SIMPLY SECURE

G DATA MOBILE MALWARE REPORT

GEFAHRENBERICHT: Q3/2015

Whitepaper MMWR DE Q3 12-2015 #531115 - 1214151215

INHALTE

Whitepaper MMWR DE Q3 12-2015 #53115 • 1214151215

AUF EINEN BLICK

- Der weltweite Marktanteil von Mobilgeräten mit Android als Betriebssystem lag im dritten Quartal 2015 bei fast 67 Prozent. Zum zweiten Quartal bedeutet das einen Anstieg um gut drei Prozent. In Deutschland nutzten rund 68 Prozent der Anwender ein Android-Mobilgerät. Hier ist der Anteil gleich geblieben.[1]
- Schadcode-Zahlen für Android-Geräte im dritten Quartal 2015 bleiben auf hohem Niveau: 574.706 neue Malware-Samples haben die G DATA Sicherheitsexperten identifiziert – das ist ein leichter Anstieg im Vergleich zum zweiten Quartal (560.671). Im Vergleich zum Vorjahreszeitraum (Q3/2014: 383.122) stieg die Anzahl neuer Schadprogramme um 50 Prozent.
- Blick auf das Gesamtjahr 2015: Bis zum dritten Quartal haben die G DATA Sicherheitsexperten bereits rund 1,6 Millionen neuer Android-Malware-Samples analysiert.
- Über 80 Prozent der Android-Geräte haben ein veraltetes Betriebssystem im Einsatz. Lediglich 20 Prozent der Smartphones oder Tablets arbeiten mit einer aktuellen Android-Version. Häufig dauert das Ausrollen der Sicherheitsupdates durch die Hersteller lange. Bekannte Sicherheitslücken können so nicht zeitnah geschlossen werden.

PROGNOSEN UND TRENDS

ANDROID ALS EINFALLSTOR IN DAS INTERNET DER DINGE

Menschen und Unternehmen setzen verstärkt auf das Internet der Dinge. Von Fitness-Apps über Autos sind immer mehr Geräte miteinander vernetzt und können mit einem Smartphone oder Tablet gesteuert werden. Diese Applikationen und das Android-Betriebssystem sind für Cyberkriminelle immer beliebter, weil sie ein Angriffsweg sein können.[2] Ein bekanntes Beispiel hierfür ist der Angriff auf eine Heizungssteuerung über eine Smartphone-App.[3]

SMARTPHONES MIT VORINSTALLIERTER MALWARE

Nach den neuen Ergebnissen im Mobile Malware Report zum zweiten Quartal 2015 bleiben die G DATA Experten weiter am Thema. Immer mehr Smartphones sind von einer manipulierten Firmware betroffen. Hier werden in den nächsten Monaten neue Ergebnisse vorliegen.

KOMPLEXE MALWARE FÜR ANGRIFFE AUF ONLINE-BANKING

Die G DATA Sicherheitsexperten rechnen mit einem Anstieg an komplexeren Schadprogrammen, die Windows und Android-Angriffskampagnen auf Online-Banking-Kunden verbinden. Zahlreiche Kunden haben im Zuge eines sicheren Zwei-Wege-Authentifizierungsverfahrens die Möglichkeit, sich die angeforderte TAN-Nummer auf das Smartphone schicken zu lassen. Hierdurch können Kriminelle am PC Online-Banking-Transaktionen manipulieren und gleichzeitig über das Mobilgerät die passende Authentifizierung stehlen.

[1] Statcounter: http://gs.statcounter.com/
[2] Der G DATA Security Evangelist Eddy Willems hat seine Einschätzung über die aktuelle Situation im Internet der Dinge im G DATA SecurityBlog veröffentlicht: https://blog.gdata.de/artikel/the-internet-of-things-trouble/
[3] http://www.heise.de/security/meldung/Vaillant-Heizungen-mit-Sicherheits-Leck-1840919.html

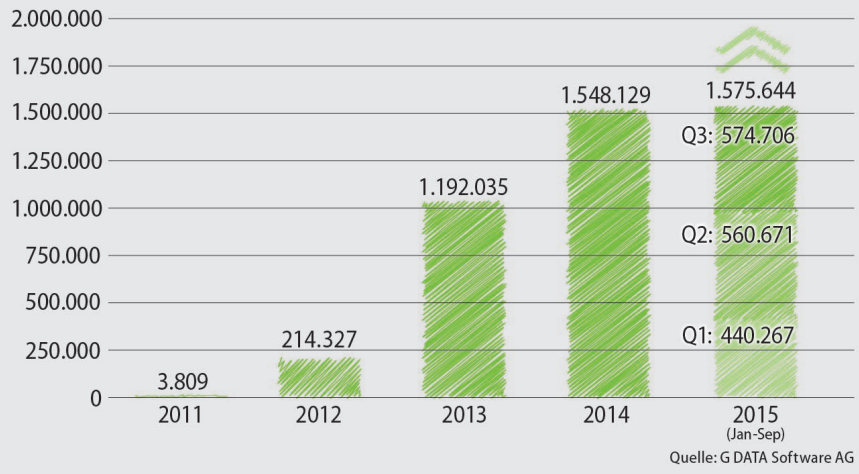
Whitepaper MMWR DE Q3 12-2015 #53115 - 1214151215

AKTUELLE LAGE: TÄGLICH 6.400 NEUE ANDROID-SCHADDATEIEN

574.706 neue Android-Schaddateien analysierten die G DATA Sicherheitsexperten im dritten Quartal 2015. Die Anzahl neuer Malware ist im Vergleich zum zweiten Quartal 2015 (560.671) weiterhin auf hohem Niveau und steigt. Zum Vorjahreszeitraum bedeutet das einen Anstieg um 50 Prozent. Durchschnittlich entdeckten die Experten in Q3/2015 pro Tag knapp 6.400 neue Android-Schaddateien.

Bis zum Ende des dritten Quartals 2015 identifizierten die G DATA Experten insgesamt über 1,5 Millionen neuer Android-Schädlinge in diesem Jahr. Damit zählten die Analysten bereits mehr Schädlinge als 2014 gesamt. Für 2015 wird eine Zahl von deutlich über zwei Millionen neuer Android-Malware immer wahrscheinlicher.[4]

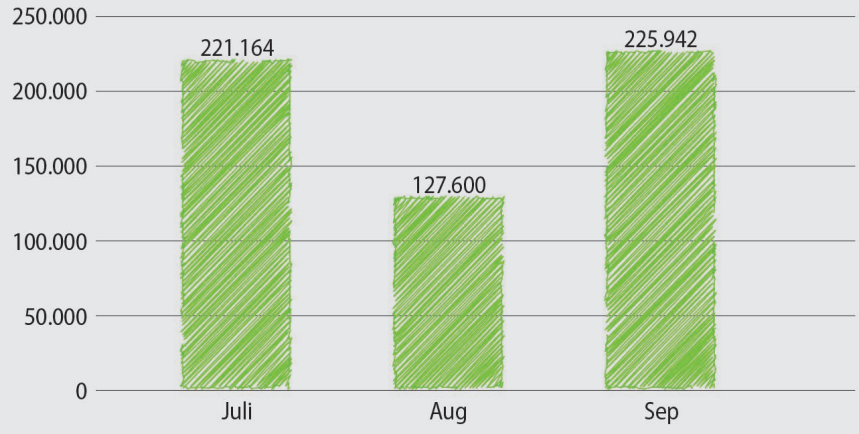
NEUE ANDROID SCHADDATEIEN



Quelle: G DATA Software AG

[4] 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 (Q3)



Quelle: G DATA Software AG

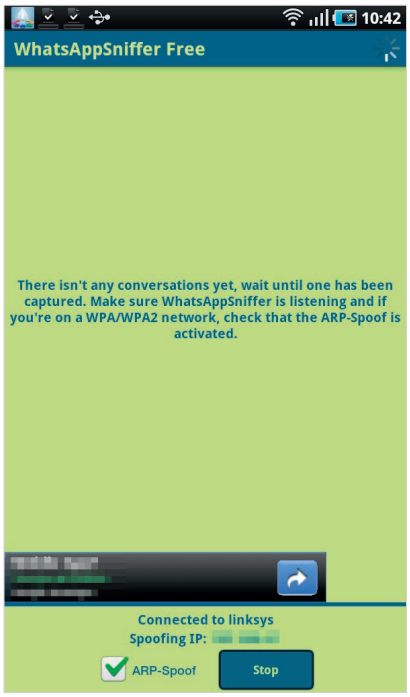
Whitepaper MMWR DE Q3 12-2015 #531115 - 1214151215

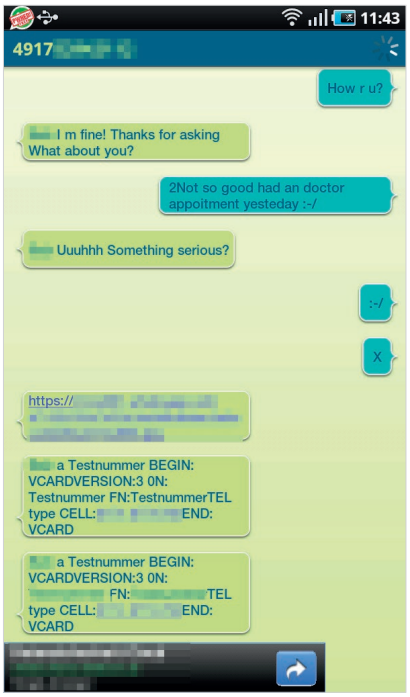
WAS SIND HACKING-TOOLS?

Hacking-Tools gibt es nicht im Google Play Store. Diese Anwendungen sind in Drittmärkten erhältlich, die neben diesen Apps auch die Gefahr einer Infektion mit Schadprogrammen bergen. Um solche Apps nutzen zu können, müssen Anwender in den Einstellungen ihres Mobilgeräts die Installation aus unbekannten Quellen aktivieren.

IT-Experten setzen solche Tools ein, um Netzwerke und Computer auf Schwachstellen abzuklopfen und erfolgreiche Angriffe auf Netzwerke und Geräte zu verhindern. Diese Apps können aber auch dazu genutzt werden, um fremde Mobilgeräte nach potenziellen Sicherheitslücken zu durchleuchten, in ein WLAN-Netz einzubrechen oder den Datenverkehr zu überwachen. Da diese Anwendungen eine Gefahr für Nutzer darstellen können, stufen die G DATA Sicherheitsexperten Hacking-Tools als Schadprogramme ein.

Anwendungen wie Hacking-Tools können strafrechtliche Konsequenzen haben. Im letzten Report haben die Sicherheitsexperten Monitor-Apps untersucht, die Mobilgeräte überwachen. In Deutschland sind die Ermittlungsbehörden kürzlich gegen Käufer der Überwachungssoftware „DroidJack“ vorgegangen. Mit dem Tool können beispielsweise Daten wie TAN-Nummern gestohlen, SMS versandt, das Smartphone lokalisiert oder Telefonate belauscht werden.[5]





Hinweis: Die G DATA Sicherheitsexperten haben sich dazu entschieden kein aktuelles Beispiel für ein Hacking-Tool zu präsentieren, um dafür keine Werbung zu machen.

WHATSAPP SNIFFER: FREMDE UNTERHALTUNGEN MITLESEN

Der WhatsApp Sniffer[6] zählte lange Zeit zu den beliebtesten Hacking-Tools, um fremde WhatsApp-Chats zu überwachen. Die Anwendung nutzte dafür eine Sicherheitslücke im beliebten Messenger aus. Besitzer dieser App konnten Gespräche und Daten aus beliebigen Unterhaltungen in Echtzeit mitlesen. Die Geräte mussten dazu lediglich in einem gemeinsamen Netzwerk angemeldet sein. Ein öffentliches WLAN an einem Flughafen oder in einem Hotel wäre für den Besitzer der Überwachungs-App eine nicht-endende Quelle zum Diebstahl sensibler Daten geworden.

Wie leicht das Belauschen der Unterhaltungen ging, zeigen auch die Screenshots. WhatsApp hat die Sicherheitslücke mittlerweile geschlossen. Dieser Sniffer ist aber bis heute ein sehr gutes Beispiel für Hacking-Tools und welche Anwendungsmöglichkeiten existieren.

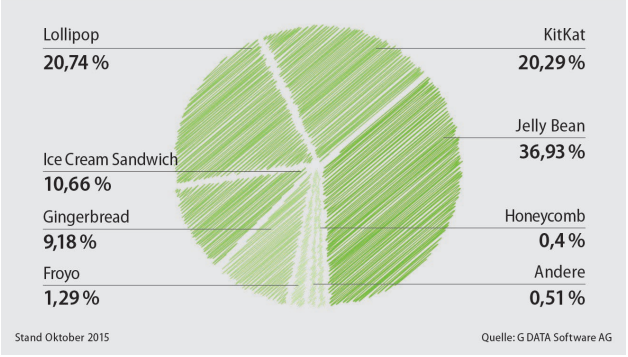
[5] http://www.heise.de/newsticker/meldung/Razzia-gegen-Kaeufer-von-Schnueffel-Software-fuer-Android-Smartphones-2860638.html
[6] https://blog.gdata.de/artikel/whatsapp-chats-koennen-in-wlan-netzen-ausgespaeht-werden/

Whitepaper MMWR DE Q3 12-2015 #53115 - 1214151215

ÜBER 80 PROZENT DER ANDROID-NUTZER HABEN EIN VERALTETES BETRIEBSSYSTEM

Die G DATA Sicherheitsexperten haben im Oktober 2015 untersucht, welche Android-Versionen auf Smartphones und Tablets mit G DATA Sicherheitslösungen im Einsatz sind. Aus diesem Grund fehlt noch das aktuelle Android 6 Betriebssystem, das erst im Oktober veröffentlicht wurde. Lediglich rund 20 Prozent der Anwender haben ein aktuelles Betriebssystem (Android 5.0 und neuer) installiert. Über 80 Prozent nutzen ein veraltetes OS, das bekannte Sicherheitslücken besitzt. Fast 12 Prozent setzten sogar noch auf die rund fünf Jahre alten Versionen Froyo und Gingerbread. Bei Gingerbread hat das FBI bereits vor über zwei Jahren vor der Nutzung des Betriebssystems gewarnt.[7]

VERBREITUNG DER ANDROID-VERSIONEN



Im Oktober 2015 hatten lediglich rund 20 Prozent der Anwender eine - zu dieser Zeit - aktuelle Android-Version im Einsatz.

ANDROID-VERSION	VERBREITUNG (IN PROZENT)
Lollipop	**20,74 %**
Android 5.1	6,63 %
Android 5.0	14,11 %
Kitkat	**20,29 %**
Android 4.4	20,29 %
Jelly Bean	**36,93 %**
Android 4.3	6,35 %
Android 4.2	12,75 %
Android 4.1	17,83 %
Ice Cream Sandwich	**10,66 %**
Android 4.0	10,66 %
Honeycomb	**0,4 %**
Android 3.2	0,4 %
Gingerbread	**9,18 %**
Android 2.3.3 - 2.3.7	9,18 %
Froyo	**1,29 %**
Android 2.2	1,29 %
Sonstige	0,51 %

Seitdem sind noch weitere Sicherheitslücken wie Stagefright [8] öffentlich geworden, welche unterschiedlichste Android-Versionen betreffen.

Android-Nutzer warten häufig lange auf Updates für ihr Betriebssystem. Veröffentlicht Google ein Update für das Android-Betriebssystem, dauert es meist Wochen bis Monate, bis die Hersteller von Mobilgeräten die Versionen für ihre Produkte modifiziert haben und an ihre Kunden ausliefern. Bei älteren Smartphones oder Tablets ist oft unklar, ob der Hersteller Sicherheitslücken überhaupt noch schließt. Häufig werden selbst Top-Geräte lediglich ein bis zwei Jahre mit notwendigen Updates unterstützt.

Einige Hersteller haben damit begonnen, ein monatliches Updateprogramm für ihre Produkte mit Android-Betriebssystem zu starten. Samsung hat beispielsweise

[7] https://publicintelligence.net/dhs-fbi-android-threats/
[8] https://blog.gdata.de/artikel/sicherheitsluecke-in-android-medien-engine-stagefright/

Whitepaper MMWR DE Q3 12-2015 #53115 - 1214151215

einen Mobile Security Blog gestartet, auf dem Kunden sehen können, welche Updates für ihr Gerät vorliegen. Hierbei orientiert sich der koreanische Hersteller an den Microsoft Patchdays, an denen jeden zweiten Dienstag im Monat die Programme des Redmonder Softwareentwicklers auf den aktuellen Stand gebracht werden. Allerdings erhalten aber nur einige Geräte aus den letzten zwei Jahren diese Sicherheitspatches.[9]

Auch andere Hersteller planen in den nächsten Monaten einen ähnlichen Service anzubieten, um Kunden besser zu informieren und eine größere Aufmerksamkeit für Sicherheitsupdates auf Mobilgeräten zu schaffen.

[9] http://security.samsungmobile.com/

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 Produkte setzen weltweit höchste Sicherheitsstandards: In jedem Vergleichstest zeigte die G DATA INTERNET SECURITY die beste Virenerkennung.

Das EU-Gemeinschaftsprojekt IPACSO zeichnete G DATA 2014 zudem als innovativstes IT-Sicherheitsunternehmen Europas aus und lobte die schnelle Reaktion auf neue Bedrohungen.

G DATA Sicherheitslösungen schützen weltweit Millionen PCs und sind in über 90 Ländern erhältlich – sowohl für Privatanwender, als auch für den Mittelstand und für Großunternehmen, sowie als Managed Service für Businesskunden über die zahlreichen G DATA Partner. Das ist Sicherheit "Made in Germany".

G DATA SIMPLY SECURE

Whitepaper MMWR DE Q3 12-2015 #53115 - 1214151215