G Data
Mobile MalwareReport

Half-yearly report
January – June 2013

G Data SecurityLabs

G Data. Security Made in Germany.

Contents

Copyright © 2013 G Data Software AG

At a glance

- The Android operating system is the number 1 attack target in the mobile area.
- More than 900 million Android mobile devices have now been activated.
- Market researchers expect the smartphone segment to grow by 33% per year.
- According to forecasts, 20% of smartphones and tablet PCs will have security solutions installed by 2015.

- The number of new malware samples increased steeply in the first half of 2013 with 519,095 new malware files compared to 185,210 in H2 2012.
- On average, G Data SecurityLabs received 2,868 new Android malware files a day!

- Malware tool kits make it easy for inexperienced attackers to create malware code.
- Due to the use of mobile malware toolkits, the number of malware strains will continue to experience strong growth over the next few months.
- Experts at G Data SecurityLabs expect the number of new Android malware programs to triple over the next six months.

- Android.Backdoor.Obad.A exploits three security vulnerabilities to attack Android mobile devices.
- Trojan FakeSite.A, aka Perkele, made a name for itself because it can be combined with any malicious code that executes webinject attacks in the browser. It is thus a flexible cross-platform Trojan that is relatively easy to create.
- A legitimate remote access tool called "AndroRAT" that was created for university purposes has been abused by cyber criminals and rewritten for their malicious purposes.

- Some new malware tries to evade automated and manual analyses and is equipped with elaborately camouflaged program code.
- Fast money is still the main motivation for attacks. However, new backdoor variants also perform more complex, longer term attacks.

Android: growth across the board

Long gone are the days in which malware for mobile devices like smartphones and tablet PCs was a rarity. Due to the ever growing sales figures of these devices, cyber criminals have not just noticed this platform but have now defined it as a worthwhile target. The focus here is clearly on the Android operating system, which is now in use on more than 900 million activated devices.[1] Market researchers are expecting sales figures in the smartphone segment to continue to rise (+33% per year), partly due to the falling average price of the all-rounder: back in 2011, one of these mobile devices cost $443 (approx. €337), compared to $372 (approx. €283) on average in 2013, and prices are expected to fall to $309 (approx. €235) by 2017.[2]

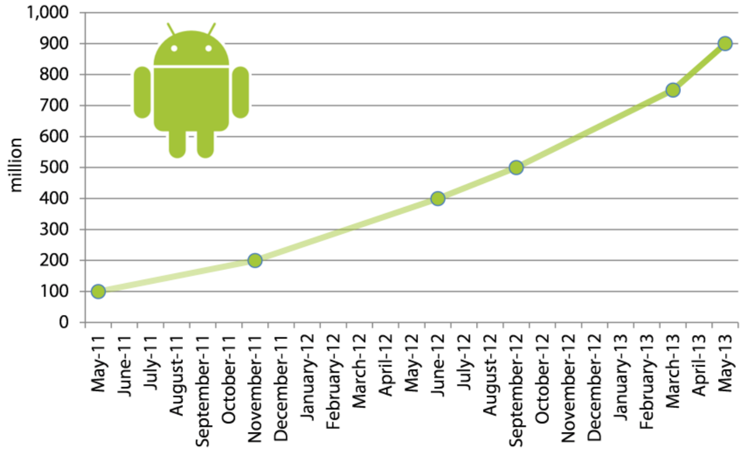


Figure 1: *Number of activated Android devices.*

As a consequence of this popularity, a varied economic structure based on attacks on smart mobile devices has gradually developed, with monetary reasons still the main motive for attacks. These days, the benefit cost ratio is quite high.

Malware authors create malware and use it for attacks, but often sell it on dubious online markets as well. Developer accounts that are registered and verified on Google's official app market (Google Play) are also traded.[3] Of course, offering all sorts of malicious apps on Google Play gives the attackers much better chances of spreading them. Hence, accounts that can be registered for $25 (approx. €19) are then traded for $100 (approx. €76). Gmail accounts are also popular prey of course, especially when they grant access to Android mobile devices and all the personal data and shopping options related to them. There are now audit tools that can determine the value of one's own Gmail account.[4]

Toolkits are a technology in the mobile sector that enables attackers to create malware in no time at all with little technical knowledge and just a few clicks of the mouse. As yet, this technology is not too widespread. These toolkits are tools for creating malicious code based on a modular principle. While this improves the quality of the malware code through ready-programmed and tested malware routines, it fundamentally increases the number of infected apps. Tried and tested popular Trojan horses are particularly favored by attackers, especially the Android.FakeInstaller family, which is described on page 4.

[1] http://venturebeat.com/2013/05/15/900m-android-activations-to-date-google-says/
[2] http://www.idc.com/getdoc.jsp?containerId=prUS24143513
[3] http://krebsonsecurity.com/2013/03/mobile-malcoders-pay-to-google-play/
[4] https://cloudsweeper.cs.uic.edu/

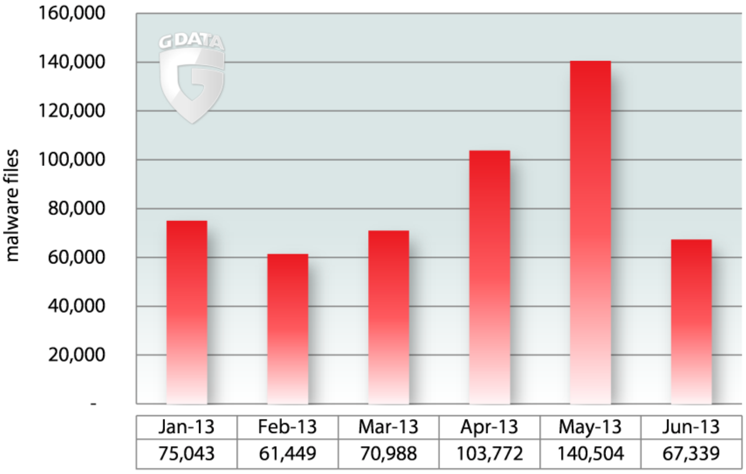
Copyright © 2013 G Data Software AG

Android malware code is still on the rise

The malware count for Android is based on the evaluation of the number of new malware strains. In the first half of 2013, G Data SecurityLabs detected a total of 519,095 new malicious files.[5] This signifies a 180% increase compared to the second half of 2012 (185,210[6]) and more than sixteen-fold growth compared to the first half of 2012 (29,595[6]).

On average, G Data SecurityLabs received 2,868 new Android malware files a day!

Based on the properties of the malicious code[7], the individual files can be assigned to certain families. 275,398 of the new malware files could be clearly assigned to certain malware families[8], as illustrated in Figure 3. Within the families, 1,919 different malware variants could be determined. These 1,919 malware variants are based on 454 different malware families. In the last six month period, the experts recorded 203 new families. Table 1 shows a list of the most productive families, that is, the families with the most variants.



Jan-13	Feb-13	Mar-13	Apr-13	May-13	Jun-13
75,043	61,449	70,988	103,772	140,504	67,339

Figure 2: *Distribution of new malware files that could be assigned to H1 2013.*

It comes as no surprise that Trojan horses are still the dominant type of malware, as they have been in the PC malware sector for years. In the mobile sector, the Trojans' share of all new samples is about 46%, with a staggering 86% in the malware classified in families.

The Android.Trojan.FakeInstaller family, in particular, has been contributing significantly to the Trojans' top position over the last six months: 59% of malware classified in families belongs to this family:

Family	# variants
Trojan.Agent	266
Trojan.FakeInstaller	168
Backdoor.GingerMaster	156
Trojan.SMSAgent	100
Trojan.SMSSend	92

Table 1: *List of Android families with the most variants in H1 2013.*

[5] Android malware can be identified on the basis of several files. An installation package (APK) contains many other files, which contain, among other things, the code and the properties. With this method of counting, detections of APK and their respective components are summarized as one malicious file, even if there are several files in our library.

[6] The retrospective figures for this half of the year are higher than in previously published reports. In some cases, G Data SecurityLabs receive collections of files with a large number of new malicious files collected over an extended period of time and these sometimes contain older files, which are then assigned to the respective month.

[7] The count of signatures and variants is based on the signatures from the G Data MobileSecurity products.

[8] Of 519,095 samples, 243,697 samples were identified as "potentially unwanted programs" or with generic signatures.

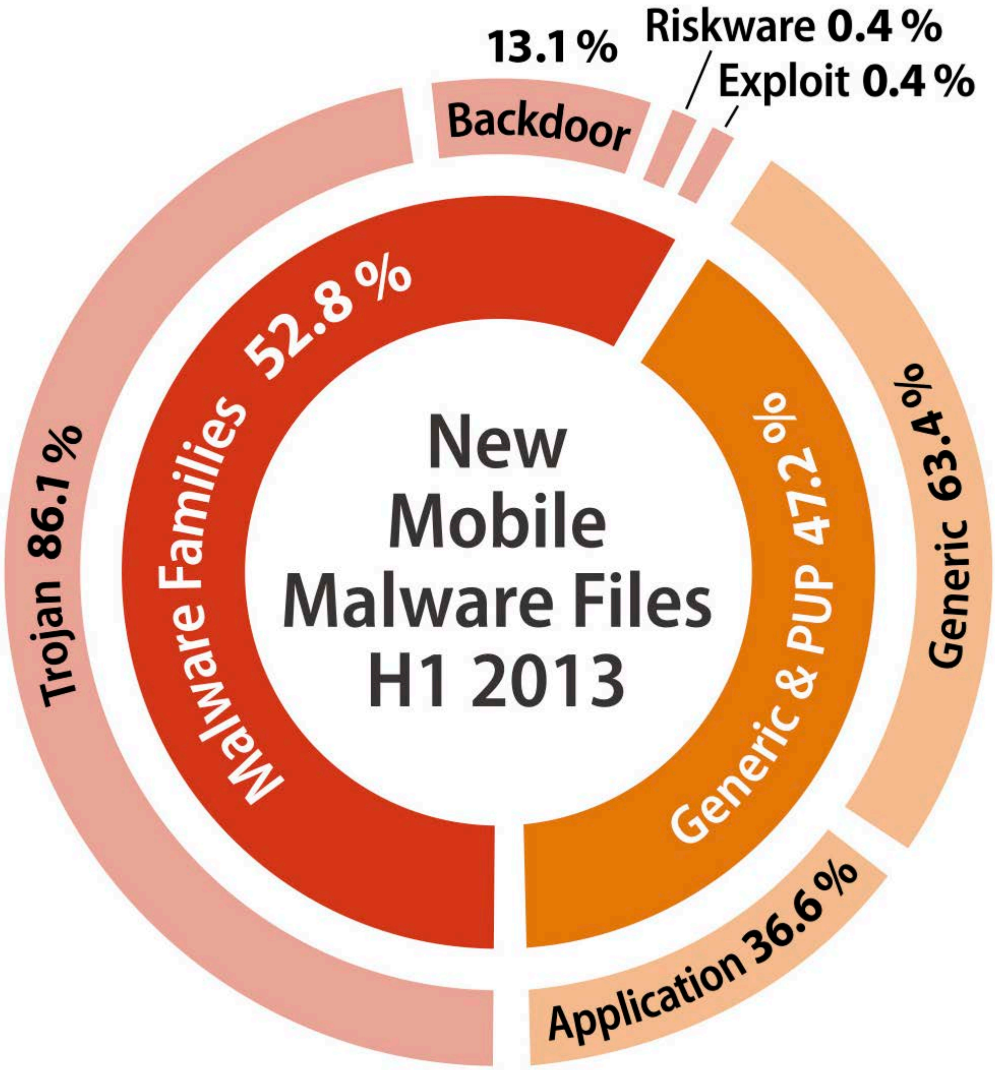


Figure 3: *Composition of new malware files from H1 2013 in percent.*

The inner circle describes the distribution of new malware in files that could be classified in malware families and those files that were detected as generic, as well as files recognized as potentially unwanted programs (PUP for short).
The outer circle illustrates the respective assignment of types as performed using the signatures of G Data MobileSecurity products.

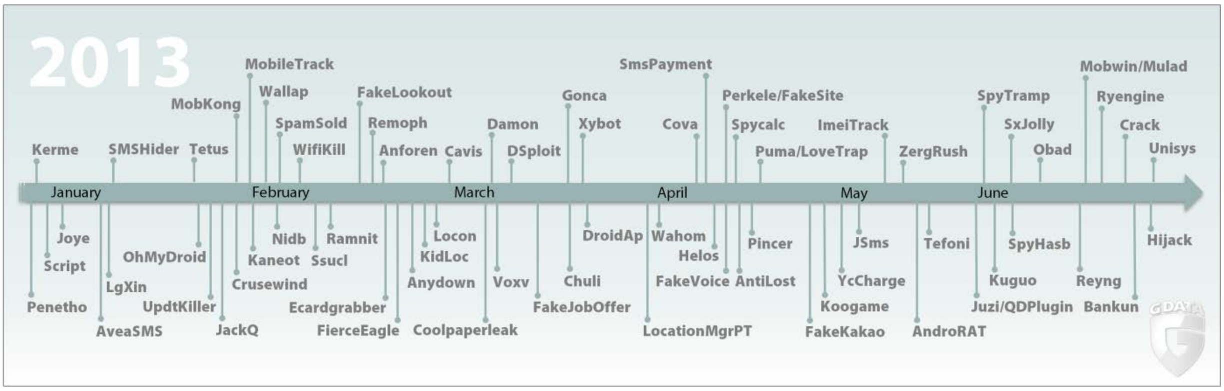


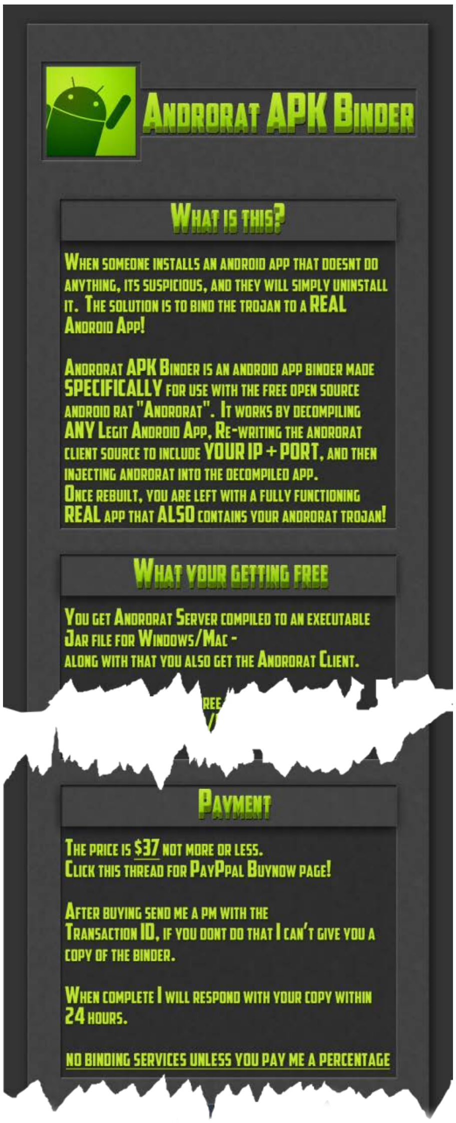
Figure 4: *Selection of malware for mobile devices in 2013.*

Copyright © 2013 G Data Software AG

AndroRAT and malware kits

The risk for Android mobile devices is on the rise globally, as is impressively illustrated by rising detection numbers and the proliferation of newly detected malware files. One reason for the rapid growth of malware is the availability of malware kits, which enable even inexperienced malware programmers to create functioning, manipulated apps using a type of modular system.

A wide range of tools for creating fully automated Android malware, such as the wide-spread Android.Trojan.FakeInstaller[9], have been available for some time. The well-known FakeInstallers are versatile and plentiful.[10] However, they only offer relatively few malicious functions and victims often remove them after a short while as they appear unnecessary for the app. FakeInstallers are chargeable installers for popular programs that send premium SMS messages when executed and therefore cost the user money in more ways than one.



Androrat APK Binder

What is this?

When someone installs an android app that doesnt do anything, its suspicious, and they will simply uninstall it. The solution is to bind the trojan to a REAL Android App!

Androrat APK Binder is an android app binder made SPECIFICALLY for use with the free open source android rat "Androrat". It works by decompiling ANY Legit Android App, Re-writing the androrat client source to include YOUR IP + PORT, and then injecting androrat into the decompiled app.
Once rebuilt, you are left with a fully functioning REAL app that ALSO contains your androrat trojan!

What your getting free

You get Androrat Server compiled to an executable Jar file for Windows/Mac -
along with that you also get the Androrat Client.

Payment

The price is $37 not more or less.
Click this thread for PayPpal Buynow page!

After buying send me a pm with the Transaction ID, if you dont do that I can't give you a copy of the binder.

When complete I will respond with your copy within 24 hours.

NO BINDING SERVICES UNLESS YOU PAY ME A PERCENTAGE

Screenshot 1: *Excerpts from an advertisement for "AndroRAT APK Binder"*

A trend towards manipulating fully functional apps has been emerging recently. This is partly due to the fact that users leave functioning apps on their devices longer than basically non-functional Trojans like FakeInstaller. This gives attackers more time to exploit the infected device. A perfect example of this is backdoor AndroRAT.A.

The open source software "Remote Admin Tool for Android", or "AndroRAT" for short, is making a name for itself as the source of this threat. The code for this tool has been publicly accessible for some time now at GitHub, a hosting service for software development projects, as well as at Google Code, a similar service. Even though the original author has removed his version from the net, copies and modifications still exist in the corresponding communities.

The "AndroRAT" project started as a scientific university project, designed to enable the legitimate and legal management of Android mobile devices. As such, the tool could be used in the end-point management area or in connection with the BYOD (bring your own device) concept. An administrator could manage the installation of apps, manage contact lists etc.

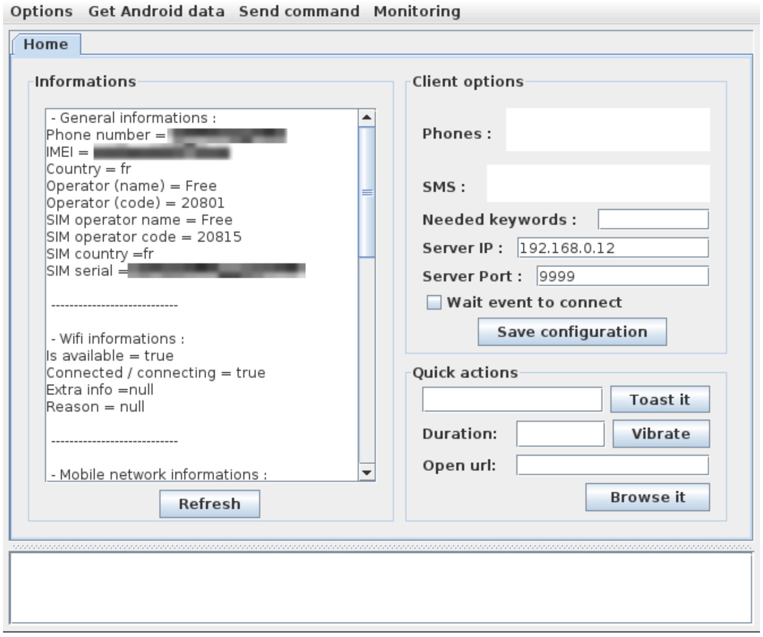
The tool is user-friendly and easily adapted to user requirements. Unfortunately, malware authors have also noticed this and have responded accordingly: For example, the "AndroRAT APK Binder" tool was offered for sale in an international underground forum. It enables attackers, even those without extensive programming knowledge (known as "script kiddies"), to integrate the "AndroRAT" framework described above into any Android app. For advertising purposes, the author of the binder even placed corresponding instructional videos on the Internet to make

[9] http://www.gdata.de/securitylab/mobile/mobile-malware.html
[10] See page 4

Copyright © 2013 G Data Software AG

buying the binder even more appealing to interested parties. This tool is now available in other international forums as well.

Compared to other malware families, only a small number of Android.Backdoor.AndroRAT samples have been detected so far. However, we are expecting significant developments in this area. The combination of the "AndroRAT" tool and the "APK Binder" will enable more people to jump on the Android.Backdoor.AndroRAT bandwagon, particularly because of its user-friendliness and the modular enhancement potential of the code.



```
 - General informations :
Phone number = [redacted]
IMEI = [redacted]
Country = fr
Operator (name) = Free
Operator (code) = 20801
SIM operator name = Free
SIM operator code = 20815
SIM country =fr
SIM serial = [redacted]

 ----------------------------

 - Wifi informations :
Is available = true
Connected / connecting = true
Extra info =null
Reason = null

 ----------------------------

 - Mobile network informations :
```

Server IP : 192.168.0.12

Server Port : 9999

☐ Wait event to connect

Screenshot 2: *Pane in the original tool, from the "AndroRAT" documentation*

The next chapter, Malware profiles, provides some technical details on "AndroRAT APK Binder" and its detection by G Data MobileSecurity products.

Malware profiles

Android.Backdoor.AndroRAT.A

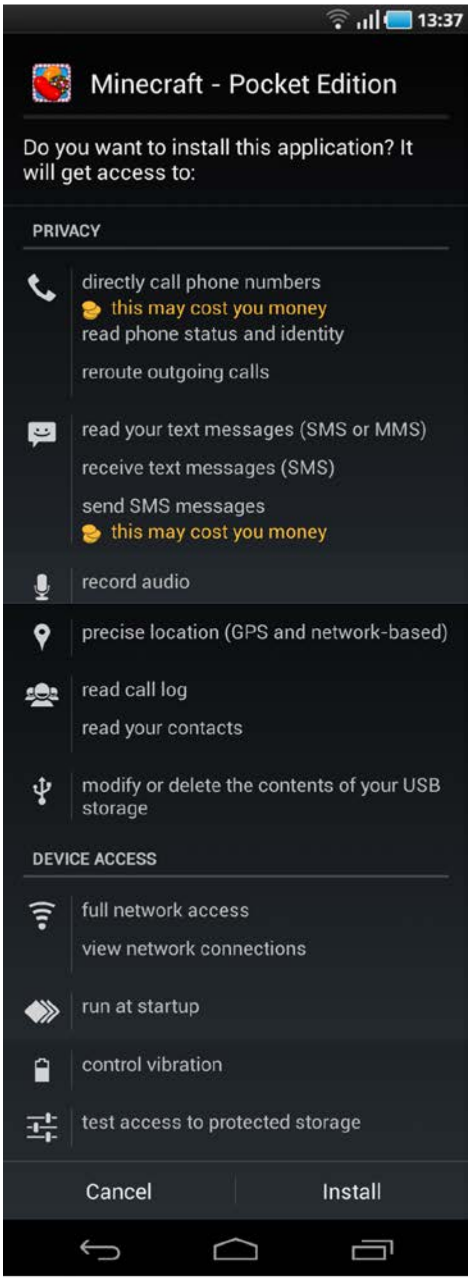
Android apps can naturally have several access points that are either manually started by the user of the device or automatically triggered by specific events such as starting the smartphone, taking an incoming call etc. For example, they enable apps from traffic associations to simultaneously open stored connections when the app is started normally.

"Android APK Binder" adds an additional access point to a manipulated legitimate app so that, when the device is booted, the "AndroRAT" component and not the legitimate app is started in the background. From then on, the phone is part of a botnet and the attacker therefore has full control over it. The publicly available version of "AndroRAT" directly supports the following commands:

- Read contacts
- Read call list
- Read SMS/MMS
- Locate the device using GPS/network cell
- Notify of incoming calls/messages etc.
- Transfer live still images, video and sound to the server
- Display toasts (small message windows)
- Send SMS
- Make calls
- Open websites
- Vibrate

Since the code of the legitimate "AndroRAT" tool is open source and therefore freely available to anyone, malware authors can copy, modify and enhance it in any way they like.

Modified apps can sometimes be detected on the basis of the usually extensive permissions they request (the unmodified original app does not need many of these permissions).



Minecraft - Pocket Edition

Do you want to install this application? It will get access to:

PRIVACY

directly call phone numbers
this may cost you money
read phone status and identity
reroute outgoing calls

read your text messages (SMS or MMS)
receive text messages (SMS)
send SMS messages
this may cost you money

record audio

precise location (GPS and network-based)

read call log
read your contacts

modify or delete the contents of your USB storage

DEVICE ACCESS

full network access
view network connections

run at startup

control vibration

test access to protected storage

Screenshot 3: *Comprehensive list of permissions requested by an app infected with Backdoor.AndroRAT.A.*

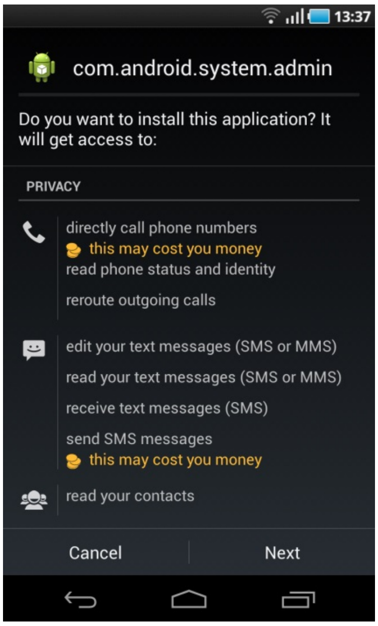
Copyright © 2013 G Data Software AG

Android.Backdoor.Obad.A

Backdoor Obad.A is highly sophisticated malware that first appeared in China this June. The malware exploits three security vulnerabilities for its attacks: a previously unknown vulnerability in the Android operating system, an error in a tool called Dex2Jar and an error in Android's handling of the file AndroidManifest.xml. The latter two are supposed to make the analysis of the malware more difficult.

List of possible commands that can be sent to an infected device:

- Full control of the device (backdoor)
- Communication with the server
- Transfer after device is started:
  - MAC address (Bluetooth)
  - Telephone number
  - IMEI
  - Query the admin–permission (yes/no)
  - Timestamp
- Query installed apps or certain apps
- Query contact data
- Queries using USSD codes (e.g. credit)
- Send SMS (premium SMS)
- Delete SMS (hide activity)
- Use as proxy
- Download/install files from server
- Send files via Bluetooth
- Block the display in the meantime



13:37

com.android.system.admin

Do you want to install this application? It will get access to:

PRIVACY

directly call phone numbers
this may cost you money
read phone status and identity
reroute outgoing calls

edit your text messages (SMS or MMS)
read your text messages (SMS or MMS)
receive text messages (SMS)
send SMS messages
this may cost you money

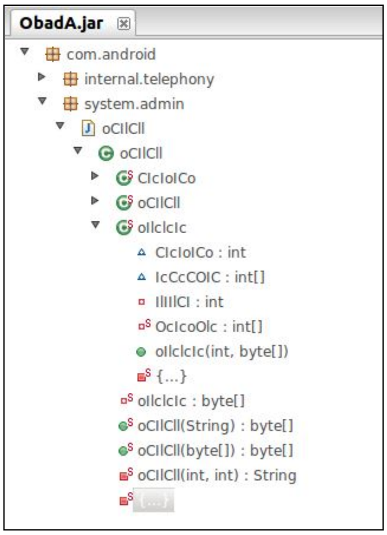
read your contacts

Screenshot 4: *The malware disguises itself as a system app. However, the authorisations that indicate possible charges are suspicious.*

What is particularly treacherous about backdoor Obad.A is that - once it's installed - it cannot usually be uninstalled, and that it also performs all activities in the background, invisible to the user.

The malware's functional scope, the sophisticated disguising of the code and the very prompt exploitation of vulnerabilities (zero-day) are all characteristics of Windows malware.

Therefore, in the future, we can not only expect more Android malware - we can also expect malicious software that is more sophisticated, elaborate and refined, posing increasingly difficult challenges to analysts.



```
ObadA.jar
com.android
  internal.telephony
  system.admin
    oCIICII
      oCIICII
        CIcIoICo
        oCIICII
        oIIcIcIc
          CIcIoICo : int
          IcCcCOIC : int[]
          IIIIICI : int
          OcIcoOIc : int[]
          oIIcIcIc(int, byte[])
          {...}
        oIIcIcIc : byte[]
        oCIICII(String) : byte[]
        oCIICII(byte[]) : byte[]
        oCIICII(int, int) : String
        {...}
```

Screenshot 5: *Disguised class names and methods make it difficult for analysts to trace and discover how the backdoor works.*

Copyright © 2013 G Data Software AG

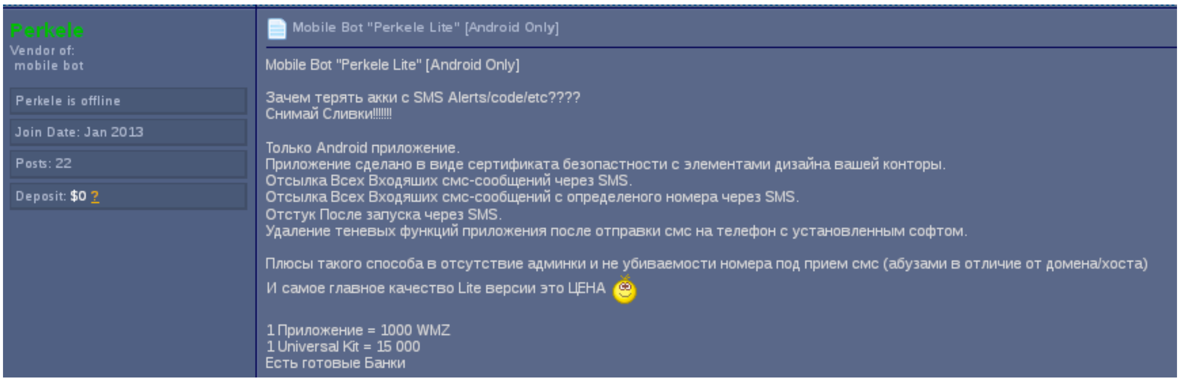
Android.Trojan.FakeSite.A, aka Perkele

FakeSite.A, aka Perkele[11], made a name for itself in the first half of 2013. However, the Trojan did not stand out thanks to the exceptionally sophisticated malware functions and well-disguised malware code. What made FakeSite.A special was the fact that attackers could use it with any malware code as long as this code used the webinject attack technology, which is supported by many banking Trojans, for example. This makes it possible to use such a combination of cross-platform malware, for example, to intercept an SMS that bank customers need for online banking (mTAN).

Attack scenario:

- A victim infected with a banking Trojan opens the online banking website of his or her bank in the PC browser as usual. The banking Trojan uses webinject to manipulate the bank website that the victim sees in the browser.
- The victim surfs to the displayed page and logs in.
- On the manipulated page, a message inserted by webinject appears, prompting the victim to install a security certificate on his or her mobile device for authentication purposes and to complete the login process.
- Once the victim enters the mobile phone number, he or she receives a link to download the alleged certificate that hides the FakeSite.A malware.
- Once the app is installed and a code is entered for verification, the app sends an SMS to the license holder of the malware kit to indicate a successful login.
- From then on, FakeSite.A intercepts all SMS that it can assign to online banking activities and forwards them to the attacker.

FakeSite.A is malware that is accessible not only to experienced attackers but also to novices, thanks to its modular structure with pre-programmed malware functions. Furthermore it offers a profitable cost-benefit ratio: In one forum, the author is offering an application created for a specific bank for WMZ 1,000 and a universal kit for WMZ 15,000 (WMZ = WebMoney; 1 WMZ = US$ 1).



Perkele
Vendor of:
mobile bot

Perkele is offline

Join Date: Jan 2013

Posts: 22

Deposit: $0 ?

Mobile Bot "Perkele Lite" [Android Only]

Mobile Bot "Perkele Lite" [Android Only]

Зачем терять акки с SMS Alerts/code/etc????
Снимай Сливки!!!!!!

Только Android приложение.
Приложение сделано в виде сертификата безопастности с элементами дизайна вашей конторы.
Отсылка Всех Входяших смс-сообщений через SMS.
Отсылка Всех Входяших смс-сообщений с определеного номера через SMS.
Отстук После запуска через SMS.
Удаление теневых функций приложения после отправки смс на телефон с установленным софтом.

Плюсы такого способа в отсутствие админки и не убиваемости номера под прием смс (абузами в отличие от домена/хоста)
И самое главное качество Lite версии это ЦЕНА

1 Приложение = 1000 WMZ
1 Universal Kit = 15 000
Есть готовые Банки

Screenshot 6: *Perkele offers the FakeSite.A bot in a forum and praises its functional scope.*

Just like malware for Windows, Android malware is expected to continue to show strong growth. Even though FakeSite.A is not one of the most sophisticated strains of malware, this Trojan has significant damage potential, due to the sheer numbers in which it can be created and spread.

[11] "In modern Finnish, the interjection "perkele!" is a common profanity, approximately equivalent to "the Devil!" in meaning and "f**k!" in intensity." Source: http://en.wikipedia.org/wiki/Perkele

Trends

The popularity of Android devices - among users and malware authors alike - will continue unabated in the second half of 2013. While malware was still pretty basic last year and aimed at short-term success, the trend has now changed. Just like in the early days of PC malware, the malicious functions in Android apps are already being disguised in the source code. This prevents automated analyses and human analysts from reading the malicious functions directly. As illustrated by Obad.A, analyses require significantly more effort.

Functions of installed malware are supposed to be invisible not only to the analyst but also to the smartphone user. As shown by FakeSite.A, relatively little basic knowledge is required in order to become a malware author. Modular kits enable more and more people with criminal intent to become active on the Android platform, and they only have to pay a small sum to the original providers of the malware kits.

Cybercrime is and will continue to be mainly financially motivated - be it directly (profit through sending premium SMS for example) or indirectly (e.g. by selling stolen data). As described, toolkits make it a lot easier for attackers to produce a large quantity of malware. Even though this malware isn't necessarily technically sophisticated, the functions are sufficient for causing damage.

Experts at G Data SecurityLabs expect the number of new Android malware programs to triple over the next six months.

In addition to the desire for fast money, which was frequently referred to as the main motivation for attacks in the past, there has now been an increase of detected backdoor activities that ensure a long-term connection with an infected device and can cause various forms of damage. Backdoors are used to create smartphone botnets that can systematically execute malicious functions in a structured way, e.g. data theft or sending of SMS.

The perceived increased customer awareness of the fact that their "phone" is a full-scale computer brightens the outlook. However, the market analysts at Canalys report that only 4% of smartphones and tablet PCs had downloaded and installed a mobile security solution in 2010, and this number is expected to increase to only 20% by 2015.[12] This proportion of protected devices must be increased! Smart devices should be handled with as much care as the home or work PC when it comes to protecting them from viruses, Trojans, backdoors etc., thus protecting personal data and valuables. Thus attackers of mobile devices will be no less dangerous than PC attackers in the future.

The race for the still young Android platform is yet to be decided. Awareness when using the mobile device, along with up-to-date security software to protect the smartphone, will significantly improve the odds of not falling victim to established attack scenarios.

[12] http://www.canalys.com/newsroom/mobile-security-investment-climb-44-each-year-through-2015