MOBILE THREAT REPORT

Q4 2011

F-Secure

F-Secure Labs

At the F-Secure Response Labs in Helsinki, Finland, and Kuala Lumpur, Malaysia, security experts work around the clock to ensure our customers are protected from the latest online threats.

Round-the-clock response work takes place in three shifts, one of which is handled in Helsinki, and two in Kuala Lumpur. At any given moment, F-Secure Response Labs staff is on top of the worldwide security situation, ensuring that sudden virus and malware outbreaks are dealt with promptly and effectively.

Protection around the clock

Response Labs work is assisted by a host of automatic systems that track worldwide threat occurrences in real time, collecting and analyzing hundreds of thousands of data samples per day. Criminals who make use of virus and malware to profit from these attacks are constantly at work on new threats. This situation demands around the clock vigilance on our part to ensure that our customers are protected.

ABSTRACT

THIS REPORT DISCUSSES THE MOBILE THREAT LANDSCAPE AS SEEN IN THE FOURTH QUARTER OF 2011, AND INCLUDES STATISTICS AND DETAILS OF THE MOBILE THREATS THAT F-SECURE RESPONSE LABS HAVE SEEN AND ANALYZED DURING THAT PERIOD.

Table of Contents

Table of Contents 2
Changes in the mobile threat landscape 4
Malware Statistics by Type 6
Figure 1: Quarterly Mobile Threats Statistics, 2011 6
Figure 2: Mobile Threats by Type, 2004–2011 7
Table 1: Malware Statistics by Type, 2004–2011 7

Potentially unwanted software 9
Application:Android/DreamStepFlash.A 9
Application:Android/Sdisp.A 9
Exploit:Android/HtcLoggers.A 10
Hack-Tool:Android/DroidRooter.G 10
Hack-Tool:Android/TattooHack.A 10
Monitoring-Tool:Android/Flexispy.L 10
Monitoring-Tool:Android/KidLogger.B 11
Monitoring-Tool:Android/Proreso.A 11
Monitoring-Tool:Android/Simchecker.A 12
Monitoring-Tool:Android/Spytrack.B 12
Riskware:Android/Boxer.D 13
Malware Statistics by Platform 14
Figure 3: Mobile Threats by Platform, 2004–2011 14
Table 2: Malware Statistics by Platform, 2004–2011 14

Spyware 15
Spyware:Android/GoneSixty.A 15
Trends in Mobile Threat Landscape 16
Figure 4: Mobile Threats Motivated by Profit, 2004–2011 16
Malicious Android's APK Received by Month, 2011 16

Malware 17
Trojan:Android/Boxer.F 17
Trojan:Android/DroidDream.E, and variant F 17
Trojan:Android/EuropaSMS.A 17
Trojan:Android/FakeBattScar.A 19
Trojan: Android/FakeNeflic.A 20
Trojan:Android/FakeNotify.A, and variant B 21
Trojan:Android/SMSFoncy.A 22
Trojan:Android/SMSFoncy.B 23
Trojan:Android/SMStado.A 24
Trojan:Android/Spitmo.B 26
Trojan:Android/YZHCSMS.B 26
Trojan-Downloader:Android/DroidKungFu.E 27
Trojan-Downloader:Android/FakeVideo.A 28
Trojan:SymbOS/ConBot.A 28
Trojan:SymbOS/Defpar.A 29
Trojan:SymbOS/Dialooper.A 29
Trojan:SymbOS/MdnPais.A 29
Trojan:SymbOS/OpFake.A, and variant B 30
Trojan:WinCE/OpFake.A 30
New variants of existing families 31
Table 3: Unique Samples Received by Malware Families, 2011 32

Changes in the mobile threat landscape

Android malware continues to expand rapidly in the fourth quarter of 2011, with malware originating from Russia forming a significant presence in the scene. This quarter, malware seen in the Russian domain has been the most widely distributed, with a single variant alone being found on a thousand unique Android application package files (APKs).

New families and variants continue to pop up, with *EuropaSMS*, *SMStado*, *SMSFoncy* and *FakeNotify* emerging in the last few months. Meanwhile, existing families *JiFake*, *FakeInst* and *Boxer* continue to spread out and evolve, now with more emphasis on features or techniques to evade detection or analysis.

Notable new families discovered in this quarter are *FakeNetflic* and *FakeBattScar*. *FakeNetflic* is a Trojan that poses as a mobile application for Netflix, a provider of subscription-based digital and DVD content. The Trojan displays a fake login page and steals the users' login credentials. *FakeBattScar* is also a Trojan that poses as a legitimate application, but is particularly interesting because it is the first to utilize advertisements as its infection vector. It displays a fake visual that resembles the one found in the original application, but secretly mines for the device's data and location while rampantly displaying advertisements.

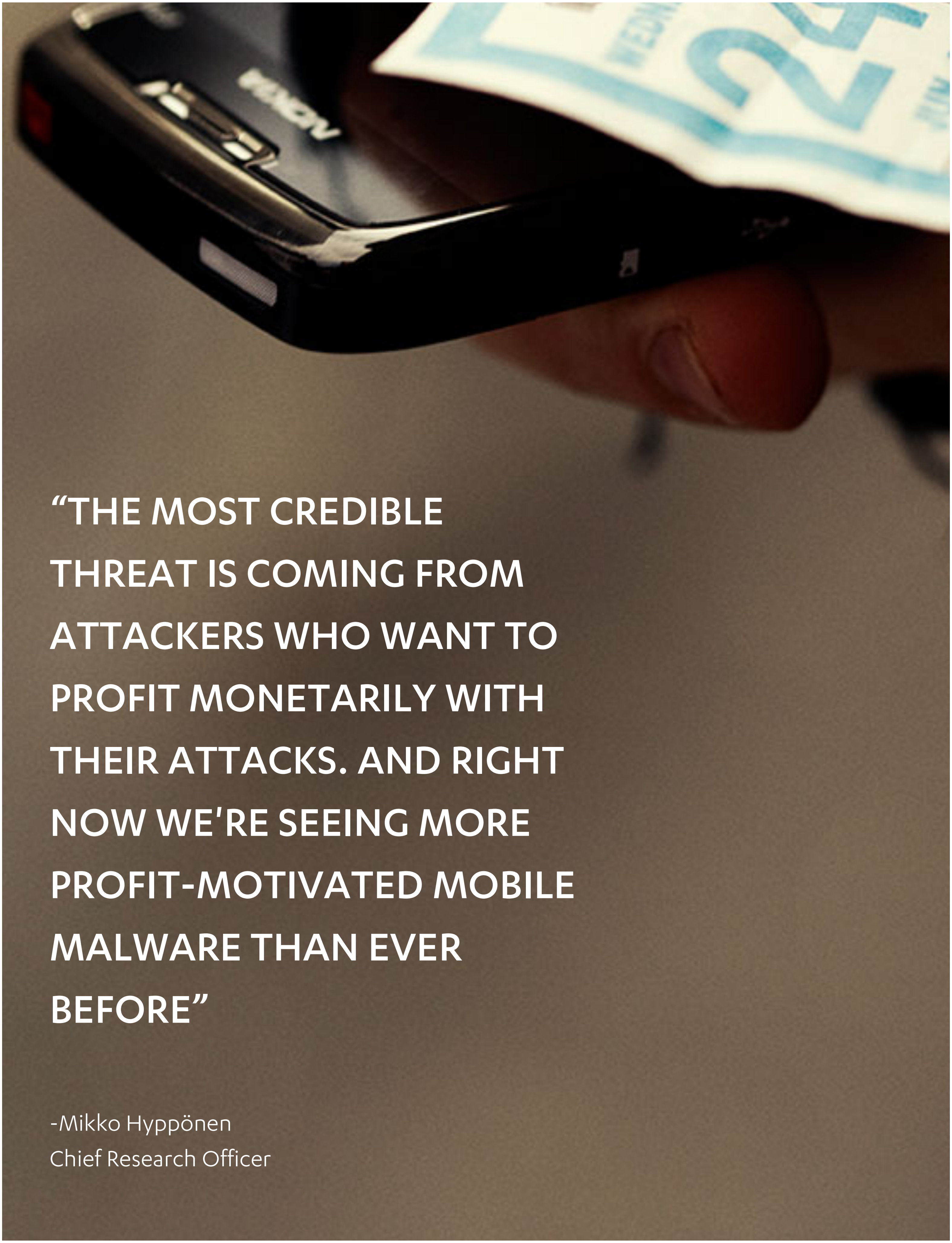
In the Chinese Android market, new variants of existing families such as *DroidKungFu*, *DroidDream* and *Geinimi* have appeared in recent months. Their malicious routines remain the same, only their techniques used to elude detection have improved. These malwares now include changes focused more on defeating anti-virus' detection technologies, with stronger encryption on the payload files and more frequent encryption key changes. Changes have also been made to the social engineering strategies used to distribute these malwares, with new download tactics or update attacks being used.

Continuing the ongoing trend of malware as 'money-makers', most of the newly discovered or existing malwares have been created to reap profit, most commonly by sending premium-rate SMS messages. Most can be classified as fake applications or installers, posing as a free version of a legitimate application. Unsuspecting users who downloaded these applications are usually not aware that they are subscribing to a premium rate service. As an example, *EuropaSMS* variants (which were distributed for a short time on the official Android Market) masqueraded as free versions of popular applications and sent out premium-rate SMS messages from the users' device.

Moving on to another platform, Symbian malware has been getting more active outside of China, with new and interesting Trojans showing up in the Russian market. In addition to the rise of new families, the amount of unique installers discovered in the fourth quarter is also worth noting, with *Trojan:SymbOS/OpFake.A* alone turning up on over 60 unique installers, the largest amount seen for a single variant since digital signatures became compulsory in S60 3rd Edition.

Finally, based on the social engineering method used (i.e., masquerading as an Opera Mini updater) and the file names and encryption algorithm used for the settings file, the same people might be behind both the Symbian and Windows Mobile versions of *OpFake.A*. A multi-platform operation like this, with a large amount of unique installers is an indication of a fairly professional operation.

"Moving on to another platform, Symbian malware has been getting more active outside of China, with new and interesting Trojans showing up in the Russian market."



“THE MOST CREDIBLE THREAT IS COMING FROM ATTACKERS WHO WANT TO PROFIT MONETARILY WITH THEIR ATTACKS. AND RIGHT NOW WE'RE SEEING MORE PROFIT-MOTIVATED MOBILE MALWARE THAN EVER BEFORE”

-Mikko Hyppönen
Chief Research Officer

Malware Statistics by Type

Figure 1: Quarterly Mobile Threats Statistics, 2011

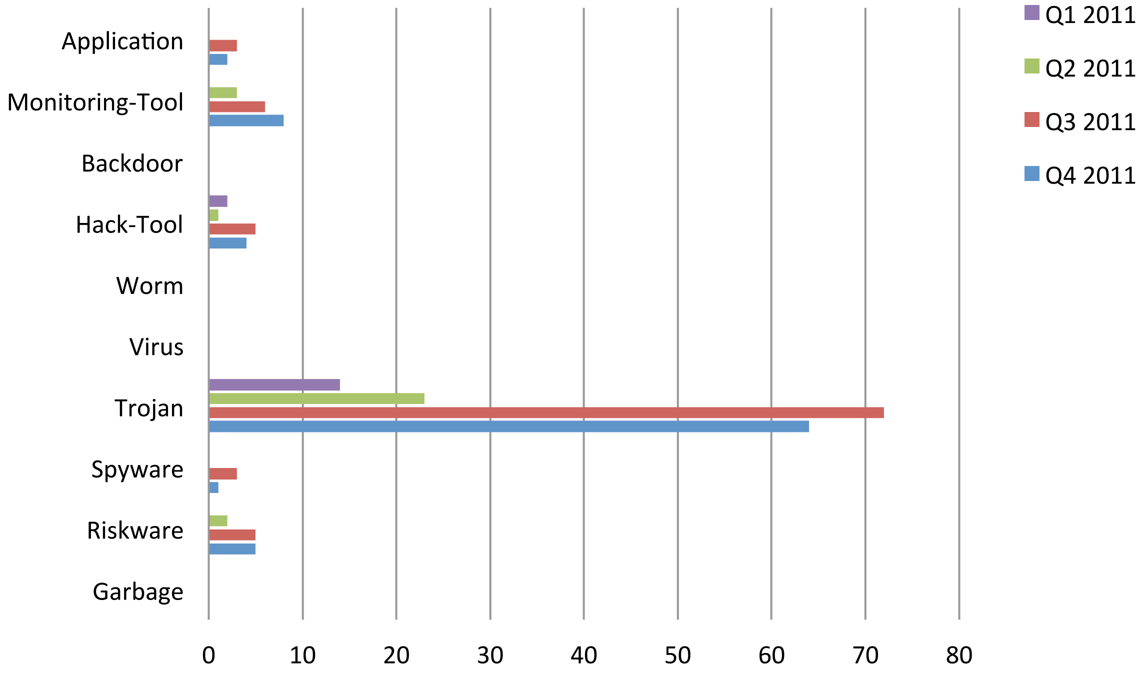


Figure 1: Trojans continue to dominate the malware scene in 2011, rising significantly compared to other types.

Figure 2: Mobile Threats by Type, 2004–2011

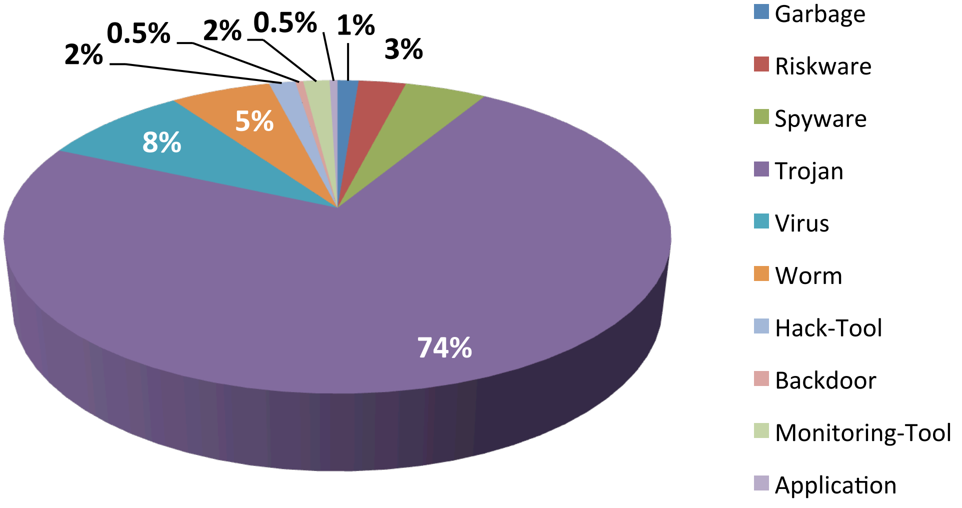


Figure 2: During the years 2004 to 2011, the mobile malware scene was dominated byTrojans.

Table 1: Malware Statistics by Type, 2004–2011

Table 1: Malware statistics by type, 2004–2011

	Year								
Type	2004	2005	2006	2007	2008	2009	2010	2011	Total
Garbage			8						8
Riskware			1		1	8	1	10	21
Spyware			5	15	6		2	4	32
Trojan	11	105	160	23	13	24	47	136	519
Virus	14	19	17	6					56
Worm				2	8	6	22		38
Hack-Tool							4	9	13
Backdoor							3		3
Monitoring-Tool							1	14	15
Application								5	5
Total	25	124	191	46	28	38	80	178	710

LATEST THREATS OF LAST THREE MONTHS

POTENTIALLY UNWANTED SOFTWARE
9

SPYWARE
15

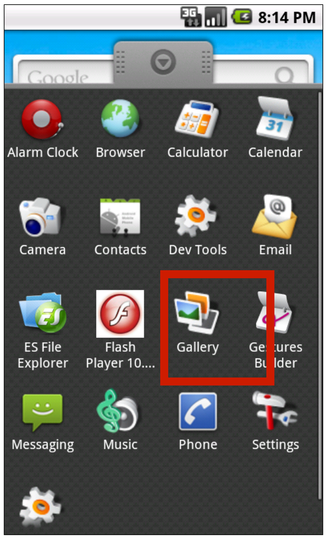
MALWARE
17

Potentially unwanted software

WE CONSIDER THE FOLLOWING PROGRAMS AS POTENTIALLY UNWANTED SOFTWARE, WHICH REFERS TO PROGRAMS THAT MAY BE CONSIDERED UNDESIRABLE OR INTRUSIVE BY A USER IF USED IN A QUESTIONABLE MANNER.

Application:Android/DreamStepFlash.A

When DreamStepFlash.A is installed on a device, a Flash Player icon would appear in the application menu. But when launched, this supposedly Flash Player application would take user to the mobile webpage of icymaze.com instead. This page is covered with a lot of banners and advertisements, some of which might contain adult-rated elements



Flash player icon that appears once DreamStepFlash.A is installed

Application:Android/Sdisp.A

Sdisp.A is an application that allows users to remotely run command and perform action via SMS and Twitter Direct Message if the message matches the preset keyword.

Some of the actions and responses include:

- **Ringing the device for 10 seconds**
- **Sending the device's current location**
- **Launching selected applications, with the content of the SMS or Twitter Direct Message forwarded to these applications**

Additionally, the application also connects to http://[...]data.flurry.com/aar.do[...].

Exploit:Android/HtcLoggers.A

HtcLoggers.A is a preinstalled application on HTC devices that could potentially leak confidential information. With HtcLoggers.A installed on a device, any other application with Internet permission might be able to access and read HtcLoggers.A's logged data, such as:

- SMS messages
- Contact numbers from phone logs
- List of user accounts
- Last known locations (GPS and network)

NOTE: HTC and Sprint had released a security patch to address this issue back in October 2011. See (http://htcsource.com/2011/10/htc-and-sprint-release-htclogger-security-patch-ota-update/)

Hack-Tool:Android/DroidRooter.G

This local root exploit is used to gain system privileges, targeting devices running on Android version 2.2 (Froyo) and 2.3 (Gingerbread). The binary and source code are publicly available, but there is yet any report or finding of this exploit being utilized by Android malware.

Hack-Tool:Android/TattooHack.A

Since /system directory holds critical components of the Android operating system, it is usually blocked from being written on by any user applications. But an old exploit for HTC Tattoo devices provides a way to bypass this constraint. TattooHack.A is a loadable kernel module that allows other application to write to the /system directory. Because of this capability, loading this module could expose a device to great risks.

Monitoring-Tool:Android/Flexispy.L

Upon execution, Flexispy.L would monitor the following activities on a compromised device:

- Incoming and outgoing call logs
- SMS messages
- Phonebook addresses
- E-mails
- Browsing history
- Photos

Monitoring-Tool:Android/KidLogger.B

Kidlogger.B is a commercial monitoring application that is advertised for tracking children's phone activities. After installation, it creates no icon on the application menu, and quietly logs the following information:

- Incoming and outgoing calls
- E-mails
- List of running applications
- Visited URLs and corresponding date
- SMS messages
- Phone state
- Contact addresses

Monitoring-Tool:Android/Proreso.A

Proreso.A captures SMS messages, phone contacts and GPS locations from a device, and later submits this information to a remote server. Its routine is triggered whenever the device is rebooted, received an SMS message or reached a particular time.

The information that Proreso.A sends out to a remote location include:

- SMS messages, senders' name and number
- IMSI
- IMEI
- SIM serial number
- Phone number
- Date
- GPS locations (longitude and latitude)

Monitoring-Tool:Android/SimChecker.A

This is a trojanized SimChecker Pro application that collects geolocation and other confidential information from a device. Upon rebooting the device, this application forwards the collected information to the author's SMS number and e-mail address that it comes preconfigured with.

Via SMS messages, the application sends out location details such as accuracy and street address, which are retrieved through WPS, GPS and the device's WiFi network.

Similar location details are also sent out via e-mail, but with additional details on the altitude, bearing and GPS speed. Along with these location details, the e-mail also includes SIM information such as:

- **IMSI, if SIM requires PIN to unlock**
- **SIM serial number, if SIM does not use PIN**
- **Operator code and service provider name**
- **Call logs (incoming, outgoing and missed)**

To send out e-mails, SimCheck.A uses the server script located at https://[...]trackdroid.org[...]/sendmail.php.

Monitoring-Tool:Android/SpyTrack.B

Spytrack.B records information on GPS location and uploads the information to the following location

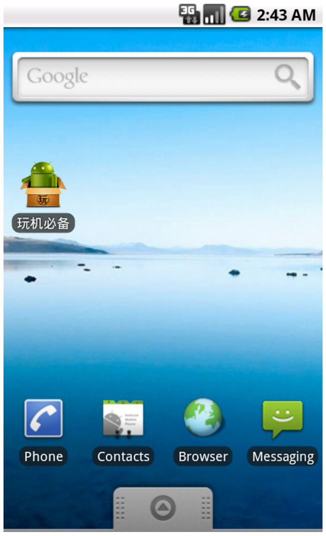
- **http://[...]spysat.pl[...]/dh/g.php?u=[LOGIN]&p=[PIN]&x=[LAT]&y=[LON]&z=[ALT]&s=[S**

where:

- **[LOGIN] is the user's login name on the Spysat website**
- **[PIN] is the numerical PIN of the tracking device**
- **[LAT] is the latitude**
- **[LON] is the longitude**
- **[ALT] is the elevation**
- **[SPD] is the speed**

Riskware:Android/Anudown.A

Upon execution, Anudown.A creates a shortcut on the launch screen, giving it visible presence and easy accessibility on the device. This move introduces a risk in a way that it
might induce users to download and install updates frequently (perhaps, unnecessarily), and because of this, have to put up with high data usage fee.



Anudown.A's shortcut on the launch screen

Riskware:Android/Boxer.D

Boxer.D is a potentially risky application because it may tempt user to send SMS messages to the contact numbers listed on the device.

Malware Statistics by Platform

Figure 3: Mobile Threats by Platform, 2004–2011

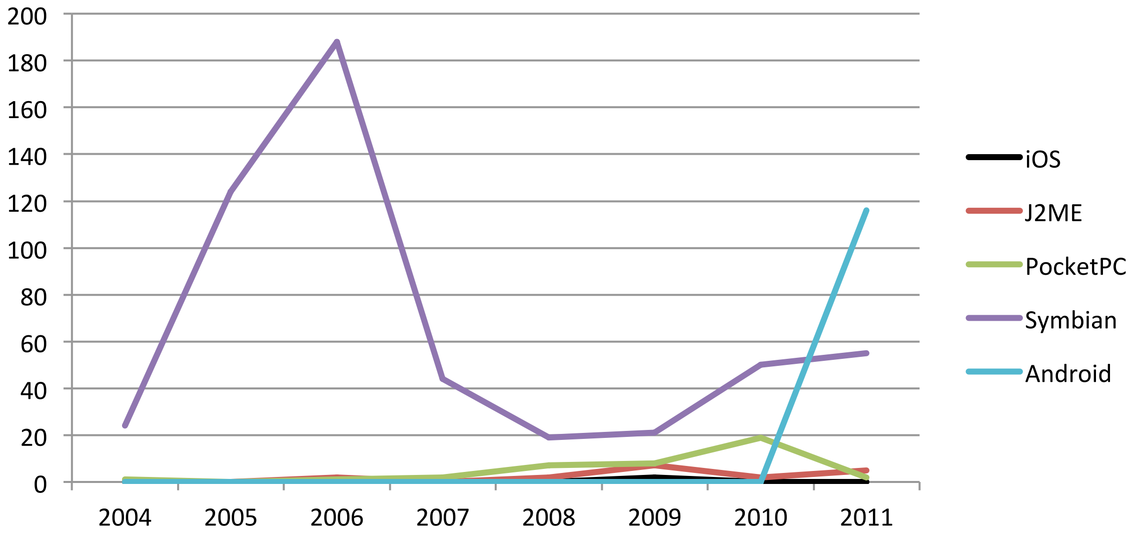


Figure 3: Mobile threats for Android are trending up while other platforms are seeing a reduction in threat numbers.

Table 2: Malware Statistics by Platform, 2004–2011

	Year								
Type	2004	2005	2006	2007	2008	2009	2010	2011	Total
iOS						2			2
J2ME			2		2	7	2	5	18
PocketPC	1		1	2	7	8	19	2	40
Symbian	24	125	188	44	19	21	50	55	525
Android							9	116	125
Total	25	124	191	46	28	38	80	178	710

Spyware

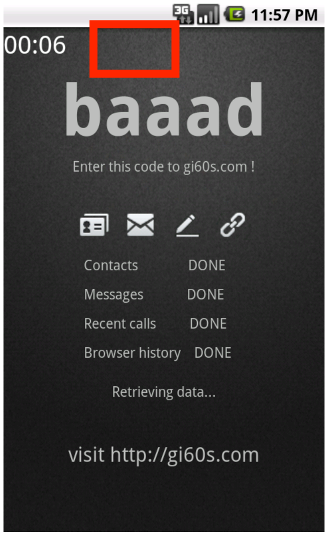
PROGRAMS CATEGORIZED AS SPYWARE SECRETLY COLLECT INFORMATION ABOUT A USER'S BROWSING HABITS, SEARCH STRINGS, SITE PREFERENCES AND PREFERRED APPLICATIONS. THIS COLLECTED INFORMATION IS EITHER SENT OUT TO ANOTHER PARTY OR STORED LOCALLY.

Spyware:Android/GoneSixty.A

Upon execution, GoneSixty.A would attempt to steal the following information:

- Contact details, including names and phone numbers
- SMS messages
- Recent calls
- Visited URLs

This stolen information is later forwarded to http://[...]gi60s.com[...]/upload.php. Sixty seconds after being executed, this Trojan would quit its processes.



11:57 PM

00:06

baaad

Enter this code to gi60s.com !

Contacts DONE
Messages DONE
Recent calls DONE
Browser history DONE

Retrieving data...

visit http://gi60s.com

Countdown for quitting the process

Trends in Mobile Threat Landscape

Figure 4: Mobile Threats Motivated by Profit, 2004–2011

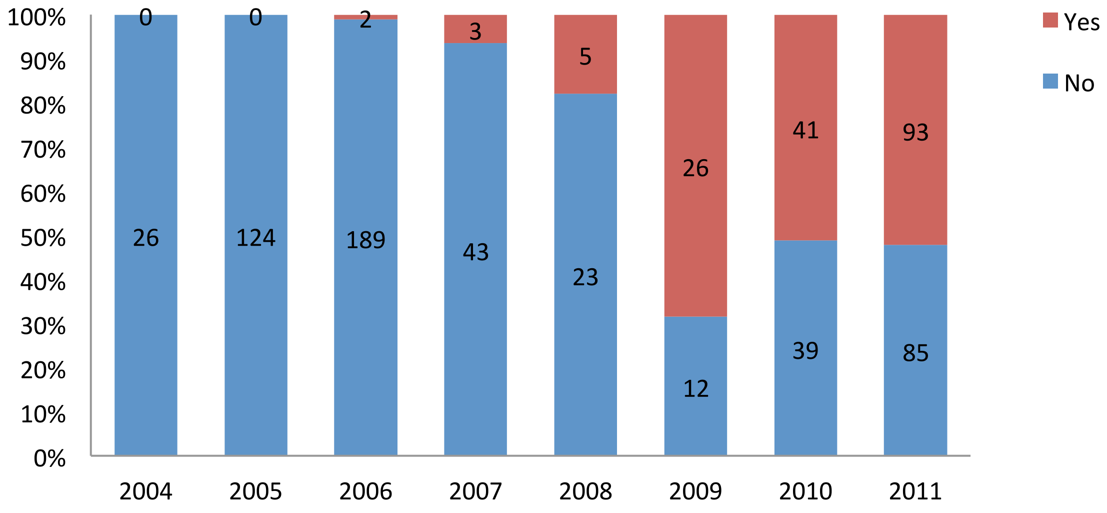


Figure 4: Beginning in 2009, more than half of the total mobile threats are profit-motivated.

Malicious Android's APK Received by Month, 2011

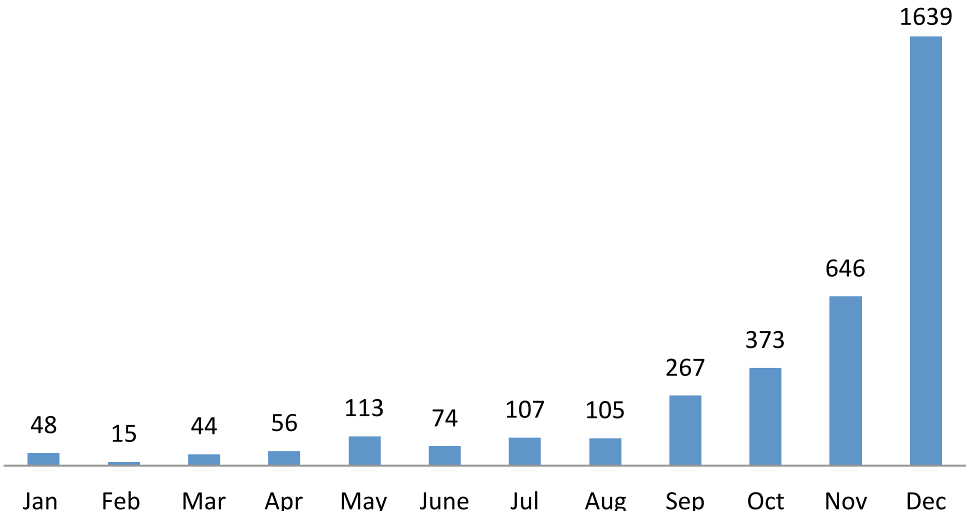


Figure 5: The number of malicious Android application package files (APKs) received per month continues to increase throughout 2011

NOTE: The data for the month of December presented in Figure 5 was accurate as of 21 December 2011.

Malware

PROGRAMS CATEGORIZED AS MALWARE ARE GENERALLY CONSIDERED TO POSE A SIGNIFICANT SECURITY RISK TO THE USER'S SYSTEM AND/OR INFORMATION.

MALICIOUS ACTIONS CARRIED OUT BY THESE PROGRAMS INCLUDE BUT ARE NOT LIMITED TO INSTALLING HIDDEN OBJECTS AS WELL AS HIDING THE OBJECTS FROM THE USER, CREATING NEW MALICIOUS OBJECTS, DAMAGING OR ALTERING ANY DATA WITHOUT AUTHORIZATION, AND STEALING ANY DATA OR ACCESS CREDENTIALS.

Related Labs Weblog post:
Premium Rate SMS Trojans in Google's Android Market
http://www.fsecure.com/weblog/archives/00002280.html

Trojan:Android/Boxer.F

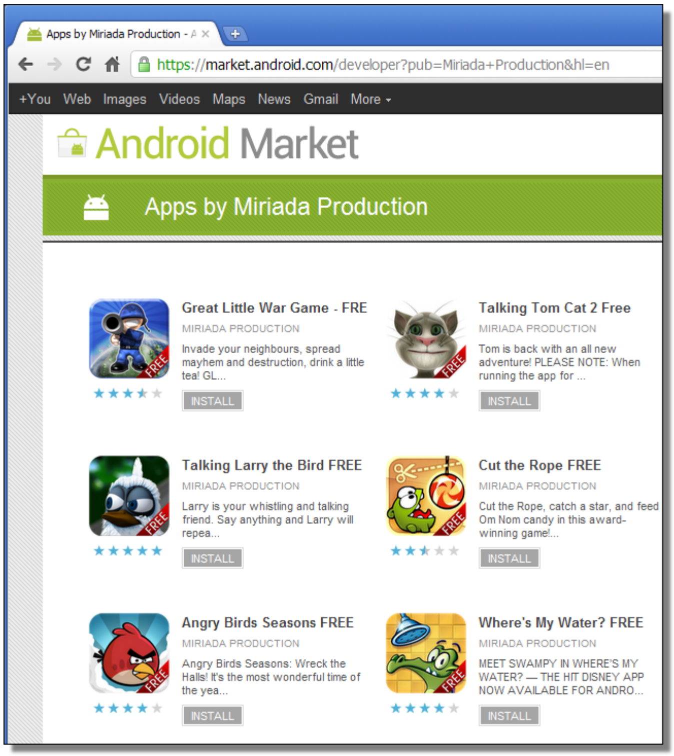
Boxer.F is an SMS-sending Android malware. Upon execution, it would prompt and ask the user to download and install updates or game applications. When the user clicks to install, it checks for the device's Mobile Country Code (MCC). Using the MCC, the Trojan would select a particular country and sends out SMS messages to this destination. This SMS-sending activity occurs in the background, with the user being unaware of the fee being charged to their bill.

Trojan:Android/DroidDream.E, and variant F

DroidDream.E is a simple application downloader, while DroidDream.F is similar to DroidDream.B (see *Mobile Threat Report Q2 2011*) in term of behavior. The difference between variant F and B can be seen in the decryption key that is used to decrypt an embedded file containing the remote server's URLs, the URLs themselves, and some IDs that are used to identify the application.

Trojan:Android/EuropaSMS.A

EuropaSMS.A is a premium rate SMS-sending malware that targets European countries. It contains two batches of application that come from different developers, identified as Logastrod and Miriada Production. The developers managed to publish their malicious applications on the official Android Market for a short time, before their accounts were shut down by Google.


Apps by Miriada Production - A ×
+You Web Images Videos Maps News Gmail More
INSTALL

https://market.android.com/developer?pub=Miriada+Production&hl=en

Android Market

Apps by Miriada Production

Great Little War Game - FRE
MIRIADA PRODUCTION
Invade your neighbours, spread mayhem and destruction, drink a little tea! GL...

Talking Tom Cat 2 Free
MIRIADA PRODUCTION
Tom is back with an all new adventure! PLEASE NOTE: When running the app for ...

Talking Larry the Bird FREE
MIRIADA PRODUCTION
Larry is your whistling and talking friend. Say anything and Larry will repea...

Cut the Rope FREE
MIRIADA PRODUCTION
Cut the Rope, catch a star, and feed Om Nom candy in this award-winning game!...

Angry Birds Seasons FREE
MIRIADA PRODUCTION
Angry Birds Seasons: Wreck the Halls! It's the most wonderful time of the yea...

Where's My Water? FREE
MIRIADA PRODUCTION
MEET SWAMPY IN WHERE'S MY WATER? — THE HIT DISNEY APP NOW AVAILABLE FOR ANDRO...

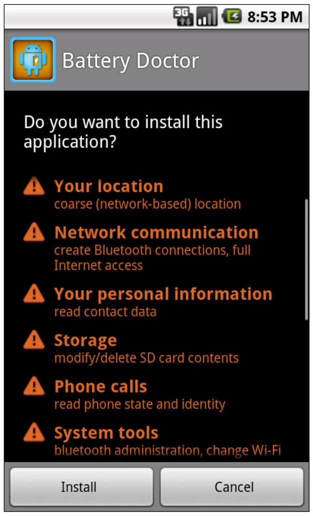
Applications by Miriada Productions were available on the Android Market for a short while

Despite originating from different developers, both batches of application use the same targeted SMS numbers and code structures. Below are the details on the targeted SMS number, country's ISO code and country's name:

Destination SMS number	ISO country code	Country name
1121	AM	Armenia
1171	TJ	Tajikistan
1645	LT	Lithuania
17013	EE	Estonia
1874	LV	Latvia
4157	KG	Kyrgyzstan
4545	IL	Israel
7540	UA	Ukraine
7781	BY	Belarus
7781	RU	Russian Federation
7790	KZ	Kazakhstan
79067	GB	United Kingdom
8014	GE	Georgia
80888	DE	Germany
81185	FR	France
9014	AZ	Azerbaijan
90901599	CZ	Czech Republic
92525	PL	Poland

Trojan:Android/FakeBattScar.A

This Trojan masquerades as Android Battery Doctor, an application that claims to help user improve a device's battery performance. Upon execution, it displays a visual of the device's battery while secretly connecting to a remote website.



8:53 PM

Battery Doctor

Do you want to install this application?

Your location
coarse (network-based) location

Network communication
create Bluetooth connections, full Internet access

Your personal information
read contact data

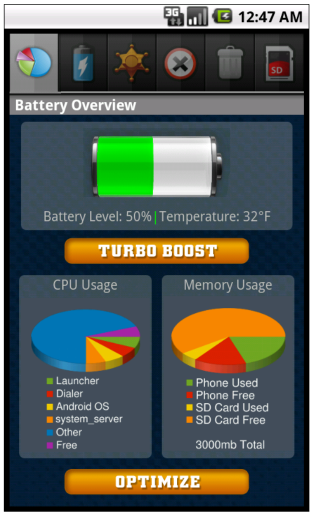
Storage
modify/delete SD card contents

Phone calls
read phone state and identity

System tools
bluetooth administration, change Wi-Fi

Install | Cancel

Requested permissions



Fake visual on the battery usage

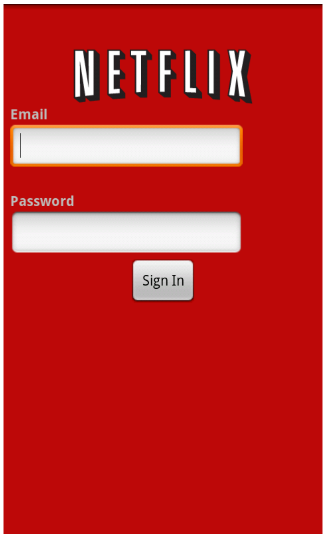
It tries to load and display advertisement from http://[...]mobsqueeze.com/[...], and forwards the following information to the same server:

- Device model and manufacturer
- Device location
- Package name
- IMEI
- OS version
- SDK version
- Browser version
- Network operator

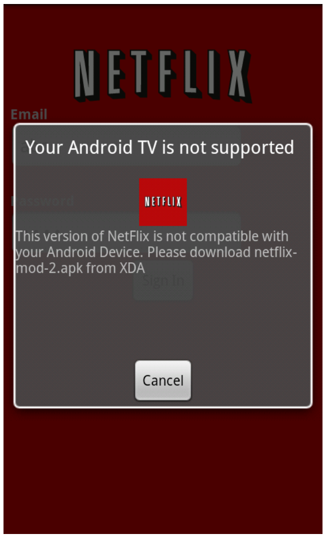
Trojan: Android/FakeNeflic.A

This Trojan disguises as a Netflix mobile application and displays a fake login page upon launching. When users enter their e-mail and password in an attempt to log in to the service, it forwards these credentials to http://[...]erofolio.no-ip.biz[...]/login.php.

Afterward, the Trojan will display an error message and uninstall itself from the device.



Fake login page



Your Android TV is not supported

This version of NetFlix is not compatible with your Android Device. Please download netflix-mod-2.apk from XDA

Error message that appears before the Trojan uninstall itself

Trojan:Android/FakeNotify.A, and variant B

FakeNotify.A is an SMS-sending Trojan, but disguises itself as an application that provides update notification.

Once installed, it displays a message to attract users into downloading a game application. When the users click a button to proceed with the download, the Trojan immediately sends out three sets of messages to the following Russian based premium numbers:

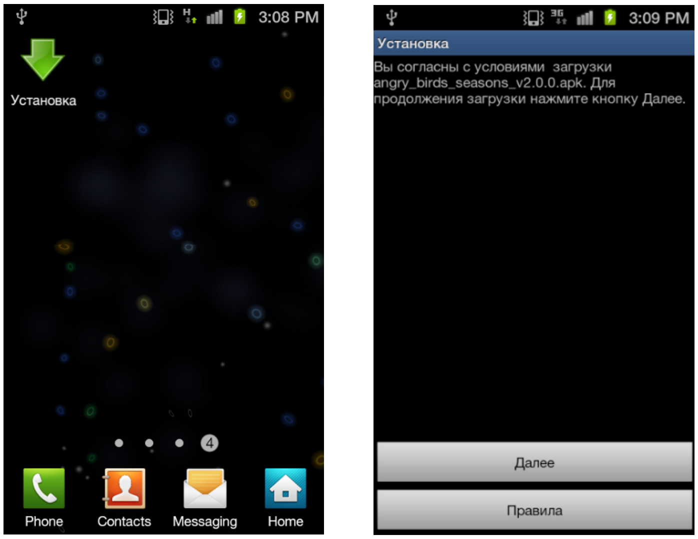
- 2855
- 1161
- 1151

Instead of getting the downloaded application, users would be directed to a website that offers more applications, which could be malicious.

Related Labs Weblog post:

Trojan:Android/SMStado.A and Trojan:Android/FakeNotify.A
http://www.f-secure.com/weblog/archives/00002278.html

Trojan:Android/FakeNotify Gets Updated
http://www.f-secure.com/weblog/archives/00002291.html



Вы согласны с условиями загрузки angry_birds_seasons_v2.0.0.apk. Для продолжения загрузки нажмите кнопку Далее.

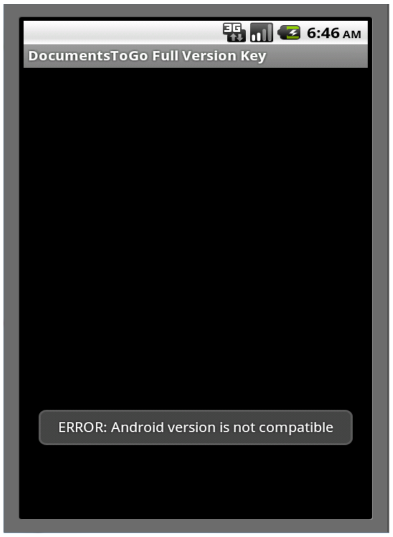
FakeNotify.A installed on a device, and a message that attracts users into downloading a popular application

FakeNotify.B acts similarly as the first variant, but the coding approach has been refreshed. Instead of the straightforward implementation used in FakeNotify.A, the later variant takes advantage of the Reflection/Dynamic Invocation feature in the Java language to accomplish the same purpose while making it harder to be analyzed and detected.

Trojan:Android/SMSFoncy.A

SMSFoncy.A is an SMS-sending malware. When running, this Trojan would show user a crafted error:

- **ERROR: Android version is not compatible**



ERROR: Android version is not compatible

Error shown when SMSFoncy.A is running

It uses an interesting method, onCreate in MagicSMSActivity, which does nothing except to obtain the user's country code:

- Fr
- Be
- Ch
- Lu
- Ca
- De
- Es
- Gb

Based on the country code, it sends out a premium rate SMS message to a specific number:

- 81001
- 9903
- 543
- 64747
- 60999
- 63000
- 35064
- 60999
- 00000

Messages sent out by the Trojan are as follows:

- STAR
- GA SP
- GEHEN SP 300
- ACCESS SP
- SP
- SP 462
- GOLD
- SP2
- WUUT

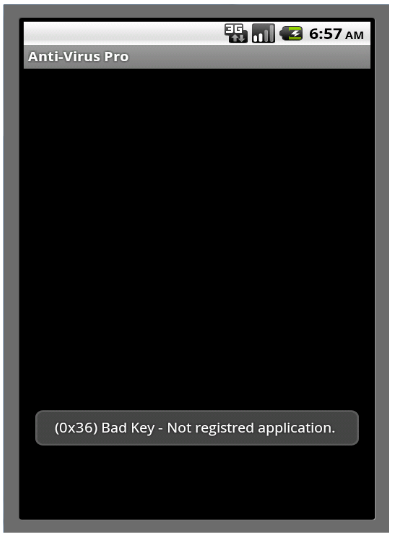
It then sends an SMS message to 0646112264, reusing the content from the SMS received from the numbers above.

Trojan:Android/SMSFoncy.B

When SMSFoncy.B is running, it would show a crafted error:

- (0x36) Bad Key – Not registered application

Related Labs Weblog post:
Trojan:Android/SMStado.A and Trojan:Android/FakeNotify.A
http://www.f-secure.com/weblog/archives/00002278.html



(0x36) Bad Key - Not registred application.

Error shown when SMSFoncy.B is running

The first method, onCreate in MagicSMSActivity, would create a file named 'sent' in the external storage directory. If the file does not exist, the SMS sending process would be triggered. First, the Trojan sends SMS messages to specific numbers:

- 81015
- 7337
- 64747
- 543

The content of the messages are as follows:

- ALL
- CODE
- ACCESS SP
- GEHEN SP 300

Meanwhile, the SMSReceiver function hides the SMS messages received from certain numbers:

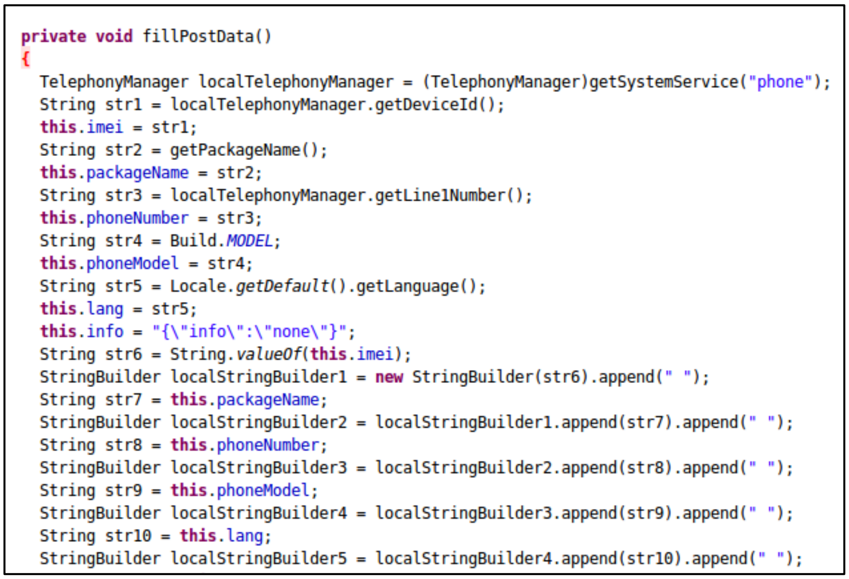
- 81015
- 7337
- 64747
- 543
- 752
- +33648552447

The Trojan then sends an SMS message to +33603561377, reusing the content from the SMS received from the numbers above.

Trojan:Android/SMStado.A

SMStado.A is a premium rate SMS-sending Trojan that targets Russian users. Upon execution, it connects to http://[...]6.antiddos.biz/[...] and forwards the following information:

- IMEI
- Package name
- Phone number
- Phone model



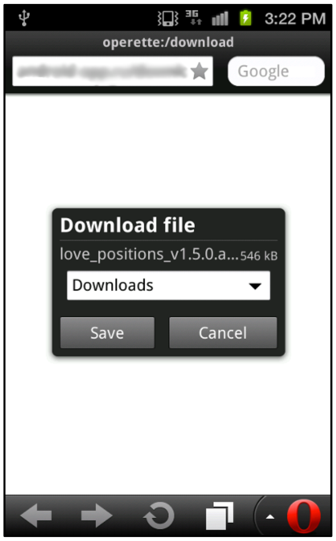
```
private void fillPostData()
{
  TelephonyManager localTelephonyManager = (TelephonyManager)getSystemService("phone");
  String str1 = localTelephonyManager.getDeviceId();
  this.imei = str1;
  String str2 = getPackageName();
  this.packageName = str2;
  String str3 = localTelephonyManager.getLine1Number();
  this.phoneNumber = str3;
  String str4 = Build.MODEL;
  this.phoneModel = str4;
  String str5 = Locale.getDefault().getLanguage();
  this.lang = str5;
  this.info = "{\"info\":\"none\"}";
  String str6 = String.valueOf(this.imei);
  StringBuilder localStringBuilder1 = new StringBuilder(str6).append(" ");
  String str7 = this.packageName;
  StringBuilder localStringBuilder2 = localStringBuilder1.append(str7).append(" ");
  String str8 = this.phoneNumber;
  StringBuilder localStringBuilder3 = localStringBuilder2.append(str8).append(" ");
  String str9 = this.phoneModel;
  StringBuilder localStringBuilder4 = localStringBuilder3.append(str9).append(" ");
  String str10 = this.lang;
  StringBuilder localStringBuilder5 = localStringBuilder4.append(str10).append(" ");
```

Code showing the information that SMStado.A is programmed to collect

When the Trojan is running, it sends out SMS messages containing the following string:

- hm78929201647+1188+51+0+1+b92be

These messages are sent out to specified premium rate numbers, all using Russia country code. Additionally, the Trojan also downloads a package named *love_position_v1.5.0.apk* from a remote site.



SMStado.A downloads a package named love_position_v1.5.0.apk from a remote site

Trojan:Android/Spitmo.B

Spitmo.B is a Trojan that steals information from a compromised device. It intercepts SMS messages originating from banks, specifically looking for mobile transaction authentication number (mTAN) that banks use as an extra layer of protection in verifying online transactions. The mTAN is then posted to http://[...] softthrifty.com/[...]/security.jsp.

Trojan:Android/YZHCSMS.B

This Trojan is another SMS-sending malware advertised as a Chinese gaming application. It connects to a remote server, http://[...]domaindev.51widgets.com/[...]/config.xml, to obtain a list of numbers. For example:

- **8613800755500**
- **1065800885566**

It then sends out SMS messages that begin with “YZHC” followed by the device’s IMEI and user value to these numbers.

Trojan-Downloader:Android/DroidKungFu.E

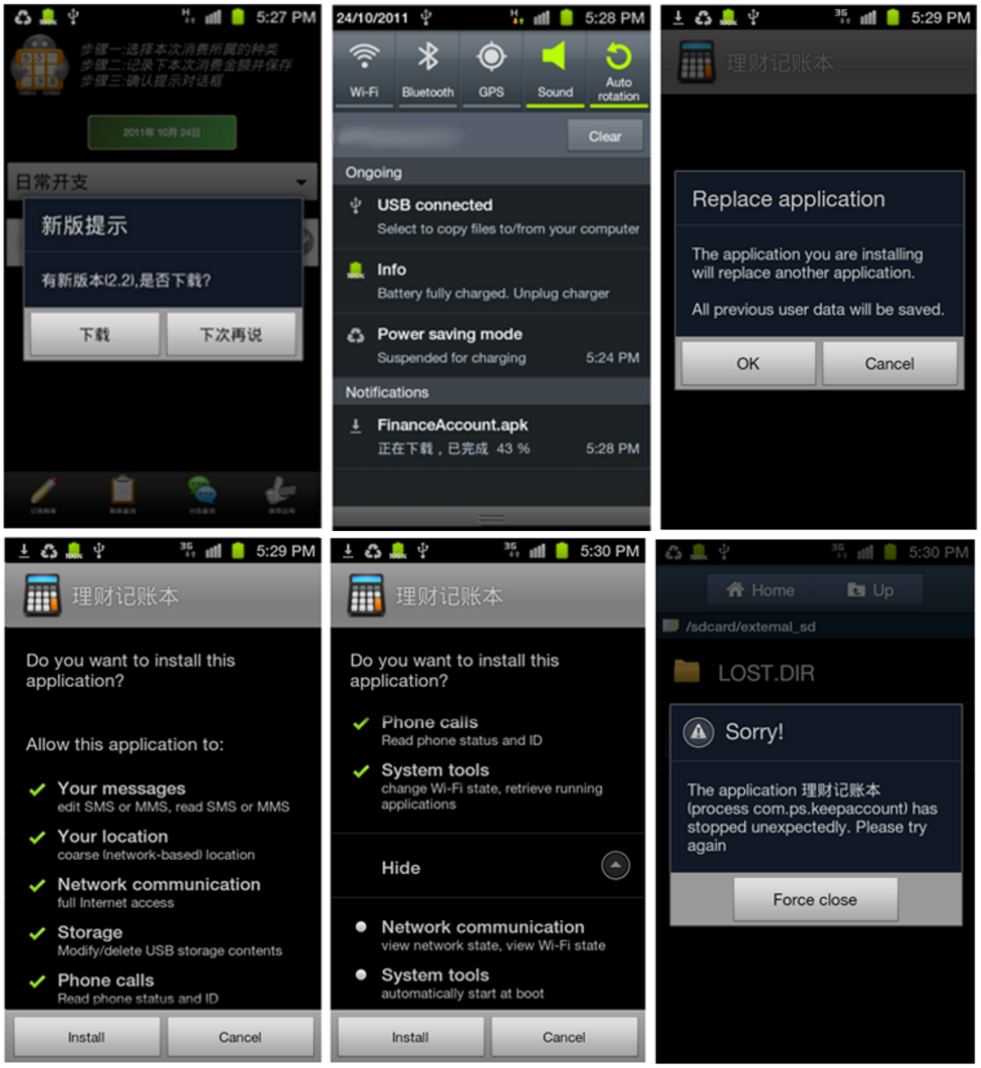
DroidKungFu.E exemplifies how Update Attack (in which a later, potentially malicious update is added to an application already installed on a user's device) is implemented as an infection method.

Once installed, the Trojan downloader would inform users that an update is available. This update would then install a variant of DroidKungFu malware.

Related Labs Weblog post:

These Aren't the Droid Updates You're Looking For
http://www.f-secure.com/weblog/archives/00002258.html

DroidKungFu Utilizes an Update Attack
http://www.f-secure.com/weblog/archives/00002259.html



5:27 PM

步骤一:选择本次消费所属的种类
步骤二:记录下本次消费金额并保存
步骤三:确认提示对话框

2011年 10月 24日

日常开支

新版提示

有新版本(2.2),是否下载?

下载 | 下次再说

24/10/2011 5:28 PM

Ongoing

USB connected
Select to copy files to/from your computer

Info
Battery fully charged. Unplug charger

Power saving mode
Suspended for charging 5:24 PM

Notifications

FinanceAccount.apk
正在下载，已完成 43 % 5:28 PM

5:29 PM

理财记账本

Replace application

The application you are installing will replace another application.

All previous user data will be saved.

OK | Cancel

5:29 PM

理财记账本

Do you want to install this application?

Allow this application to:

✓ Your messages
edit SMS or MMS, read SMS or MMS

✓ Your location
coarse (network-based) location

✓ Network communication
full Internet access

✓ Storage
Modify/delete USB storage contents

✓ Phone calls
Read phone status and ID

Install | Cancel

5:30 PM

理财记账本

Do you want to install this application?

✓ Phone calls
Read phone status and ID

✓ System tools
change Wi-Fi state, retrieve running applications

Hide

● Network communication
view network state, view Wi-Fi state

● System tools
automatically start at boot

Install | Cancel

5:30 PM

/sdcard/external_sd

LOST.DIR

Sorry!

The application 理财记账本 (process com.ps.keepaccount) has stopped unexpectedly. Please try again

Force close

Screenshots showing the sequence of the update process

After the update, the application which was originally clean would contain extra functionalities, similar to that found in DroidKungFu malware. The updated application was detected as Trojan:Android/DroidKungFu.C, a variant discovered earlier in August 2011.

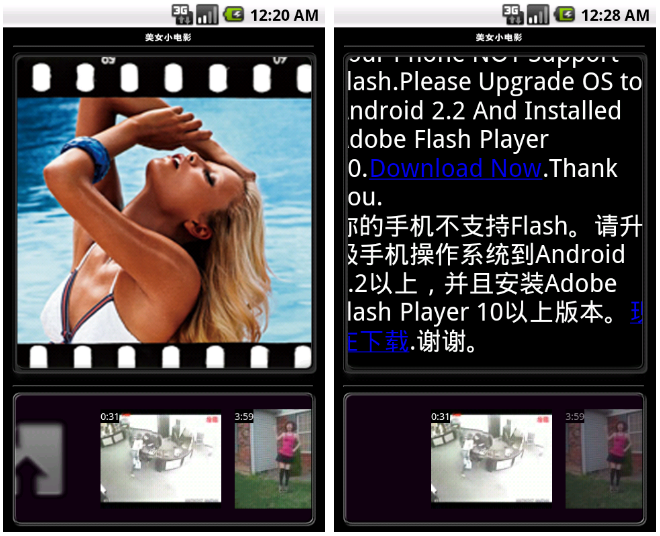
Trojan-Downloader:Android/FakeVideo.A

As indicated by its name, FakeVideo.A is a fake video application that tries to connect to the following locations upon execution:

- http://[...]users.51.la/[...]/802.js
- http://[...]web1.51.la:82[...]
- http://[...]ajiang.net/[...]/icon_0.gif

It also tries to obtain the following information from a compromised device:

- IMEI
- IMSI
- SDK version



lash.Please Upgrade OS to
ndroid 2.2 And Installed
dobe Flash Player
0.Download Now.Thank
ou.
r的手机不支持Flash。请升
及手机操作系统到Android
.2以上，并且安装Adobe
lash Player 10以上版本。现
在下载.谢谢。

Screenshots of FakeVideo.A

Trojan:SymbOS/ConBot.A

ConBot.A exhibits bot characteristics and shares code with another malware known as Trojan:SymbOS/Spitmo.A.

It monitors for incoming SMS messages and messages that have been moved from the Outbox to the Sent folder. If certain conditions are met, the intercepted messages would be deleted.

An interesting feature in ConBot.A is its ability to update the command and control (C&C) server's URL via text messages. If it notices an incoming message that begins with zlhd[...], it extracts the remaining of the message and stores it to settings.dat, replacing the old URL.

Related Labs Weblog post:
Another Cousin of Spitmo: SymbOS/ConBot
http://www.f-secure.com/weblog/archives/00002271.html

Trojan:SymbOS/Defpar.A

Defpar.A is a Chinese Trojan that uses an uncommon method to protect itself from anti-virus programs. As a protective mechanism, Symbian Trojans usually terminate processes that belong to anti-virus programs. Defpar.A however, observes when a focus is changed to a new program (e.g., an infection notification from an anti-virus product), and dismisses the program based on the focused tasks as mentioned in the caption. Wangqin and 360 Safeguards are among the anti-virus products that have been silently dismissed by Defpar.A.

Other functionality of Defpar.A includes monitoring SMS messages, and downloading and installing extra software onto a compromised device.

Trojan:SymbOS/Dialooper.A

Dialooper.A is a Chinese Symbian Trojan that connects to the internet, installs new software, updates itself and makes phone calls. It is typically distributed in files named management.sis, and uses the name 'SystemUpdate' under the list of installed applications.

Trojan:SymbOS/MdnPais.A

MdnPais.A plays WAP/SMS games while the associated fees are charged to user's account. This is its most distinctive payload. Additionally, the Trojan also sends and monitors SMS messages, and installs additional software onto the device.

It receives information for SMS sending and other functionality from a remote server. The file *Stop.cfg* contains a list of UIDs, which are used to identify several processes and applications, such as processes that should be terminated, processes that belong to anti-virus products, and applications that can be used to investigate or monitor activities on the device (e.g., 360 Safeguard, Callmaster and MCleaner).

Trojan:SymbOS/OpFake.A, and variant B

OpFake.A makes its way into a device by pretending to be an Opera Mini updater. Its installer would add an Opera icon on the menu, and shows a fake download progress bar when the application is purportedly running. The Trojan also displays a fake "license" to boost its credibility.
OpFake.A is designed to send out SMS messages to Russian-based premium rate numbers. It monitors SMS messages, and is capable of deleting and moving messages based on the phone numbers and message content. The code that handles message interception functionality is largely identical to that found in Trojan:SymbOS/Spitmo.A, making it clear that both malware shares the same source code.

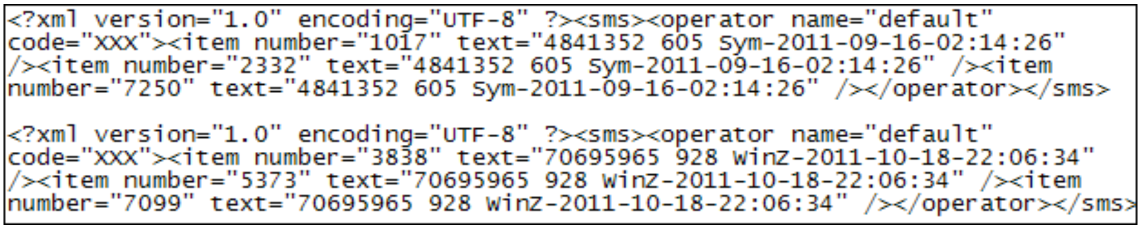
OpFake.B is very similar to the first variant, except that it uses 'Porno' on its package name instead of taking Opera Mini's icon and package name. The fraudulent license that it displays, however, still refers to Opera Mini. OpFake.B also monitors SMS messages, but unlike variant A,
it does not perform any action with these messages.

Related Labs Weblog post:
OpFake: Premium Rate SMS Trojan That Shares Code w/ Spitmo
http://www.f-secure.com/weblog/archives/00002260.html

Trojan ymbOS/OpFake.ARelated Labs Weblog post:
OpFake: Premium Rate SMS Trojan That Shares Code w/ Spitmo

Trojan:WinCE/OpFake.A

The Windows Mobile version of OpFake.A is similar to the Symbian version, but slightly simpler. Both are designed to send out SMS messages to Russian-based premium rate numbers. However, unlike its Symbian counterpart, the Windows version does not monitor SMS messages.



```
<?xml version="1.0" encoding="UTF-8" ?><sms><operator name="default"
code="XXX"><item number="1017" text="4841352 605 Sym-2011-09-16-02:14:26"
/><item number="2332" text="4841352 605 Sym-2011-09-16-02:14:26" /><item
number="7250" text="4841352 605 Sym-2011-09-16-02:14:26" /></operator></sms>

<?xml version="1.0" encoding="UTF-8" ?><sms><operator name="default"
code="XXX"><item number="3838" text="70695965 928 WinZ-2011-10-18-22:06:34"
/><item number="5373" text="70695965 928 WinZ-2011-10-18-22:06:34" /><item
number="7099" text="70695965 928 WinZ-2011-10-18-22:06:34" /></operator></sms>
```

Decrypted configuration files of Symbian (first) and Windows Mobile (second) variants of OpFake.A showing its SMS sending capability

New variants of existing families

THE FOLLOWING IS A LIST OF NEW VARIANTS OF EXISTING MALWARE FAMILIES. THEIR FUNCTIONALITY IS NOT SIGNIFICANTLY DIFFERENT COMPARED TO THE EARLIER VARIANTS DESCRIBED IN PREVIOUS REPORTS.

- Trojan:Android/Geinimi.D, and variant E
- Trojan:Android/JiFake.F, and variant G and H
- Trojan:Android/DroidKungFu.F and variant G
- Trojan:SymbOS/Killphone.C
- Trojan:SymbOS/Zhaomiao.E and variant F
- Trojan:SymbOS/MapUp.C
- Trojan:SymbOS/Netserv.B and variant C
- Trojan:SymbOS/Monsoon.C
- Trojan:SymbOS/Newrad.C
- Trojan:J2ME/Swapi.C
- Trojan:J2ME/SMSer.E
- Trojan:J2ME/Boxer.E

For a list of popular Android malware families that is based on the number of unique samples received, please refer to **Table 3** on page 32.

Table 3: Unique Samples Received by Malware Families, 2011

Table 3: Android malware families with the most unique samples received, sorted from the most to the least amount

Family	Number of Samples
FakeInst	1241
Boxer	531
JiFake	217
Geinimi	176
DroidKungFu	162
DroidRooter	136
PjApps	111
BaseBridge	94
BgServ	88
DroidDream	80
Kmin	61
MobileTX	46
YZHCSMS	39
SndApps	27
GoldDream	26
Adrd	25
EWalls	25
MobileSpy	23
SMStado	22
DiHes	21
OpFake	20
FakeNotify	19
DroidDeluxe	18
Zsone	17
FakeLogo	15
Nickispy	15
EuropaSMS	14
FakeBattScar	14
Smspacem	14
Plankton	13
GoneSixty	12
AutoSPSubscribe	11
FakePlayer	11
Lovetrap	10
PremiumDownloads	10
FaceNiff	7
FakeNetflic	7
Flexispy	7
MobileMonitor	7
SmsSpy	7
SpyTrack	7
AdSMS	6
Antares	6
SMSReplicator	6
Spitmo	6
SpyBubble	6
CruiseWind	5
MobiStealth	5
GBFM	4
KidLogger	4
RemoteControlPhone	4
SMSFoncy	4
Superuser	4
Twalktupi	4
Anydown	3
GGTracker	3
HippoSMS	3
MobileNanny	3
PrivacyFarmBaby	3
TattooHack	3
Bosm	2
Dogowar	2
GoManag	2
MobiSmsSpy	2
Proreso	2
SafeKidZone	2
SmsBomber	2
Spyoo	2
Binder	1
Cracker	1
DreamStepFlash	1
FakeVideo	1
GinMaster	1
GoldenEagle	1
HtcLoggers	1
NetiSend	1
Pirates	1
PremiumText	1
Sdisp	1
SimChecker	1
Tapsnake	1

Cont.

Cont.

Total number of samples received: 3517

NOTE: The data presented in **Table 3** was last updated on 21 December 2011.

Protecting the irreplaceable

This document was previously released under controlled distribution, intended only for selected recipients.

Document made public since: 28 February 2012

F-Secure.