TRUST IN
GERMAN
SICHERHEIT

MOBILE MALWARE REPORT

GEFAHRENBERICHT: H2/2014

INHALTE

Whitepaper MMWR DE 03-2015 • 3913240315

TRUST IN GERMAN SICHERHEIT

AUF EINEN BLICK

MARKTANTEILE VON ANDROID-SMARTPHONES UND -TABLETS

- 1,301 Milliarden Smartphones wurden 2014 laut Marktanalysten weltweit verkauft – allein über 702 Millionen im zweiten Halbjahr.[1] Der Marktanteil von Android im Smartphone-Markt lag in diesem Zeitraum bei durchschnittlich 81 Prozent.[2] Rechnerisch hatten 569 Millionen der verkauften Smartphones ein Android-Betriebssystem installiert, hinzukommen insgesamt 91,6 Millionen verkaufte Android-Tablets.[3]

ANDROID SCHADCODE-ZAHLEN

- Absolute Schadcode-Zahlen für Android-Geräte: 796.993 neue Malware-Samples haben die G DATA Sicherheitsexperten im zweiten Halbjahr 2014 identifiziert und analysiert. Zum ersten Halbjahr bedeutet das einen Anstieg von 6,1 Prozent (751.136). Insgesamt wurden 2014 von den G DATA Experten über 1,5 Millionen neue Android-Schadprogramme untersucht. Im Vergleich zum Gesamtjahr 2013 bedeutet das einen Anstieg von fast 30 Prozent an neuen Android-Schaddateien.

DRITTMÄRKTE FÜR ANDROID-APPS

- Im Vergleich schneiden europäische und amerikanische Anbieter besser ab als Märkte in China oder Russland. Einige App-Märkte in China sind zu einem Viertel mit Malware und PUP (potentiell unerwünschte Programme) infiziert.

VORINSTALLIERTE SPIONAGEPROGRAMME

- Wieder haben die G DATA Sicherheitsexperten ein Smartphone eines namhaften Herstellers mit einem fest installierten digitalen Spion entdeckt. Der Schädling versteckte sich in einer gefälschten App und verschickt Daten an Dritte.

[1] http://www.idc.com/getdoc.jsp?containerId=prUS25407215
[2] http://blogs.strategyanalytics.com/WSS/post/2015/01/29/Android-Shipped-1-Billion-Smartphones-Worldwide-in-2014.aspx
[3] http://www.strategyanalytics.com/default.aspx?mod=pressreleaseviewer&a0=5617 , http://www.strategyanalytics.com/default.aspx?mod=pressreleaseviewer&a0=5640

Whitepaper MMWR DE 03-2015 • 3913240315

PROGNOSEN UND TRENDS

ABSOLUTE ANZAHL VON NEUEN SCHADDATEIEN EXPLODIERT

- Für 2015 erwarten die G DATA Sicherheitsexperten eine rasant steigende Anzahl an neuen Schaddateien. Eine Zahl von über 2 Millionen neuer Android-Schädlinge ist realistisch. Immer häufiger setzen Anwender bei der alltäglichen Internet-Nutzung für Banking oder Shopping auf die beliebten Android-Geräte. Cyberkriminelle werden hier verstärkt versuchen Malware in den Umlauf zu bringen.

WERBEN, SPIONIEREN, MANIPULIEREN: ADWARE WIRD RAFFINIERTER

- Adware ist für viele Anwender nervig. Diese Kategorie wird immer raffinierter. Aktuelle Fälle auf dem Computer deuten darauf hin, dass SSL-Verschlüsselungen durch Adware ausgehebelt werden. Cyberkriminelle können dies ausnutzen und sensible Daten, wie fürs Online-Banking oder in sozialen Netzwerken, ausspähen. Die Sicherheitsexperten erwarten, dass sich dieser Trend auch auf Mobilgeräten verbreitet.

ANWENDER SETZEN VERSTÄRKT AUF VERSCHLÜSSELUNG

- Das Bewusstsein für Sicherheit und Privatsphäre ist nach den Enthüllungen über Spionage und Cyberkriminalität gewachsen. Verschlüsselung wird immer mehr zum Standard. Anwender können mit einfachen Mitteln ihre Daten insbesondere auf Android-Geräten absichern und verschlüsseln. Android bietet bereits in den Einstellungen eine Funktion an, um alle Daten auf dem internen und externen Speicher vor Zugriffen zu sichern.

CROSS-PLATTFORM-MALWARE: DER SCHLÜSSEL ZUM UNTERNEHMENSNETZWERK

- Cross-Plattform-Malware, also Schadprogramme die sowohl auf PCs als auch auf Mobilgeräten einsetzbar sind, werden häufiger von Cyberkriminellen eingesetzt, um Zugang zu Firmennetzwerken zu erhalten. Cross-Plattform-Infektionen werden nach Einschätzung von G DATA deutlich zunehmen.

„QUANTIFIED SELF"-DATEN SIND BEI KRIMINELLEN BEGEHRT

- Fitness-Apps und -Zubehör für das Smartphone sind im Trend. Personenbezogene Daten („Quantified Self") werden immer häufiger aufgezeichnet und analysiert. Die G DATA Sicherheitsexperten befürchten, dass der Datendiebstahl in diesem Bereich zunehmen wird.

SPEZIELLE SCHADSOFTWARE SIEHT ES AUF BANKDATEN AB

- Das Jahr 2015 steht im Zeichen von spezieller Malware, die Bank- und Finanzdaten im Visier hat. Bereits 2014 nutzten rund ein Drittel aller Bankkunden ihr Mobilgerät für Online-Bankgeschäfte – Tendenz steigend.[4] Cyberkriminelle setzten auf gefälschte oder manipulierte Banking-Apps, die genau hier ansetzen.

[4] http://de.statista.com/statistik/daten/studie/308412/umfrage/geraetenutzung-beim-online-banking/

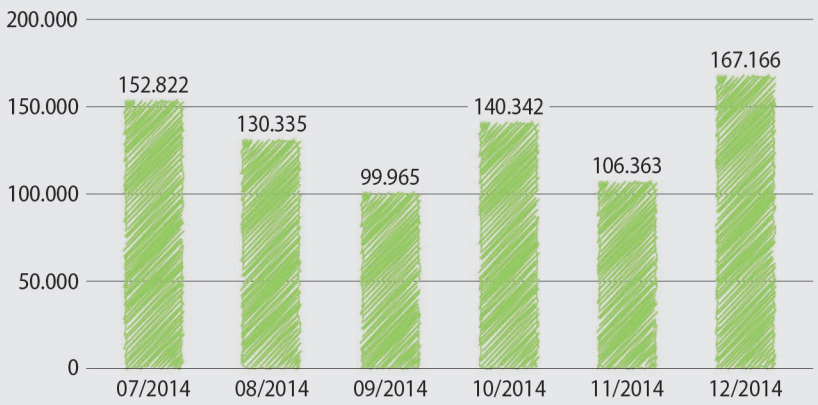
Whitepaper MMWR DE 03-2015 • 3913240315

TRUST IN GERMAN SICHERHEIT

AKTUELLE LAGE: TÄGLICH 4.500 NEUE ANDROID-SCHADDATEIEN

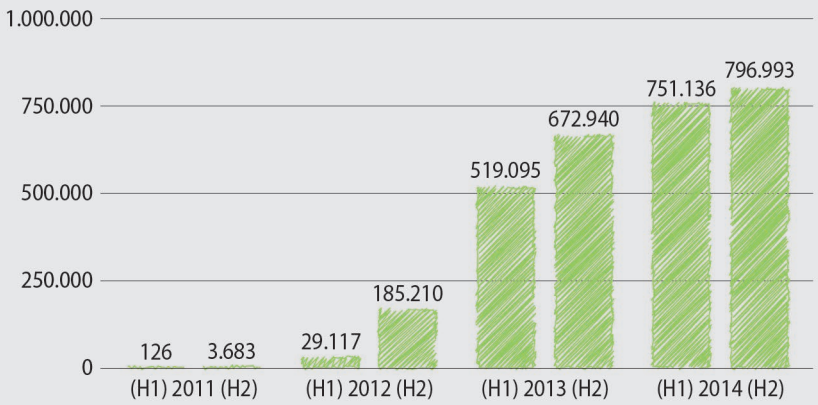
In der zweiten Jahreshälfte 2014 registrierten die G DATA Sicherheitsexperten 796.993 neue Schadprogrammtypen. Durchschnittlich entdecken die Experten im zweiten Halbjahr pro Tag fast 4.500 neue Android-Schaddateien. Zum ersten Halbjahr bedeutet das einen Anstieg von 6,1 Prozent (751.136). Die Anzahl neuer Schadprogrammtypen ist sogar um 18 Prozent im Vergleich zum zweiten Halbjahr 2013 (672.940) gestiegen. Im Gesamtjahr 2014 identifizierten die Sicherheitsexperten 1.584.129 neue Android Malware Samples. Im Vergleich zu 2013 (1.192.035) bedeutet das einen Anstieg neuer mobiler Schaddateien von fast 33 Prozent.

NEUE ANDROID SCHADDATEIEN 2014 / MONATLICH (H2)



Quelle: G DATA Software AG

ANDROID SCHADDATEIEN / HALBJÄHRLICH



Quelle: G DATA Software AG

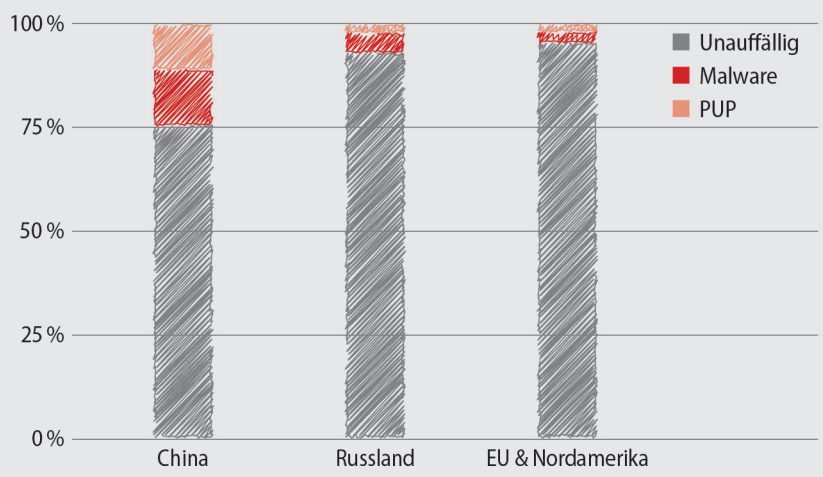
DRITTANBIETER APP-STORES

Im zweiten Quartal 2014 hatte das Betriebssystem Android auf Smartphones einen weltweiten Marktanteil von nahezu 85 Prozent.[5] Malware-Programmierer wollen sich diesen Trend zu Nutze machen und entwickeln gezielt Schadprogramme für das Google-Betriebssystem. Die Aussicht auf hohen finanziellen Profit mit vergleichsweise wenig Aufwand ist hier am höchsten.

Anders als iOS oder Windows Phone ist Android ein quelloffenes Betriebssystem. Durch diese Freiheiten sind auch zahlreiche App-Stores von Drittanbietern neben dem Google Play Store entstanden. Google überprüft alle im eigenen Store eingestellten Apps automatisch auf verdächtige Inhalte.

In den alternativen App-Stores findet eine solche Analyse häufig nicht statt. Viele Drittanbieter prüfen nur sehr ungenau oder gar nicht, ob Anwendungen mit Schadcode infiziert sind. Um einen alternativen App Marktplatz nutzen zu können, müssen Anwender in den Einstellungen des Android-Geräts die Installation von Anwendungen aus anderen Quellen als den Play Store erlauben. Dadurch ist die zentrale Schutzfunktion von Android deaktiviert und Schadprogramme können sich einen Weg auf das Mobilgerät bahnen. Malware-Autoren können Android-Nutzer dadurch in die Falle locken. Häufig sollen günstige Angebote von eigentlich teuren Apps oder vermeintlich wichtige System-Updates Smartphone-Besitzer dazu verführen, die Schutzfunktion auf ihrem Gerät zu deaktivieren. Anwender, die dennoch einen Drittanbieter Store nutzen möchten, sollten sich vorher über die Vertrauenswürdigkeit erkundigen.

ANDROID-MALWARE IN ALTERNATIVEN APP STORES



Quelle: G DATA Software AG

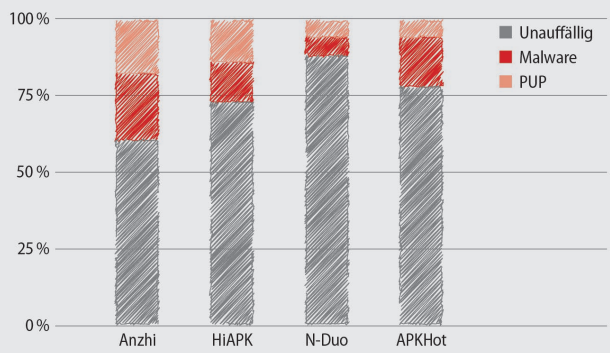
[5] http://www.idc.com/getdoc.jsp?containerId=prUS25037214

TRUST IN GERMAN SICHERHEIT

EINIGE CHINESISCHE APP-MÄRKTE WEISEN SCHADPROGRAMME AUF

In amerikanischen und europäischen App-Stores haben die G DATA Sicherheitsexperten lediglich bei 3,4 Prozent der angebotenen Anwendungen Malware oder potentiell unerwünschte Programme (PUP), wie Adware oder Riskware, gefunden. In chinesischen Marktplätzen sind in manchem App-Store über 25 Prozent der Anwendungen infiziert – davon allein 13 Prozent mit Malware.

ANDROID-MALWARE IN CHINESISCHEN APP STORES

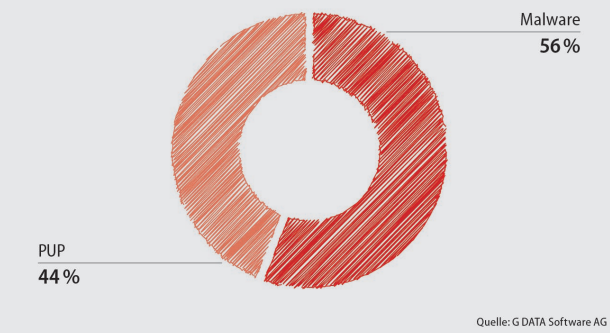


Quelle: G DATA Software AG

WELCHE SCHÄDLINGE DOMINIEREN APP MÄRKTE?

Über die Hälfte (56 Prozent) der identifizierten Schadprogramme sind Trojaner oder andere Malware. Malware steht hier als ein Obergriff für verschiedene Arten von Schadprogrammen. Dies können Exploits, Trojaner oder Backdoors sein.

WELCHE SCHADPROGRAMME SIND HÄUFIG VERTRETEN?



Quelle: G DATA Software AG

44 Prozent der anderen Schadprogramme fallen in die Kategorie PUP. Zur Kategorie PUP gehört beispielsweise Adware oder Riskware. Mit Adware sind Programme gemeint, die Werbeinhalte haben und diese mit unlauteren Methoden dem Anwender präsentieren. Diese Apps müssen nicht schädlich sein, dennoch sind sie störend für den Anwender. Riskware hingegen ist potentiell gefährliche Software. Die Installation dieser Apps kann zu Schäden am Gerät führen. Apps dieser Kategorie können ebenfalls legitime Anwendungen sein, die aber Schwachstellen aufweisen oder kompromittiert wurden.

SICHERHEIT IN APP-STORES MUSS MEHR IN DEN FOKUS

Derzeit werden wenige App-Märkte von Drittanbietern durch Antivirenscanner überprüft. Die vorliegenden Statistiken beruhen auf bekannten Schädlingen. Die Sicherheitsexperten gehen davon aus, dass die Dunkelziffer höher liegt. Um auch die Sicherheit in diesen Märkten sicherzustellen, müssen diese kontinuierlich überwacht und analysiert werden.

Whitepaper MMWR DE 03-2015 • 3913240315

WIEDER SMARTPHONE MIT SCHADPROGRAMM IN DER FIRMWARE

Im Frühjahr 2014 haben die G DATA Sicherheitsexperten erstmals vorinstallierten Schadcode auf einem Smartphone entdeckt. Das unter dem Namen Star N9500[6] verkaufte Gerät war bereits ab Werk mit einem umfassenden Spionageprogramm ausgestattet. Nun sind die Experten wieder auf ein Gerät gestoßen, dessen Firmware mit Schadcode infiziert ist. Das Xiaomi Mi4 hatte in einigen nicht-authorisierten Versionen einen Trojaner vorinstalliert. Betroffen waren Geräte, die mit deutschen Menüs ausgeliefert und in bestimmten Onlineshops gekauft wurden. Daher vermuten die G DATA Sicherheitsexperten einen Zwischenhändler hinter dieser Masche, der die manipulierte Firmware auf die Geräte installiert. Diese Masche ist besser bekannt als grauer Markt.

SCHADCODE VERSTECKT SICH IN MANIPULIERTER TWITTER-APP

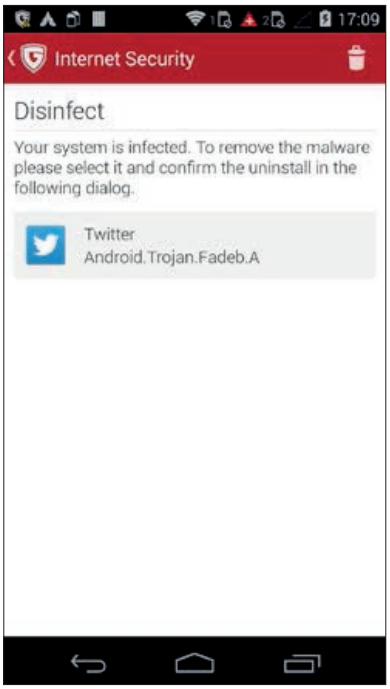
Der Schädling verbarg sich in einer manipulierten Twitter-App. Im Gegensatz zur originalen App, nimmt die Fälschung mehr Rechte in Anspruch. Neben dem Zugriff auf die Anrufliste, will die App laufende Programme verfolgen und selbständig Anwendungen installieren und entfernen. Kriminelle könnten so im Hintergrund persönliche Daten abrufen, Gespräche belauschen, SMS und E-Mails lesen oder Kamera und Mikrofon fernsteuern. Ebenso kann der Schädling unbemerkt weitere Apps nachinstallieren. Darüber hinaus verschickt das Schadprogramm Informationen über das Smartphone, das genutzte Betriebssystem, Sprachversion und Standortdaten an anonyme Server. Die Möglichkeiten sind für Angreifer somit unbegrenzt.

SENSIBLE NUTZERDATEN AN ANONYME SERVER VERSCHICKT

Die Sicherheitsexperten konnten in Ihrer Analyse feststellen, dass die Daten nach Asien geschickt wurden. Die Malware hat durch die Integration in die Firmware des Geräts weitreichende Rechte und kann unbemerkt vom Anwender weitere Anwendungen installieren. Unliebsame Apps deinstalliert der Trojaner bei Bedarf. Eine Deinstallation der manipulierten App und des Spionageprogramms ist wegen der Integration innerhalb der Firmware nicht möglich.

VORHERSAGE HAT SICH BEWAHRHEITET

Bereits im Zuge der Entdeckungen des Star N9500 haben die G DATA Sicherheitsexperten vermutet, dass das Smartphone mit vorinstalliertem Spionageprogramm kein Einzelfall bleiben wird. Das Gerät von Xiaomi bestärkt diese Annahme. Der Fall ist aber noch nicht abgeschlossen. Die Analysten untersuchen noch andere Geräte, die mit einer ähnlichen Firmware ausgeliefert wurden.



G DATA INTERNET SECURITY FÜR ANDROID erkennt die manipulierte Twitter-App.

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

Whitepaper MMWR DE 03-2015 • 3913240315