Android is the first platform after Microsoft Windows to become a prime target for cyber criminals. This statement has been made by most IT security specialists in 2011, including G Data. But why Android over other (mobile) platforms?

This paper attempts to shed light on this matter and show that the three crucial factors for any crime: motive, means and opportunity, are now present in Android.

1 Motive

Cybercrime started with Microsoft Windows. The reason of this is not, as many people tend to think, because Windows is a weak system, with many security holes. If any talented hacker were to look closely at any operating system, he/she would find vulnerabilities.

The reason why so many leaks have been found in Windows versions over the years, is because millions of man hours are spent searching for them. This time investment is only done, because there is a positive pay off. About 90% of computer users use Windows, which translates into approximately 1.35 billion people around the world (estimating that there are about 1.5 billion active computers in the world today).

Finding a “good” security hole and writing some “efficient” malware to exploit it, means a potential “market” of all those computers. With the right mal-
ware, it is possible to grab control of those computers, by hooking them to a botnet, and browsing through the computer to search for personal and financial data that can be used for either selling in the underground market, or using the found identity for all kinds of criminal activities. The money that is made by cyber criminals per year is estimated to be of a bigger volume than the turnover of the drugs industry. In short: it pays to invest time into writing malware for Windows.

Of course there have been, and still are, other popular platforms besides Windows. Apple's OS X and Linux for instance, are still growing in popularity. Many people believe these systems to be far safer than Windows. However, that is a conclusion that can only be reached with certainty after putting as many man hours into searching for weaknesses as has been done with Windows. This, of course, has not happened, so we refrain from celebrating the safety of one system over another.

This theory also applies to mobile platforms. Smartphones have been around for many years. Even though IDC reported that more smartphones are being sold than PC's in February of 2011, a mobile counterpart of Windows did not surface.

Many different operating systems coexisted, not one much more popular than the other for many years. The theory that all of these systems have their weaknesses, but not many people were looking for them, because it would not be worth their time investment, still holds up. But this fact seems to be changing.

In 2010, Android showed its first signs of ambitions to rule the mobile world. In 2011, the ambitions proved to be realistic. Research by several analysts and researchers in 2011 shows a clear preference of the public for the Android system. Gartner reported that Android reached the absolute majority of the market share worldwide in the third quarter of 2011: 52.5% of all sold smartphones in that period used Android.

Number two was Symbian, with only 16.0%. The third position was held by Apple, with 15%.

Of all operating systems, Android was the only one that grew its market share in this third quarter. The security industry therefore now feels it is safe to say Android is in fact the winning horse of this race. And the malware writers agree.

The possibility of reaching a large public with Android and to steal money from 52.5% of all smartphone users provides a strong motive for malware writers to create high quality malware for this particular platform.
Means

Before Android, there was another contender that seemed to be winning the race: Symbian. Why was a strong motive for creating malware for Symbian not enough for an epidemic outburst of Symbian malware? This is due to a lack of means to spread Symbian malware.

All mobile operating systems have one thing in common: their architecture is very different to the architecture of Microsoft Windows for computers. In general, it seems developers have looked closely at “what went wrong” with the early operating systems for PCs and created systems that are far safer (although there are still plenty of possibilities to find vulnerabilities in them).

Infecting a smartphone and then spreading the malware further is not easy through traditional attacks. The most effective way for attacks on Symbian proved to be through Bluetooth. But this required physical proximity of a smartphone that had its Bluetooth connection switched on for a successful attack. This reduces the target audience to such a small number, that spending time on writing malware for Symbian was very unattractive.

In the case of Android, there is a simple solution to spreading malware: apps. They are downloaded and installed manually by smartphone owners all over the world. A free local app with average popularity is downloaded over 10,000 times. International free apps of average popularity can get downloaded over 1 million times. Fraudulent apps that appeared in the Android Market, like the ones that harbored the Trojan horse DroidDream, got downloaded over 250,000 times in only a few days. Apps are thus a very attractive means of spreading malicious code to smartphones. Social engineering makes apps look very attractive and persuades users to download and install them. Up to now, automatic installs have not been seen in the wild, but that might just be a matter of time.

Opportunity

But Android is not the only platform with popular apps. In fact, Apple was, until the second quarter of 2011, far more successful with apps than Android. And Apple seemed to be the winning horse for quite some time, right after Symbian’s downfall and before Android’s spectacular rise. So why has Apple dodged the bullet for all this time? There was a motive, and the apps provided a theoretical means for infection.

The answer comes down to opportunity. Apple and Android have different processes of app creation and app admissions. In this case, we need to acknowledge, that Apple seems to have a safer system. That is not to say the operating system of Apple in itself is safer than Android. It is, however, more difficult to investigate Apple’s operating system due to its closed nature. And when a weakness is found, it is very difficult to sneak an exploiting app into the Appstore, because of the extensive processes Apple has in place for creating and authorizing new apps.

With Android, this situation is completely different. Android is a semi open-source platform, meaning that much of the code is available for everyone to see.

<table>
<thead>
<tr>
<th>Conditions for publishing an app for Apple and Android</th>
<th>Apple</th>
<th>Android</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration fee for publishers (by credit card)</td>
<td>€ 99</td>
<td>€ 25</td>
</tr>
<tr>
<td>Annual fee for publishers (by credit card)</td>
<td>€ 99</td>
<td>–</td>
</tr>
<tr>
<td>App checked by market before publishing on technical level?</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
This makes it far easier to find security holes. It also makes it much easier to create an (exploiting) app. Other than Apple, Android relies on users to keep their smartphones clean by letting them determine whether or not certain permissions are granted to an app or not. The presumption that users are always alert and attentive when it comes to installing apps, is slowly proving to be a rather naïve one.

These facts, combined with a not very stringent process of authorizing new apps, make Android a much easier target than Apple ever was, and thus giving ample opportunity for the crime.

A further feature that makes developing Android apps interesting for cyber criminals is the way that app permissions are granted. During installation it is not possible for the user to grant only specific permissions and therefore an app must be installed with its complete functions and permissions. If users download an additional application from a particular publisher or developer from whom they already have an application installed, it is not possible to automatically transfer the existing permissions to the new application.

The Android System always demands that the user confirms the permissions to be granted. If two applications share the exact same certificate, it is possible to transfer data between them but it is still not possible for permissions to be transferred. This makes it possible for example for an application to spy out data that is then transmitted by a further app covertly. To make this viable however, criminals must persuade unwary users to install two different apps. It is simpler for the offenders to smuggle in a malicious app that can root the Android device after installation and which will then download further arbitrary malicious code from the Internet.

It is easy to imagine how excited cyber criminals are about apps which allow users to pay by mobile phone, or participate in mobile banking. This can be profitable in a much faster way than subscribing the hijacked phone to an expensive sms service, which is one of the main ways they have historically made money. In the Far East and also in Russia “paying with your mobile” is becoming very popular. We see that malicious apps aimed at this possibility are spread in those areas much more than elsewhere, which implicates that cyber criminals are following the money.

Besides these effective measures, Apple also has a mechanism in place to quickly remove malicious apps from any iPhone. This way the efforts that go into creating a malicious app and having it published in the Appstore are struck down within minutes.

4 Conclusion

Having looked at the different elements of crime and to what degree the three most popular mobile operating systems offer these elements, it is time to make the final comparison. The bars below represent the three elements. In order to be a perfect target for cyber criminals, all bars should be 100% filled. Android is the only system that comes close to being the perfect target. The only part that’s missing, from an opportunity point of view, is the possibility to install fraudulent apps on a system without the owner of the device having to approve the permissions of the app. Even though we have not yet seen apps that can completely self install in the wild, we estimate this is only a matter of time. We fear that, once that last hurdle is taken, writing malware for Android will indeed be the perfect crime.
Eddy Willems
G Data Security Evangelist
Belgian Eddy Willems has been active in the field of IT security for over two decades since 1989. In that period, he has worked for influential institutes, such as EICAR, of which he is a co-founder, several CERT associations, international Police Forces, and the organisation behind the WildList, as well as for commercial companies, such as NOXS and Kaspersky Lab Benelux.

In his position as global security officer & security evangelist at G Data, Eddy Willems forms the link between technical complexity and the user. He is responsible for the clear communication of G Data’s SecurityLabs towards the security community, press, distributors, resellers and end users and often speaks at international security conferences like Virus Bulletin, EICAR, InfoSecurity, AVAR, RSA, etc.

Memberships / Organisations:
EICAR, member (co-founder) • AMTSO, member

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

Editorial Contact
G Data Software AG

International:
Thorsten Urbanski (Headquarters Germany)
Königsallee 178 b, 44799 Bochum, Germany
Phone: +49 (0) 234 97 62 0
E-mail: press@gdatasoftware.com
www.gdatasoftware.com

Germany – Austria – Switzerland:
Thorsten Urbanski
Phone: +49 (0) 234 97 62 239
E-mail: thorsten.urbanski@gdata.de
Kathrin Beckert
Phone: +49 (0) 234 97 62 376
E-mail: kathrin.beckert@gdata.de
www.gdata.de

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

Italy:
Eliana Squillacioti
Phone: +39 051 6188712
E-mail: eliana.squillacioti@gdata.it
www.gdata.it

Spain & Latin America:
Ignacio Heras
Phone: +34 917 45 30 73
E-mail: pr-espana@gdatasoftware.com
www.gdata.es

France & North Africa:
Jérôme Granger
Phone: +33 (0) 141 48 51 46
E-mail: jerome.granger@gdata.fr
www.gdata.fr

With headquarters in Bochum, Germany, G Data Software AG is an innovative and rapidly expanding software house that focuses on IT security solutions.

A specialist in Internet security and a pioneer in the field of virus protection, the company, which was founded in Bochum in 1985, developed the first anti-virus program more than 20 years ago.

Therefore, G Data is one of the oldest security software companies in the world. For over five years now, no other European security software provider has won as many national and international tests and awards as often as G Data.

The product range consists of security solutions for end customers and medium to large-sized enterprises. G Data security solutions are available in more than 90 countries around the world.

You can find more information about the company and G Data security solutions at www.gdatasoftware.com

Copyright 2012 G Data Software AG. All rights reserved. No portions of this document may be reproduced without prior written consent of G Data Software AG, Germany. Specifications are subject to change without notice. Microsoft and Windows are registered trademarks of Microsoft Corporation. Android is a trademark of Google Inc. Use of this trademark is subject to Google Permissions. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.