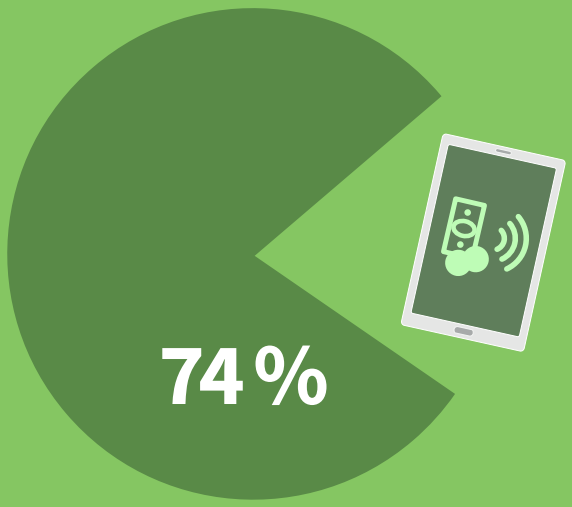
Gefahrenbericht: Q4/2015

G DATA
SIMPLY
SECURE

G DATA Mobile Malware Report

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



74 Prozent der Bankgeschäfte werden mit Smartphones abgewickelt

758.133

neue Malware-Samples im vierten Quartal 2015/2,3 Millionen im Gesamtjahr 2015

SIMPLY SECURE

Inhalte

Whitepaper MMWR DE Q4 01-2016 • 13091002l6

Auf einen Blick

- 67 Prozent der Smartphones in Deutschland hatten im vierten Quartal 2015 das Android-Betriebssystem installiert. Der Anteil hat sich zum dritten Quartal mit 68 Prozent nicht stark verändert. Weltweit hatten 66 Prozent der Anwender im vierten Quartal 2015 (Q3: 67 Prozent) ein Mobilgerät mit Android-Betriebssystem im Einsatz. Im Vergleich zum dritten Quartal 2015 ist der Marktanteil von Android-Betriebssystemen konstant geblieben.[1]
- 758.133 neue Android-Schaddateien haben die G DATA Sicherheitsexperten im vierten Quartal 2015 entdeckt. Zum dritten Quartal 2015 (574.706) beträgt der Anstieg damit fast 32 Prozent. Im zweiten Halbjahr 2015 wurden somit insgesamt 1.332.839 neue Schad-Apps gezählt. Für das Gesamtjahr 2015 ergibt das einen neuen Rekord von 2.333.777 Schaddateien allein für das Android-Betriebssystem. Zum Jahr 2014 (1.548.129) beträgt die Steigerung über 50 Prozent.
- Android sollte immer auf dem neuesten Stand sein: Sicherheitslücken für Android werden immer schneller bekannt und von Kriminellen ausgenutzt. Die Enthüllungen rund um das italienische Hacking-Team hat auch die Verwundbarkeit von Android unterstrichen.[2] Das Update auf die aktuelle Android-Version ist daher für alle Anwender elementar. Die G DATA Sicherheitsexperten empfehlen, beim Kauf eines neuen Mobilgerätes darauf zu achten, dass die aktuellste Android-Version installiert oder ein Update möglich ist. Insbesondere vermeintliche Schnäppchen entpuppen sich oft als Geräte mit veralteten Android-Versionen, für die auch keine Updates mehr vorliegen.
- Mobile Banking-Trojaner sind komplexer: Immer mehr Menschen tätigen ihre Bankgeschäfte mobil. Cyberkriminelle rüsten nach und verbreiten immer ausgeklügeltere Malware, um gezielt Bankkunden ins Visier zu nehmen.

Prognosen

Evolution der Android-Malware

Nahezu 2,5 Millionen neue Android Schad-Apps analysierten die G DATA Sicherheitsexperten im Gesamtjahr 2015. Diese rasante Steigerung unterstreicht den Bedeutungsgewinn mobiler Betriebssysteme – insbesondere von Android. Cyberkriminelle sehen hier die Zukunft und die Möglichkeit auf hohe finanzielle Gewinne. In 2016 wird sich dieser Wandel vom PC zum Mobilgerät weiter entwickeln. Die Experten rechnen daher erneut mit deutlich steigenden Schadcode-Zahlen.

Das Internet der Dinge im Cybercrime-Visier

Gehackte Autos, Fitness-Armbänder oder Netzwerke: Das Internet der Dinge wird immer beliebter, sowohl in den eigenen vier Wänden als auch im Unternehmen. Kriminelle verstärken hier ihre Aktivitäten und suchen gezielt nach Sicherheitslücken, um diese auszunutzen. Zahlreiche Endgeräte im IoT-Bereich werden über Android-Apps gesteuert. 2016 erwarten die Experten eine steigende Bedrohung.

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

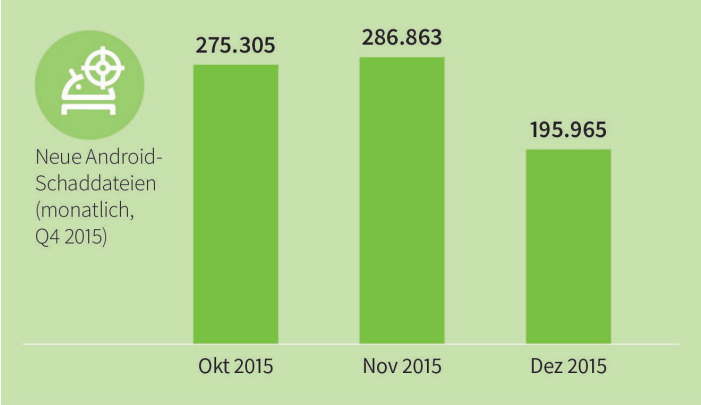
[2] http://www.heise.de/security/meldung/Super-Spion-Android-Ueberwachungssoftware-von-Hacking-Team-nutzt-allerhand-schmutzige-Tricks-2759365.html

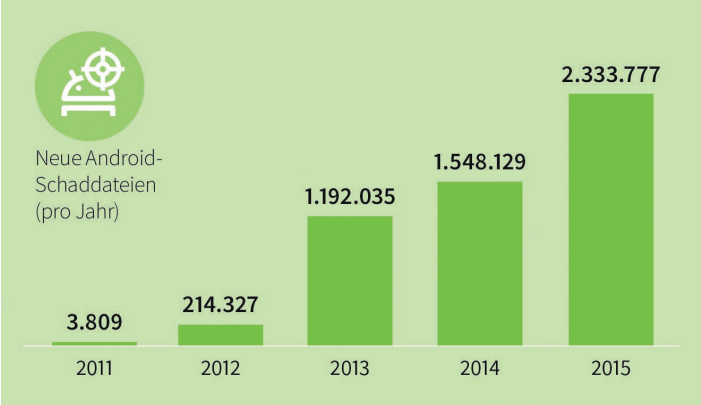
Whitepaper MMWR DE Q4 01-2016 • 1309100216

Die aktuelle Lage:
Alle 11 Sekunden ein neuer Android-Schädling

Die Anzahl neuer Android-Malware ist im vierten Quartal 2015 wieder deutlich gestiegen. In diesem Zeitraum zählten die G DATA Analysten 758.133 neue Android-Schaddateien. Zum dritten Quartal (574.706) bedeutet das einen Anstieg um rund 32 Prozent. Pro Tag entdeckten die Experten im vierten Quartal durchschnittlich über 8.240 neue Android-Schad-Apps - über 1.800 mehr als noch im Quartal zuvor.

Für das Gesamtjahr 2015 ergibt sich ein neuer Rekord von 2.333.777 neuen Schaddateien allein für das Android-Betriebssystem. Das ist eine Steigerung von über 50 Prozent zu 2014 (Gesamtzahl 1.548.129).





Was sind Stagefright-Detection-Tools?

In den letzten Mobile Malware Reports haben die G DATA Sicherheitsexperten verschiedene Kategorien von potentiell unerwünschten Programmen (PUP) erläutert. Auch in diesem Report geht es wieder um einen Bereich. Diesmal sind es Detection-Apps.

Die Sicherheitslücke Stagefright[3] sorgte im Juli 2015 für Aufruhr und stellte für Android-Nutzer den Super-GAU dar. Weltweit sollen bis zu einer Milliarde Geräte von dieser Schwachstelle betroffen gewesen sein.

Durch das Ausführen von Schadcode (Remote Code Execution) sollte die totale Übernahme des Gerätes mit dem bloßen Anzeigen einer Multimedia Messaging Service (MMS) möglich sein. Die Lücke zwingt Smartphone-Hersteller, ihre Strategie für Sicherheitsaktualisierungen bei ihren Geräten zu verändern, um Anwender zügiger Updates zur Verfügung zu stellen.

Im Zuge dieser Problematik mit Stagefright erschienen zahlreiche Apps, die das Mobilgerät auf die Sicherheitslücke überprüfen. Diese Apps nutzen in vielen Fällen ebenfalls eine Sicherheitslücke in Android aus, um so das Betriebssystem auf eine Anfälligkeit auf Stagefright zu testen.

[3] https://blog.gdata.de/artikel/sicherheitsluecke-in-android-medien-engine-stagefright/u

Whitepaper MMWR DE Q4 01-2016 • 1309100216

Android-Apps, die mit der Erkennung „Android.Application.StageFrightDetector.A“ gemeldet werden, sind Anwendungen, um zu überprüfen, ob ein Android-Gerät über die Sicherheitslücke angreifbar ist.

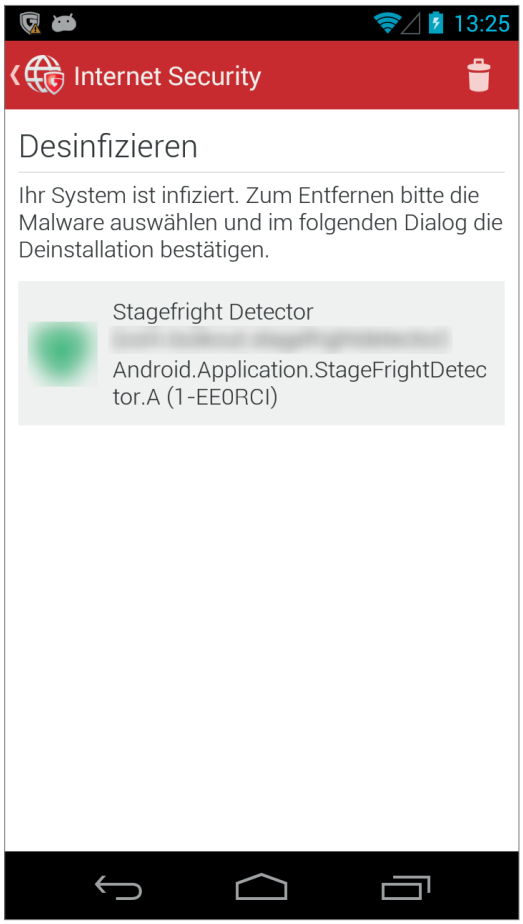
G DATA Sicherheitslösungen erkennen und deklarieren aus diesem Grund die Stagefright-Detector-Apps als schädliche Anwendungen.

Was ist Stagefright?

Die Stagefright-Engine wird zur Aufnahme und Wiedergabe von Audio- und Videodateien benutzt. Im Android-Betriebssystem gibt es in einer Bibliothek zur Anzeige von Medieninhalten mehrere Sicherheitslücken. Über diese Schwachstellen können Angreifer Audio- und Videodateien nutzen, um Schadcode auf dem betroffenen Gerät auszuführen. Dieser Vorgang kann automatisch im Hintergrund geschehen, ohne das Wissen des Nutzers.

Der Markt an Android-Geräten ist unüberschaubar groß. Es gibt viele verschiedene Softwareversionen. Der einzig mögliche Weg für eine Detektor-App ist bisher, das jeweilige Gerät aktiv auf die Sicherheitslücke zu testen. Hierfür muss der Angriff allerdings durchgeführt werden. Dazu beinhalten die Stagefright-Erkennungs-Apps die jeweiligen Sicherheitslücken. Die Stagefright-Lücke umfasst nicht nur eine Angriffsmöglichkeit, sondern gleich mehrere.

Es ist allerdings nicht bekannt, dass diese Apps Schadcode ausführen oder nachladen. Dennoch nutzen diese Apps Sicherheitslücken im Mobilgerät aus.



Über G DATA

Die G DATA Software AG ist der Antivirus-Pionier. 1985 gegründet, entwickelte das Bochumer Unternehmen bereits vor 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.

G DATA SIMPLY SECURE

Whitepaper MMWR DE Q4 01-2016 • 1309100216