SIMPLY SECURE

G DATA
MOBILE MALWARE REPORT

GEFAHRENBERICHT: Q1/2015

INHALTE

Whitepaper Mobile Malware Report DE V2 06-2015 • 2914250615

AUF EINEN BLICK

- Der weltweite Marktanteil von Android-Smartphones und –Tablets an der Internetnutzung lag im ersten Quartal 2015 bei über 61 Prozent. In Europa gingen über 62 Prozent der Anwender mobil mit einem Gerät mit Android-Betriebssystem ins Internet, in Deutschland sogar 68,5 Prozent der Nutzer. [1]
- Absolute Schadcode-Zahlen für Android-Geräte: 440.267 neue Malware-Samples haben die G DATA Sicherheitsexperten im ersten Quartal 2015 identifiziert und analysiert. Zum vierten Quartal 2014 bedeutet das einen Anstieg von 6,4 Prozent (413.871). Zum ersten Quartal 2014 stieg die Schadcodezahl um 21 Prozent (363.153).
- Finanziell motivierte Android-Schadprogramme machen rund die Hälfte der analysierten Malware aus (50,3 Prozent). Diese Art von Schädlingen umfassen unter anderem Banking-Trojaner, Ransomware oder SMS-Trojaner.
- Viele Apps, insbesondere kostenlose, setzen auf die Einblendung von Werbung, aber ab wann werden solche Anwendungen als Adware deklariert? Verstecken sich Apps im Hintergrund, verschleiern sie dem Anwender Funktionen oder werden legitime Apps mit weiteren Werbenetzwerken versehen, stufen die Analysten diese als PUP (Potentiell unerwünschte Programme) ein.

PROGNOSEN UND TRENDS

ABSOLUTE ANZAHL VON NEUEN SCHADDATEIEN STEIGT DEUTLICH

Für 2015 erwarten die G DATA Sicherheitsexperten eine rasant steigende Anzahl an neuen Schaddateien. Eine Zahl von über 2 Millionen neuen Android-Schädlingen 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.

DAS „INTERNET DER DINGE“: EINFALLSTOR MOBILGERÄT

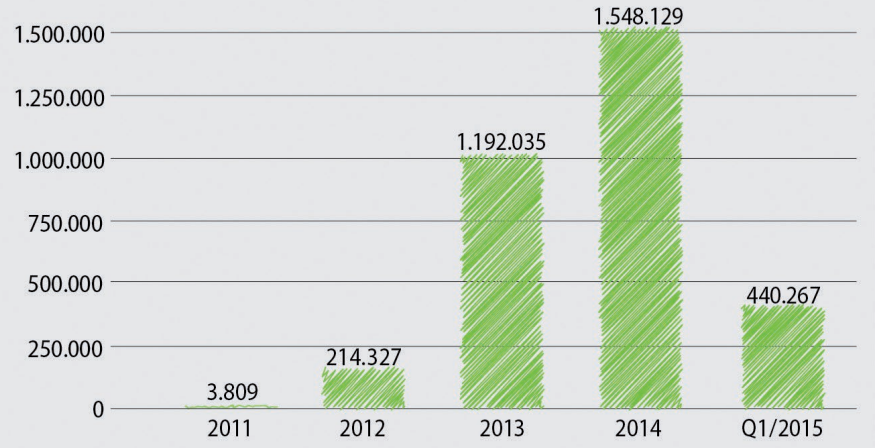
Intelligente Geräte sind häufig angreifbar. Ob nun intelligente Autos oder Router, Forscher decken immer wieder Sicherheitsmängel auf. Zur Steuerung der Geräte sind in vielen Fällen Smartphones oder Tablets im Einsatz. Die G DATA Sicherheitsexperten erwarten, dass mit steigender Verbreitung des „Internets der Dinge“ die Mobilgeräte als Steuerzentralen dieser Verbindung als Angriffsvektor stärker in den Fokus geraten. Beispiele sind Fitness-Apps oder Tracker. Werden die Daten nicht ordentlich verschlüsselt, können die gesammelten Daten gestohlen werden.

[1] Statcounter: http://gs.statcounter.com/#mobile_os-ww-monthly-201501-201503

AKTUELLE LAGE: TÄGLICH 4.900 NEUE ANDROID-SCHADDATEIEN

Im ersten Quartal 2015 analysierten die G DATA Sicherheitsexperten 440.267 neue Schaddateien. Zum vierten Quartal 2014 bedeutet das einen Anstieg von 6,4 Prozent (413.871). Die Anzahl neuer Schadprogramme ist sogar um 21 Prozent im Vergleich zum ersten Quartal 2014 (363.153) gestiegen. Durchschnittlich entdeckten die Experten im ersten Quartal 2015 pro Tag fast 4.900 neue Android Schaddateien, das sind täglich fast 400 neue Schaddateien mehr als im zweiten Halbjahr 2014. Alle 18 Sekunden identifizieren die Analysten im ersten Quartal 2015 einen neuen Schädling, pro Stunde macht das über 200 neue Schadprogramme.

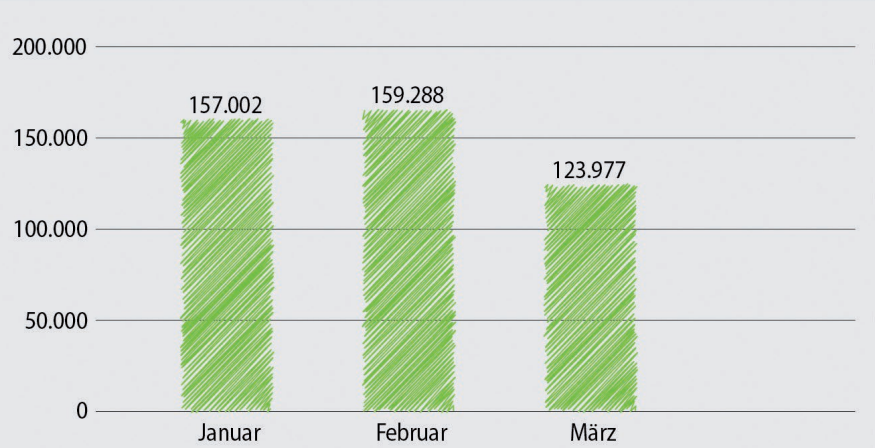
NEUE ANDROID SCHADDATEIEN



Quelle: G DATA Software AG

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 (Q1)

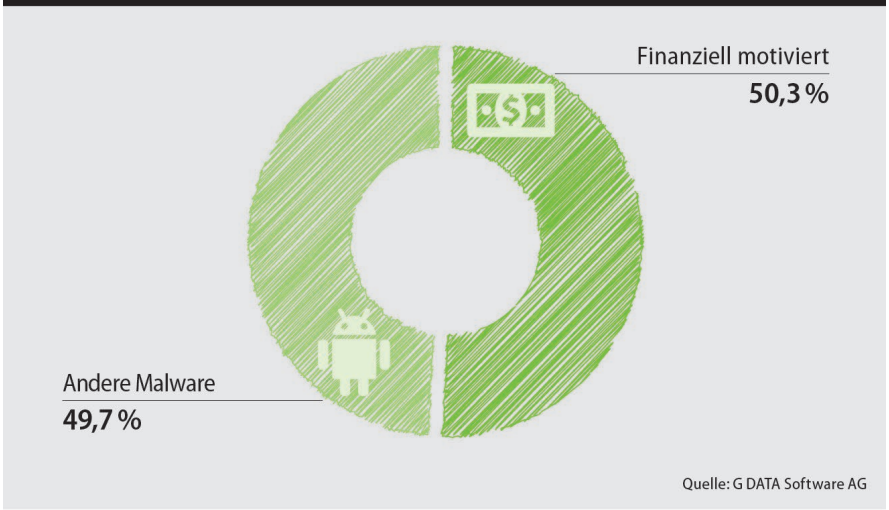


Quelle: G DATA Software AG

DIE HÄLFTE DER ANDROID-MALWARE IST FINANZIELL MOTIVIERT

Über 40 Prozent der Deutschen nutzen ein Smartphone oder Tablet für ihre Bankgeschäfte.[3] Jeder Dritte möchte künftig mit seinem Smartphone für Fahrten in Bus, Bahn oder Taxi bezahlen.[4] Das Erledigen von Finanzgeschäften auf dem Smartphone oder Tablet erlebt rasante Zuwächse, dem auch Cyberkriminelle folgen. Die G DATA Sicherheitsexperten haben dazu die neuen Schaddateien genauer unter die Lupe genommen und festgestellt, dass mindestens 50 Prozent der aktuell verbreiteten Android-Schadprogramme einen finanziell motivierten Hintergrund haben, was unter anderem Banking-Trojaner und SMS-Trojaner umfasst. Die Dunkelziffer könnte noch höher liegen, da die Experten nur Malware mit direkter finanzieller Motivation untersucht haben. Sollte ein Schadprogramm erst im weiteren Verlauf nach Zahlung Apps nachinstallieren oder Kreditkartendaten stehlen, taucht diese Malware in der vorliegenden Statistik nicht als finanziell motiviert auf.

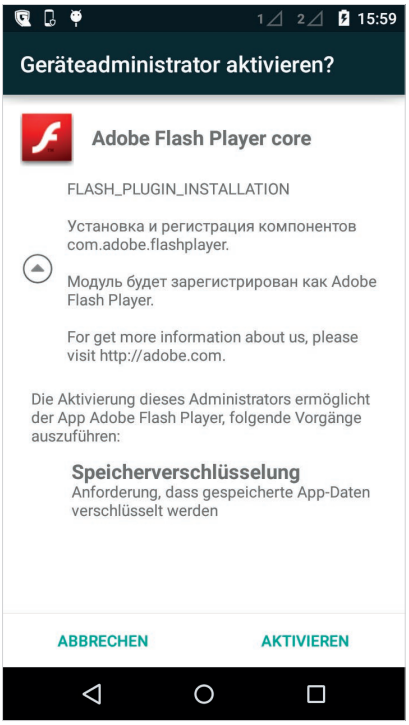
ANTEIL FINANZIELL MOTIVIERTER ANDROID-MALWARE



Die analysierten Werte beziehen sich in dieser Statistik auf benannte Malware (non-generic). Ebenfalls wurden keine potentiell unerwünschten Programme (PUP) in diese Statistik aufgenommen.

[3] http://www.ezonomics.com/ing_international_survey/mobile_banking_2015
[4] http://www.bitkom.org/de/markt_statistik/64034_81657.aspx

BEISPIELE FÜR TROJANER

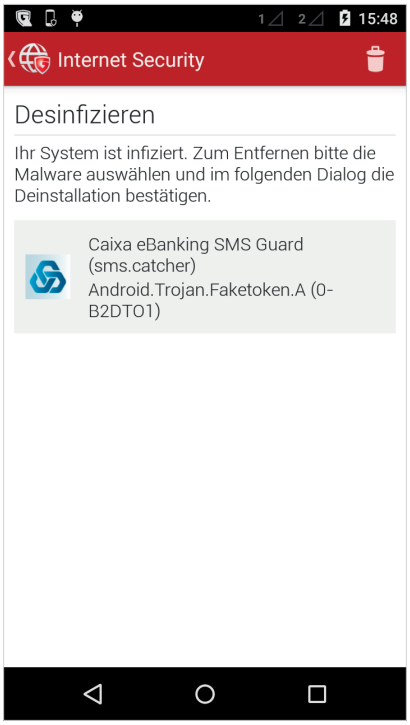


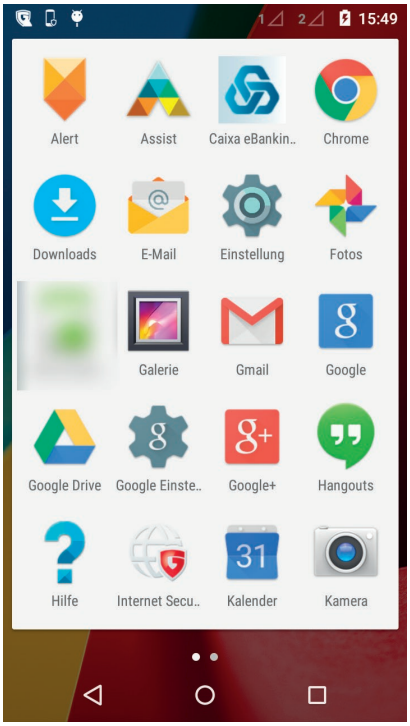
TROJANER SVPENG

Der Android-Trojaner Svpeng ist ein Beispiel für finanziell motivierte Malware. Svpeng, der von G DATA als „Android.Trojan.Svpeng.A“ erkannt wird, kombiniert die Funktionen eines Finanz-Schädlings mit den Möglichkeiten von Ransomware. Je nach Variante stiehlt die Malware bei der Nutzung einer Banking-App Zugangsdaten oder verschlüsselt das Gerät, um Lösegeld zu erpressen (Ransomware). Auf dem Beispielbild ist die Fälschung daran zu erkennen, dass die Beschreibungen auf Russisch sind. Ebenfalls wird als Recht eine Speicherverschlüsselung gefordert, die der Anwendung das Recht gibt, App-Daten zu verschlüsseln. Zudem gibt es keinen Flash Player für das Android-Betriebssystem.

TROJANER FAKETOKEN

Der Banking-Trojaner FakeToken (Android.Backdoor.FakeToken.A) soll gezielt auf das Smartphone gesendete mTANs stehlen. Dabei tarnt sich der Android-Schädling als eine von der Hausbank des Nutzers bereitgestellte Anwendung zum Erstellen von TANs. Eine Meldung, die zur Installation der App auffordert, wird durch eine Attacke während einer Online-Banking-Sitzung auf dem Mobilgerät realisiert. Wird die bösartige App dann installiert nutzen die Cyberkriminellen den Trojaner, um Zugriff auf das Konto des Opfers zu erhalten. Angreifer können sich mit den gestohlenen Zugangsdaten im Konto des Nutzers anmelden und mTANs abfangen und Geld auf ihre eigenen Konten überweisen. Die Daten können die Täter dann für ihre Zwecke einsetzen.





WANN WIRD AUS WERBUNG ADWARE?

Adware hat das Ziel dem Nutzer Werbung zu zeigen und durch diese Anzeige in erster Linie monetäre Gewinne und häufig auch Daten zum Weiterverkauf zu generieren. Dabei geht es aber nicht um einmalige Einblendungen, sondern um fest in das System verankerte Werbung, die zum Beispiel bei jedem Programmstart oder auch bei einem Neustart des Geräts angezeigt wird. Diese Meldungen empfinden Anwender auf die Dauer als störend. Adware versteckt sich häufig in manipulierten oder gefälschten Apps. Adware findet sich meist in Apps, die aus anderen Quellen als dem Play Store installiert werden.

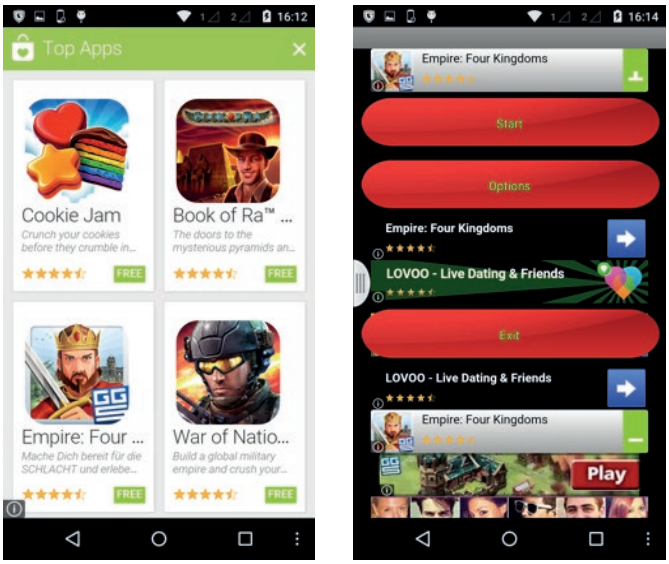
Aber wann werden Apps als Adware eingestuft? Die G DATA Sicherheitsexperten ziehen bei dieser Frage eine klare Linie: Verstecken sich Apps im Hintergrund, täuschen dem Anwender Funktionen vor oder werden legitime Apps mit weiteren Werbenetzwerken versehen, stufen die Analysten diese als PUP (Potentiell unerwünschte Programme) ein und melden dies dem Anwender.

WIE GELANGT PUP AUF DAS MOBILGERÄT?

Google hat solchen Apps bereits vor geraumer Zeit den Kampf angesagt. Anwendungen müssen bestimmte Richtlinien einhalten, beispielsweise muss Werbung innerhalb der App angegeben werden. Verboten sind Werbeformen, die einer Systemnachricht ähneln und Anwender täuschen oder verunsichern könnten. Beispielsweise darf keine Werbung gezeigt werden, die den Google Play Store nachbildet. Genauso ist es untersagt, Shortcuts oder Icons außerhalb der Anwendung zu platzieren. Ebenso dürfen keine Icons verwendet werden, die einer bereits vorhandenen und verbreiteten App ähneln.

Doch wie können dennoch solche Anwendungen auf das Mobilgerät gelangen? Die Antwort liegt meist bei alternativen App Stores oder aufdringlichen Werbenetzwerken. Hier sind häufig Kopien kostenpflichtiger Original-Anwendungen günstiger oder sogar gratis erhältlich, kommen dann aber gepackt mit potentiell unerwünschten Zusätzen. Die Richtlinien und Prüfverfahren sind in vielen Fällen nicht klar geregelt oder es gibt schlicht keine. So können Herausgeber hier Adware in den Anwendungen platzieren und anbieten.

BEISPIEL FÜR ADWARE



Adware hat das Ziel Nutzern Werbung zu zeigen und mit diesen Anzeigen finanzielle Gewinne und Daten zu erlangen. Im Beispiel werden kostenlose Kopien bekannter Apps in einer Anzeige, die wie Google Play aussieht, beworben. Hinter solchen Anzeigen verbergen sich dann häufig manipulierte Apps, die neben der eigentlichen Funktion auch andere Funktionen, wie Spyware oder noch mehr Adware beinhalten. Das kann dazu führen, dass eine regelrechte Werbelawine auf Anwender einstürzt.

Whitepaper Mobile Malware Report DE V2.06-2015 • 2914250615