MOBILE THREAT REPORT

Q2 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.

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 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 SECOND 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 WERE COLLECTED BETWEEN 1 APRIL–27 JUNE 2012.

Contents

EXECUTIVE SUMMARY

CHANGES IN THE ANDROID THREAT LANDSCAPE

Every quarter, Android malware continues to grow in number, and Q2 2012 is no exception. We received a total of 5033 malicious Android application package files (APKs), most of which are coming from third-party Android markets. This amount is a 64% increase compared to the number in the previous quarter. Out of this amount, we identified 19 new families and 21 new variants of existing families. A high concentration of these new variants is coming from FakeInst and OpFake, two families that are found to be related. Malware in these two families share a lot of similarities that in some instances, they can be classified as one family. In general, the new variants retain the same malicious behavior as found in the previous ones, only improving on the method used in defeating anti-virus technology in order to avoid detection.

"In May 2012, the first Android malware to use the drive-by download method was spotted in the wild."

After a while on the scene, Android malware has begun to explore new methods of infection as evidenced by NotCompatible.A and Cawitt.A. In May 2012, the first Android malware to use the drive-by download method was spotted in the wild, detected as Trojan-Proxy:Android/NotCompatible.A. A simple visit to a malicious website could render a device infected, if the device is configured to allow installations from unknown sources. When visiting a specially crafted website, the device will automatically download an application from the site. This application is then shown in the notification menu, waiting for the user to install it. To convince the user into installing it, the malware relies on social engineering tactics, naming the application as "com.Security.Update' and the filename as "Update.Apk." Once infected, the device is turned into a proxy or becomes part of a bot network.

In addition to drive-by download, another infection method discovered in this quarter is the utilization of Twitter as a bot mechanism. Cawitt.A for instance, accesses a Twitter account (possibly set up by the malware) to obtain a server address, from which it communicates with and receives further command from. Upon receiving instructions, this malware sends out SMS messages to certain numbers, and forwards data on the device's International Mobile Equipment Identity (IMEI) number, phone number, and Android ID to the aforementioned server.

Aside from the continuing growth of Android malware and the discovery of new infection methods, the second quarter also reveals a trend in regionally-based attack. In Spain for instance, we tend to get a lot of reports on banking-related attacks. This quarter, SmsSpy.F which is related to Zitmo, is a fairly popular case being reported. The malware appears to be specifically targeting users who perform an online banking transaction and need the Mobile Transaction Authorization Number (mTAN). It arrives as an SMS message, notifying the user to download a security application from the provided link.

LATEST THREATS IN THE LAST THREE MONTHS

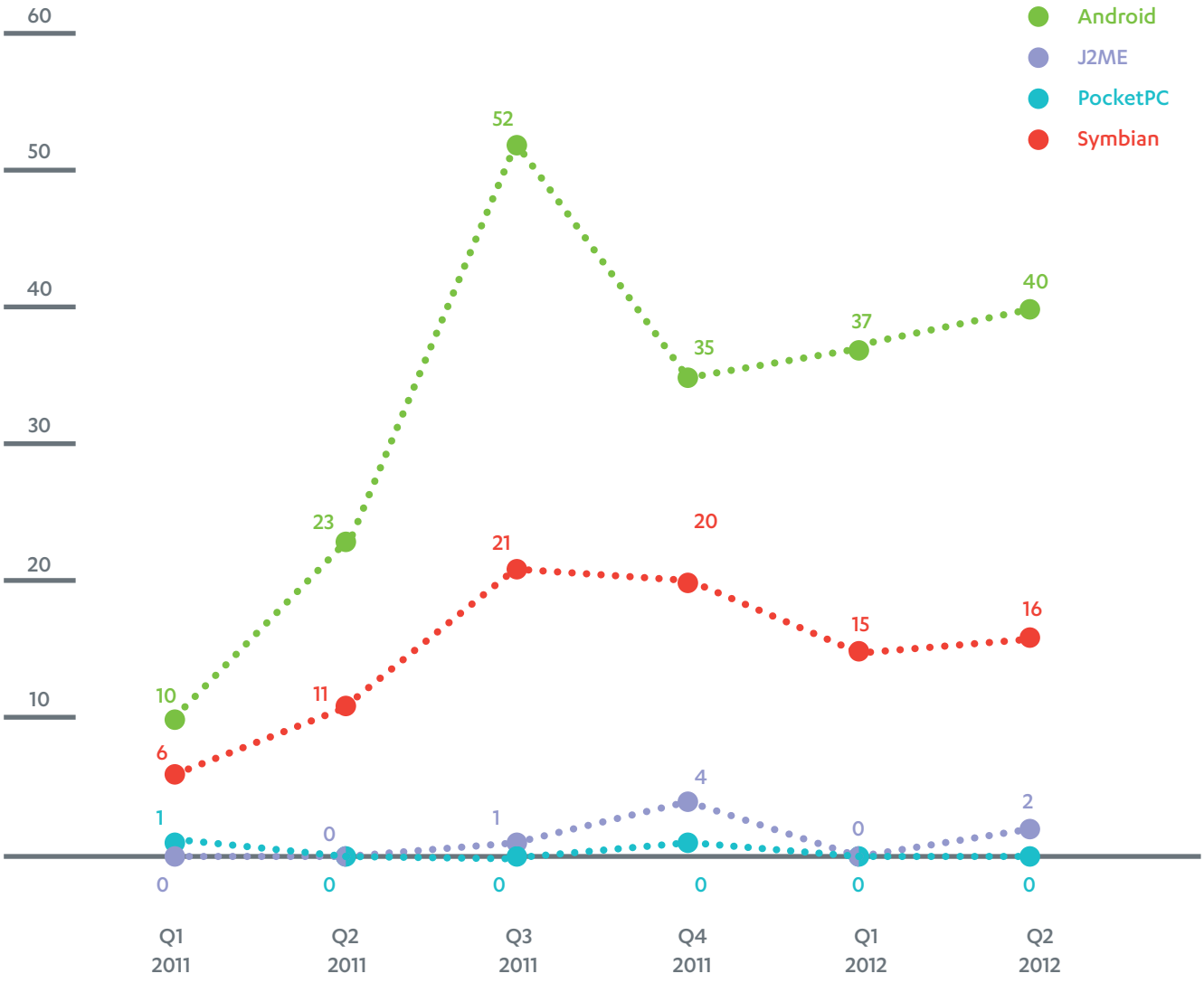


FIGURE 1: NEW FAMILIES AND VARIANTS RECEIVED PER QUARTER

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.

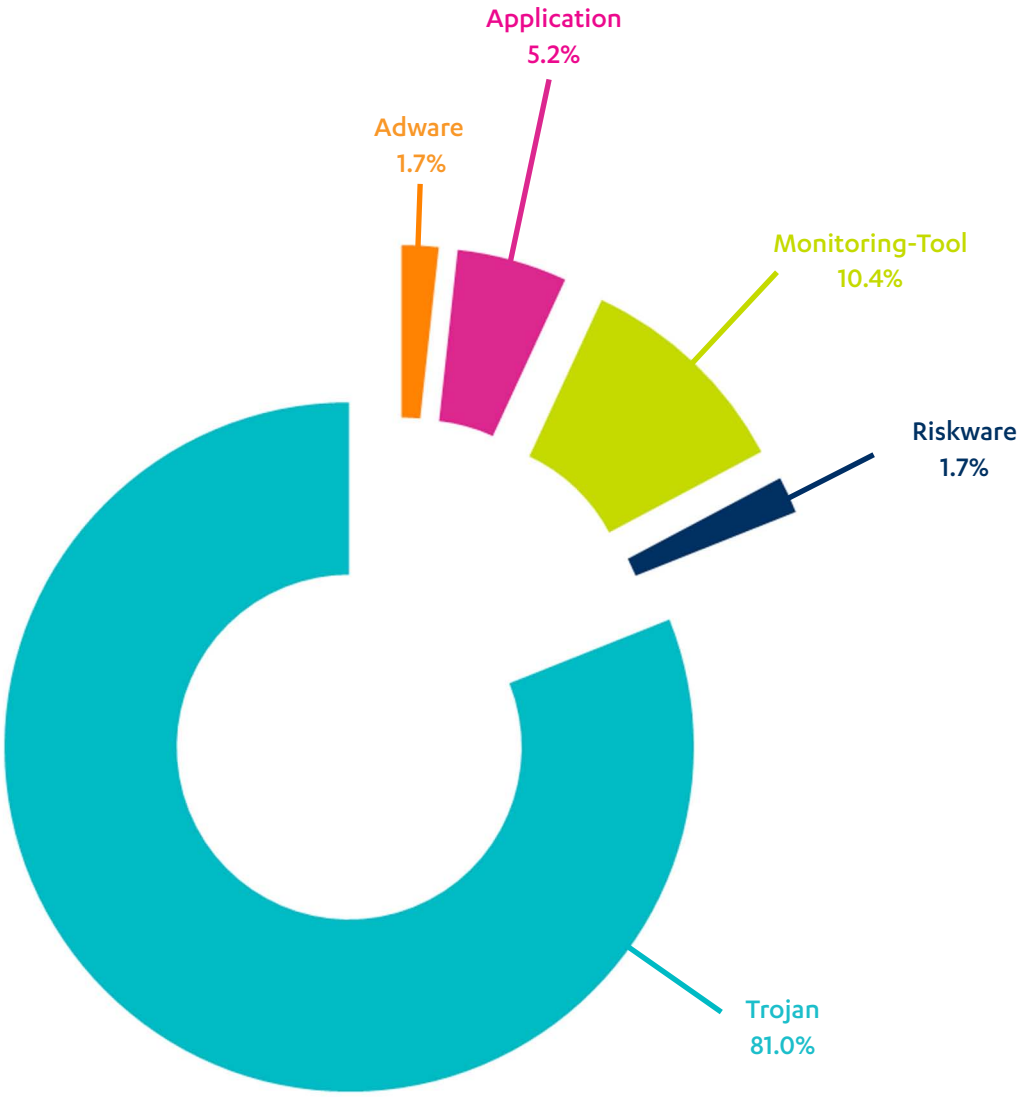


FIGURE 2: MOBILE THREATS BY TYPE, Q2 2012

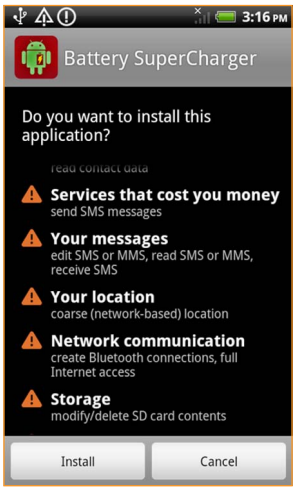
NOTE: The threat statistics used in **Figure 2** are made up of families and variants instead of unique files. For instance, if two samples are detected as Trojan:Android/GinMaster.A, they will only be counted as one in the statistics.

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.

Adware:Android/Mobsqueeze.A

Mobsqueeze.A is an adware module that was found to be exclusively used by Trojans in the FakeBattScar family to advertise the rogue Battery Optimizer or Battery Optimizer Application. A separate detection has also been added to detect applications that promote the FakeBattScar Trojans.



Permissions requested by Mobsqueeze.A

Application:Android/AdOp.A

AdOp.A is an application that arbitrarily creates shortcuts and advertisement-motivated notifications, which link to a website or an application. The application that users is being led to may not even be present on the device, but it does not stop Ropin.A from creating its corresponding shortcut.

AdOp.A is not directly harmful to the device, but it may poses some risks if the shortcut or notification leads users to a questionable website.

Monitoring-Tool:Android/AndSpy.A

AndSpy.A is a monitoring and anti-theft program that originated from China, but is also marketed to several English speaking regions. Its capabilities can be remotely triggered by sending a particular SMS message to the device. If the message contains a valid command, it will silently perform the corresponding task. For example:

- 0# : Register the Master number that will be used to send replies
- 1# : Enable SMS forwarding
- 2# : Disable SMS forwarding
- 8# : Send device's contacts
- 10# : Send location details

AndSpy.A is a stealthy program. It performs malicious activities quietly, and leaves no visible clue that can indicate its presence on the device.

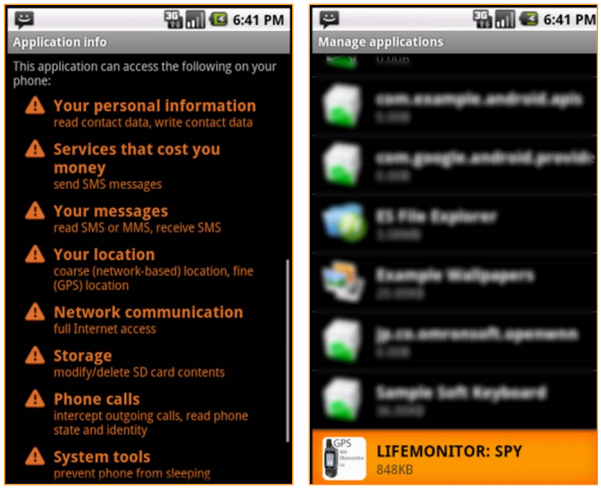
Monitoring-Tool:Android/Lifemonspy.A

Lifemonspy.A is a monitoring and anti-theft program that provides the user with some control of the device through SMS messages. It allows the user to perform these actions from a remote location:

- Deleting contacts
- Deleting contents of the external storage (SD card)
- Transferring SMS messages in the inbox to a Gmail account
- Deleting previously sent messages from the outbox
- Turning off the device

The program places no visible icon on the menu screen, but can be seen listed on the 'Manage applications' window. From time to time, it forwards the device's location to a remote website.

Upon detecting a change in the device's Subscriber Identity Module (SIM), Lifemonspy.A will send out an alert message to a configured number and log the event on the aforementioned website.



Permissions requested by Lifemonspy.A (left), and Lifemonspy.A as viewed on the 'Manage applications' window (right)

Monitoring-Tool:Android/MobileTracker.A

MobileTracker.A is a part of Samsung DIVE, a free service that allows device owners to track and control their device remotely. In case of theft, the owner can lock and wipe the device, receive notification on SIM card change, as well as track the device.

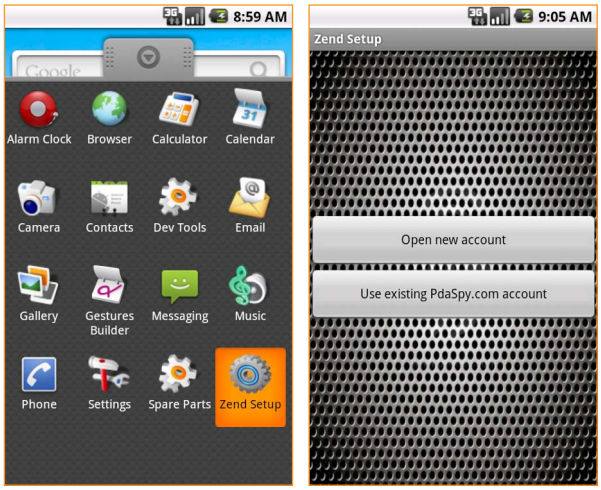
Monitoring-Tool:Android/PdaSpy.A

PdaSpy.A is a commercial monitoring application with a 24-hours free or trial lock. It must be manually installed on the targeted device, and an account at PdaSpy.com must be created.

Once installed, it places no icon on the application menu to avoid being noticed. It just runs silently in the background, logging the following information:

- Phone calls
- SMS messages
- GPS locations

The information can be viewed by visiting the PdaSpy website and logging in to the user account.

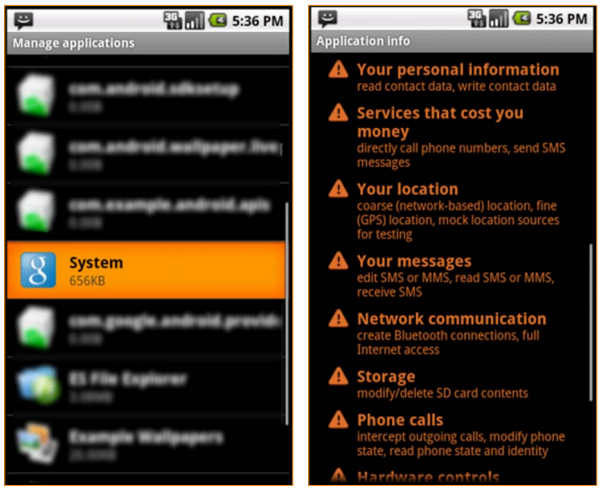


An account at PdaSpy.com is needed to view logged data

Monitoring-Tool:Android/SpyEra.A

SpyEra.A is programmed to monitor and retrieve data from a compromised device. Its malicious activities are triggered when the device receives a specially crafted SMS message.

SpyEra.A places no visible icon on the application menu, but its presence is revealed with a quick look under the 'Manage applications' in Settings.



SpyEra.A as listed under 'Manage applications' (left), and the permissions it requested (right)

Monitoring-Tool:Android/SpyHasb.A

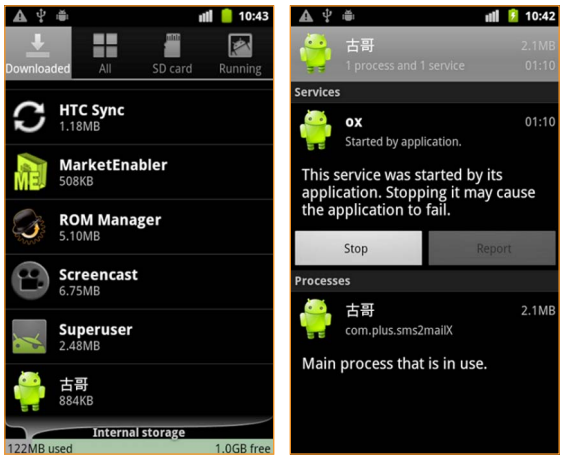
SpyHasb.A is a commercial monitoring tool that is marketed as 'Phone Tracker,' 'Husband Tracker,' 'Wife Tracker,' and 'Android Locator' among other names. Its capabilities include monitoring the following information:

- Phone calls
- SMS messages
- GPS locations

SpyHasb.A's user interface, as seen on a device

Riskware:Android/QPlus.A

QPlus.A is a tool that gathers information from the device it was installed on. It runs silently in the background, and cannot be seen on the list of applications. Its presence however, becomes visible when looking into application management.



QPlus.A runs as a service in the background

When monitoring a device, QPlus.A runs in the background as a service. It monitors and collects the following information, which is later sent to a proxy mail server:

- Call logs
- SMS messages
- Instant Messenger Chat History

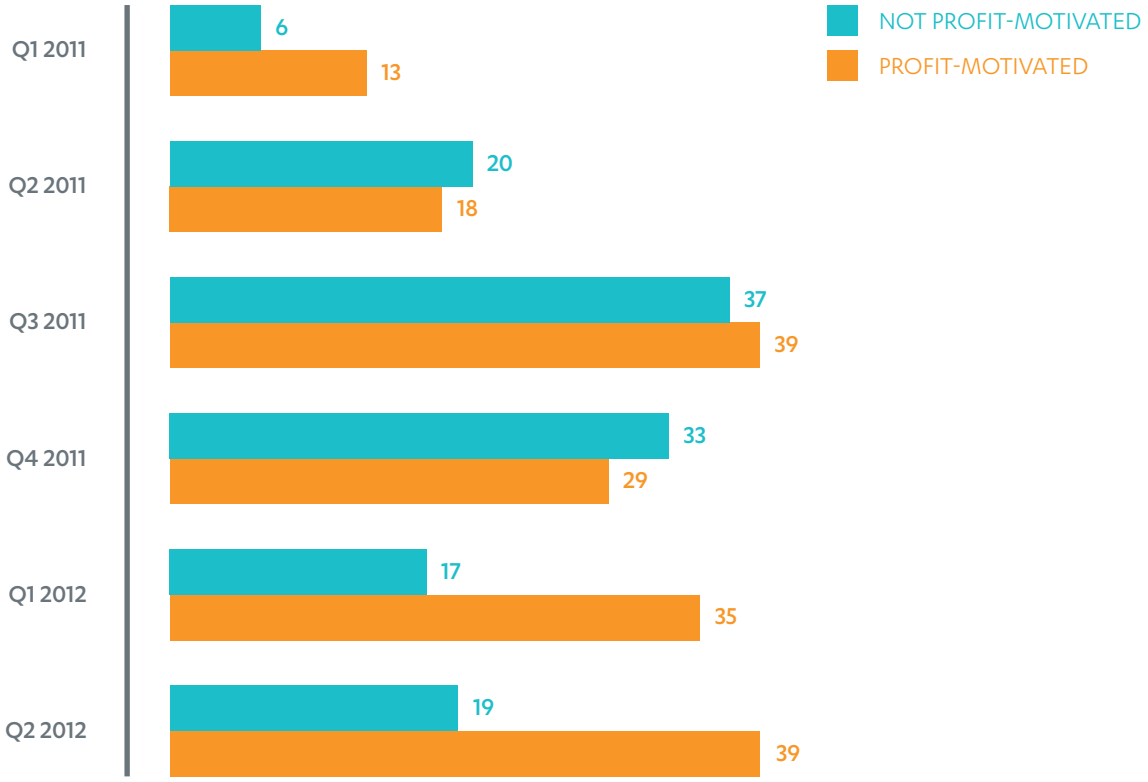


FIGURE 3: MOBILE THREATS MOTIVATED BY PROFIT

NOTE: The threat statistics used in **Figure 3** 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.

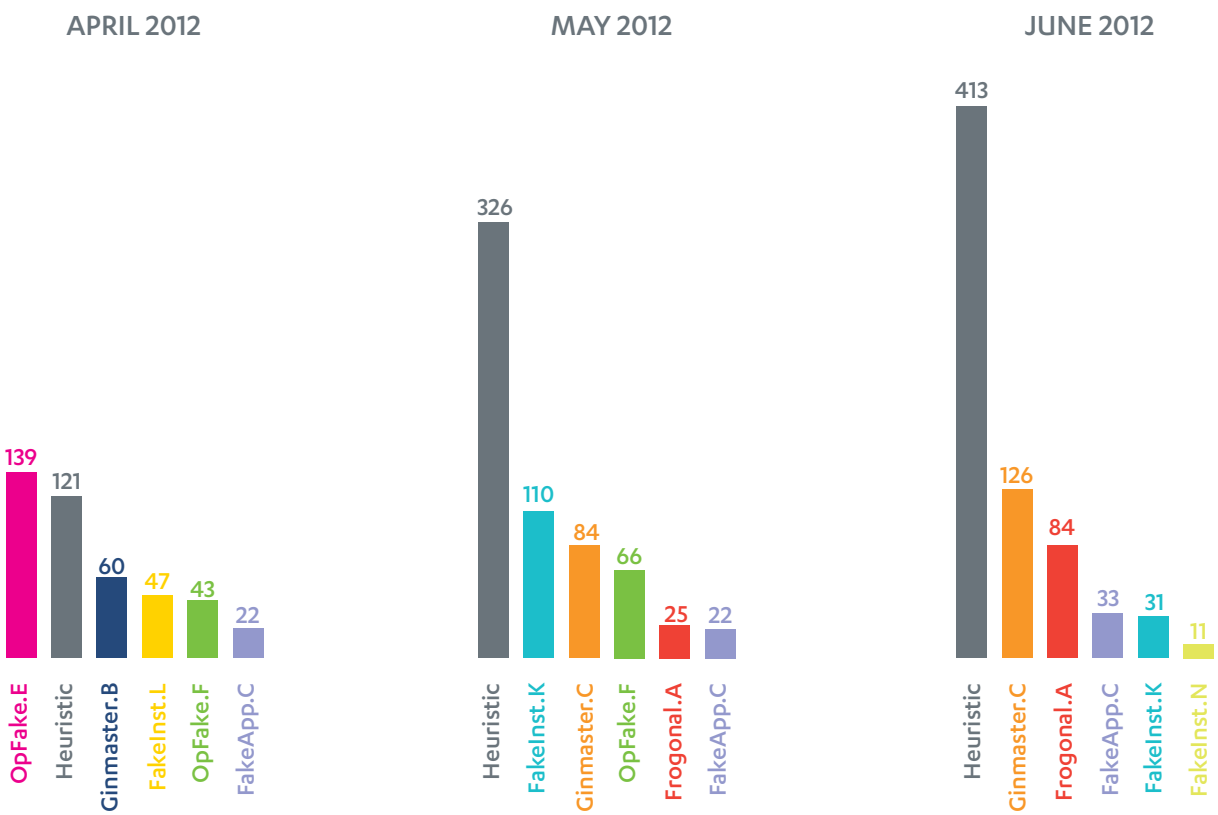


FIGURE 4: TOP-6 ANDROID DETECTIONS PER MONTH, Q2 2012

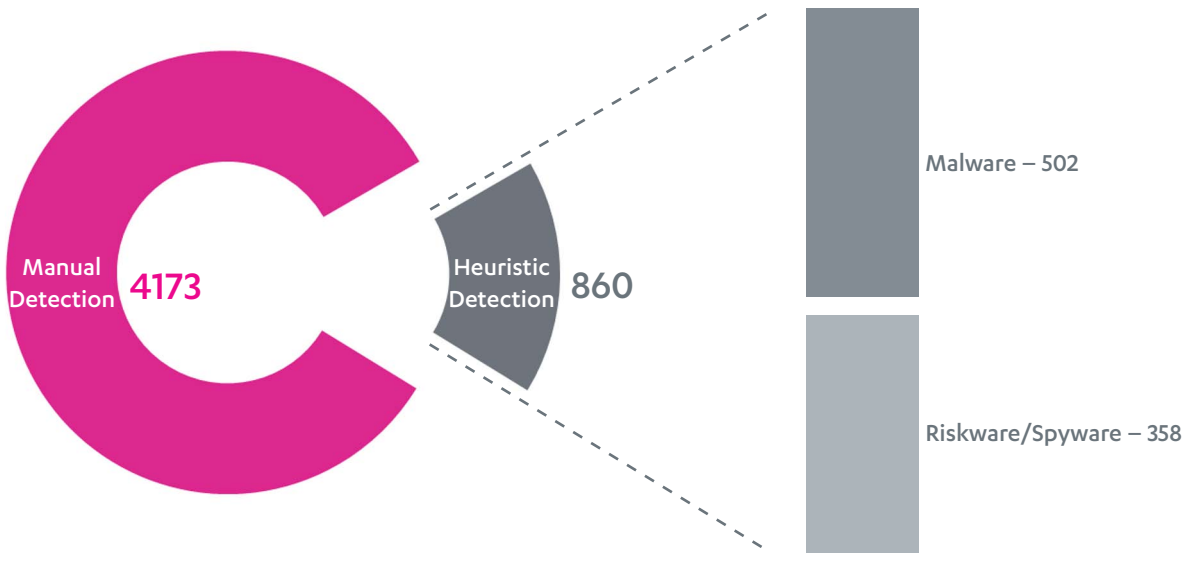


FIGURE 5: BREAKDOWN OF DETECTION COUNT, Q2 2012

NOTE: The threat statistics used in **Figure 4** and **Figure 5** are made up of the number of unique Android application package files (APKs).

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.

Trojan:Android/AcnetSteal.A

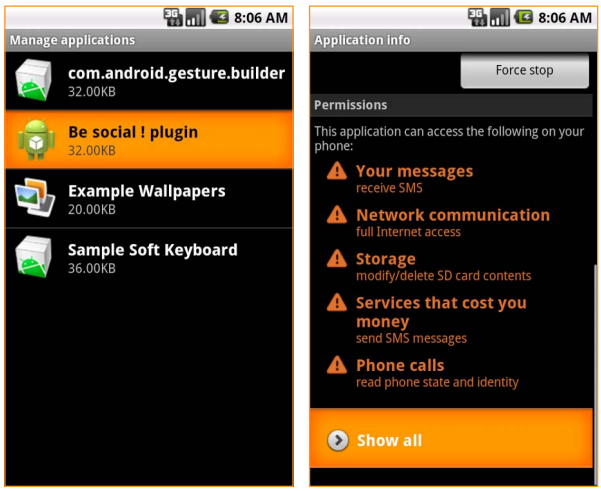
AcnetSteal.A is a program that harvests data and information from the device. It obtains the following information:

- Email addresses
- Phone numbers

AcnetSteal.A as seen on a device

Trojan:Android/Cawitt.A

Once installed, Cawitt.A will not place a launcher icon in the application menu to prevent it from being noticed by the user. Its presence, however, can be revealed with a quick look under the 'Manage applications' in Settings.



Cawitt.A as listed in the device, and the permissions it requested

Cawitt.A operates silently in the background, gathering device information which it later forwards to a remote server. Collected information include:

- Device ID
- International Mobile Equipment Identity (IMEI) number
- Phone number
- Bot ID
- Modules

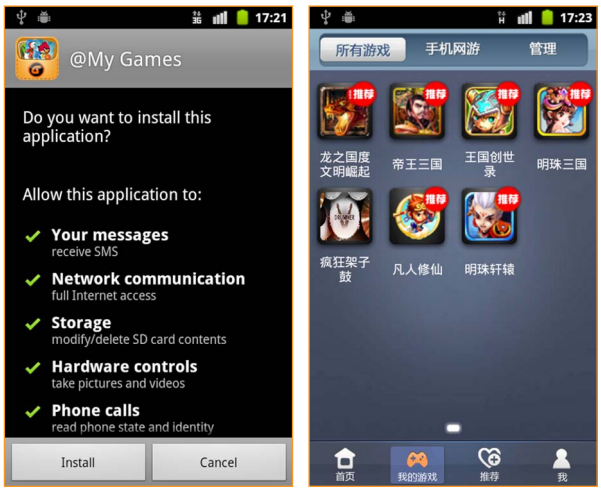
It also sends out premium-rate SMS messages from the device upon receiving command from the remote server.

Trojan:Android/Frogonal.A

Frogonal.A is a trojanized malware; it is a repackaged version of an original application where extra functionalities used for malicious intent have been added into the new package.

Frogonal.A harvests the following information from the compromised device:

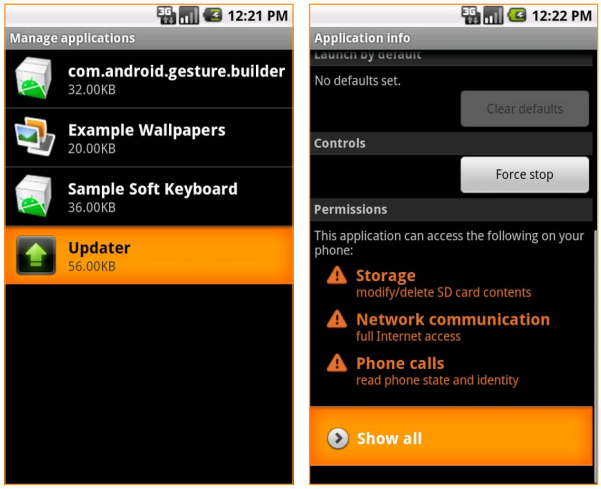
- Identification of the trojanized application
  - » Package name
  - » Version code
- Phone number
- IMEI number
- IMSI number
- SIM serial number
- Device model
- Operating system version
- Root availability



Requested permissions and offered games in Frogonal.A

Trojan:Android/Gamex.A

Gamex.A hides its malicious components inside the package file. Once it is granted a root access by the user, it connects to a command and control (C&C) server to download more applications and to forward the device IMEI and IMSI numbers. Additionally, it also establishes a connection to an external link which contains a repackaged APK file, and proceeds to downloading and installing the file.



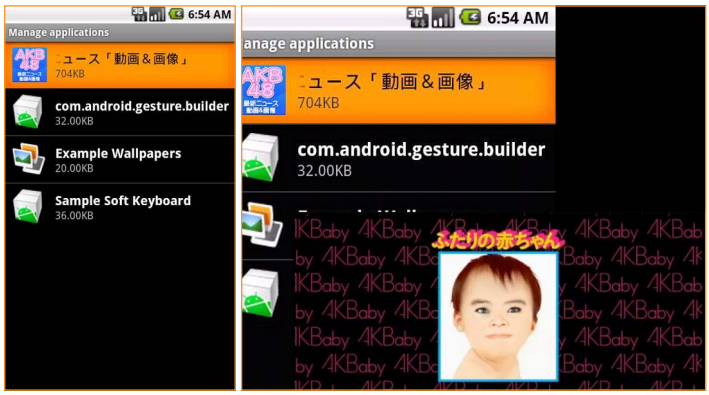
Gamex.A listed as 'Updater' (left), and the permissions it requested (right)

Trojan:Android/KabStamper.A

KabStamper.A is a malware that circulated in Japan during the AKB48 'election.' AKB48 is a Japanese pop group that consists of 48 members. The 'election' was held to select the most popular member who will become the face of the group.

AKB48: A popular music act in Japan, this pop group consists of 48 members.

KabStamper.A is distributed via trojanized applications that deliver news and videos on the AKB48 group. Malicious code in the malware is highly destructive; it destroys images found in the **sdcard/DCIM/camera** folder that stores images taken with the device's camera. Every five minutes, the malware checks this folder and modifies a found image by overwriting it with a predefined image.

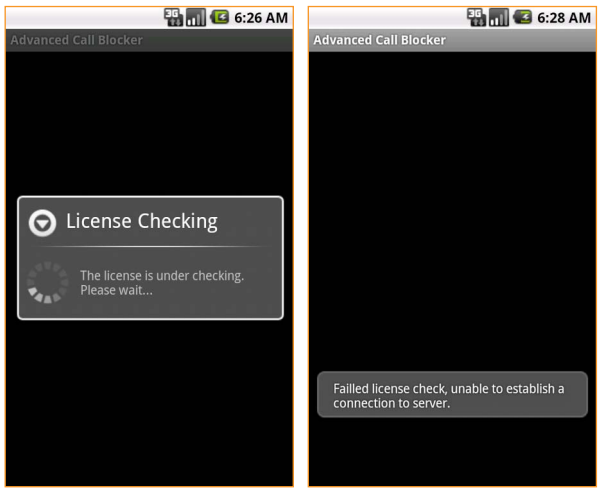


Comparison between before and after KabStamper.A's infection

Trojan:Android/Mania.A

Mania.A is an SMS-sending malware that sends out messages with the content "tel" or "quiz" to the number 84242. Any reply from this number is redirected to another device to prevent user from becoming suspicious.

While running, Mania.A appears to be performing license checking, but this process always fails and never seems to be completed. The license checking is a cover up for the SMS sending activities that are taking place in the background.



Mania.A pretends to perform license checking, which always failed

Mania.A is known for using the trojanization technique, where it is repackaged with another original application in order to dupe victims. Some known legitimate applications that have this malware trojanized in their package include:

- Phone Locator Pro
- CoPilot Live Europe
- Setting Profile Full
- Tasker

Trojan:Android/PremiumSMS.A, and variant B

PremiumSMS.A is a Trojan that reaps profit from its SMS sending activities. It has a configuration file that contains data on the content of the SMS messages and the recipient numbers.

Example of the sent messages:

- Number: 1151
- Content: 692046 169 BGQCb5T3w

- Number: 1161
- Content: 692046 169 BGQCb5T3w

- Number: 3381
- Content: 692046 169 BGQCb5T3w

- Number: 1005
- Content: kutkut clsamg 6758150

- Number: 5373
- Content: kutkut clsamg 6758150

- Number: 7250
- Content: kutkut clsamg 6758150

Trojan:Android/SmsSpy.F

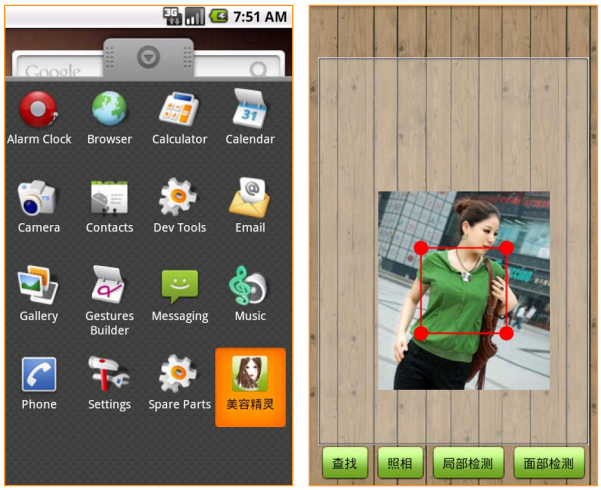
SmsSpy.F poses as an Android Security Suite application that actually does nothing in ensuring the device's security. It does however, records received SMS messages into a secsuite.db instead.

SmsSpy.F poses as an Android Security Suite application

This malware targets banking consumers in Spain where it is spammed via a message indicating that an extra Security Protection program that protects the device is available for download.

Trojan:Android/UpdtKiller.A

UpdtKiller.A connects to a command and control (C&C) server, where it forwards users' data to and receives further command from. This malware is also capable of killing anti-virus processes in order to avoid being detected.



UpdtKiller.A as seen on a device

Trojan:Android/Uranico.A

Uranico.A is a Trojan that harvests the following information from an infected device:

- Phone number
- IMEI number
- IMSI number
- Contacts or Address Books (phone numbers and email addresses)

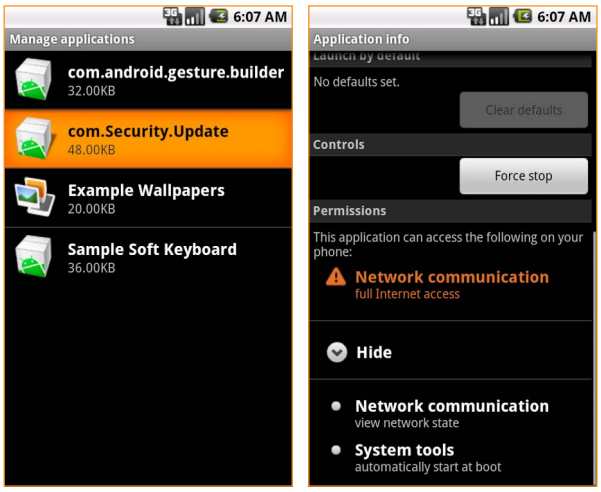
The harvested information are later forwarded to a remote server.

Uranico.A as seen on a device

Trojan-Proxy:Android/NotCompatible.A

NotCompatible.A operates like a drive-by download threat. It gains entry into a device when the user visits a compromised website, and proceeds to downloading a package, update.apk. But for the installation to begin, the user needs to click on it.

Once installed, the malware may also communicate with certain command and control (C&C) servers as evidenced by two addresses found in an encrypted file within the malware.



NotCompatible.A pretends to be a security update file

Trojan:J2ME/CuteFreeSMS.A

CuteFreeSMS.A is a Trojan that collects profit by sending SMS messages to premium-rate numbers. The SMS-sending activities take place in the background, without the device user's authorization or acknowledgement.

Trojan:J2ME/ValeSMS.A

ValeSMS.A is a Trojan that collects profit by sending SMS messages to premium-rate numbers. The SMS-sending activities take place in the background, without the device user's authorization or acknowledgement.

Trojan:Symbian/AndroGamer.A

AndroGamer.A is Trojan that appears to be playing online or WAP games in the background. Its other malicious activities include:

- Downloading and installing new software
- Downloading configuration data from a remote host
- Sending device information to a remote host
- Dialing numbers to make new calls

Trojan:SymbOS/Kensoyk.A

Kensoyk.A contains references to anti-virus vendors, and is capable of killing anti-virus processes. It also downloads and installs software onto the compromised device.

Trojan:Symbian/LaunchOut.A

LaunchOut.A hides itself and avoids appearing on the device's user interface to keep its presence unnoticed. Its activities, which are carried out silently in the background, include:

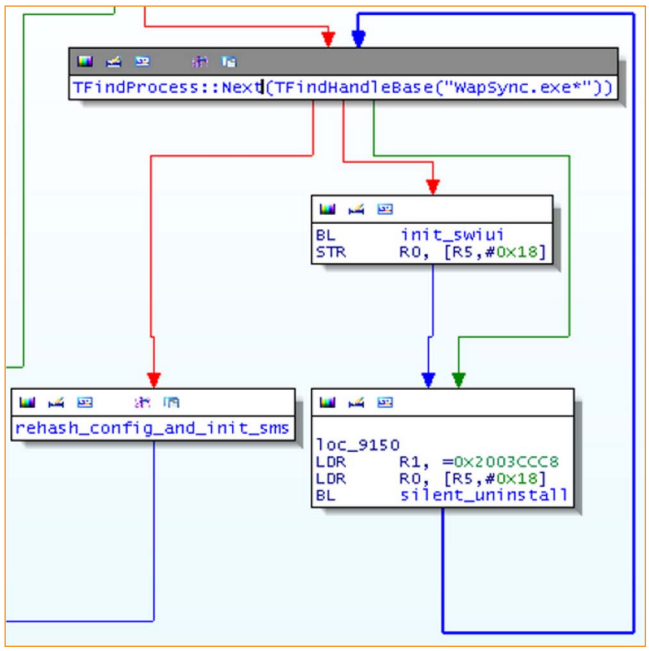
- Downloading and installing new software
- Monitoring and sending out SMS messages

Trojan:SymbOS/Lipcharge.A

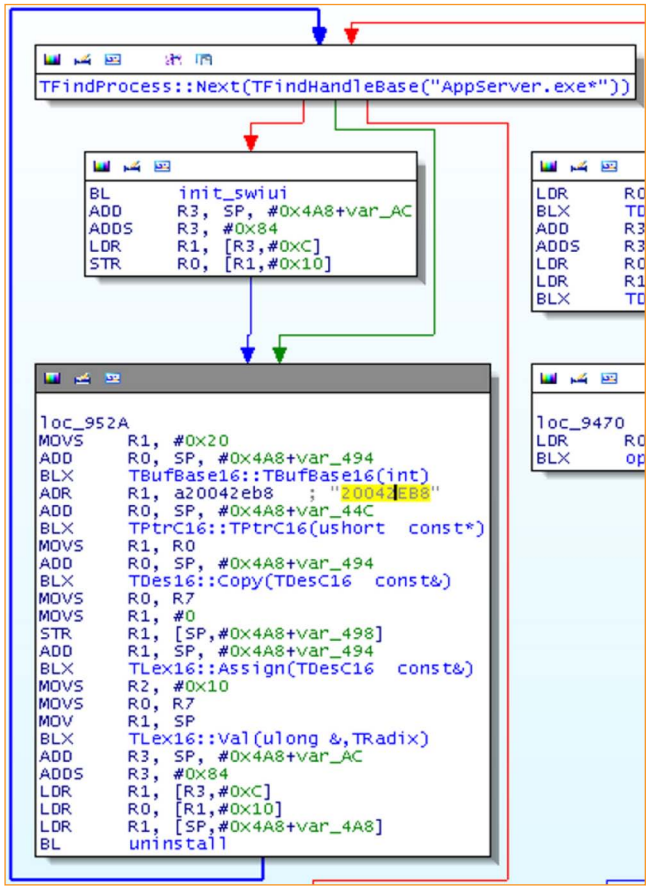
Lipcharge.A is possibly a downloaded component for another Trojan. It downloads configuration data and new software, which are later installed onto the compromised device. Other functionalities include sending and receiving SMS messages, and filtering certain SMS messages from the system log.

Trojan:SymbOS/Monlater.A, and variant B

Monlater.A contains a function that allows it to detect AppServer.exe processes and proceeds to uninstall a package with UID 0x20042EB8 from an infected devices. Similar functionality is also found in Monlater.B sample, but uses a different file name and UID.



Annotated disassembly of a Monlater.B sample, which shows similarities with Monlater.A



A disassembled and annotated function of a Monlater.A sample

Upon further inspection, samples in the Monlater family show a lot of similarities with those from another family — Monsoon, which was first discovered in early 2011. It is highly likely that Monsoon and Monlater connects to the same command and control (C&C) server. The same update channel may also have been used to push new versions of malware and hide the original ones to avoid detection.

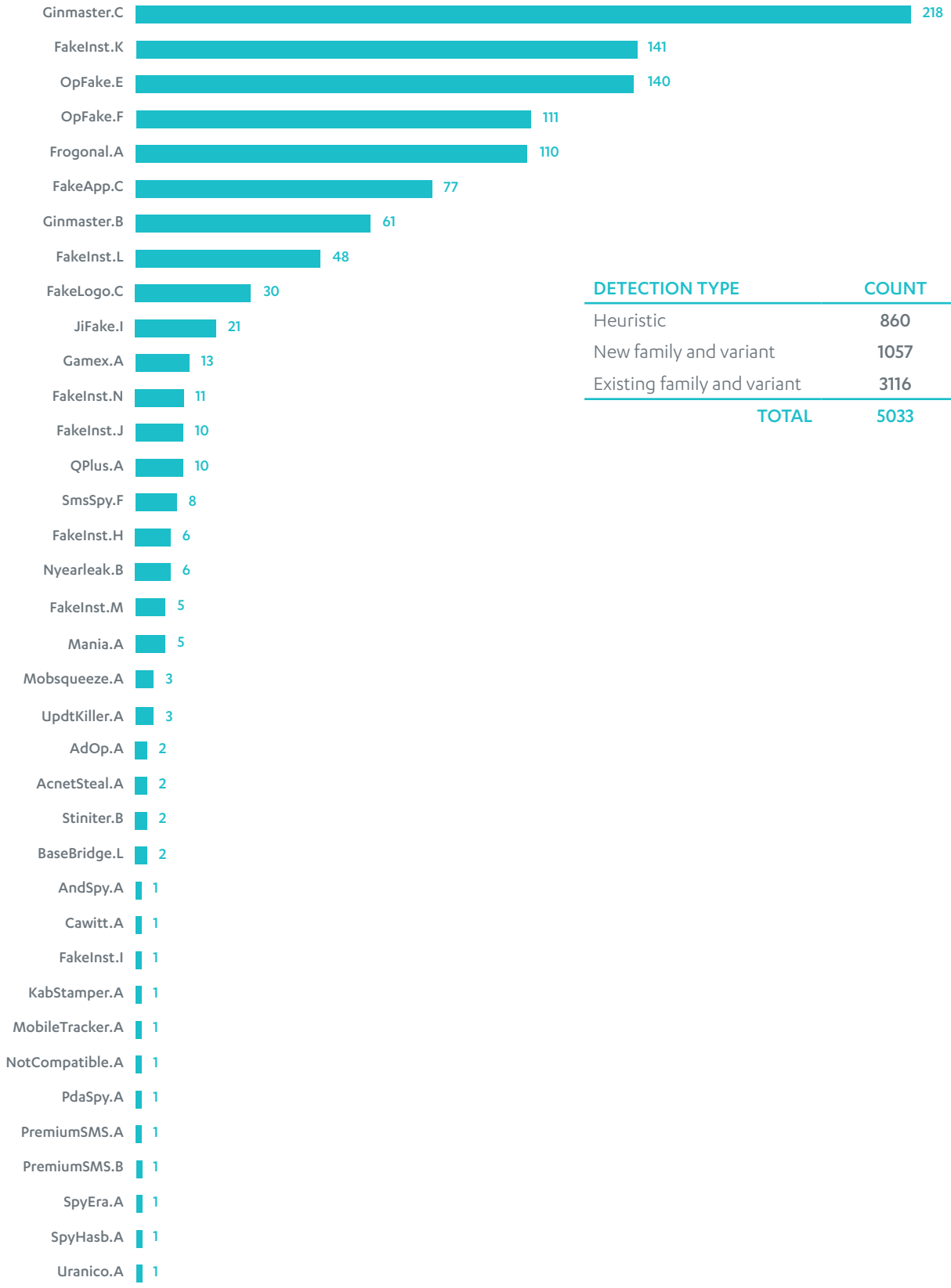
Trojan:Symbian/RandomTrack.A

RandomTrack.A is a Trojan which creation is not motivated by profit. It downloads an installer from a remote host, and proceeds to silently install this file onto the compromised device. It is also capable of killing anti-virus processes in order to avoid being detected.

New variants of already known families

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

- Trojan:Android/BaseBridge.L
- Trojan:Android/DroidKungFu.I
- Trojan:Android/FakeApp.C
- Trojan:Android/FakeInst.H, and variant I, J, K, L, M and N
- Trojan:Android/FakeLogo.C
- Trojan:Android/Ginmaster.B, and variant C
- Trojan:Android/JiFake.I
- Trojan:Android/Nyearleak.B
- Trojan:Android/OpFake.E, and variant F
- Trojan:Android/SmsSpy.F (see page 21 for description)
- Trojan:Android/Stiniter.B
- Trojan:Android/Zsone.C
- Trojan:Symbian/AndroGamer.B, and variant C
- Trojan:Symbian/FakeApp.C
- Trojan:Symbian/Melon.C
- Trojan:Symbian/Moporil.C
- Trojan:Symbian/SystemSync.B, and variant C and D
- Trojan:Symbian/Yorservi.E



DETECTION TYPE	COUNT
Heuristic	860
New family and variant	1057
Existing family and variant	3116
TOTAL	5033

FIGURE 6: NEW ANDROID MALWARE SORTED BY SAMPLE COUNT, Q2 2012

NOTE: The threat statistics used in **Figure 6** are made up of the number of unique Android application package files (APKs).

TABLE 1: TOP ANDROID SAMPLES RECEIVED IN Q2 2012

TOP-30 MALWARE

DETECTION	COUNT
Trojan:Android/Boxer.C	389
Trojan:Android/Ginmaster.C **	218
Trojan:Android/FakeInst.K **	141
Trojan:Android/OpFake.E **	140
Trojan:Android/OpFake.F **	111
Trojan:Android/Frogonal.A **	110
Trojan:Android/FakeInst.E	86
Trojan:Android/OpFake.C	77
Trojan:Android/Ginmaster.B **	61
Trojan:Android/Ginmaster.A	49
Trojan:Android/FakeInst.L **	48
Trojan:Android/Kituri.A	46
Trojan:Android/DroidKungFu.C	32
Trojan:Android/FakeLogo.C **	30
Trojan:Android/FakeInst.C	29
Trojan:Android/DroidKungFu.H	27
Trojan:Android/JiFake.I	21
Trojan:Android/BaseBridge.A	20
Trojan:Android/FakeBattScar.A	20
Trojan:Android/Bizimovie.A	16
Trojan:Android/Gamex.A **	13
Trojan:Android/Kmin.C	11
Trojan:Android/FakeInst.N **	11
Trojan:Android/JiFake.F	10
Trojan:Android/FakeInst.J **	10
Trojan:Android/SmsSpy.F **	8
Trojan:Android/SMStado.A	8
Trojan:Android/BaseBridge.B	7
Trojan:Android/DroidKungFu.F	6
Trojan:Android/FakeInst.H **	6

SPYWARE AND RISKWARE

DETECTION	COUNT
Adware:Android/Ropin.A	1617
Application:Android/Counterclank.A	545
Application:Android/FakeApp.C **	77
Spyware:Android/EWalls.A	14
Riskware:Android/QPlus.A **	10
Riskware:Android/Boxer.D	8
Application:Android/Nyearleak.B **	6
Exploit:Android/DroidRooter.B	4
Monitoring-Tool:Android/MobileSpy.C	3
Adware:Android/Mobsqueeze.A **	3
Application:Android/AdOp.A **	2
Hack-Tool:Android/TattooHack.A	2
Monitoring-Tool:Android/SpyBubble.B	1
Hack-Tool:Android/DroidRooter.M	1
Monitoring-Tool:Android/SpyHasb.A **	1
Exploit:Android/DroidDeluxe.A	1
Riskware:Android/MobileTX.A	1
Hack-Tool:Android/DroidRooter.A	1
Monitoring-Tool:Android/SpyEra.A **	1
Monitoring-Tool:Android/MobileMonitor.A	1
Monitoring-Tool:Android/Spyoo.A	1
Hack-Tool:Android/DroidRooter.B	1
Riskware:Android/GoManag.B	1
Monitoring-Tool:Android/MobileTracker.A **	1
Exploit:Android/DroidRooter.A	1
Monitoring-Tool:Android/PdaSpy.A **	1
Spyware:Android/SndApps.A	1
Monitoring-Tool:Android/AndSpy.A **	1
Monitoring-Tool:Android/CellShark.A	1

** New family or new variant discovered in Q2 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

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

Document made public since: 6 August 2012

F-Secure proprietary materials. © F-Secure Corporation 2012. All rights reserved.

F-Secure and F-Secure symbols are registered trademarks of F-Secure Corporation and F-Secure names and symbols/ logos are either trademark or registered trademark of F-Secure Corporation.

F-Secure