G Data

Mobile MalwareReport

Halbjahresbericht
Juli – Dezember 2013

G Data SecurityLabs

G Data. Security Made in Germany.

Inhalt

Auf einen Blick

- Die Zahl der aktivierten Android Mobilgeräte liegt inzwischen bei über einer Milliarde.[10]
- Laut Gartner betrug die Zahl der verkauften Android Mobilgeräte im vergangenen Jahr über 877 Millionen Smartphones und Tablets weltweit. Im Vergleich zu 2013 bedeutet das eine Steigerung von über 70 Prozent. Die Analysten rechnen bis 2015 pro Jahr mit mehr als einer Milliarde neu verkauften Android-Geräten und einem Marktanteil von 50 Prozent.

- Schadcode für Android: Die Anzahl neuer Mobile Malware-Samples ist im zweiten Halbjahr 2013 weiter gestiegen – es waren 672.940 neue Schaddateien, gegenüber 526.818 in der vorangegangenen Jahreshälfte.
- Steigerungsraten 2013: Im Vergleich zum ersten Halbjahr 2013 bedeutet das einen Zuwachs der Anzahl neuer Schaddateien von 30%.
- Vorjahresvergleich: Ein Vergleich der Gesamtzahlen neuer Schaddateien aus 2012 und 2013 zeigt eine Steigerung um 460%.

- Der Anteil der Backdoors hat leicht zugenommen (+5,7%) – dies belegt, dass immer mehr Smartphones in Botnetze integriert werden.
- Schad-Apps, die als Android.Application erkannt werden und damit in die Gruppe der potentiell unerwünschten Programme (PUP) gehören, haben einen großen Anteil am Gesamtbild der neuen Dateien (40,4%). Dazu gehören Schädlinge mit vielfältigen Schadfunktionen.
- Hacktools sind dabei eine auffällige Form von Android.Application. Diese Apps werden häufig zweideutig genutzt – als legitimer Systemtest, oder aber auch als Spionagetool, wenn es in die falschen Hände gerät.

Prognosen:

- Es ist zu erwarten, dass die Angreifer immer weniger SMS-Schädlinge erstellen und verbreiten, denn die Sicherheitsmechanismen gegen diese Bedrohung werden immer effizienter. Unter anderem werden nun Datendiebstahl und die Entwicklung/Verbreitung von Ransomware weiter an Bedeutung gewinnen.
- Da Geld auch weiterhin das Ziel Nummer eins der Angreifer bleiben wird, könnte der Angriff auf Kryptowährungen wie Bitcoin und Co. in Zukunft auch, und besonders wenn die digitalen Geldbörsen auf den Mobilgeräten sind, eine Rolle spielen.
- Smartphones werden häufiger als Zugang zu Firmennetzen missbraucht. Cross-Plattform-Infektionen zwischen PCs und Mobilgeräten werden in beide Richtungen zunehmen.
- Das „Internet der Dinge“ hält immer häufiger Einzug in das tägliche Leben und die Android-Plattform wird dabei nicht selten als Betriebssystem verwendet. Groß angelegte Angriffe gegen diese Geräte sind daher auch nur eine Frage der Zeit.
- Wir erwarten im kommenden Jahr erste Angriffe auf Smart TVs.

Android-Schadcode: Der Anteil von PUP steigt deutlich

Die Zählung der Android-Malware basiert auf der Auswertung der Anzahl neuer Schadprogramme.[1] In den G Data SecurityLabs wurden im zweiten Halbjahr 2013 insgesamt 672.940 neue Schaddateien erkannt. Das bedeutet eine Steigerung um knapp 30% gegenüber dem ersten Halbjahr 2013 (526.818[2]). Hier kam es jedoch nicht zur prognostizierten Verdreifachung der Anzahl neuer Mobile-Schadprogramme. Durchschnittlich erreichten die G Data SecurityLabs täglich 3.657 neue Schaddateien!

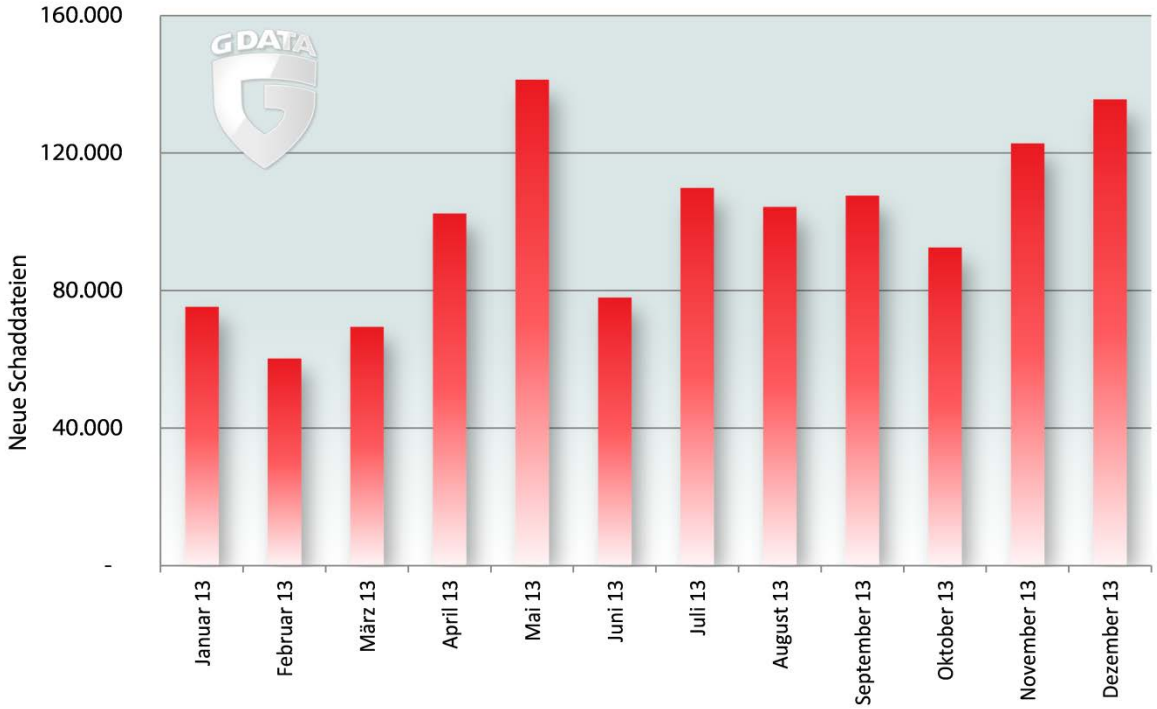


Abbildung 1: *Verteilung neuer Schaddateien, die dem Jahr 2013 zugeordnet werden konnten.*

Die einzelnen Dateien werden anhand der Eigenschaften des Schadcodes[3] bestimmten Familien zugeordnet. 312.438 der neuen Schaddateien konnten eindeutig zu Malware-Familien klassifiziert werden[4], wie in Abbildung 2 dargestellt. Innerhalb der Familien konnten 2.859 verschiedene Schädlingsvarianten ermittelt werden. Diese Varianten basieren auf 581 unterschiedlichen Schädlingsfamilien. Im letzten Halbjahr zählten die Experten 176 neue Familien. Eine Auflistung der produktivsten Familien, also den Familien mit den meisten Varianten, geht aus Tabelle 1 hervor.

Familie	# Varianten
Trojan.Agent	586
Trojan.SMSSend	171
Backdoor.GingerMaster	159
Trojan.SMSAgent	96
Trojan.Boxer	80

Tabelle 1: *Liste der Android Malware-Familien mit den meisten Varianten in H2 2013.*

[1] Ein Android Schädling kann aufgrund mehrerer Dateien identifiziert werden. Das Installationspaket (APK) enthält viele weitere Dateien, die u.a. den Code und die Eigenschaften enthalten. Bei der vorliegenden Zählweise werden Erkennungen für APK und ihre jeweiligen Komponenten zu einer Schaddatei zusammengefasst, auch wenn tatsächlich mehrere Dateien in unserer Sammlung vorliegen.

[2] Die rückwirkenden Zahlen in diesem Halbjahresbericht fallen höher aus, als die in den zuvor veröffentlichten Berichten. In einigen Fällen empfangen die G Data SecurityLabs 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.

[3] Die Zählung der Signaturen und Varianten basiert auf den Signaturen der G Data Schutzlösungen für Mobile-Produkte.

[4] Von 672.940 Samples wurden 360.502 Samples als „potentiell unerwünschte Programme" oder mit generischen Signaturen identifiziert und werden daher nicht eindeutig zu Malware gezählt.

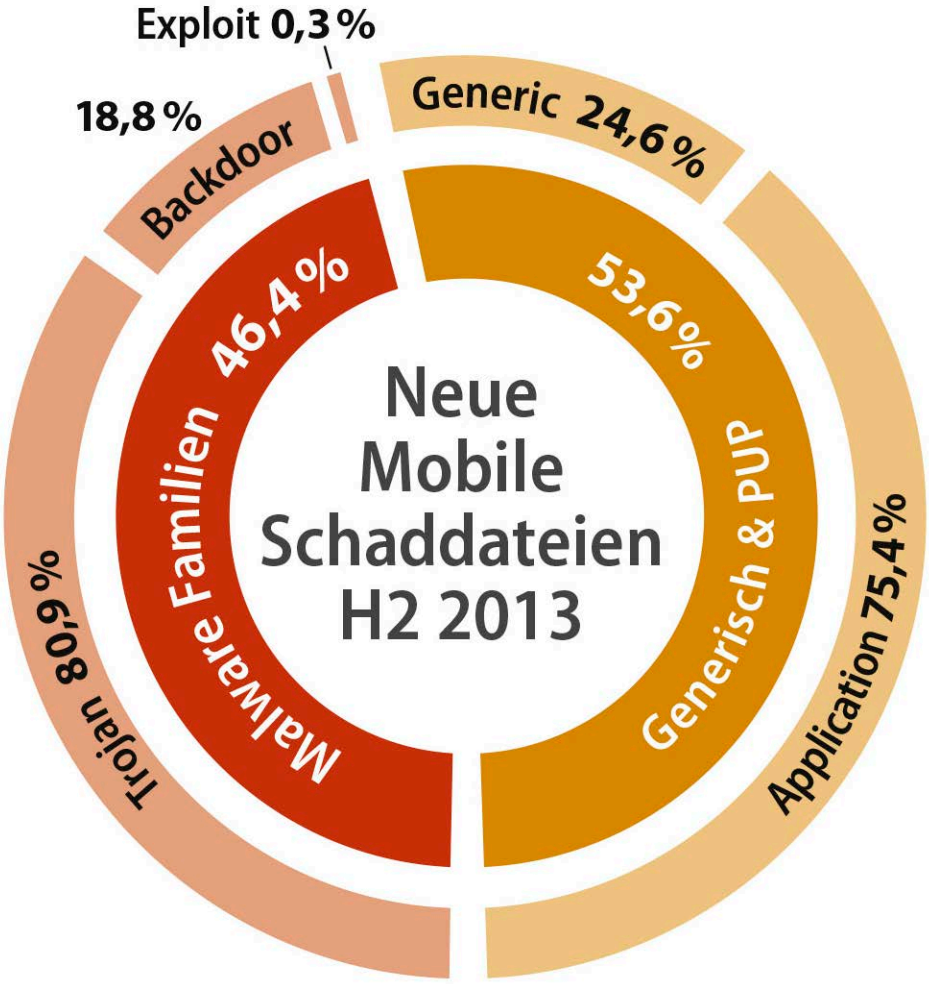


Abbildung 2: *Zusammensetzung der neuen mobilen Schaddateien aus H2 2013 in Prozent.*

Der innere Ring beschreibt die Aufteilung der neuen Schaddateien in Dateien, die zu Malware-Familien klassifiziert werden konnten und den Dateien, die generischer erkannt wurden sowie Dateien, die als potentiell unerwünschte Programmen (kurz: PUP) erkannt wurden. Der äußere Ring zeigt die respektive Zuordnung der Typen, wie sie mit den Signaturen der G Data MobileSecurity Produkte vorgenommen wird.

Generell haben sich die Verhältnisse im zweiten Halbjahr nicht stark verändert: die Einordnung in Malware Familien und generischen Erkennungen sowie PUP[5] halten sich in etwa die Waage, auch wenn „Generisch und PUP“ dieses Mal mehr als die Hälfte ausmachen.[6]

[5] PUP sind keine klassischen Schadprogramme. Als Schadprogramm wird im Allgemeinen Software betrachtet, deren Zweck es ist, das infizierte Gerät zu schädigen oder Informationen zu stehlen, mit denen dann, ohne Zustimmung des Nutzers, Straftaten wie z.B. Identitätsdiebstahl oder Betrug begangen werden. Aber es ist nicht immer ganz einfach, eine klare Linie zwischen Malware und anderen Ärgernisse wie Adware oder PUP zu ziehen. In den häufigsten Fällen diese sie Browser-Einstellungen (Browser-Hijacker), blenden ungebetene Werbung ein (Adware), spionieren im Hintergrund den Nutzers aus (Spyware) und nisten sich mitunter tief im System ein. Aber schädlich, im engeren Sinne, sind die Programme nicht. Manch einer möchte die Funktionen der Software wirklich nutzen. Daher auch der Name „Potentiell“ Unerwünschte Programme.

[6] Durch Optimierung der Verfahren zur Schadcode-Benennung, ist es gelungen, mehr generische Erkennungen eindeutig passenden Bereichen zuzuordnen. Daher rührt der starke Anstieg des Anteils von Android.Application im Bereich „Generisch und PUP“.

Android.Application ist vielseitig

Der Bereich PUP (die Erkennung lauten Android.Application) nimmt einen beachtlichen Anteil ein: 40,4% der neuen Samples wurden als Android.Application erkannt. Hinter dieser Erkennung sind zum Beispiel Apps einsortiert, wie die Anfang 2014 entdeckten gefälschten Adobe Flash Player Apps, die im Google Play Store auf Beutezug gingen.[7]
Außerdem zählen auch als Copycat bezeichnete Apps zu dieser Kategorie – dies sind Kopien von ganz regulären Applikationen, die potentiell unerwünschte Zusätze enthalten, wie z.B. Werbeeinblendungen oder die Einforderung zusätzlicher Berechtigungen. Zur Erstellung solcher App-Kopien mit Zusätzen bedienen sich die Angreifer sogenannter „Binder", wie schon im vergangenen Mobile MalwareReport berichtet.[8]
Auch wenn die reguläre App nach der Installation zunächst funktioniert und ein Benutzer sie deswegen nicht direkt wieder von seinem System löscht, liefern die Betrüger zu diesen Apps meist keine Updates mehr aus. Der Benutzer bleibt also auf einem App-Stand, der eventuell Sicherheitslücken enthält und/oder ohne Optimierungen durch den Entwickler auskommen muss. Daher raten die Experten der G Data SecurityLabs weiterhin eindringlich dazu, Apps immer nur von den Original-Herstellern zu laden.

Spezialfall: Hacktools

Eine weitere Art von als Android.Application gekennzeichneten Apps sind Hacktools, wie beispielsweise Programme zum Überwachen von Netzwerken.
Die Anwendung der Programme ist jedoch ambivalent, da sie sowohl für legitime, gutartige Zwecke benutzt werden kann, aber eben auch zum Ausspionieren und Überwachen. Viele der Pentesting-Tools[9] stammen aus dem wissenschaftlichen Bereich und wurden zu Forschungszwecken erstellt, später jedoch für betrügerische Aktivitäten missbraucht. Erkenntnisse, die mit Hacktools und Pentesting-Tools über Sicherheitslücken und Programmierschwachstellen gewonnen wurden und werden sind demnach auch Grundlagenwissen für Malware-Autoren.

[7] G Data SecurityBlog: http://blog.gdata.de/artikel/da-lohnt-sich-ein-zweiter-blick-gefaelschte-flash-player-apps-im-google-play-store/
[8] G Data Mobile MalwareReport H1 2013: http://www.gdata.de/rdk/dl-de-mmwr
[9] Pentesting ist die Kurzform des englischen Begriffs Penetration Testing und beschreibt das Prüfen von Rechnern oder Netzwerken auf Sicherheitslücken. Beim Testen werden Methoden angewendet, wie sie ein Angreifer anwenden würde, um in das System einzudringen.

Trends

Die Begeisterung der Smartphone-Nutzer für die Android-Plattform ist ungebrochen – Anfang September 2013 meldete Googles Sundar Pichai, SVP für Android, Chrome und Apps, dass die Zahl der aktivierten Android-Geräte die bedeutende Marke von einer Milliarde durchbrochen hat.[10]

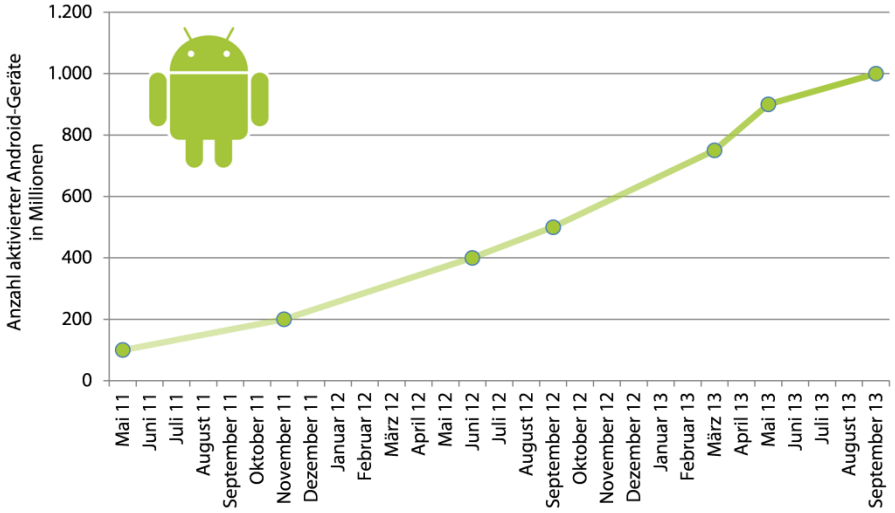
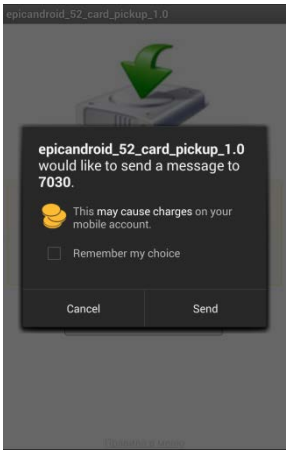


Abbildung 3: *Anzahl der aktivierten Android-Geräte.*

Mit den rasant steigenden Benutzerzahlen stieg selbstverständlich auch das Interesse der Cyberkriminellen, aus der Plattform Profit zu schlagen. Dazu wurden von jeher die verschiedensten Angriffstechniken sowie Täuschungsmanöver benutzt. Nun, da die Konzentration auf SMS-Schädlinge nicht mehr Faktor Nummer 1 ist, müssen neue Bedrohungsszenarien und Einnahmequellen kreiert werden:

SMS-Schädlingen geht nach und nach die Luft aus



Screenshot 1: *Android warnt den Nutzer vor dem Absenden einer Premium-SMS.*

Android Mobilgeräte mit dem Betriebssystem Version 4 gewinnen immer mehr an Marktanteil und damit steigt auch die Sicherheit gegenüber SMS-Schädlingen. Die Anzeige von App-Berechtigungen wurde von vielen Benutzern achtlos ignoriert und der Hinweis auf kostenpflichtige Berechtigungen allzu schnell überlesen und das obwohl Google diese Hinweise in den neuen Android-Versionen schon farblich auffällig und mit Münzsymbolen ausgestattet hervorhebt.[11]
Seit Version 4.2 hat das Betriebssystem jedoch unter anderem einen Premium-SMS Filter integriert, der den Nutzer nicht nur bei der Installation warnt, sondern sogar vor dem Versenden einer solchen SMS einen speziellen Screen zeigt und ihm Interventionsmöglichkeiten bietet.
Eine wichtige Neuerung in Android KitKat (Version 4.4) ist die Tatsache, dass nur noch die als Standard ausgewählte SMS-App Nachrichten verwalten darf – senden, löschen, etc.[12] Damit wird ein unbemerktes Versenden erneut erschwert und ein Abfangen und Löschen von eingehenden SMS, z.B. zum Verschleiern von Abonnement-Abschlüssen

[10] https://plus.google.com/+SundarPichai/posts/NeBW7AjT1QM
[11] Siehe Screenshot 1
[12] http://android-developers.blogspot.de/2013/10/getting-your-sms-apps-ready-for-kitkat.html

oder mTAN-Empfang, ist standardmäßig nicht mehr möglich.

Im Februar 2013 lag der Anteil der Android-Mobilgeräte mit Version 4.2 bei 1,4%. Im November 2013 entfielen schon 15,8% auf Android 4.2 und 4.3 und im Dezember 2013 erreichten die Versionen 4.2 bis 4.4 zusammen 18,2% - Tendenz natürlich steigend!

Die Angreifer werden also ihre Maschen verfeinern oder aber sich auf andere Geschäftsfelder einstellen müssen, wenn das schnelle Geld durch SMS-Betrug nicht mehr die Masche mit der besten Kosten-Nutzen-Rechnung sein wird. Unter anderem werden nun Datendiebstahl und die Entwicklung/Verbreitung von Ransomware weiter an Bedeutung gewinnen.

Kryptowährungen – das digitale Geld gerät sicher in den Fokus

Die wohl bekannteste Kryptowährung ist Bitcoin, doch die Liste der populären Anbieter wird stetig länger und Zahlungen mit diesen Währungen sind im Internet gang und gäbe – auch, oder gerade besonders, bei Untergrundgeschäften. Geschätzt werden von den Nutzern die vielbeschriebene Anonymität und auch die Unabhängigkeit von Zentralinstanzen wie etwa Banken.

Die Währung basiert jedoch rein auf digitalen Daten und hat keinen physikalischen Gegenpart, wie etwa ein Stück Edelmetall. Daraus ergibt sich, dass auch die Speicherung der Währungsdaten rein digital abläuft und diese Speicherdaten, im Speziellen die privaten Kryptoschlüssel der User und auch die sogenannten Wallets, die Geldbörsen, verstärkt in das Visier der Cyber-Angreifer geraten werden. Durch den Hype, der in den letzten Wochen und Monaten wieder um die Kryptowährungen gemacht wurde, springen viele neue Benutzer auf den Zug auf und benutzen dabei u.a. auch Apps für ihre Mobilgeräte, in denen die Wallets gespeichert sind. Kommen die Angreifer an diese digitalen Geldbörsen heran, können Sie das enthaltene Kryptogeld direkt einstreichen und müssen nicht einmal mehr Umwege über Money Mules oder andere Zwischenstellen gehen.

Die Experten der G Data SecurityLabs erwarten, dass sich Android Malware in Zukunft daran machen wird, relevante Daten für Kryptowährungen von den Mobilgeräten zu stehlen.

Cross-Plattform Malware weiter im Kommen

Im Bereich des Onlinebankings spielen Mobilgeräte seit Einführung der mTAN-Funktion eine wichtige Rolle und werden deshalb auch in diesem speziellen Bereich von Angreifern immer wieder ins Visier genommen.[13] Infizierte PCs locken nicht selten Mobilgerätenutzer dazu, angebliche Sicherheits-Apps aus dem Netz herunterzuladen und zu installieren, die dann z.B. mTANs abfangen. Gut für den Benutzer: Das Herunterladen der Apps kann zwar automatisiert geschehen, doch die Installation muss der Benutzer in diesem Fall selbst aktivieren – es handelt sich um Drive-by-Downloads, jedoch nicht im Drive-by-Infektionen.

Automatisierte Infektionen sahen wir bisher von Mobilgeräten zum PC: ein infiziertes Mobilgerät kann beispielsweise den Befehl erhalten, Windows-Malware herunterzuladen und im Speicher abzulegen und diese per Autorun-Funktion auf dem PC auszuführen, sobald das Handy an den Computer angeschlossen wird.[14]

Erwartet wird nun, dass auch PC-Malware häufiger bei angeschlossenen Mobilgeräten eine Installation von infizierten .apk-Dateien auf dem Mobilgerät vornimmt. Befindet sich ein Android-

[13] G Data SecurityBlog: http://blog.gdata.de/artikel/angebliches-sicherheitszertifikat-entpuppt-sich-als-android-malware/
[14] G Data SecurityBlog: http://blog.gdata.de/artikel/android-malware-infiziert-windows-pc-mit-spionage-bot/

Gerät im Debug-Modus, wenn es an den PC angeschlossen wird, kann die Installation über den PC automatisiert erfolgen, ohne Rückfrage an den oder Interaktion mit dem Nutzer.

Was außerdem noch interessant wird

- Mobilgeräte könnten, als Teil eines Botnetzes, verstärkt als Instrument für DDoS-Angriffe verwendet und auch missbraucht werden.
- Das „Internet der Dinge“ basiert immer häufiger auf dem Android Betriebssystem und bietet damit mehr spezifische Angriffsflächen, vor allem auch in der häuslichen Umgebung: intelligente Kühlschränke, über das Internet bedienbare Heizungsanlagen, Multimedia-TV-Geräte, Spielekonsolen und vieles mehr. Alles ist vernetzt und aus Komfortgründen meist auch von außerhalb des Hauses erreichbar. Auf die Entwicklung neuer Funktionen und Features wird viel mehr Wert gelegt, als auf die Implementierung von Sicherheitsfunktionen.