MOBILE THREAT REPORT

Q4 2012

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.

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

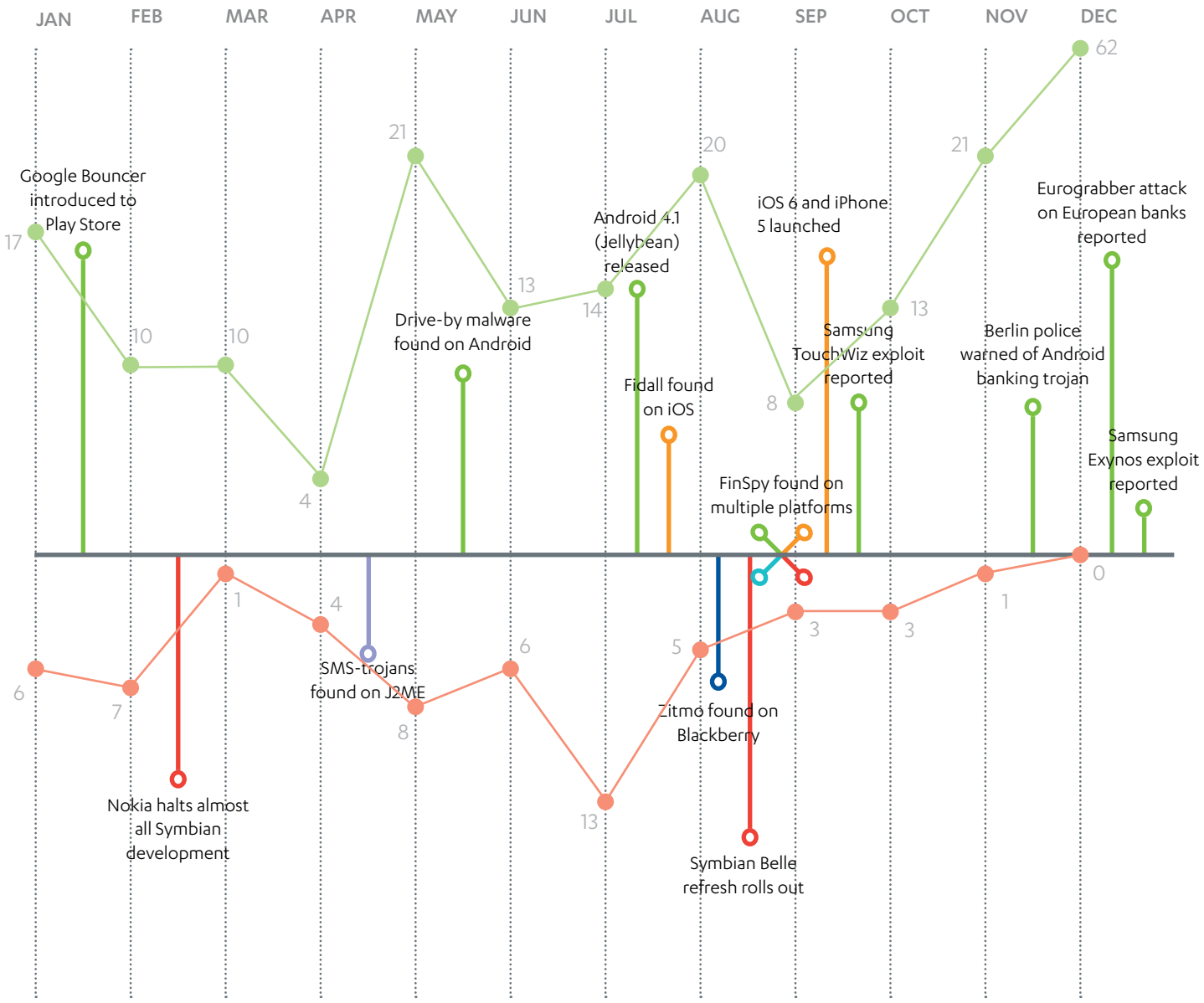
Response Labs work is assisted by a host of automatic systems that track worldwide threat occurences in real time, collecting and analyzing hundreds of thousands of data samples per day. Criminals who make use of virus and malware to profit from these attacks are constantly at work on new threats. This 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 2012, AND INCLUDES STATISTICS AND DETAILS OF THE MOBILE THREATS THAT F-SECURE RESPONSE LABS HAVE SEEN AND ANALYZED DURING THAT PERIOD. THE DATA PRESENTED IN THIS REPORT WAS LAST UPDATED ON 31 DECEMBER 2012.

CONTENTS

2012 MOBILE LANDSCAPE CALENDAR



THREAT STATISTICS

- New families/variants on Android
- New families/variants on Symbian

NOTABLE EVENTS

- Android
- Blackberry
- iOS
- J2ME
- Windows Mobile
- Symbian

EXECUTIVE SUMMARY

Android malware has been strengthening its position in the mobile threat scene. Every quarter, malware authors bring forth new threat families and variants to lure more victims and to update on the existing ones. In the fourth quarter alone, 96 new families and variants of Android threats were discovered, which almost doubles the number recorded in the previous quarter. A large portion of this number was contributed by PremiumSMS—a family of malware that generates profit through shady SMS-sending practices—which unleashed 21 new variants.

Quite a number of Android malware employ an operation similar to PremiumSMS. It is a popular method for making direct monetary profit. The malware quietly sends out SMS messages to premium rate numbers or signs up the victims to an SMS-based subscription service. Any tell-tale messages or notifications from these numbers and/or services will be intercepted and deleted; therefore, the users will be completely unaware of these activities until the charges appear on their bills.

In addition to SMS-sending malware, some malware authors or distributors may choose to make profit through banking trojans. Citmo.A (a mobile version of the Carberp trojan) recently made its debut in Q4. Just like Zitmo (Zeus for mobile) and Spitmo (SpyEye for mobile), Citmo.A operates in the same manner—it steals the mobile Transaction Authentication Number (mTAN) that banks send via SMS to customers to validate an online banking transaction. Using this number, it can transfer money from the victims' account and the banks will proceed with the transaction because it appears to be coming from the rightful account owner.

Such is the case with Eurograbber, a variant of the Zeus trojan; Bank Info Security reported that Eurograbber managed to steal USD47 million from over 30,000 retail and corporate accounts in Europe[1]. It first infected the victims' personal computers before tricking them into installing a version of it onto their mobile devices. By positioning itself on both the victims' computers and devices, Eurograbber can impersonate the victims and carry out transactions without raising suspicions from either the victim or the banking institution. The trojan had been found to infect not only devices running on Android, but also Symbian and BlackBerry operating systems.

The rise of Android malware can be largely attributed to the operating system's increasing foothold in the mobile market. Android's market share has risen to 68.8% in 2012, compared to 49.2% in 2011[2]. On the threat side, its share rose to 79% in 2012 from 66.7% in 2011. Symbian on the other hand, is suffering from the opposite fate. In 2012, it only held 3.3% market share which is a huge drop from 16.5% in the year before[3]. Its share in the threat scene also reflected this drop, going from 29.7% in 2011 to 19% in 2012. Nokia's decision to halt all Symbian development in February 2012 may have contributed to the huge drop in numbers. As its market share declines, so does malware authors' interest in the platform as evidenced by the statistics seen in Q4 where only four new families and variants of Symbian malware were recorded.

As for the other platforms, i.e., Blackberry, iOS, Windows Mobile, they may see some threats popping up once in a while. But most likely, the threats are intended for multiple platforms similar to the case of FinSpy[4].

"Bank Info Security reported that Eurograbber managed to steal USD47 million from over 30,000 retail and corporate accounts in Europe."

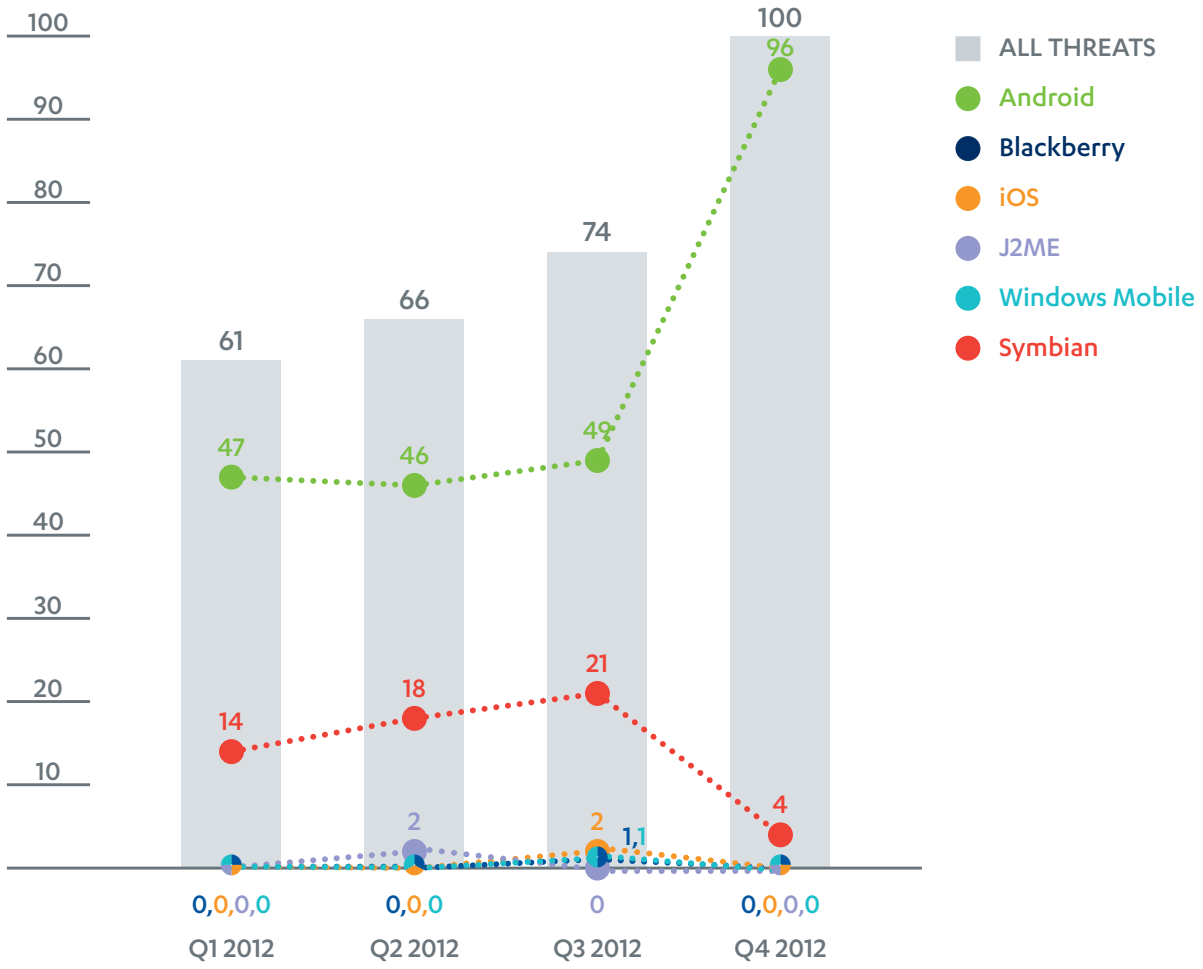
[1] Bank Info Security; Tracy Kitten; *Eurograbber: A Smart Trojan Attack*; published 17 December 2012; http://www.bankinfosecurity.com/eurograbber-smart-trojan-attack-a-5359/op-1

[2,3] Engadget; Jon Fingas; *IDC: Android surged to 69 percent smartphone share in 2012, dipped in Q4*; published 14 February 2013; http://www.engadget.com/2013/02/14/idc-android-surged-to-69-percent-smartphone-share-in-2012/

[4] F-Secure Weblog; Mikko Hyppönen; *Egypt; FinFisher Intrusion Tools and Ethics;* published 8 March 2011; https://www.f-secure.com/weblog/archives/00002114.html

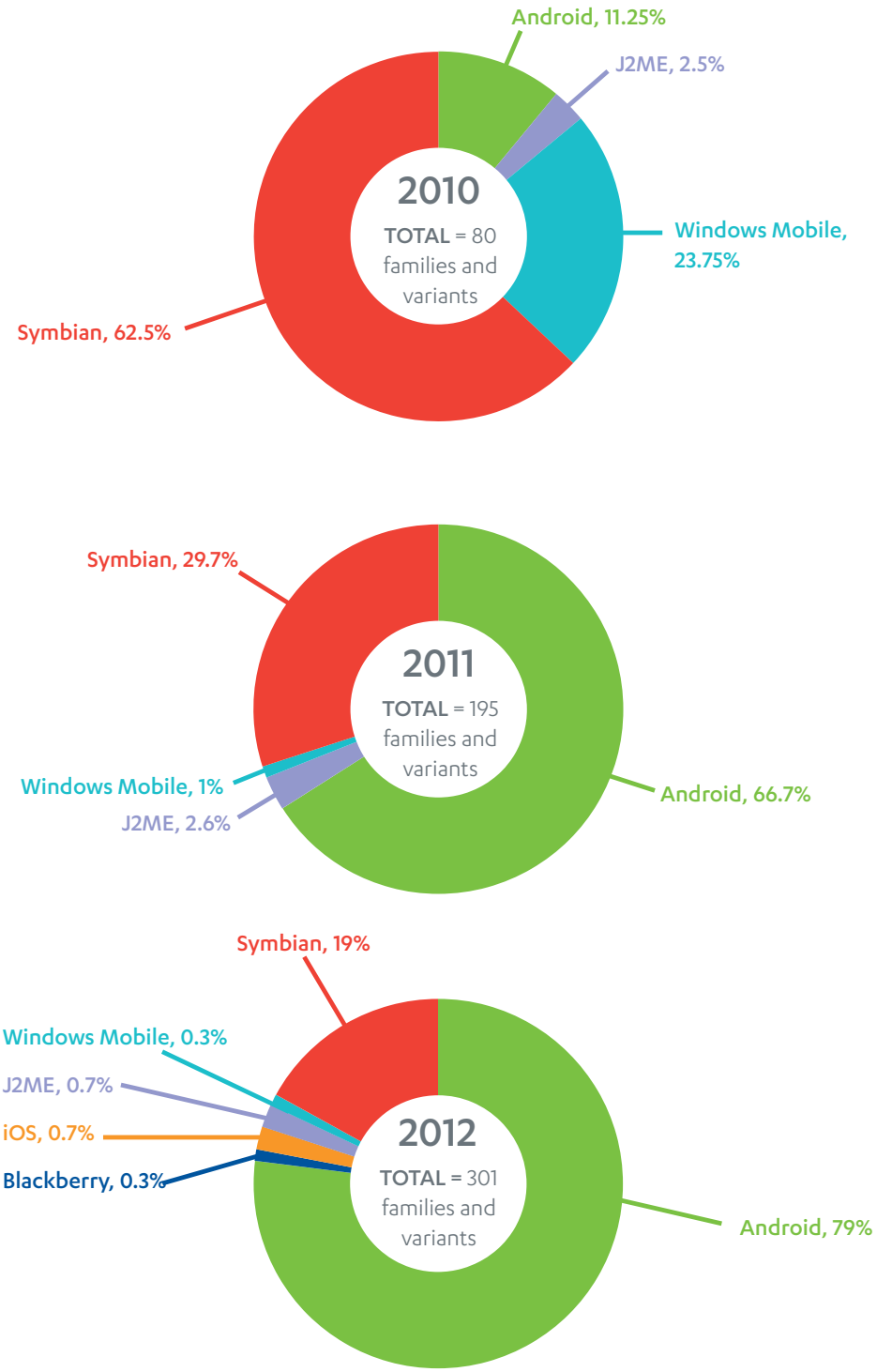
LATEST THREATS IN THE LAST THREE MONTHS

FIGURE 1: NEW MOBILE THREAT FAMILIES AND VARIANTS RECEIVED PER QUARTER, Q1–Q4 2012



NOTE: The threat statistics used in **Figure 1** are made up of families and variants instead of unique files. For instance, if two samples are detected as Trojan:Android/GinMaster.A, they will only be counted as one in the statistics.

FIGURE 2: THREAT FAMILIES AND VARIANTS BY PLATFORM,2010–2012



NOTE: The threat statistics used in **Figure 2** are made up of families and variants instead of unique files. For instance, if two samples are detected as Trojan:Android/GinMaster.A, they will only be counted as one in the statistics.

Potentially unwanted software

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

Hack-Tool:Android/Aniti.A

Also known as the Android Network Toolkit, Aniti.A is a penetration testing tool that allows user to perform certain tests via its automation interface. Using the tool, the user may evaluate or demonstrate a weak security point in the network by:

- Performing network scanning
- Generating network report
- Checking the password strength
- Checking for vulnerable machines in the network
- Attacking a vulnerable machine
- Monitoring unsecured connections
- Sniffing 'man-in-the-middle' attacker
- Performing a denial of service (DoS) attack

Like most penetration testing programs, this tool is intended for use in a legitimate context. It may however also be misused by malicious parties.

Hack-Tool:Android/DroidSheep.A

DroidSheep.A is a tool that is capable of hijacking a logged-on session conducted over a shared wireless network. It is intended to demonstrate poor security properties in a network connection, but may be misused for malicious intent by irresponsible parties.

Hack-Tool:Android/EksyPox.A

EksyPox.A is a program that offers a workaround for a vulnerability found on the Exynos 4 chip. This vulnerability, if successfully exploited, could allow any application to gain root access on devices running on the Exynos 4 chip. EksyPox.A provides a way to patch the security hole, but not without exploiting the vulnerability first.

Exynos 4: A system-on-chip (SoC) that is used by some Samsung devices, e.g., Galaxy S III, Galaxy Note II, Galaxy Camera, etc.

NOTE: For additional reading, please refer to the article at (http://www.xda-developers.com/android/dangerous-exynos-4-security-hole-demoed-and-plugged-by-chainfire/).

Monitoring-Tool:Android/GpsSpyTracker.A, and variant B

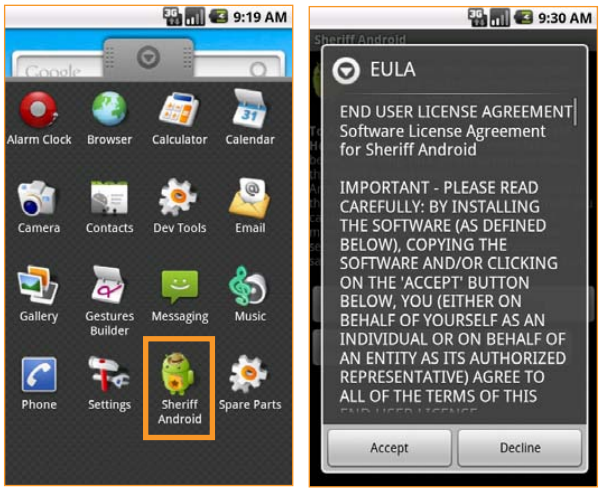
GpsSpyTracker.A is a location tracking tool that performs its tracking function using a specific key and an email address assigned to a particular device. Once activated, it tracks the device's location every 15 minutes. It displays the current location on a map and keeps the location history in a local file.

Monitoring-Tool:Android/SheriDroid.A

SheriDroid.A is advertised as an application that allows the user to perform these activities using its monitoring and alarm setting features:

- Record pre-alarm warning message
- Remotely trigger a location tracker using a password
- If lost or stolen, enable the device to stealthily send SMS messages related to alarm or location tracking
- Set system unlock pattern

However, without the user's consent or knowledge, the application keeps track of the user's web surfing behaviors and other activities carried out on the device.



SheriDroid.A's icon (left), and EULA (right)

Monitoring-Tool:Android/SmsSpy.A

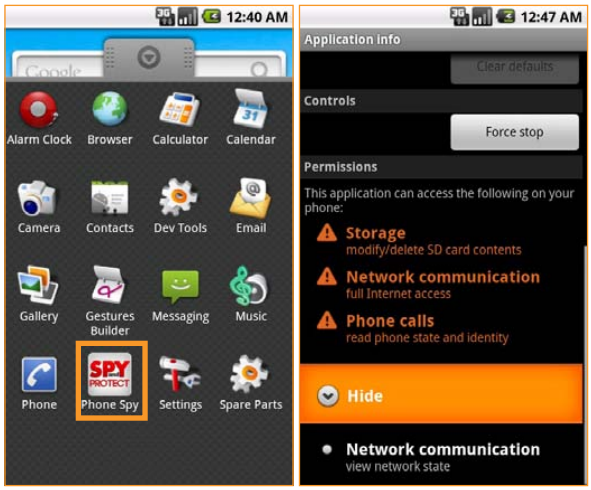
Please refer to Riskware:Android/SmsSpy.A on page 16.

Monitoring-Tool:Android/SmsUploader.A

SMSUploader.A uploads every SMS messages' content found on the device to a remote server. Once installed, SmsUploader.A places an icon titled 'SMSUpload' on the application menu. When launched, it requests that the user restart the device and informs the user that the application will be running in the background.

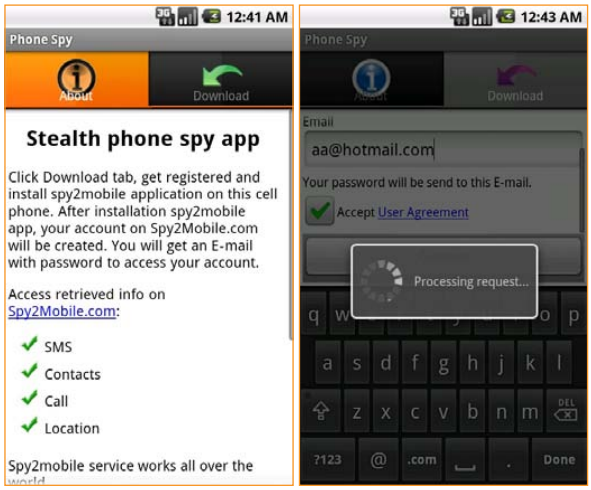
Monitoring-Tool:Android/SpyMob.A

SpyMob.A is a commercial monitoring tool that collects information pertaining to SMS messages, contact list, call log and GPS location of a targeted device. These details are later uploaded to Spy2Mobile servers and can be viewed by logging in to the user's account at Spy2Mobile.com.



SpyMob.A's icon (left), and requested permissions (right)

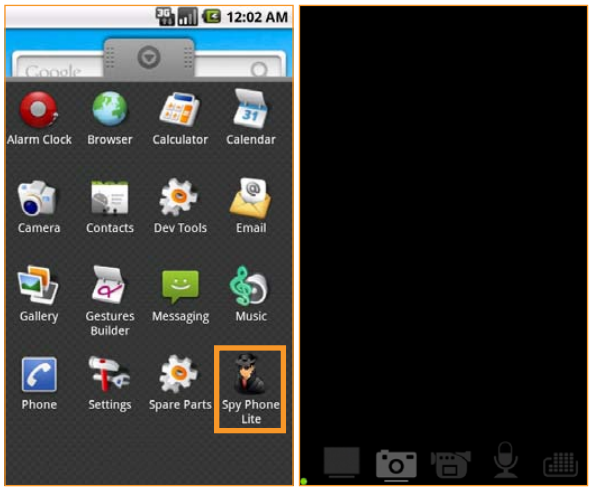
To use this application, the user must first installs SpyMob.A onto the targeted device and register an account at SpyMobile.com.



Installation and registration

Monitoring-Tool:Android/SpyPhone.A

SpyPhone.A is promoted as an application that lets user sneakily capture a photo or record a video/audio. However, it also keeps track of activities on the device and collects information such as a log of events, GPS locations, visited URLs, and the user ID.



SpyPhone.A's icon (left), and user interface (right)

Monitoring-Tool:Android/TheftAware.A

TheftAware.A is a commercial monitoring tool that helps the user to locate a stolen or a missing device. It allows the user to obtain the device's GPS location, lock it, and delete data by issuing commands through SMS messages.

Monitoring-Tool:Android/TrackPlus.A

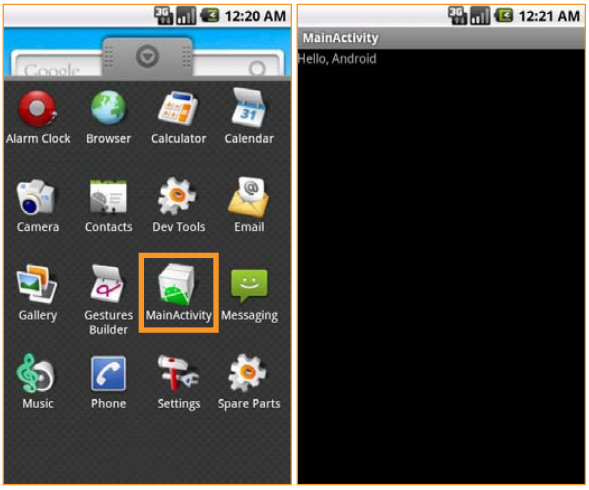
TrackPlus.A is a tracking tool that can be used to locate a device. It sends out the device's International Mobile Equipment Identity (IMEI) number to a remote server, and has a web portal to keep track of the device's location.

Once installed, TrackPlus.A does not place an icon on the application menu but appears as a transparent widget on the device.

Riskware:Android/AutoRegSMS.A

Upon launching, AutoRegSMS.A displays the message "Hello, Android" but in the background, it secretly activates a game application using the user's information. It also sends out SMS messages to the user's contact list to get an activation serial number.

AutoRegSMS.A is represented by an icon titled 'Main Activity' which can be located on the main application menu.



AutoRegSMS.A's icon (left), and the message it displays (right)

Riskware:Android/SmsReg.A, and variant.B

SmsReg.A is marketed under the name 'Battery Improve,' and claims to help maximizes a device's battery usage.

SmsReg.A as 'Battery Improve'

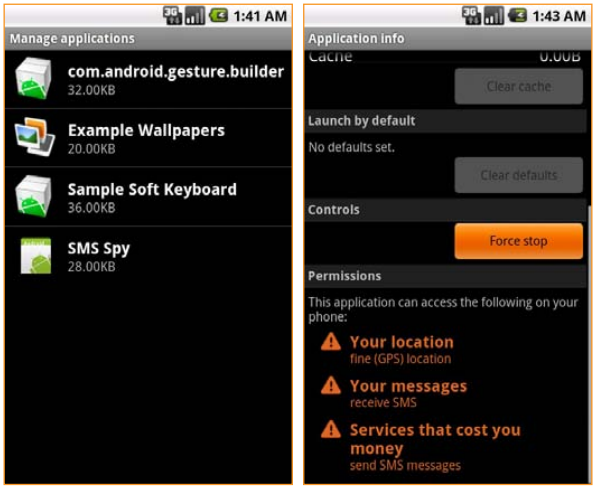
Unbeknownst to the user, the application also collects the following information:

- API key
- Application ID
- Carrier
- Device manufacturer
- Device model
- GPS location
- IMEI number
- Network operator
- Package name
- SDK version

Riskware:Android/SmsSpy.A

SmsSpy.A is a stealthy application that places no visible icon on the application menu; its presence is only visible from the 'Manage applications' option under Settings.

All of its activities are carried out inconspicuously in the background. These activities include tracking the device's GPS location, accessing and reading SMS messages received on the device, and sending out SMS messages.



SmsSpy.A as seen from 'Manage applications' (left), and requested permissions (right)

FIGURE 3: MOBILE THREATS BY TYPE, Q4 2012

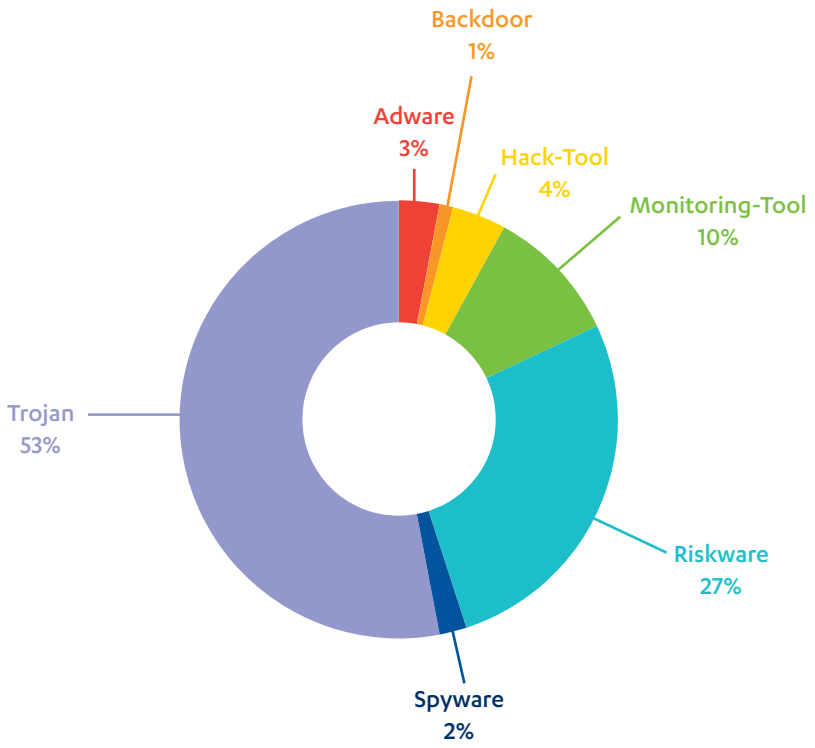
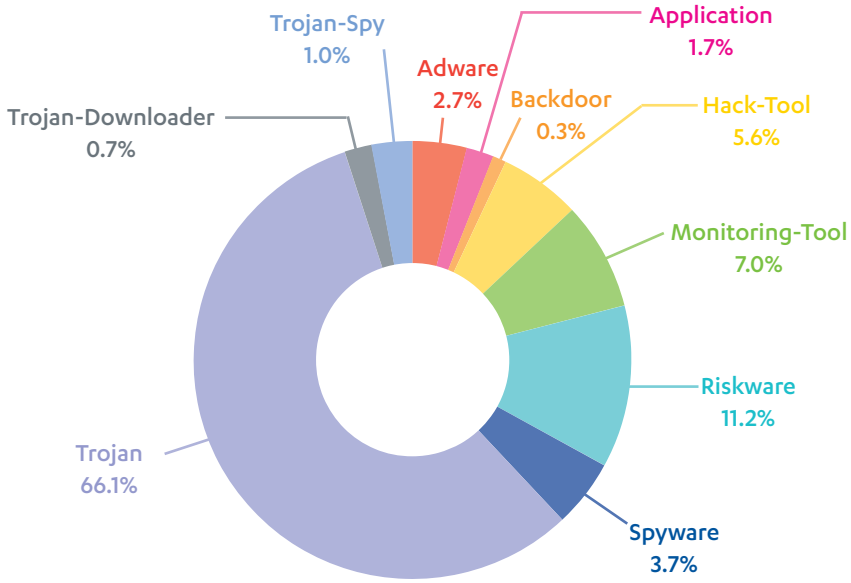


FIGURE 4: MOBILE THREATS BY TYPE, 2012



NOTE: The threat statistics used in **Figure 3** and **Figure 4** are made up of families and variants instead of unique files. For instance, if two samples are detected as Trojan:Android/GinMaster.A, they will only be counted as one in the statistics.

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.

Backdoor:Android/FakeLook.A

FakeLook.A avoids placing an icon on the application menu to hide its presence from the device owner. However, it can be seen listed as 'Updates' under the 'Manage applications' option in Settings.

FakeLook.A connects to a command and control (C&C) server to receive further instructions. It collects information such as the device ID and SMS messages, gets files list from the SD card, and compress files before uploading them to an FTP server using the username 'ftpuser' and the password 'upload.'

Trojan:Android/Citmo.A

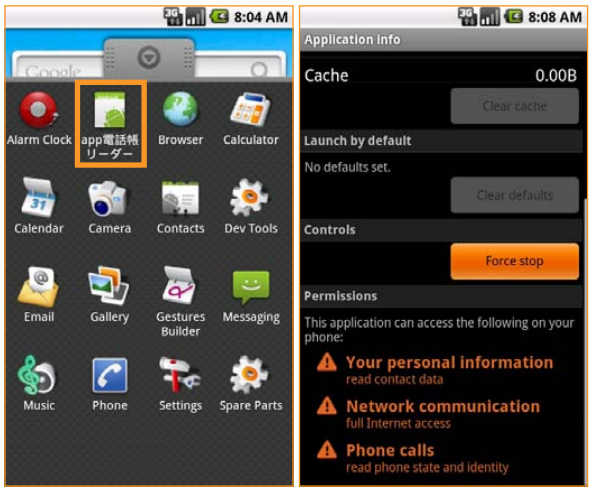
Citmo.A is the mobile version of Carberp, a banking trojan that infects personal computers to steal banking credentials. Citmo.A's functions are similar to Zitmo (Zeus for mobile) and Spitmo (SpyEye for mobile)—it monitors incoming SMS messages and steals the mobile Transaction Authentication Number (mTAN) that banks send to their customers to validate an online banking transaction.

mTAN: Mobile Transaction Authentication Number. This number is used to authenticate an online banking transaction.

NOTE: For additional reading on banking trojan, please refer to the article 'Berlin Police: Beware Android Banking Trojans' at (http://www.f-secure.com/weblog/archives/00002457.html).

Trojan:Android/EcoBatry.A

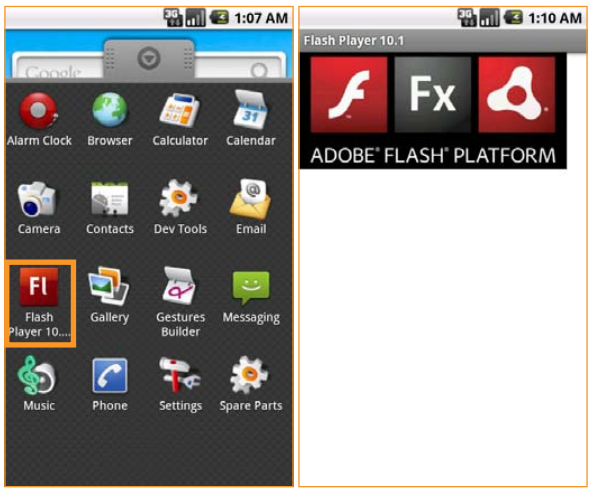
Upon installation, EcoBatry.A requests for permissions that will allow it to access Internet, contact data, and information on the device. The malware then establishes an outgoing connection to a remote server, where it will be instructed to collect user's contact information and upload the details to the server.



EcoBatry.A's icon (left), and requested permissions (right)

Trojan:Android/FakeFlash.A

FakeFlash.A takes the appearance of a legitimate Flash application. When launched, it displays a messages to the user notifying that the Flash Player application has been successfully installed, and then redirects the user to another website.



FakeFlash.A's icon (left), and the application it supposedly has installed (right)

Trojan:Android/FakeGuard.A

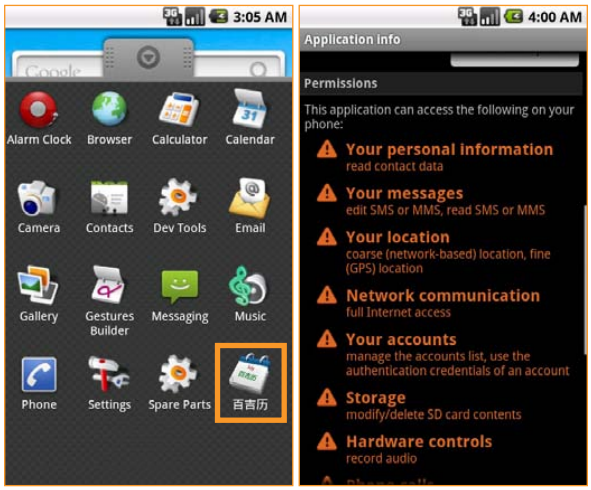
FakeGuard.A is a malware that is capable of handling incoming SMS/WAP Push. It steals user information, and establishes a connection to a remote server. The response received from the server will be decoded using MS949 character set, while the outgoing data is encoded in EUC_KR character set.

WAP Push: A specially encoded message that includes a link to a WAP address.

Trojan:Android/GeoFake.A, and variant B

GeoFake.A is distributed as a Chinese calendar application, but requests for unnecessary permissions during the installation process. The permissions it requested are as follows:

- Manage account list
- Access and use the account's authentication credentials
- Read and edit SMS or MMS messages
- Read system log files
- Access location information



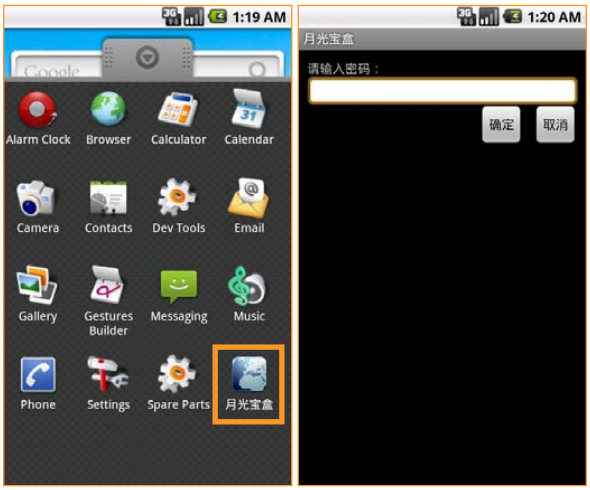
GeoFake.A's icon (left), and requested permissions (right)

Once successfully installed on a device, the malware sends SMS messages to premium rate numbers. It uses the GoogleMaps API to select which premium services should be used according to the geolocation of the device.

GeoFake.A is distributed as a Chinese calendar application

Trojan:Android/Gmuse.A

Gmuse.A is marketed as an application that allows the user to store files and documents in a secret, password-protected location. However, without the user's consent, it will sync the user's file list through an SMTP server to an unknown user using the email "hbwhhouse.gmail.com" with the password "whwxhjbu."



Gmuse.A's icon (left), and user interface (right)

Gmuse.A also connects to a remote server to download an updated version of the application, which is named as "lightbox.apk."

Trojan:Android/InfoStealer.A

InfoStealer.A, as clearly indicated by its name, is a malware that steals contact information and uploads the details to a remote MySQL server. Stolen information includes:

- Device ID
- Email address
- Latitude and longitude
- Phone number
- Postal code
- Region
- Street
- Username

Trojan:Android/MaleBook.A

MaleBook.A collects device information, and later forwards the details to several remote servers. The collected information include:

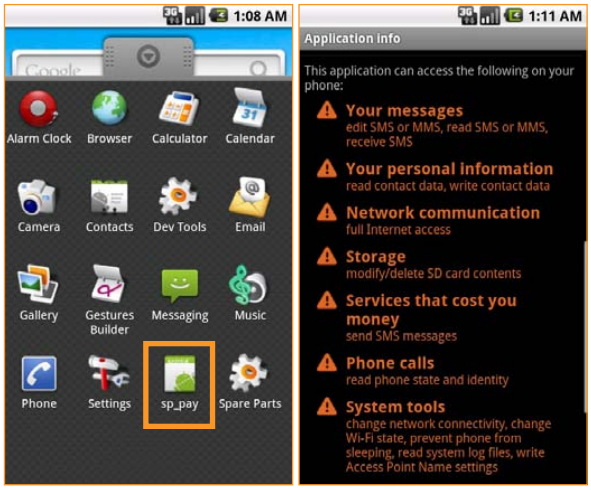
- Application ID
- Application version
- Country code
- Device name
- Device type
- Device width and height
- International Mobile Equipment Identity (IMEI) number
- International Mobile Subscriber Identity (IMSI) number
- Language
- Operation system version
- SDK version

Additionally, the malware also attempts to download advertisements from the servers onto the infected device.

MaleBook.A's icon (left), and user interface (right)

Trojan:Android/Placsms.A

Placsms.A appears as 'sp_pay' on the application menu, and requests for permissions that will allow it to access the Internet, SMS messages, SD card contents, and the device's system during the installation process.



Placsms.A's icon (left), and requested permissions (right)

The application collects information such as the device's International Mobile Equipment Identity (IMEI) number and phone number; it later uploads the details to a remote server.

NOTE: Placsms.A exhibits behavior that are similar to trojans in the PremiumSMS family (http://www.f-secure.com/v-descs/trojan_android_premiumsms.shtml).

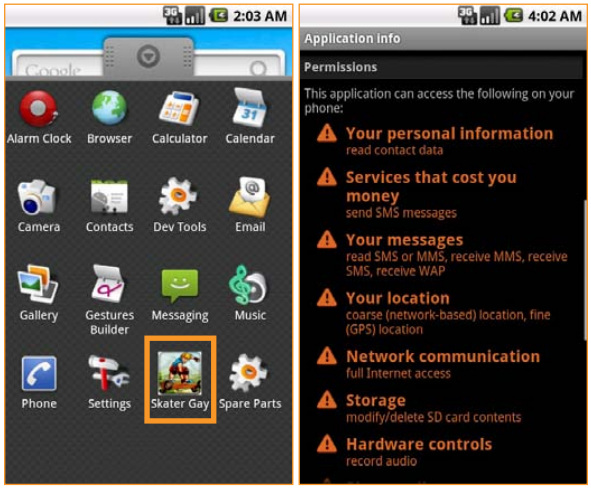
Trojan:Android/QdPlugin.A

QdPlugin.A is repackaged into another legitimate application before being distributed to potential victims. Once installed and activated on a device, the malware will send out device information such as IMEI number and IMSI number to remote servers.

It also receives commands from the servers, which may instruct it to carry out actions such as installing and removing packages. The command and control (C&C) servers' URLs are stored and encoded with a simple byte shift algorithm within the embedded malicious APK.

Trojan:Android/SMSAgent.A

SMSAgent.A appears as a game application, but silently performs malicious routines in the background. It attempts to download other potentially malicious files from a remote server and sends out SMS or MMS messages that place expensive charges on the user's bill.



SMSAgent.A's icon (left), and requested permissions (right)

Additionally, SMSAgent.A displays advertisements and collects the following information which are later uploaded to the remote server:

- Device ID
- IMEI number
- Network type
- Operator

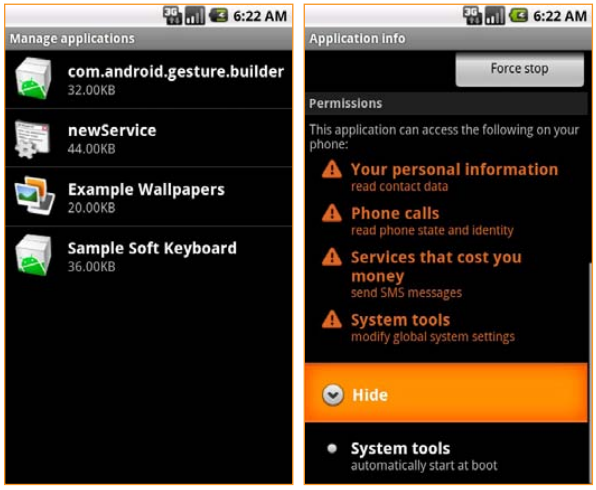
Trojan:Android/SpamSoldier.A

SpamSoldier.A is distributed via unsolicited SMS messages that contain a link for a free application download. Once successfully installed on a device, the malware contacts a command and control (C&C) server and obtains a list of phone numbers. To these numbers, it sends out more spam messages containing a link that entices users with attractive freebies.

Trojan:Android/Stesec.A

Once installed on the device, Stesec.A does not place any icon on the application menu to hide its presence from the user. It can only be viewed from the 'Manage applications' option in Settings, listed as 'newService.'

Stesec.A sends out SMS messages containing the device information such as IMEI number, software version, and other details to a remote server.



Stesec.A listed as 'newService' (left), and the permissions it requested (right)

Trojan:Android/Stokx.A

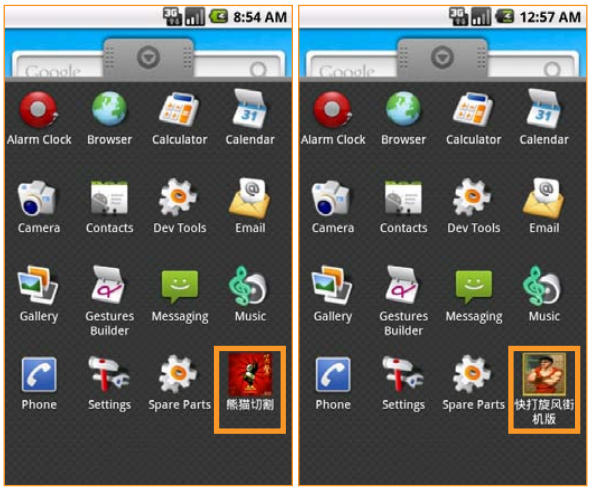
Stokx.A connects to a remote server and receives an XML file. The file contains details such as client ID, phone number that it will send SMS messages to, and URL for downloading additional APKs.

The malware will forward the device's International Mobile Equipment Identity (IMEI) number to the remote server, and sends out an SMS message with the content "SX357242043237517" to the number 13810845191.

Trojan:Android/Temai.A

Temai.A collects the following device information, and later forwards the details to a few remote addresses:

- Application ID
- Application version
- Country code
- IMEI number
- IMSI number
- Operating system version



Different icons used by Temai.A

In addition to collecting and forwarding device information, the malware also downloads and installs potentially malicious APKs and script files onto the infected device. Users may also be exposed to other risk resulting from the various permissions granted to the malware during the installation process.

Permissions requested by Temai.A during installation

Trojan:Android/Tesbo.A

Tesbo.A establishes connection to a couple of remote servers, to which it forwards details such as the device's International Mobile Subscriber Identity (IMSI) number and application package name.

Furthermore, the malware will also send out SMS messages with the content "*[IMSI]@[random from 1-10]*" to the number 10658422.

Trojan:SymbOS/Ankaq.A

Ankaq.A is a program that sends out SMS messages to premium-rate numbers, and silently installs new software onto the infected device. To avoid detection, it terminates all processes belonging to anti-virus products.

Trojan:SymbOS/Khluu.A

Khluu.A is a program that sends out SMS messages to premium-rate numbers, and silently installs new software onto the infected device. To avoid detection, it terminates all processes belonging to anti-virus products.

FIGURE 5: MOBILE THREATS MOTIVATED BY PROFIT PER YEAR, 2006-2012

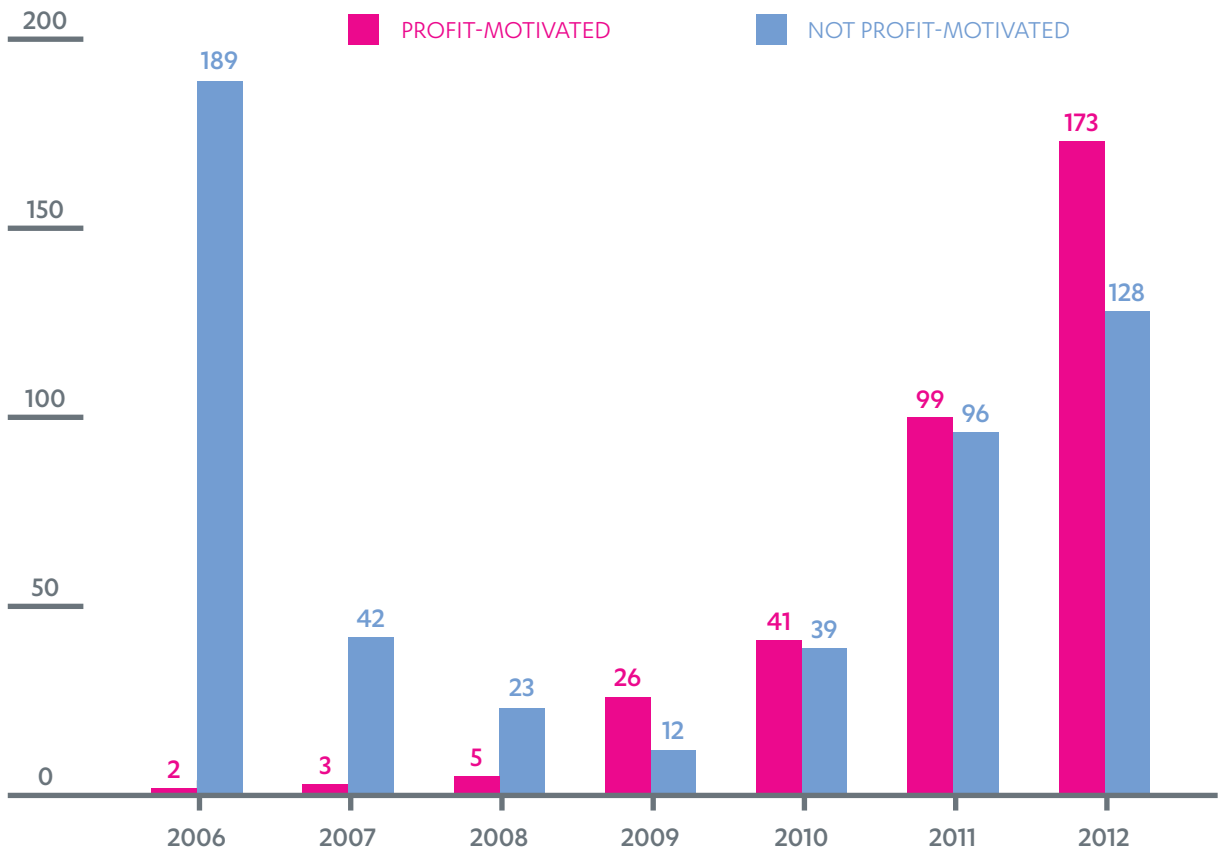
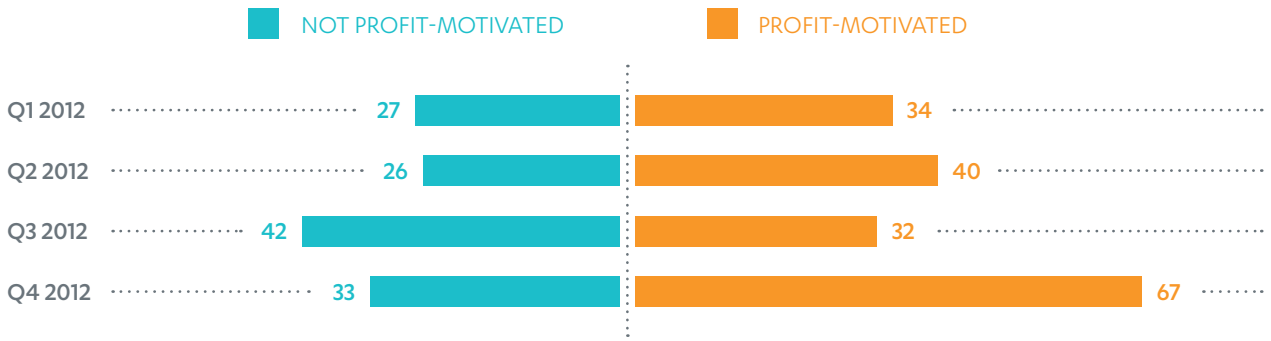
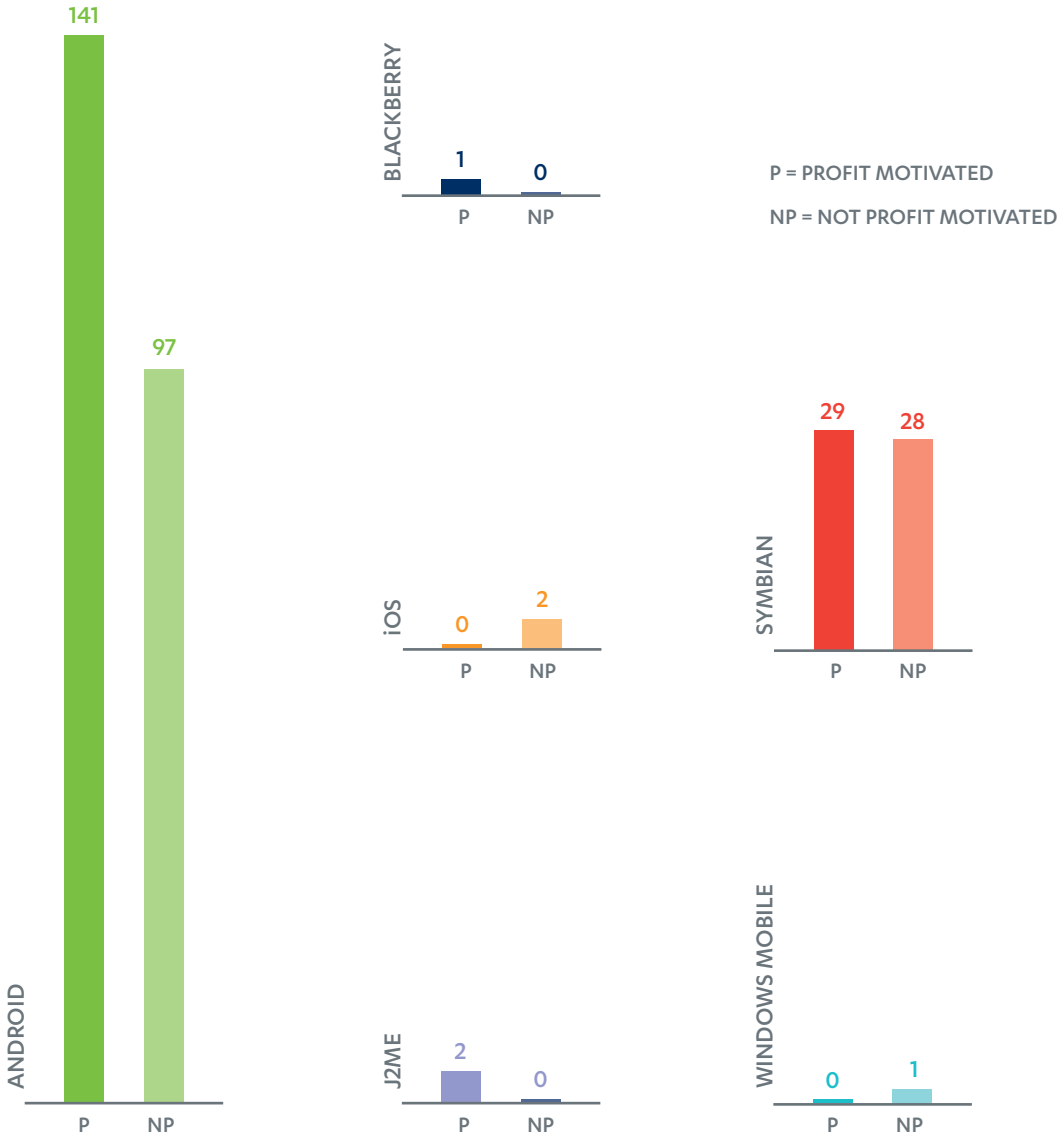


FIGURE 6: MOBILE THREATS MOTIVATED BY PROFIT PER QUARTER, Q1–Q4 2012



NOTE: The threat statistics used in **Figure 5** and **Figure 6** are made up of families and variants instead of unique files. For instance, if two samples are detected as Trojan:Android/GinMaster.A, they will only be counted as one in the statistics.

FIGURE 7: PROFIT-MOTIVATED THREATS BY PLATFORM, 2012



NOTE: The threat statistics used in **Figure 7** are made up of families and variants instead of unique files. For instance, if two samples are detected as Trojan:Android/GinMaster.A, they will only be counted as one in the statistics.

New variants of already known 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.

- Adware:Android/AdWo.C
- Adware:Android/AirPush.B
- Adware:Android/Gappusin.B
- Hack-Tool:Android/SmsBomber.B
- Monitoring-Tool:Android/AccuTrack.B
- Riskware:Android/Boxer.E
- Riskware:Android/Maxit.B
- Riskware:Android/PremiumSMS.F-Z (21 variants)
- Spyware:Android/EWalls.B
- Spyware:Android/SmsSpy.I
- Trojan:Android/DroidDream.H
- Trojan:Android/FakeInst.S-Y (7 variants)
- Trojan:Android/GinMaster.E-J (6 variants)
- Trojan:Android/GoldDream.B, and variant D
- Trojan:Android/HippoSms.B
- Trojan:Android/IconoSys.B
- Trojan:Android/JiFake.J
- Trojan:Android/MarketPay.B
- Trojan:Android/OpFake.I, L-O, (5 variants)
- Trojan:Android/SmsSend.E-G
- Trojan:Android/SmsSpy.G, H
- Trojan:Android/Vdloader.B
- Trojan:SymbOS/Foliur.B
- Trojan:SymbOS/CCAsrvSMS.D

FIGURE 8: NUMBER OF ANDROID THREATS RECEIVED PER QUARTER, Q1–Q4 2012

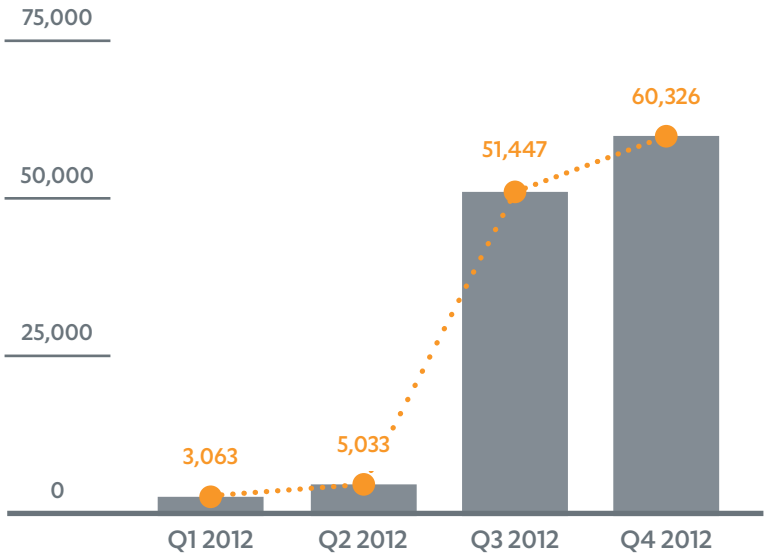
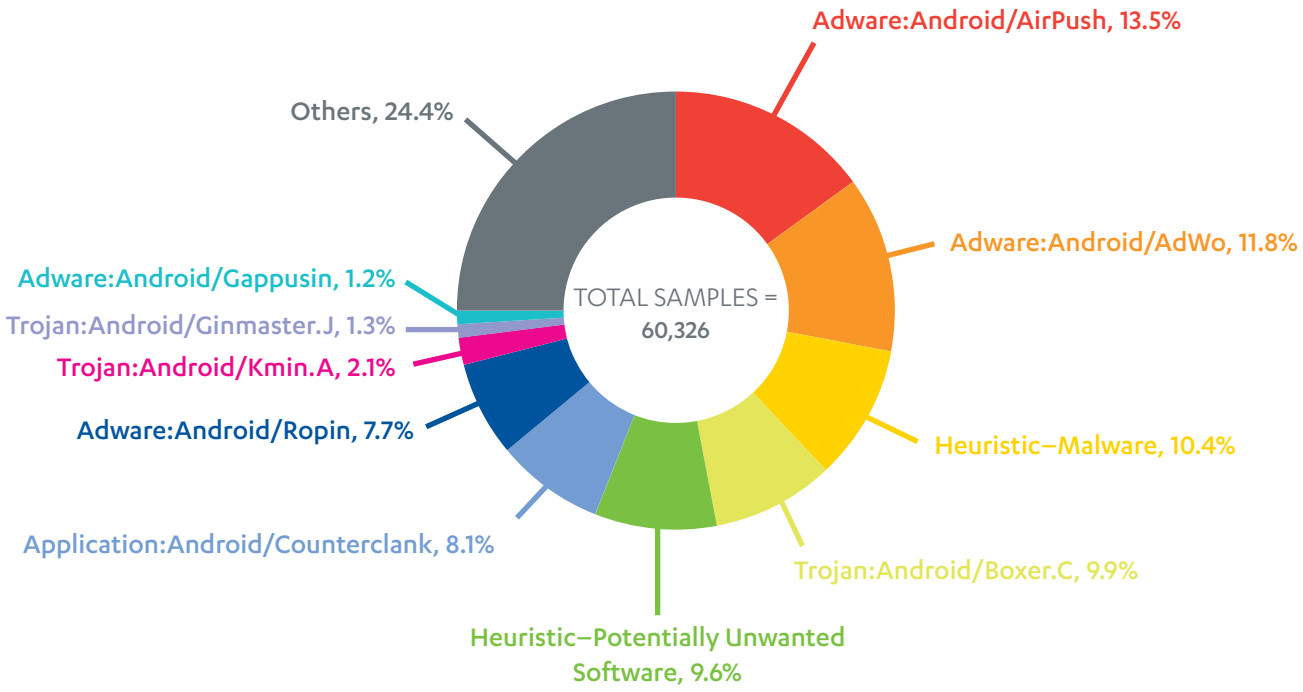


FIGURE 9: TOP ANDROID DETECTIONS, Q4 2012



NOTE: The threat statistics used in **Figure 8** and **Figure 9** are made up of the number of unique Android application package files (APKs).

TABLE 1: TOP MALWARE AND POTENTIALLY UNWANTED SOFTWARE ON ANDROID, Q4 2012

TOP-30 MALWARE

DETECTION	COUNT
Heuristic – Malware	6265
Trojan:Android/Boxer.C	5989
Trojan:Android/Kmin.A	1270
Trojan:Android/Ginmaster.J**	775
Trojan:Android/FakeInst.A	723
Trojan:Android/Ginmaster.G**	615
Trojan:Android/FakeBattScar.A	608
Trojan:Android/SmsSend.A	543
Trojan:Android/FakeInst.K	502
Trojan:Android/SMStado.A	472
Trojan:Android/Temai.A**	443
Trojan:Android/Ginmaster.I**	434
Trojan:Android/Ginmaster.F**	423
Trojan:Android/Ginmaster.E**	368
Trojan:Android/Ginmaster.C	347
Trojan:Android/Ginmaster.B	336
Trojan:Android/Geinimi.D	295
Trojan:Android/FakeBattScar.B	269
Trojan:Android/RuFailedSMS.A	257
Trojan:Android/DroidKungFu.C	238
Trojan:Android/FakeInst.T**	230
Trojan:Android/OpFake.F	199
Trojan:Android/FakeInst.U**	188
Trojan:Android/Nyearleak.A	186
Trojan:Android/SMSLoader.A	163
Trojan:Android/FjCon.A	158
Trojan:Android/Kmin.B	146
Trojan:Android/JiFake.E	144
Trojan:Android/Kmin.C	139
Trojan:Android/IconoSys.A	118

TOP-30 POTENTIALLY UNWANTED SOFTWARE

DETECTION	COUNT
Adware:Android/AirPush	8137
Adware:Android/AdWo	7127
Heuristic – Potentially Unwanted Software	5783
Application:Android/Counterclank	4860
Adware:Android/Ropin	4647
Adware:Android/Gappusin	733
Application:Android/FakeApp	549
Hack-Tool:Android/DroidRooter.A	230
Hack-Tool:Android/DroidRooter.B	161
Riskware:Android/Boxer	115
Riskware:Android/MobileTX	106
Spyware:Android/EWalls	91
Riskware:Android/PremiumSMS.F	69
Hack-Tool:Android/DroidRooter.I	51
Riskware:Android/SMSAgent	46
Application:Android/Steveware	39
Riskware:Android/FakeAngry	34
Monitoring-Tool:Android/MobileSpy.C	33
Hack-Tool:Android/TattooHack.A	32
Application:Android/NandroBox	32
Monitoring-Tool:Android/SpyTrack.B	28
Riskware:Android/AutoRegSms	25
Riskware:Android/PremiumSMS.J	23
Riskware:Android/PremiumSMS.AA	22
Riskware:Android/SmsReg	19
Riskware:Android/PremiumSMS.L	18
Monitoring-Tool:Android/MobileTracker.A	16
Monitoring-Tool:Android/SpyBubble.B	16
Riskware:Android/PremiumSMS.M	15
Hack-Tool:Android/DroidSheep.A**	15

**New family or new variant discovered in Q4 2012

NOTE: The threat statistics used in **Table 1** are made up of the number of unique Android application package files (APKs).

Protecting the Irreplaceable

Document made public since: 7 March 2013

F-Secure