Android im Visier

Eine Analyse der Ursachen

von Eddy Willems

Hatten sich Online-Kriminelle bisher bevorzugt auf das Betriebssystem Windows eingeschossen, so rückt Android zunehmend in den Fokus der Schadcode-Programmierer und -Betrüger. Eine Einschätzung, die von fast allen IT-Security-Anbietern bereits 2011 getroffen wurde – auch von G Data. Doch warum Android und nicht andere (mobile) Plattformen?

Dieser Frage geht G Data Security Evangelist Eddy Willems im Redpaper „Android im Visier – eine Analyse der Ursachen" nach. Dabei geht der Experte auf drei entscheidende Faktoren für kriminelle Handlungen ein: Motiv, Mittel und Gelegenheit.

1 Motiv

Cyber-Kriminalität ist zweifellos eng verbunden mit der flächendeckenden Verbreitung und Nutzung des Internets als Kommunikationsplattform. Ein weiterer Faktor, und dieser ist sicherlich von ebenso großer Relevanz, ist der Siegeszug und die daraus resultierende marktbeherrschende Stellung eines Betriebssystems: Microsoft Windows. Weit verbreitet ist dabei die Annahme, dass Windows ein schwaches System mit vielen Sicherheitslücken und somit der eigentliche Verursacher des Problems ist. Würden talentierte Hacker ein beliebiges Betriebssystem genau unter die Lupe nehmen, würden sie in puncto Schwachstellen ebenfalls fündig werden. Der eigentliche Grund, weshalb in den verschiedenen Versionen von Windows im

Laufe der Jahre so viele Sicherheitslücken gefunden wurden, sind die Millionen von Arbeitsstunden, die für die Suche nach derartigen Schwachstellen aufgewendet werden. Dieser enorme Zeitaufwand wird deshalb investiert, weil es sich für die Täter lohnt. Auf etwa 90 % aller Computer wird Windows eingesetzt. [1]

Somit wird das System von etwa 1,35 Milliarden Menschen weltweit genutzt (wenn man davon ausgeht, dass es heute weltweit etwa 1,5 Milliarden aktive Computer gibt). [2]

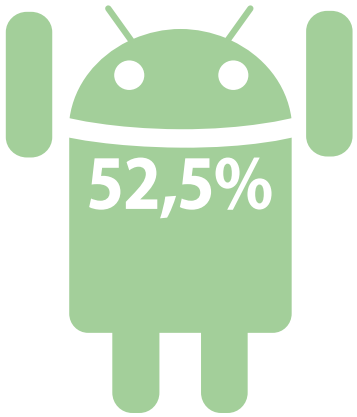
Findet man eine „geeignete" Sicherheitslücke und entwickelt daraufhin effiziente Malware, um diese zu nutzen, eröffnet sich ein potentieller Markt, der aus all diesen Rechnern besteht. Mit geeignetem Schadcode und fehlenden Sicherheitslösungen wäre es theoretisch möglich, die Kontrolle über diese PCs zu gewinnen, sie in Botnetze einzubinden oder personenbezogene Daten zu stehlen. Von Online-Kriminellen erbeutete Datensätze, wie Kreditkarteninformationen, vertrauliche Firmendaten, Zugangsdaten oder vollständige digitale Identitäten, haben sich unlängst zu einem florierenden Geschäft in den unzähligen Untergrundmärkten entwickelt. Man schätzt, dass die Geldsummen, die pro Jahr von Cyber-Kriminellen „erwirtschaftet" werden, bereits jetzt den Gesamtumsatz aus dem illegalen Drogenhandel übersteigen. Es ist also sehr lukrativ, Computerschädlinge für Windows-Systeme zu entwickeln.

Natürlich gab und gibt es neben Windows noch weitere Betriebssysteme, so erfreuen sich beispielsweise OS X von Apple und Linux einer stetig steigenden Popularität. Viele Menschen sind der Ansicht, dass diese Plattformen wesentlich sicherer sind als Windows. Diese Schlussfolgerung ließe sich jedoch nur dann verlässlich bestätigen, wenn man genauso viele Arbeitsstunden in die Suche nach Sicherheitslücken investieren würde, wie es bei Windows der Fall ist. Deshalb wäre es fatal und auch falsch, ein bestimmtes System per se als definitiv sicherer oder unsicherer zu bezeichnen.

Dasselbe gilt auch für mobile Plattformen. Seit vielen Jahren gibt es Smartphones, doch eine ähnlich bedeutsame Plattform wie Windows ist auf dem Mobilgerätemarkt nicht entstanden. Viele Jahre lang konnte keines der dortigen Betriebssysteme eine marktbeherrschende Position erlangen. Nach wie vor gilt die Theorie, dass all diese Systeme Schwachstellen haben, nach denen jedoch nicht gesucht wird, da sich der Zeitaufwand nicht lohnt. Dies ändert sich jetzt offenbar.

Im Jahr 2010 zeigte Android erstmals Ambitionen, eine herausragende Stellung im Bereich mobiler Geräte einzunehmen. Im Folgejahr erwiesen sich diese Ambitionen als realistisch, so zeigten Untersuchungen mehrerer Analysten und Fachleute im Jahr 2011, dass sich in der breiten Öffentlichkeit eine deutliche Präferenz für das System Android ergeben hatte. Gartner meldete, dass Android im dritten Quartal 2011 weltweit die absolute Mehrheit im Markt erreicht hatte: Android ist in diesem Zeitraum auf 52,5 % aller verkauften Smartphones installiert. An zweiter Stelle folgt Symbian mit nur 16,0 %. Die dritte Position nimmt Apple mit einem Anteil von 15 % ein.

Android war das einzige mobile Betriebssystem, das im dritten Quartal 2011 einen steigenden Marktanteil verzeichnen konnte. [3]
Die Sicherheitsindustrie behauptet daher nicht zu Unrecht, dass Android bei diesem Rennen die Nase wirklich weit vorn hat.



Diese Einschätzung teilen die Schadcode-Schreiber, da sie über Android-Geräte eine sehr große Zielgruppe von theoretisch 52,5 % aller verkauften Smartphones erreichen können, um Geld oder Daten zu stehlen.

So ergibt sich für Cyber-Kriminelle ein starkes Motiv, hochwertige und effektive Malware für die mobile Plattform zu entwickeln und zum Einsatz zu bringen.

2 Mittel

Vor dem Android-Erfolg gab es einen anderen Rivalen, der Aussichten auf die Spitzenposition hatte: Symbian. Warum aber reichte das starke Motiv zum Entwickeln von Symbian-Schadcode nicht für eine massenhafte Verbreitung von Schadprogrammen aus?

Der Grund ist das fehlende Mittel zur Verbreitung von Malware für Symbian. Allen mobilen Betriebssystemen ist eines gemein: Ihr Aufbau weicht stark von der Architektur von Microsoft Windows für PCs ab. Die Entwickler änderten Strukturen, die in früheren Computer-Betriebssystemen nicht so gut gelungen waren.
So entstanden wesentlich sicherere Plattformen, die allerdings immer noch zahlreiche Möglichkeiten eröffneten, Sicherheitslücken zu finden.

Ein Smartphone mit Malware zu infizieren und die Malware dann weiterzuverbreiten war mithilfe herkömmlicher Angriffsmethoden schwierig. Zwar fanden die Schadcode-Entwickler heraus, dass Bluetooth das effizienteste Mittel für Angriffe auf Symbian ist, doch für einen erfolgreichen Angriff ist die räumliche Nähe zum Zielgerät erforderlich und die Bluetooth-Verbindung muss zum Zeitpunkt des Angriffs eingeschaltet sein. Damit reduziert sich die Zielgruppe auf einen so kleinen Personenkreis, dass der Aufwand für die Schadprogrammentwicklung und die Attacke sehr unattraktiv ist.

Bei Android gibt es eine einfache Lösung für die Verbreitung von mobiler Malware: Apps. Diese werden von Smartphone-Nutzern auf der ganzen Welt manuell herunter geladen und installiert. Eine kostenlose, lokal vertriebene Applikation mit einer durchschnittlichen Popularität wird mehr als 10.000 Mal herunter geladen. Kostenfreie, international vertriebene mobile Anwendungen mit einer durchschnittlichen Beliebtheit erzielen sogar Download-Werte von über einer Million. Infizierte Apps, die in Google Play auftauchten, wie etwa jene, die den Trojaner DroidDream enthielten, wurden in wenigen Tagen über 250.000 Mal herunter geladen. Applikationen stellen somit ein sehr attraktives Mittel für die Verbreitung von Schadcode auf Smartphones und Tablet-PCs dar. Dank Social Engineering lassen sich die Programme zudem sehr attraktiv präsentieren, so dass die Anwender diese bereitwillig herunter laden und installieren. Bisher wurden in der Praxis noch keine automatischen Installationsvorgänge festgestellt - doch das ist möglicherweise nur eine Frage der Zeit.

3 Gelegenheit

Android ist nicht die einzige Plattform mit populären Apps. So war Apple bis zum zweiten Quartal 2011 [4] mit Applikationen viel erfolgreicher als Android. In der Zeit zwischen dem Niedergang von Symbian und vor dem spektakulären Erfolg von Android hatte Apple das bei Nutzern favorisierte mobile Betriebssystem. Aber weshalb konnte der Hersteller der Gefahr von Angriffen und schädlichen Apps so lange ausweichen? Schließlich gab es ein Motiv und mit den Applikationen auch ein theoretisches Mittel der Infizierung.

Die Antwort liegt in der mangelnden Gelegenheit: Bei Apple und Android unterscheiden sich die Pro-

zesse für die Entwicklung und Zulassung von Apps. In diesem Fall müssen wir einräumen, dass Apple offenbar das sicherere System besitzt. Das bedeutet aber nicht notwendigerweise, dass das Betriebssystem von Apple an sich sicherer ist als Android. Aufgrund der geschlossenen Architektur ist es jedoch schwerer, in das Apple-Betriebssystem einzudringen und falls doch eine lohnende Schwachstelle entdeckt wird, ist das Einschleusen von schadhaften Apps in den Appstore äußerst schwierig. Apple schreibt sehr umfangreiche Verfahrensschritte für die Erstellung und Zulassung von neuen Apps vor, so dass Kriminelle kaum eine Chance haben, ihren Schadcode dort einzustellen.

Bei Android sieht dies ganz anders aus. Android ist ein Semi-Open source-Betriebssystem, ein Großteil des Programmcodes ist daher öffentlich zugänglich. Dadurch können Sicherheitslücken wesentlich einfacher entdeckt und sowohl Apps, als auch schädliche Applikationen leichter entwickelt werden.

Aufgrund dieser Fakten und eines nicht sehr strengen Zulassungsverfahrens für neue Apps, ist Android ein wesentlich einfacheres und lohnenderes Ziel für Schadcode-Angriffe, als es Apple je war. Die Android-Plattform bietet daher viele Gelegenheiten für kriminelle Handlungen.

Ein weiterer Punkt, der die Entwicklung von schädlichen Android-Apps für Cyber-Kriminelle noch attraktiver macht, ist die Art und Weise, wie App-Berechtigungen erteilt werden. Bei der Installation ist es dem Anwender nicht möglich, nur spezifische Berechtigungen zu erteilen. So können Anwender eine App nur mit dem vollen Umfang an Funktionen und Berechtigungen installieren. Wenn Nutzer eine weitere Applikation des gleichen Herstellers bzw. Entwicklers herunterladen, vom dem zuvor schon eine App installiert ist, ist es also nicht möglich deren Berechtigungen automatisch auf die neue Anwendung zu übertragen. Das Android-System verlangt immer eine Bestätigung der angeforderten Befugnisse. Nur wenn zwei Apps die exakt gleichen Zertifikate verwenden, ist zumindest ein Datenaustausch möglich, weiterhin aber nicht die Übertragung von Berechtigungen. So kann eine Applikation beispielsweise Daten ausspähen, die von einer weiteren App schließlich unbemerkt verschickt werden. Hierzu müssen die Kriminellen ahnungslose Nutzer aber dazu bringen, gleich zwei verschiedene Anwendungen zu installieren. Einfacher ist für die Täter das Einschleusen von schädlichen Apps, die das Android-Gerät nach der Installation rooten und dann weiteren beliebigen Schadcode aus dem Internet nachladen.

Bedingungen für die Veröffentlichung von Apps für Apple bzw. für Android	Apple	Android
Regisitrierungsgebühr für Entwickler (per Kreditkarte)	€ 99	€ 25
Jährliche Gebühr für Entwickler (per Kreditkarte)	€ 99	–
Überprüfung der Apps vor der Veröffentlichung im Markt?	Ja	Nein

Man kann sich leicht vorstellen, wie sehr sich Cyber-Kriminelle über Apps freuen, mit denen die Nutzer über das Mobiltelefon Zahlungen tätigen oder mobiles Online-Banking betreiben können. Auf diese Weise lässt sich ggf. viel schneller Beute machen als durch den Abschluss eines teuren SMS-Dienstvertrags für das infizierte Telefon – auf letztere Weise wurde bisher hauptsächlich Kasse gemacht. Im Fernen Osten und auch in Russland genießen Bezahlfunktionen mit dem Mobiltelefon immer größere Popularität.

Wir stellen fest, dass sich Malware-Apps, die diese Möglichkeit ins Visier nehmen, in diesen Regionen wesentlich stärker verbreiten als anderswo. Das zeigt, dass Cyber-Kriminelle den Geldströmen folgen.

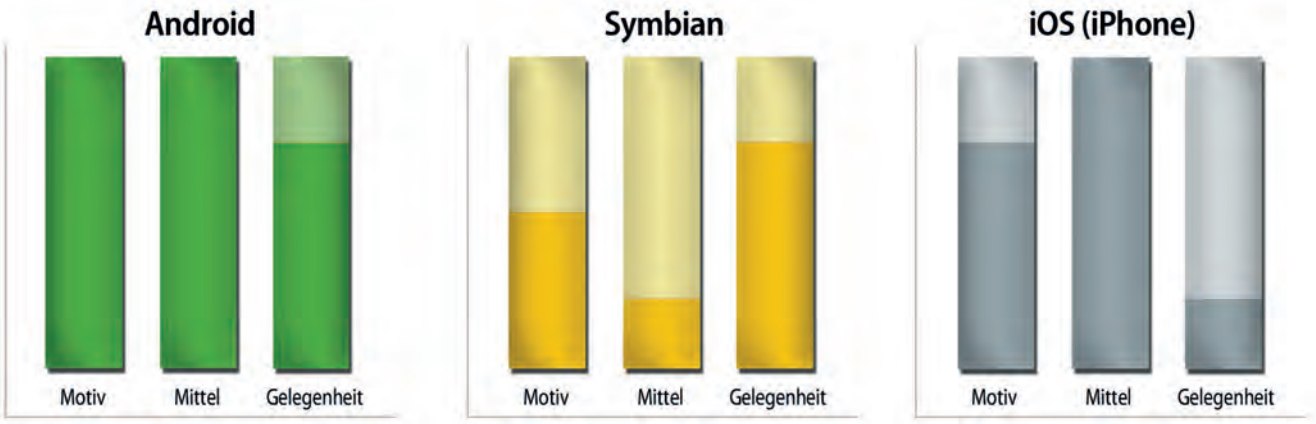
4 Schlussfolgerung

Nach der Analyse der verschiedenen Elemente krimineller Handlungen und der Nutzungsmöglichkeiten dieser Elemente bei den drei meist verbreiteten mobilen Betriebssystemen, kommen wir zum Fazit. Die unten dargestellten Säulen stellen die drei Elemente dar. Sind alle drei Säulen zu 100 % gefüllt dargestellt, handelt es sich um ein ideales Angriffsziel für Cyber-Kriminelle.

Android ist die einzige Plattform, die dem idealen Angriffsziel nahe kommt. Der einzige fehlende Aspekt in punkto Gelegenheit ist die bisher nicht vorhandene Möglichkeit, Schadcode-Apps ohne Nutzer-Interaktion zu installieren bzw. ohne den Apps die jeweils eingeforderten Berechtigungen zu erteilen. In der Praxis haben wir bisher noch keine mobilen Anwendungen kennengelernt, die sich wie beim PC ohne Interaktion selbst installieren.

Wir gehen jedoch davon aus, dass dies nur eine Frage der Zeit ist. Es ist zu befürchten, dass Android tatsächlich zur idealen Plattform von Malware-Autoren und Cyber-Kriminellen werden könnte, wenn auch diese letzte Hürde genommen wird. ■

Inwieweit bieten mobile Betriebssysteme die drei Elemente krimineller Handlungen?



Eddy Willems
G Data Security Evangelist

Der Belgier Eddy Willems ist im Bereich IT-Sicherheit schon seit 1989 aktiv.

In den vergangenen 20 Jahren war er für einflussreiche Institute wie EICAR, dessen Mitbegründer er war, für verschiedene CERT-Organisationen, die internationale Polizei sowie für WildList und kommerzielle Unternehmen wie NOXS und Kaspersky Lab Benelux tätig.

In seiner Position als Global Security Officer und Security Evangelist bei den G Data SecurityLabs bildet Eddy Willems die Schnittstelle zwischen technischer Komplexität und dem Anwender. Er ist zuständig für eine klare Kommunikation der G Data SecurityLabs in der Sicherheits-Fachwelt, bei Presse, Händlern, Wiederverkäufern und Endkunden und er spricht häufig auf internationalen Konferenzen, wie Virus Bulletin, EICAR, InfoSecurity, AVAR, RSA etc.

Mitgliedschaften/Organisationen:
EICAR (Mitbegründer) • AMTSO

Fußnoten:

[1] http://en.wikipedia.org/wiki/Microsoft_Windows#Usage_share

[2] http://www.worldometers.info/computers/

[3] http://www.idc.com/about/viewpressrelease.jsp?containerId=prUS22689111&sectionId=null&elementId=null&pageType=SYNOPSIS

[4] http://www.gartner.com/it/page.jsp?id=1848514

Redaktionskontakt
G Data Software AG

International:
Thorsten Urbanski (Hauptsitz in Deutschland)
Königsallee 178 b, 44799 Bochum
Tel.: +49 (0) 234 97 62 0
E-mail: press@gdatasoftware.com
www.gdatasoftware.com

Deutschland – Österreich – Schweiz:
Thorsten Urbanski
Tel.: +49 (0) 234 97 62 239
E-mail: thorsten.urbanski@gdata.de

Kathrin Beckert
Tel.: +49 (0) 234 97 62 376
E-mail: kathrin.beckert@gdata.de

www.gdata.de

Benelux & Großbritannien:
Daniëlle van Leeuwen
Tel.: +31 (0) 20 808 08 35
E-mail: danielle.van.leeuwen@gdata.nl
www.gdata.nl

Italien:
Eliana Squillacioti
Tel.: +39 (0) 51 61 88 712
E-mail: eliana.squillacioti@gdata.it
www.gdata.it

Spanien & Lateinamerika:
Ignacio Heras
Tel.: +34 917 45 30 73
E-mail: pr-espana@gdatasoftware.com
www.gdata.es

Frankreich & Nordafrika:
Jérôme Granger
Tel.: +33 (0) 141 48 51 46
E-mail: jerome.granger@gdata.fr
www.gdata.fr

G Data Software AG
Königsallee 178b
D-44799 Bochum

Die G Data Software AG, mit Unternehmenssitz in Bochum, ist ein innovatives und schnell expandierendes Softwarehaus mit Schwerpunkt auf IT-Sicherheitslösungen. Als Spezialist für Internetsicherheit und Pionier im Bereich Virenschutz entwickelte das 1985 in Bochum gegründete Unternehmen bereits vor mehr als 20 Jahren das erste Antiviren-Programm.

G Data ist damit eines der ältesten Security-Software-Unternehmen der Welt. Seit mehr als fünf Jahren hat zudem kein anderer europäischer Hersteller von Security-Software häufiger nationale und internationale Testsiege und Auszeichnungen errungen als G Data.

Das Produktportfolio umfasst Sicherheitslösungen für Endkunden, den Mittelstand und für Großunternehmen. G Data Security-Lösungen sind in weltweit mehr als 90 Ländern erhältlich.

Weitere Informationen zum Unternehmen und zu G Data Security-Lösungen finden Sie unter ***www.gdata.de***