G Data

Report

Trends 2012

G Data SecurityLabs

12-2011

Geschützt. Geschützter. **G Data.**

Inhalt

Mobile Geräte (Smartphones und Tablet-Computer)

Das Thema „**mobile Geräte**“ war eines der Top-Themen in 2011 und das wird es auch in 2012 sein. Der Medienmogul Rupert Murdoch kündigte Anfang des Jahres in einem Interview an, dass jeder, der es sich leisten kann, einen Tablet-Computer kaufen wird und dass es schließlich über eine Milliarde davon auf der Welt geben wird.
Auch noch zu Weihnachten 2011 sind Elektronikgeschenke hoch im Kurs: Laut einer Umfrage des Hightech-Verbands BITKOM wollen 13% der Deutschen einen Tablet-Computer und sogar 16% Smartphones verschenken oder anschaffen.[1] Es wird erwartet, dass allein in Deutschland 2,1 Millionen Tablet-Computer verkauft werden und damit im Gegensatz zum Vorjahr ein Absatzplus von 162% erreicht wird.[2]

Beliebt sind dabei seit längerem Mobilgeräte, die mit dem Betriebssystem Android ausgestattet sind. So erreichte das Android OS auch im dritten Quartal dieses Jahres die absolute Mehrheit im Marktanteil der mobilen Alleskönner: 52,5% aller in diesem Zeitraum verkauften Smartphones hatten dieses Betriebssystem, vor Symbian (16,9%) und Apple (15,0%).[3] Diese nun etablierte Führung in der Gunst der Kunden ist auch für Schadcode-Autoren ein klares Zeichen dafür, dass sie sich auf diese Plattform konzentrieren können, um ihren Nutzen aus der hohen Verbreitung der Geräte zu ziehen.

Der komfortabelste Weg, den Schadcode zu verbreiten, bieten dabei die Applikationen, kurz Apps. Jeder Besitzer eines von Google zertifizierten Android-Geräts kann mit seinem Google-Account kinderleicht Apps im offiziellen Android Markt einkaufen oder alternativ auch in inoffiziellen Märkten oder von Webseiten herunterladen. Bösewichte verstecken ihren Schadcode in Apps, die entweder einer populären App zum Verwechseln ähnlich sehen oder sonst irgendwie das Interesse der Kundschaft wecken. Entschließt sich der Benutzer dann, die App auf seinem Mobilgerät zu installieren, ist es schon geschehen – das Telefon ist infiziert und der Schädling kann dem Besitzer auf vielfältige Art und Weise Schaden zufügen: Er kann SMS verschicken, SMS-Abos bei Premiumnummern abschließen, persönliche Daten stehlen, das Telefon ‚rooten', das Gerät in eine Spionage-Wanze verwandeln und vieles mehr. Das Tempo, in dem neue Schadfunktionen implementiert werden, nimmt merklich zu, wohingegen die Verfügbarkeit von Updates für das Android Betriebssystem mitunter erschreckend gering ist. Nicht selten wurde schon erwähnt, dass Android in Bezug auf Malware möglicherweise das neue Microsoft Windows sei – die Zahl der Malware steigt, aber das stoppt nicht die rasante Verbreitung des Betriebssystems.

Auswahl neuer Schadfunktionen - Mobile

Malware	Neue Funktion	Seit
FakePlayer	Premium-SMS	08/2010
Geinimi	Botnetz	12/2010
ADRD	SEO	02/2011
DroidDream	Root	03/2011
Plankton	Code nachladen	06/2011
Spitmo	Man in the middle Angriff	07/2011
NickySpy	Anrufe und Umgebungs-geräusche aufzeichnen; Botnetzfunktion per SMS	08/2011
Walkinwat	Cyberbullying	10/2011
RuFraud	Premium-SMS in Mitteleuropa	12/2011

Aktuell werden schädliche Applikation ausschließlich vom Benutzer selbst installiert, nachdem man ihn mit Täuschungen, Tricks und Überredungskunst (Social Engineering) dazu gebracht hat. Die Mobilgeräte haben jedoch so vielfältige technische Möglichkeiten, dass es nur noch eine Frage der Zeit ist, bis wir automatischen Angriffen und Infektionen begegnen werden, bei denen der Benutzer nicht aktiv beteiligt ist. Wir erwarten, dass solche automatisierten Angriffe 2012 erstmals in freier Wildbahn durchgeführt werden, wahrscheinlich in Form von Drive-by-Infektionen, ausgelöst von

[1] http://www.bitkom.org/70427_70422.aspx
[2] http://www.bitkom.org/de/presse/8477_70631.aspx
[3] http://www.gartner.com/it/page.jsp?id=1848514

besuchten Webseiten – so, wie es bei Computer Malware schon etabliert ist. Die entsprechenden Machbarkeitsnachweise (Proof of Concept) existieren bereits seit Anfang des Jahres.

Gezielte Angriffe

Sollten diese Angriffe in der Zukunft gelingen, so müsste auch das Kapitel „**gezielte Angriffe**" um ein Gefahrenszenario erweitert werden, denn gerade Geschäftsleute sind lohnende Ziele für Cyber-Kriminelle und die Benutzung von mobilen Geräten im professionellen Kontext ist absolut keine Seltenheit. Der Anreiz, gerade die mobilen Alleskönner anzugreifen, die im professionellen Bereich genutzt werden, ist hoch, denn mit und in den Geräten sind viele Daten zentral abgreifbar.

Auch in 2011 hat ein besonderer Spionage-Schadcode Aufsehen erregt, der speziell für Firmen konzipiert wurde: DuQu. In vielen Kreisen irrtümlich als Nachfolger von Stuxnet bewertet, ist dieses Spionagewerkzeug jedoch nicht auf die Sabotage bestimmter Industriesteuerungsanlagen ausgerichtet. Die Vorstellung, dass Angreifer sich – teils mit hohem Aufwand – Zugang zu elementaren Steuerungssystemen verschaffen können ist spätestens seit den Berichten über Stuxnet in einer iranischen Uran-Anreicherungsanlage, bzw. dem Kernkraftwerk Buschehr keine Fiktion mehr.

DuQu ist anders, jedoch nur bedingt. DuQu ist in der Lage jegliche Art Firma ausspionieren, ist also mehr ein Datendieb als ein Spezial-Tool zur Zerstörung eines Angriffsziels. Es zielt darauf ab, möglichst viele Informationen zu sammeln und Angriffe, wie die von Stuxnet, vorzubereiten. Erschreckend ist nun auch, dass es Hinweise im Code von DuQu gibt, dass die gleiche Gruppe, die Stuxnet geschrieben hat, auch DuQu geschrieben hat. Aber nicht nur politisch motivierte Gruppen sind hier interessiert. Kaum auszudenken, was passiert, wenn solche Informationen von Kriminellen zur Erpressung genutzt werden.
Sogar das FBI erklärte im November, dass Cyber-Sicherheit „ein großer Wachstumsfaktor" sei und erwartet, dass die Größe ihrer „Cyber Einheit" sich in den kommenden 12 bis 18 Monaten verdoppeln wird. Auslöser für diese Einschätzung war das Eindringen von Hackern in die Steuerung der Versorgungssysteme dreier großer US-amerikanischer Städte.[4]

Großereignisse

Das personelle Aufrüsten der digitalen Ordnungshüter weltweit ist aber nicht nur auf die erwähnten „Targattacks" (= Targeted + Attacks) gegen Firmen zurückzuführen. Große Ereignisse werfen ihre Schatten voraus und im kommenden Jahr sind gleich mehrere **Großereignisse** weltweit im Fokus von Gesellschaft und Medien, wie z.B.

- Fußball Europameisterschaft (Polen & Ukraine) – 8. Juni bis 1. Juli 2012
- Olympische Spiele (England) – 27. Juli bis 12. August 2012
- Präsidentschaftswahlen (USA) – 6. November 2012

Allein die britische Metropolitan Police hat ein Budget von £600 Millionen, um sowohl traditionelle als auch Cyber-Gefahren aufzudecken und abzuwehren.[5] Zu den digitalen Gefahren bei den erwähnten sportlichen Großereignissen gehören dabei unter anderem:

[4] http://www.information-age.com/channels/security-and-continuity/news/1676243/hackers-accessed-city-infrastructure-via-scada-fbi.thtml
[5] http://news.sky.com/home/uk-news/article/15579707

- Spam-Wellen und Suchmaschinenmanipulationen für den Online-Betrug mit gefälschten oder gar nicht vorhandenen Eintrittskarten oder Memorabilien
- Gefälschte Ticket-Shop Webseiten für Phishing-Delikte
- Der Angriff auf offizielle Webseiten der olympischen Spiele durch potentielle Protestler
- Die Einrichtung von speziell präparierten WLAN Netzen für die Besucher vor Ort, mit denen dann Daten abgegriffen werden können.
- Nahfeldangriffe auf Smartphones

Die Liste der potentiellen Angriffe ist lang. Nicht zu vergessen, die gezielten Attacken gegen Infrastrukturen zur Sabotage oder Erpressung, wie bereits oben erwähnt.

Die Organisatoren und Verantwortlichen arbeiten im Vorfeld hart daran, durch ausreichend Tests, Technologien und unabhängige, exklusive Netzwerke für die Olympischen Spiele gegen Cyber-Angriffe bestens gerüstet zu sein.[6] Der Kampf gegen Ticketbetrug begann für die britischen Spezialeinheiten dabei schon Anfang 2010.[7]

Auch die Präsidentschaftswahlen in den USA werden in den Fokus von Angreifern rücken. Denkbare Szenarien sind Suchmaschinenmanipulationen zu scheinbar offiziellen Webseiten oder schockierenden Videos, bzw. exklusivem Fotomaterial (Black Hat SEO). Diese Form des Social Engineering wird häufig von Angreifern eingesetzt, um Internetnutzer durch die Sensationslust auf Webseiten zu locken, die dann Schadcode verbreiten. Auch in Spam E-Mails werden sich mit großer Wahrscheinlichkeit ähnliche Meldungen finden, die den Empfänger zum Besuch manipulierter Webseiten auffordern.

Ein weiterer möglicher Betrugsversuch in Bezug auf die weltweit mit Spannung betrachteten Wahlen könnten fingierte Angebote für Wähler sein, denen Geld für die Wahl eines bestimmten Wahlmannes versprochen wird. Um das versprochene Geld zu erhalten, müssten lediglich Bankdaten und persönliche Daten angegeben werden – eine klassische Phishing-Attacke, die u.U. sogar Auswirkung auf die Wahl haben könnte, wenn sie erfolgreich ist.

Im Bereich von Phishing könnte im kommenden Jahr zudem eine große Welle sehr ausgefeilter und gezielter Attacken auf die Computerbenutzer zukommen, als Folge der großen Datendiebstähle, die in 2011 für Aufsehen sorgten. Weltweit hatte der Hack in das Sony PlayStation®Network die Schlagzeilen gefüllt, da persönliche Daten von rund 77 Millionen Kunden entwendet wurden. Dies war nicht der einzige Fall von Datendiebstahl, jedoch einer der größten. Und die erbeuteten Daten könnten nun eingesetzt werden, um z.B. E-Mails zu erstellen, die den Empfänger hinters Licht führen, da sie mit echten Daten (Anrede, Adresse, etc.) gespickt werden können.[8] Denkbare Betrugsansätze wären unter anderem angebliche Rechnungen, Lotteriegewinne oder ähnliches.

Banking-Trojaner

Gerade versprochenes Geld ist ein häufiges Motiv, von dem sich Nutzer leider noch immer leiten lassen, wenn es um Phishing-Attacken geht. Geld ist allerdings auch das Hauptmotiv für die Großzahl der Cyber-Kriminellen, ihre illegale Arbeit aufzunehmen. Eins der beliebtesten Mittel zum Geldgewinn war 2011 der Einsatz von **Banking-Trojanern** und es ist nicht abzusehen, dass dieser Trend rückläufig ist, da auch hier, ähnlich wie bei den Mobilgeräten, die Zahl der Nutzer immer weiter zunimmt. Besonders Banking-Trojaner sind eine ernstzunehmende Gefahr, denn ein erfolgreicher Angriff hat oft nicht unerhebliche finanzielle Verluste für das Opfer zur Folge. Nach

[6] http://sports.espn.go.com/espn/wire?section=oly&id=7084244
[7] http://www.itpro.co.uk/619900/met-police-start-to-combat-2012-olympics-cybercrime
[8] http://blog.gdatasoftware.com/blog/article/sophisticated-spam-mails-after-data-leak-in-company-database.html

Auskunft von Eurostat haben bereits im vergangenen Jahr 43% der Deutschen Online-Banking genutzt. Damit liegt Online-Banking hierzulande voll im Trend und wird unlängst nicht mehr von einer kleinen Gruppe technisch versierter Anwender genutzt. Das BKA meldete für 2010 insgesamt 5.331 Fälle mit einer Schadenssumme von €21,2 Millionen, wobei jedoch außerdem von einer großen Dunkelziffer auszugehen ist, da dem BKA „lediglich ungefähr 40% der tatsächlichen Fälle bekannt werden."[9]

Virtuelle Währungen

Auch für die Akquirierung von **virtuellem Geld** könnten sich 2012 neue Möglichkeiten ergeben. Betrug mit virtuellem Geld lebt stark durch Web-Angebote wie Spiele oder virtuelle Gemeinschaften, in denen In-Game Käufe und Extraoptionen gegen reales Geld ermöglicht werden. In diesem breiten Segment gibt es mitunter sehr vielfältige und ausgefeilte Attacken (Phishing und Malware), die den Benutzern die virtuellen Taler, Goldmünzen und ähnliches abjagen wollen. Die verschiedenen virtuellen Währungen haben einen realen Gegenwert.

Eine der bekanntesten Online-Gelder ist dabei BitCoin. Um BitCoins zu bekommen, kann man zum Beispiel seinen Computer und dessen Rechenleistung für ausgelagerte Rechenoperationen zur Verfügung stellen. Ein kostenloses und gemeinnütziges Projekt, das solch einen Rechenansatz verfolgt, ist z.B. das SETI@home-Projekt der Universität von Kalifornien. Man bekommt bei diesem Projekt jedoch keine Vergütung. Andere Rechenprojekte jedoch vergüten die geleisteten Rechenoperationen und auf dieser Basis entstehen inzwischen so genannte Miner-Botnetze, wobei sich der Begriff vom englischen „to mine" (deutsch: abgraben) ableitet. Bösewichte infizieren also Computer mit einem Miner-Bot, der dann die fremden Geräte unter dem Namen der Angreifer in den Projekten arbeiten lässt. Die damit gewonnenen virtuellen Währungen können dann von den Angreifern später in bare Münze umgewandelt werden. Auch heimische Internetrouter könnten gewinnbringend in ein solches Miner-Botnetz integriert werden. Zwar ist ihre Rechenleistung bei weitem nicht so hoch, aber sie werden in der Regel selten aktualisiert oder gewartet – sie werden eingerichtet und laufen meist 24 Stunden am Tag, verbunden mit dem Internet.

Internetfähige Unterhaltungselektronik (Smart-TVs und Konsolen)

Abseits von klassischen Computerwegen führt der Blick in diesem Kontext zu **internetfähiger Unterhaltungselektronik**, wie z.B. webfähigen TV-Geräten oder auch modernen Spielekonsolen mit Internetanbindung. Die in diesen Geräten verbauten Grafikprozessoren sind sehr leistungsstark und könnten unter anderem für das ‚minen' von virtuellem Geld benutzt werden. Schaffen Angreifer es, auf die relativ ungeschützten Geräte, die nur recht selten aktualisiert werden, Schadcode aufzuspielen, könnten sie die hohe Rechenleistung der Grafikeinheiten missbrauchen.

[9] http://www.bka.de/nn_224082/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime2010,templateId=raw,property=publicationFile.pdf/cybercrime2010.pdf