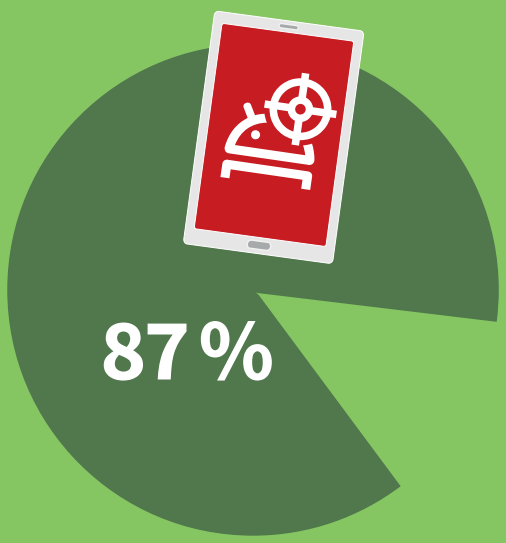
Gefahrenbericht: H1/2016

G DATA SIMPLY SECURE

G DATA
Mobile Malware Report

In Deutschland nutzten weiterhin 67 Prozent der Anwender ein Mobilgerät mit einem Android-Betriebssystem



87 Prozent der Android-Nutzer hatten im Juni 2016 ein veraltetes Betriebssystem auf ihrem Gerät installiert

1.723.265

neue Android Malware-Samples im ersten Halbjahr 2016

SIMPLY SECURE

Inhalte

Whitepaper MMWR DE H1 2016 • 4910080816

Auf einen Blick

- Im ersten Halbjahr 2016 bleibt der Anteil von Smartphones mit Android-Betriebssystem in Deutschland konstant bei 67 Prozent. Weltweit hat sich der Anteil von Mobilgeräten mit Android auf 68 Prozent erhöht (Q4/2015: 66 Prozent).[1]
- **1.723.265 neue Android-Schaddateien** im ersten Halbjahr 2016 bedeuten einen Anstieg von über 29 Prozent zum zweiten Halbjahr 2015 (1.332.839). Mit über 1,7 Millionen neuen Schaddateien ist bereits weit über die Hälfte des Ergebnisses für das Gesamtjahr 2015 (2.333.777) erreicht. Der erwartete Wandel vom klassischen PC hin zum Mobilgerät gewinnt an Geschwindigkeit.
- Mit Android 6.0 ist die Verschlüsselung des Gerätespeichers ab Werk voreingestellt. Bereits mit der Version 5.0 wollte Google die Verschlüsselung als Standard einführen, hat dies jedoch nicht umgesetzt.[2]
- 13 Prozent der Android-Nutzer, die den Play Store genutzt haben, hatten im Juni 2016 das aktuelle Android 6.0 auf ihren Geräten. Die Mehrzahl (30,1 Prozent) hat noch immer Version 4.4 („KitKat“) im Einsatz.[3]
- Drive-by-Infektionen für Android werden zu einer ernsthaften Bedrohung für Anwender. Aktuelle G DATA Analysen zeigen, dass diese Infektionswege/Angriffswege aktuell von Cyberkriminellen ausgenutzt werden.

Prognosen

Neuer Negativrekord - über vier Millionen neue Android-Malware

Fast 2,5 Millionen neue Android Schad-Apps im Jahr 2015 stellten bereits einen Rekord dar. Die G DATA Sicherheitsexperten beobachteten allerdings im ersten Halbjahr 2016 schon eine rasante Zunahme neuer Schadprogramme.

Die Prognose für das Jahr 2016 fällt mit über 4 Millionen neuer Android-Schadprogramme dementsprechend hoch aus.

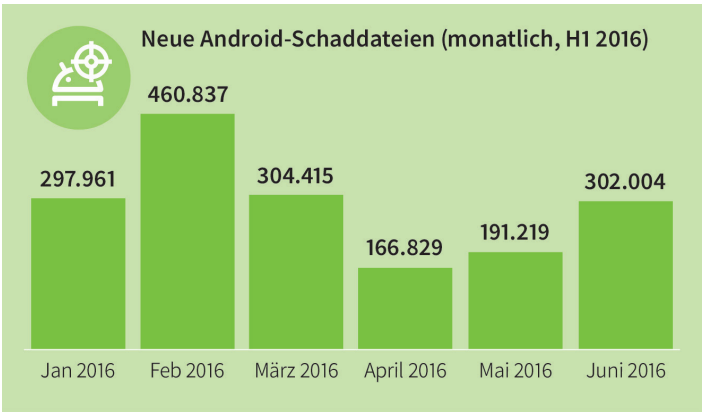
[1] http://gs.statcounter.com/
[2] https://security.googleblog.com/2016/04/android-security-2015-annual-report.html
[3] http://developer.android.com/about/dashboards/index.html; Stand 15. Juli 2016

Whitepaper MMWR DE H1 2016 • 4910080816

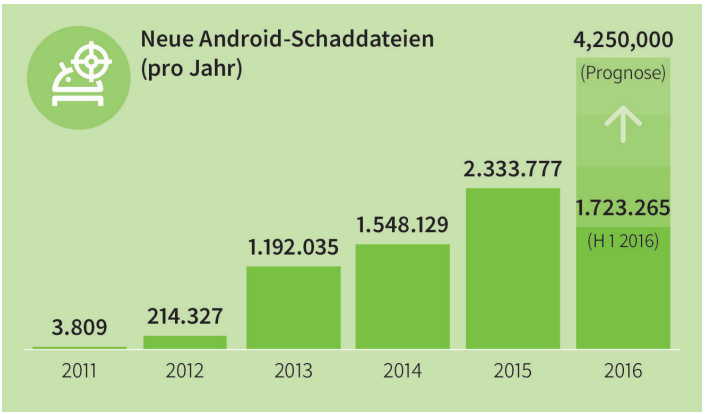
Die aktuelle Lage: Täglich 9.468 neue Android-Schaddateien

1.723.265 neue Android Schad-Apps identifizierten die G DATA Sicherheitsexperten im ersten Halbjahr 2016.

Zum zweiten Halbjahr 2015 (1.332.839) bedeutet dies einen Anstieg von über 29 Prozent an neuen Erkennungen. Pro Tag erkannten die Experten durchschnittlich 9468 neue Schad-Apps für das Android-Betriebssystem. Heißt: **Alle 9 Sekunden** identifizierten die Analysten eine neue Malware.



Seit 2011 haben die G DATA Sicherheitsexperten insgesamt über 7 Millionen Schaddateien für das Android-Betriebssystem gezählt.



Der rasante Schadcode-Anstieg belegt, dass das digitale Leben mobil stattfindet. Online-Banking und -Shopping werden zunehmend mit dem Smartphone oder Tablet erledigt. Das wissen auch Cyberkriminelle. Die Angriffsszenarien werden zunehmend komplexer.

Für eine erfolgreiche Infektion mit Schadprogrammen reicht bereits der Besuch einer manipulierten Webseite.

Warum sind Rooting-Apps für Android problematisch?

Durch den Root (auf Deutsch: Wurzel) eines Android-Geräts erhalten Nutzer umfassende Rechte auf ihrem Mobilgerät und haben vollen Zugriff auf das gesamte Dateisystem und tiefverankerte Systemfunktionen.

Vorteile des Rootens sind, dass Nutzer einige Systemeinstellungen und Veränderungen vornehmen können, wie zum Beispiel vorinstallierte Apps zu deinstallieren.

Es stellt aber deswegen auch eine ernsthafte Bedrohung dar, da so das Sicherheitskonzept von Android außer Kraft gesetzt wird. Um das Gerät zu rooten, wird oft eine Sicherheitslücke im Betriebssystem ausgenutzt.

Ähnlich wie bereits die Stagefright Detection-Tools müssen diese Anwendungen keine bösen Absichten verfolgen. Dennoch unterwandern diese Anwendungen Sicherheitsfunktionen des Betriebssystems.

Sie können aber auch dazu genutzt werden, um einen Zugang auf das Mobilgerät zu erhalten. Hierdurch können die Apps ohne jede Einschränkung auf dem Mobilgerät agieren und zum Beispiel private Daten stehlen, weitere Anwendungen installieren oder Schadprogramme einschleusen. Der Nutzer des Geräts würde davon nichts mitbekommen.

Dem gegenüber stehen positiv zu sehende neue Möglichkeiten wie zum Beispiel das Entfernen von unerwünschten vorinstallierten Apps oder erweiterte Backupmöglichkeiten.

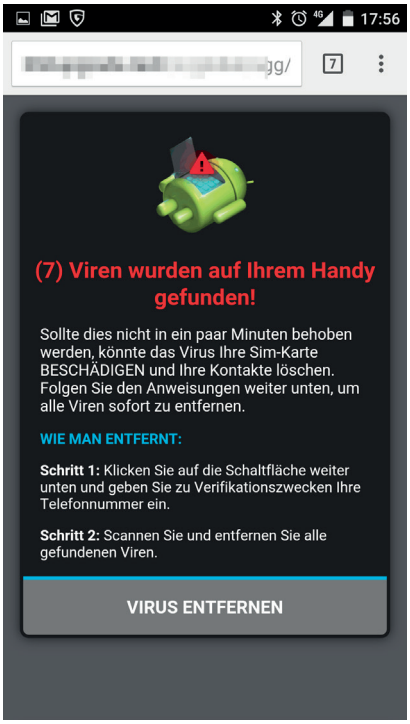
Towelroot ist eine App, die es ermöglicht, Root-Zugriff auf Android-Geräte zu erhalten. Um dies zu erreichen, nutzt die Anwendung einen Fehler im Linux-Kernel aus. Diese App kann aber auch manipuliert werden und so Schadsoftware auf das Mobilgerät einschleusen oder unerwünschte Dienste einrichten. Anwender, die so eine App trotzdem nutzen wollen, sollten diese aus einer vertrauenswürdigen Quelle herunterladen und sich der Sicherheitsprobleme bewusst sein.

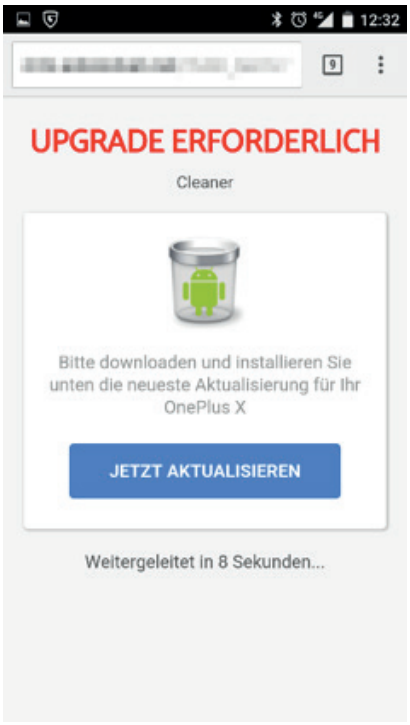
Da aber das Sicherheitskonzept von Android umgangen werden kann, stufen die G DATA Sicherheitsexperten diese Apps als problematisch ein und melden diese.

Malvertisement: Werbung gaukelt Virenfund vor

Surfen mit dem Smartphone oder Tablet kann plötzlich dazu führen, dass eine fingierte Warnung erscheint, das Mobilgerät wäre mit einem vermeintlichen Virus infiziert oder ein Update sei verfügbar. Dazu müssen Nutzer keine zwielichtigen Seiten ansteuern.

Solche Meldungen sollten niemals angeklickt, sondern mit der Zurück-Taste geschlossen werden. Es handelt sich hierbei um einen Betrugsversuch. Ein Virus ist **nicht** auf dem Mobilgerät und es ist auch **kein** Update erforderlich.





Die drei Screenshots zeigen Beispiele für fingierte Warnungen über Virenfunde oder erforderliche Updates. Anwender sollten auf keinen Fall die Buttons drücken.

Auch ein Update des Betriebssystems kündigt sich **nicht** über den Browser an.

Sollte diese Werbung angeklickt werden, wird in vielen Fällen eine .apk-Datei heruntergeladen und dadurch gelangt kostenpflichtige Software für Batterie- oder Speicherplatzoptimierung auf das Gerät, ein teures Abo wird abgeschlossen oder schädliche Apps werden installiert.

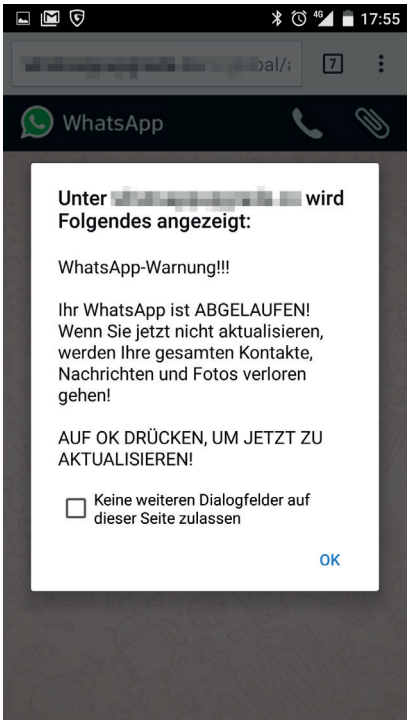
Was ist Pay-per-Install?

Pay-per-Install ist ein gängiges Marketing-Instrument, das es Herstellern einer App ermöglicht, ihre Software zu verbreiten und höhere Download-Zahlen zu erreichen. Anwender werden häufig durch Werbeschaltungen auf die App aufmerksam gemacht. Je mehr Installationen eine App vorweisen kann, desto sichtbarer wird diese in einem App-Store und zieht weitere Nutzer an, die diese App auf ihr Gerät installieren. Es gibt verschiedene Dienstleister, die sich auf diese Marketing-Methode spezialisiert haben. Dieser Weg ist absolut legitim.

Es gibt aber auch in der IT-Sicherheit den Begriff Pay-per-Install, der die betrügerische Form dieser Methode als Malvertisement bezeichnet (zusammengesetztes Wort aus Malware und Advertisement) und beschreibt eine Online-Werbung, die Schadcode ausspielt.

Cyberkriminelle bieten in Untergrund-Foren ihre Dienstleistungen an. Hier wird ebenfalls in vielen Fällen mit Werbung gearbeitet und die Betrüger nach der Menge der Installationen bezahlt. Diese Werbung ist aber irreführend und hat das Ziel, den Nutzer zu verwirren.

Mit vorgegaukelten Virenfunden oder angeblich verfügbaren Updates für Android soll der Anwender zu Handlungen gezwungen werden, die zur Installation kostenpflichtiger oder schädlicher Apps beziehungsweise teuren Abos führen. Die Mobilgeräte können schlimmstenfalls nach der Installation für kriminelle Aktivitäten genutzt werden.



Eine andere Masche ist die Anzeige, dass WhatsApp abgelaufen sei. Auch hier wird mit Konsequenzen gedroht, falls der Anwender nicht sofort reagiert.

Drive-by-Infektion: Angriffsvektor bedroht auch Android-Geräte

Die G DATA Sicherheitsexperten haben bereits 2015 prognostiziert, dass sich Schadprogramme für das Android-Betriebssystem weiterentwickeln. Insbesondere die Enthüllungen über das italienische IT-Unternehmen Hacking Team haben Möglichkeiten aufgezeigt, wie Mobilgeräte allein durch den Besuch von präparierten Webseiten mit Schadcode infiziert werden können. Dadurch ist keine Interaktion des Anwenders mehr notwendig. Gelangt die Schadsoftware auf das Gerät, findet die Infektion automatisch statt.

Aktuelle Analysen der G DATA Experten zeigen, dass Drive-by-Infektionen nun auch von Angreifern genutzt werden, um Android Smartphones und Tablets zu infizieren. Sicherheitslücken im Android-Betriebssystem sind dadurch eine noch ernstere Bedrohung. Insbesondere die langen Zeitspannen, bis ein Update für Android auf die Nutzergeräte gelangt, können diese Problematik noch verschärfen.

Wie funktionieren Drive-by-Infektionen?
Online-Kriminelle hacken Web-Server und stellen dort präparierte Seiten ein. Anschließend versenden sie Spam-Mails mit Links zu diesen Seiten und optimieren sie für Suchmaschinen. Wenn Anwender auf diese Webseiten gehen oder per Werbung dorthin geleitet werden, kann schnell und unbemerkt Schadsoftware auf das System gelangen. Die Infektion findet statt, ohne dass das Opfer etwas bemerkt – allein durch den Besuch der Seite.

Derzeit werden diese Angriffswege genutzt, um Anwender mit Erpresser-Trojanern, sogenannter **Ransomware**, zu infizieren. Wie der Name schon sagt, handelt es sich um eine Form von Schadsoftware, die Lösegeld vom Opfer fordert, um die Daten bzw. das Gerät wieder frei zu geben.

Es gibt zwei gängige Arten von Ransomware: Screen-Locker und Crypto-Ransomware. Screen-Locker sperren das Display und der Nutzer hat keinen Zugang mehr auf das Mobilgerät. Crypto-Ransomware verschlüsselt die Daten auf dem Smartphone oder Tablet.

G DATA SIMPLY SECURE

Ransomware: Erpressung im digitalen Zeitalter

Tipps zum Schutz gegen Ransomware:

- Eine **umfassende Sicherheitslösung**, die vor Viren und anderen Bedrohungen schützt.
- Es sollten **regelmäßige Backups** von wichtigen Dokumenten und Daten gemacht werden.
- Installierte Apps und das Betriebssystem sollten stets **auf dem neuesten Stand** sein.
- Apps sollten nur aus den **offiziellen Stores** der Hersteller, wie Google Play, heruntergeladen werden.
- E-Mails unbekannter Absender gehören generell **ungelesen gelöscht**. Dateianhänge sollten ebenso wie Links **nicht aufgerufen werden**.
- Ein Lösegeld sollte **niemals** gezahlt werden. Es signalisiert den Erpressern die Zahlungswilligkeit und motiviert diese, es ein zweites Mal zu versuchen.

Über G DATA

Die G DATA Software AG ist der Antivirus-Pionier. 1985 gegründet, entwickelte das Bochumer Unternehmen bereits vor über 30 Jahren die erste Software gegen Computerviren.

Heute gehört G DATA zu den führenden Anbietern von Internetsicherheitslösungen und Virenschutz mit weltweit mehr als 400 Mitarbeitern.

Kontakt: www.gdata.de / presse@gdata.de / Tel. 0234 97 62 - 0

Whitepaper MMWR DE H1 2016 • 4910080816