore verboten sind.

Dieser Umstand führt dazu, dass viele Android-Nutzer bei Drittanbietern nach günstigen Alternativen Ausschau halten. Um diese Stores verwenden zu können, muss im Mobilgerät die Installation von unbekannten Quellen gestattet sein. Erst dadurch können Nutzer die App des Stores und die angebotenen Programme herunterladen.

Ist die Option aktiviert, wird eine wichtige Schutzfunktion von Android deaktiviert. Auf diesem Weg können sich Schadprogramme den Weg auf das Mobilgerät bahnen. Viele Drittanbieter prüfen nur sehr ungenau oder gar nicht, ob Anwendungen mit Schadcode infiziert sind. Malware-Autoren können Android-Nutzer dadurch in die Falle locken. Anwender, die dennoch einen Drittanbieter Store nutzen möchten, sollten sich vorher über die Vertrauenswürdigkeit erkundigen.

Digitaler Spion ab Werk: Schadcode versteckt sich in Firmware

Die G DATA Sicherheitsexperten haben im Frühjahr 2014 erstmals vorinstallierten Schadcode auf einem Smartphone entdeckt. Das unter dem Namen Star N9500[9] verkaufte Gerät war bereits ab Werk mit einem umfassenden Spionageprogramm ausgestattet. Das Modell erinnert in seinem Aussehen an das Smartphone eines namhaften asiatischen Herstellers. Auch technisch muss sich das Gerät mit seinen Quad-Core-Prozessor nicht hinter teuren Alternativen verstecken. Vergleichbare Geräte kosten fast das Dreifache. Das N9500 war weltweit bei großen Online-Händlern zu Preisen zwischen 130 und 165 Euro erhältlich.

Sensible Nutzerdaten an Server verschickt

Die Malware ist als Google Play Store-Dienst getarnt und Teil der vorinstallierten Firmware. Das Spionageprogramm arbeitet im Hintergrund und ist für den Besitzer des Mobilgeräts auf den ersten Blick nicht zu entdecken. Die Malware versendet heimlich sensible Informationen an einen Server in China. Die Schadsoftware besitzt die Möglichkeit, beliebige Apps auf das Gerät zu installieren. Kriminelle könnten so persönliche Daten abrufen, Gespräche belauschen, Online-Banking-Daten bekommen, SMS und E-Mails lesen oder Kamera und Mikrofon fernsteuern.

[9] https://blog.gdata.de/artikel/android-smartphone-von-werk-aus-mit-spionageprogramm-ausgestattet/

Die Malware hat durch die Integration in die Firmware des Geräts weitreichende Rechte und kann unbemerkt vom Anwender weitere Anwendungen installieren. Eine Deinstallation der manipulierten App und des Spionageprogramms ist wegen der Integration innerhalb der Firmware nicht möglich.

Android.Trojan.Uupay.D

Abbildung 4: *G DATA INTERNET SECURITY FÜR ANDROID erkennt den Schädling als „Android.Trojan.Uupay.D“.*

Der enthaltene Trojaner wurde vom G DATA Mobile-Security-Team als Android.Trojan.Uupay.D identifiziert. Das Programm ist lediglich in den laufen Prozessen des Smartphones sichtbar. Anwender können die App nicht deinstallieren. Protokolle, die einen Zugriff für Besitzer dokumentieren würden, werden durch die Schadsoftware sofort gelöscht. Sicherheits-Software wird durch das Spionageprogramm blockiert und nachträglich deinstalliert. Der Schädling hat auf dem Gerät umfassende Rechte und kann Programme nachladen oder SMS verschicken.

Kurzübersicht der Funktionen von Trojan.Uupay.D.:

Rechte

- Install_/ Delete_Packages
- Read_/Write_/Send_SMS
- Install_Shortcut➔Playstore Icon

Aktionen

- Versendet regelmäßig Informationen an einen Server in China, IMEI,IMSI,SIM Typ, OS Informationen, etc.
- Verändert libsec.so

N9500 ist kein Einzelfall

Die Sicherheitsexperten bei G DATA sind seit Entdeckung des Star N9500 dem Thema weiter nachgegangen und rechnen mit einer deutlich größeren Zahl an Smartphone-Modellen, die ab Werk mit einem Spionageprogramm ausgestattet sind.

Custom-Firmware birgt Sicherheitsrisiken

Viele Smartphone- und Tablet-Hersteller versorgen ihre Geräte ein bis zwei Jahre mit Updates für das Android-Betriebssystem. Sollte nach dieser Zeit eine Sicherheitslücke bekannt werden, stehen die Besitzer der Geräte meist vor Problemen. Eine Lösung ist der Einsatz einer sogenannten Custom-Firmware. Bei dieser Firmware handelt es sich meist von Privatpersonen entwickelte Betriebssysteme, die auf der aktuellen Android-Version beruhen.
Für das Einspielen dieser Software müssen Anwender jedoch zahlreiche Android-Schutzfunktionen deaktivieren und den Entwicklern vollen Zugriff auf das eigene Smartphone geben.

Unkalkulierbares Risiko

Die Gefahr des Missbrauchs ist immens, da es für kriminelle Entwickler ein leichtes ist, Malware als Teil der Firmware zu integrieren. Laut einem Paper von Forschern der Universität Wien, der University of California und der Universität Amsterdam[10] beinhalten Custom-Firmwares häufig Apps, die sich weitgehende Rechte auf dem Android-Mobilgerät erschleichen. Bei 250 überprüften Custom-Firmwares wurde herausgefunden, dass 134 (53,6 Prozent) frei verfügbare Schlüssel des Android Open Source Projekts (AOSP) zum Signieren der Firmware verwenden. Über diesen Weg könnten Angreifer manipulierte Updates auf Geräte mit der entsprechenden Custom-Firmware verbreiten oder durch das Kapern von App-Rechten Zugriff auf das Smartphone oder Tablet erhalten. Ebenfalls problematisch: Custom-Firmware durchläuft keine Qualitätsprüfung, wie diese bei Markenherstellern oder Providern üblich sind.

[10] http://iseclab.org/papers/andrubis_badgers14.pdf