MOBILE THREAT REPORT

Q1 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 FIRST 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 LAST UPDATED ON 29 MARCH 2012.

CONTENTS

CHANGES IN THE MOBILE THREAT LANDSCAPE

Since its debut, Android has quickly claimed significant market share in the mobile market. Unfortunately, such popularity (amongst other factors) makes Android a lucrative target for malware authors. New families and variants of malware keep cropping up each quarter, and this trend shows no sign of slowing down. In Q1 2011, 10 new families and variants were discovered. A year later, this number has nearly quadrupled with 37 new families and variants discovered in Q1 2012 alone (please refer to **Figure 4** on Page 18). A comparison between the number of malicious Android application package files (APKs) received in Q1 2011 and in Q1 2012 reveals a more staggering find — an increase from 139 to 3063 counts. This growth in number can be attributed to malware authors crafting their infected or trojanized applications to defeat anti-virus signature detection, distributing their malware in different application names, and trojanizing widely popular applications.

"A comparison between the number of malicious Android application package files (APKs) received in Q1 2011 and in Q1 2012 reveals a more staggering find — an increase from 139 to 3063 counts."

With Android malware growing exponentially in number, there rises a need to protect users against up-and-coming threats in a more proactive manner. Utilizing cloud-based technology, the heuristics detection implemented in our new product has performed well in detecting unclassified threats based on malicious behavior, and in discovering new malware families and variants. A significant finding this quarter is the discovery of FakeToken.A, a Trojan that pretends to be a token generator for a mobile banking application. It was originally detected as a variant of FakeInst, but turns out to be a new but related family. Additionally, the heuristics technology is also responsible for discovering Boxer.H, a new variant of the existing Boxer family, which pretends to be Google Play.

In Q1 2012, malware authors are focusing on improving their malware's techniques in evading detection, as well as exploring new infection methods. Existing malware families such as DroidKungFu, GinMaster, and the Fakeinst umbrella family (which consists of Boxer, JiFake, SMSTado, FakeNotify, and OpFake) are adopting encryption and randomization techniques in order to evade detections. At the same time, some malware are also figuring out how to hide their data in an image file, as shown by FakeRegSMS.

Some prominent malware discovered in this quarter are Trojan-Downloader:Android/RootSmart.A, Trojan:Android/DroidKungFu.H, and Trojan:Android/Stiniter.A. They demonstrate an increasing complexity in their evolution or infection behavior. RootSmart.A for instance, downloads a root exploit to gain elevated privileges on the infected device, which allows it to install more applications onto the device. It also has a bot component that can receive command from a server to perform malicious routine such as making unauthorized call, sending premium-rate SMS messages, and accessing pay-per-view videos.

CONTINUE >>

DroidKungFu.H exhibits a tremendous improvement in its infection method. It now only requires a service in a trojanized application in order to load its native or binary component, which contains the rooting or privilege escalation code and the malicious routine, into a device. Once it gains user privileges, the Trojan can make system changes such as dropping the native copy into the system bin folder, and changing the configuration to enable automatic execution of the native component on reboot. By employing this method, the Trojan can no longer be removed easily using the traditional way, i.e., uninstalling the application.

Finally, Stiniter.A employs a different, yet still complex, infection technique. It is a multiple-component malware that has three installed applications, and a native component for rooting and installing other APK components. Similar to DroidKungFu.H, its native component is implemented in a way that no longer requires the generic or precompiled binary exploit. One of its APK can serve as a standalone malware, and can be installed as a service that carries out data gathering and SMS-sending activities.

The three malware (RootSmart.A, DroidKungFu.H, and Stiniter.A) mentioned above suggest that Android malware are focusing on utilizing the native component, and only downloading a root exploit when needed. Even then, the root exploit would be quickly deleted to prevent the malware from being profiled or detected as malicious by anti-virus products since the native component has yet to exist in their packages.

Over the year, Android threats have continued to improve their techniques in evading detection and their methods of infection, yet, nothing much has changed in their operation in collecting profit. The majority of malware discovered in Android markets are SMS-sending malware that reap profit from sending messages to premium numbers. Most of these malware are found on third-party market stores, but occasionally, some do manage to wriggle their way into the official Android Marketplace (now integrated into Google Play).

MALWARE FAMILY	COUNT
Boxer	246
DroidKungFu	23
EuropaSMS	2
Fakeinst	15
Fakeinst (FakeToken)	22
FakeRegSMS	2
JiFake	514
Others	4
TOTAL	828

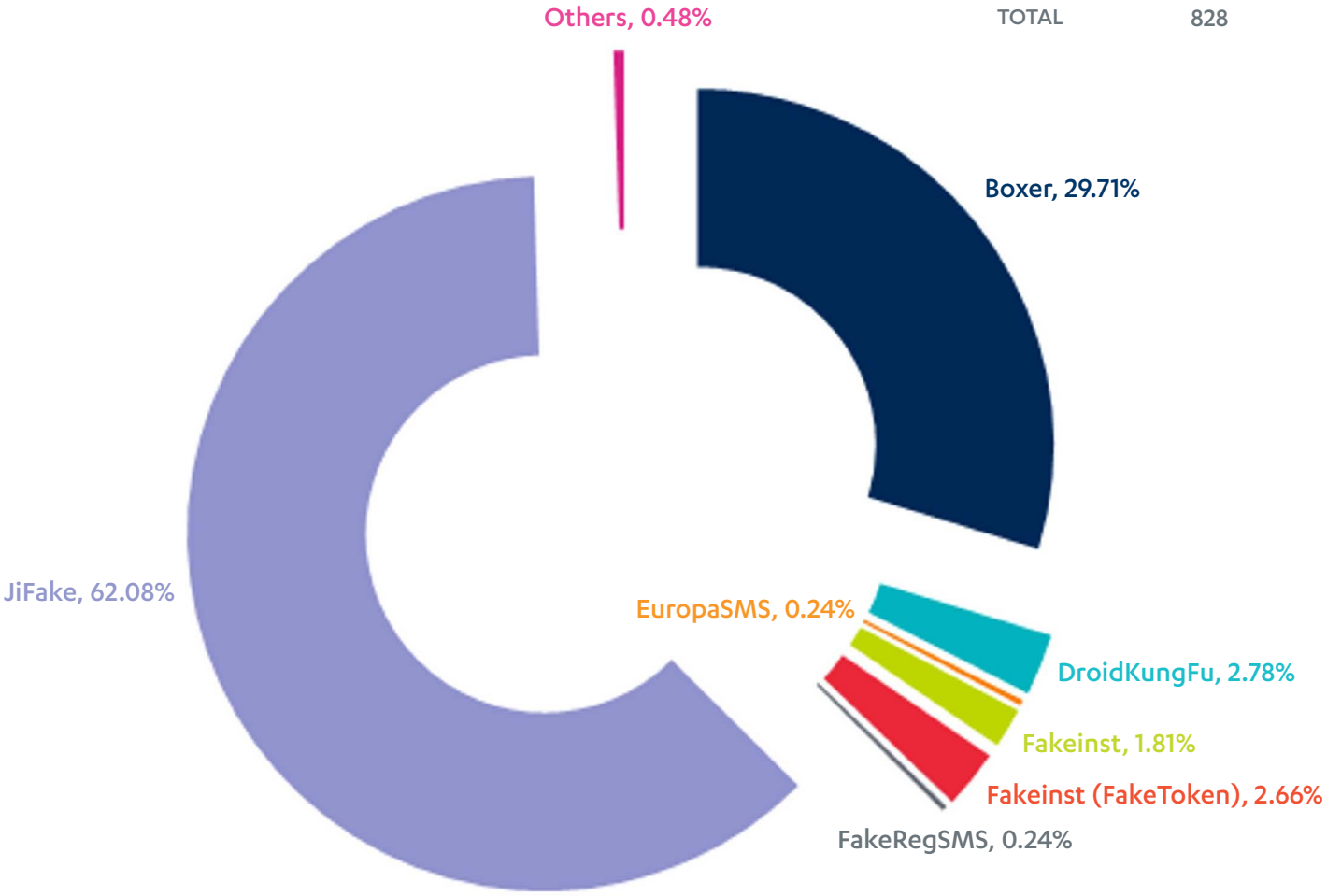


FIGURE 1: MALWARE FAMILIES DETECTED BY HEURISTIC DETECTION, Q1 2012

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.

LATEST THREATS IN THE LAST THREE MONTHS

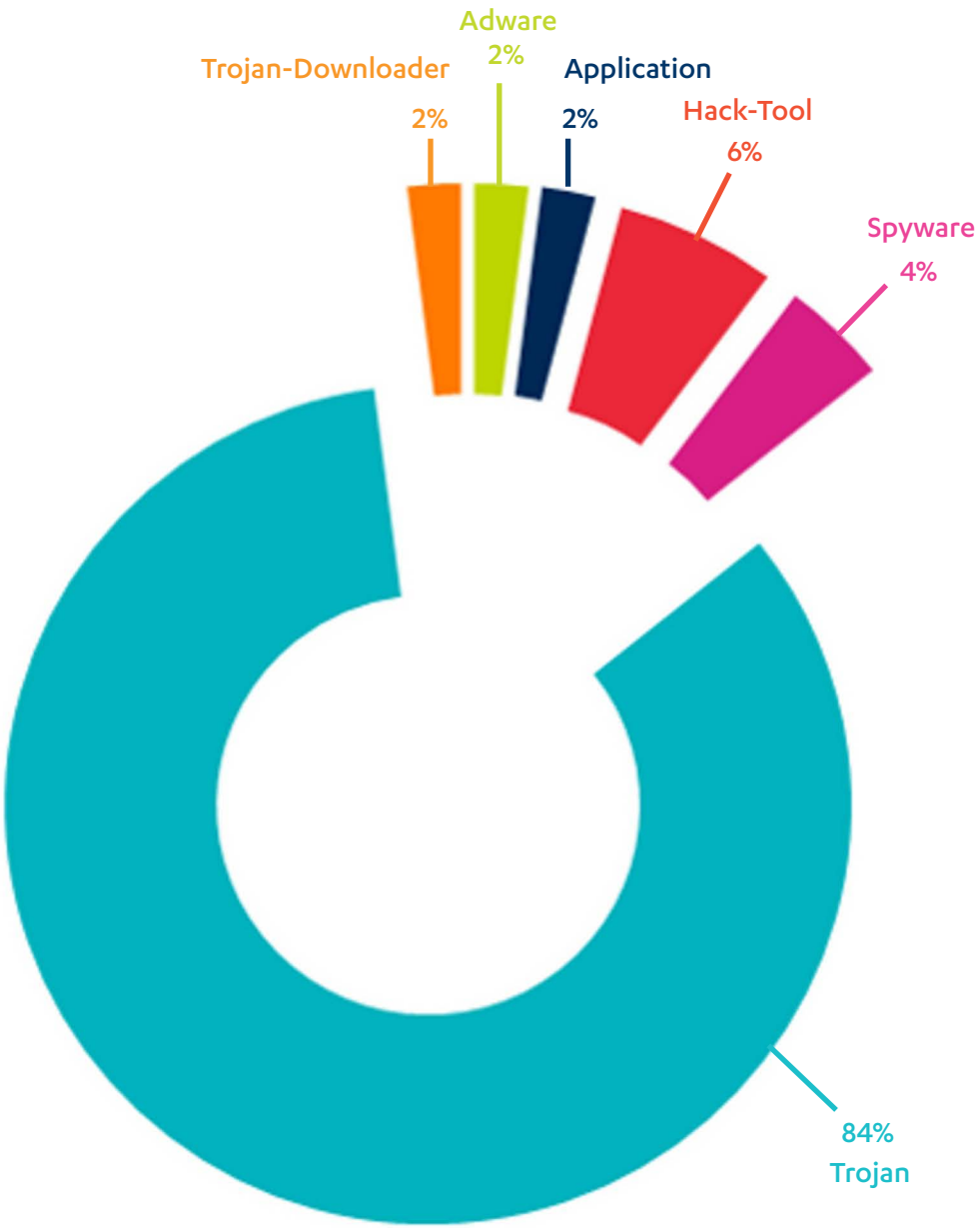


FIGURE 2: MOBILE THREATS BY TYPE, Q1 2012

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.

Application:Android/Counterclank.A

Counterclank.A is a Trojan that poses as a game application. While running, it retrieves information from the compromised device on which it was installed on. The information includes:

- IMEI (International Mobile Equipment Identity) number
- Phone number
- Operating system version

The Trojan then connects to a remote server, and forwards the retrieved information.

Counterclank.A posing as a game application

Application:Android/Steveware.A

Steveware.A attracts users by offering popular game applications at no charge, under the pretense of offering the trial versions.

During installation, it displays a message requesting for users to enter their email addresses to unlock the full version. The exact message is as follows:

> "Please click here to finish the installation process.
> To unlock the full version of this game for free, enter your email on the page and return to this application."

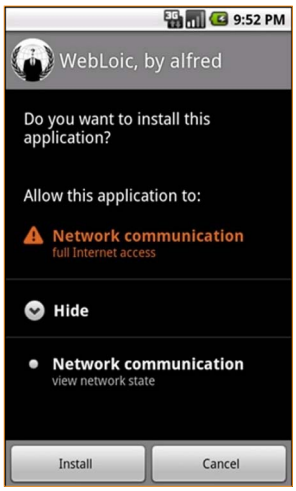
Messages displayed by Steveware.A, asking for users to provide their email addresses

Exploit:Android/DroidRooter.F

DroidRooter.F makes its way onto a device through another program; it is downloaded by Trojan-Downloader:Android/RootSmart.A. Once installed, it will root the device and gain root permissions that would allow it to run services or perform actions without any user intervention.

Hack-Tool:Android/LoicDos.A

Upon installation, LoicDos.A requests for the 'Network communication' permission, which will grant it full Internet access on the compromised device.



LoicDos.A requesting for full Internet access

When executed, it opens up to a website that contains Javascript to perform denial of service attack on a targeted server.

LoicDos.A getting ready to perform DoS attack

Hack-Tool:Android/MemPoDroid.A

This is the Android port of the recently released "Mempodipper" exploit that affects the non-Android distribution of the Linux kernel.

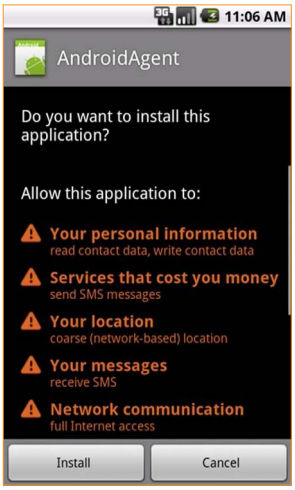
MemPoDroid.A is an Android Native binary executable that exploits the mem_write function in the Android Linux kernel version 2.6.39 and above. This version of Android Linux kernel is commonly found on newer releases of Android devices, which runs on the Android 4.0 (Ice Cream Sandwich) version of operating system.

A successful exploitation may result in gaining a major user access to the affected device, granting the attacker the capability to perform any action on the device.

NOTE: For additional details on the Mempodipper exploit, please refer to 'Linux Local Privilege Escalation via SUID /proc/pid/mem Write' at (http://blog.zx2c4.com/749).

Monitoring-Tool:Android/AndroidAgent.A

During installation, AndroidAgent.A requests for a number of permissions that will allow it to access contact data, SMS messages, location and Internet access on the affected device.
Once installed, it hides its presence by not placing any significant icon on the home screen.



Permissions requested by AndroidAgent.A

AndroidAgent.A silently records all incoming and outgoing calls, and checks for specific incoming SMS messages. The content found at the beginning of these messages will determine further actions to be carried out next.

- **0# :** **Master Number. Store the number from the sender as Administrator.**
- **99# :** **Register Shareware. Use the number to register shareware.**
- **9# :** **Send an SMS message containing IMEI and SIM serial number to the Master Number.**
- **18# :** **Store the string after '#' as 'UserName,' and use it for uploading recorded files in a remote location.**
- **10# :** **Start 'MyPeopleService' that sends SMS messages containing contact details from the phone book to the Master Number.**
- **8# :** **Start 'MyLocationService' that sends the location of the device.**

Shareware: A proprietary software offered as a trial version with limited functionality or availability.

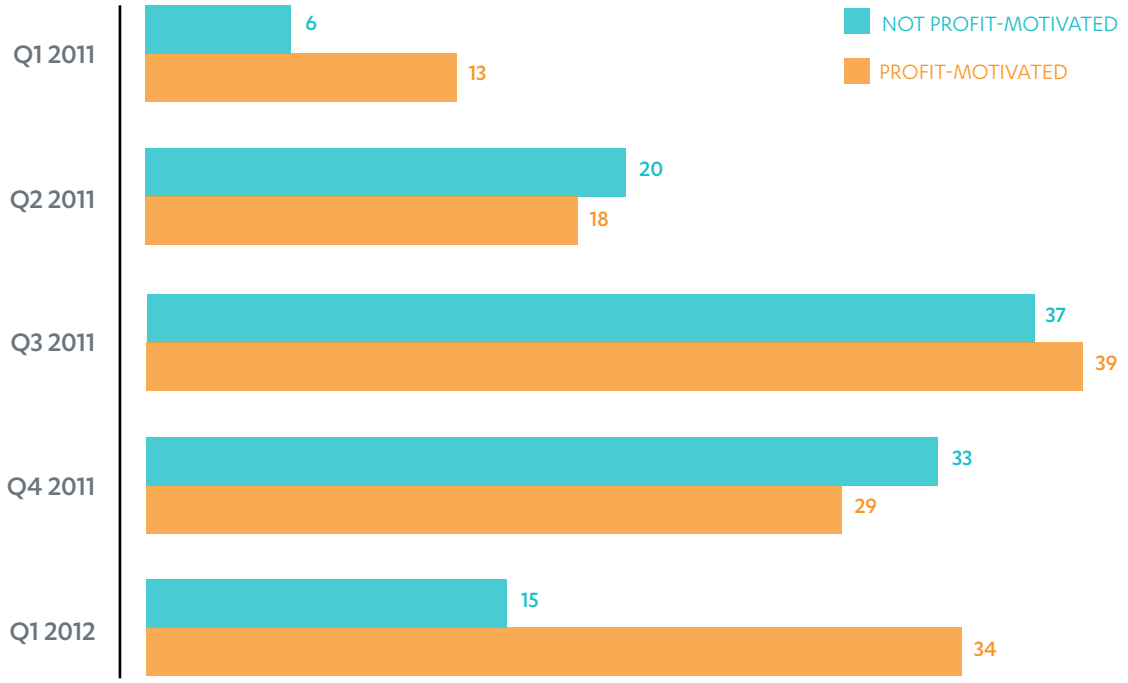


FIGURE 3: MOBILE THREATS MOTIVATED BY PROFIT PER QUARTER, 2011-2012

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.

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/Adboo.A

Adboo.A is an application that lets users select a pre-composed message from the provided list, and send it to their contacts. These messages are grouped into four categories: New Year wishes, friendship, love, and jokes.

Adboo.A presenting a selection of messages that users can choose from

When a message is selected, the application prompts a dialog box asking for the next action: Contact, Edit or Cancel. If Contact is selected, it tries to read the stored contact data. Presumably, it needs to know to whom the message should be sent to.

However, once the contact data is obtained, it does not send the message to the intended recipient, and displays the message "Sending fail." Instead, it silently collects the following details from the device:

- Device model
- Operating system version
- Phone number
- IMEI (International Mobile Equipment Identity) number

These details are then forwarded to a remote server. A look at Adboo.A's certificate revealed that it comes from the same developer of Trojan:Android/Zsone.A which was discovered in Q2 2011.

RELATED LABS WEBLOG POST

New Year's Wishes - with Side Order of Data Harvesting

http://www.f-secure.com/weblog/archives/00002293.html

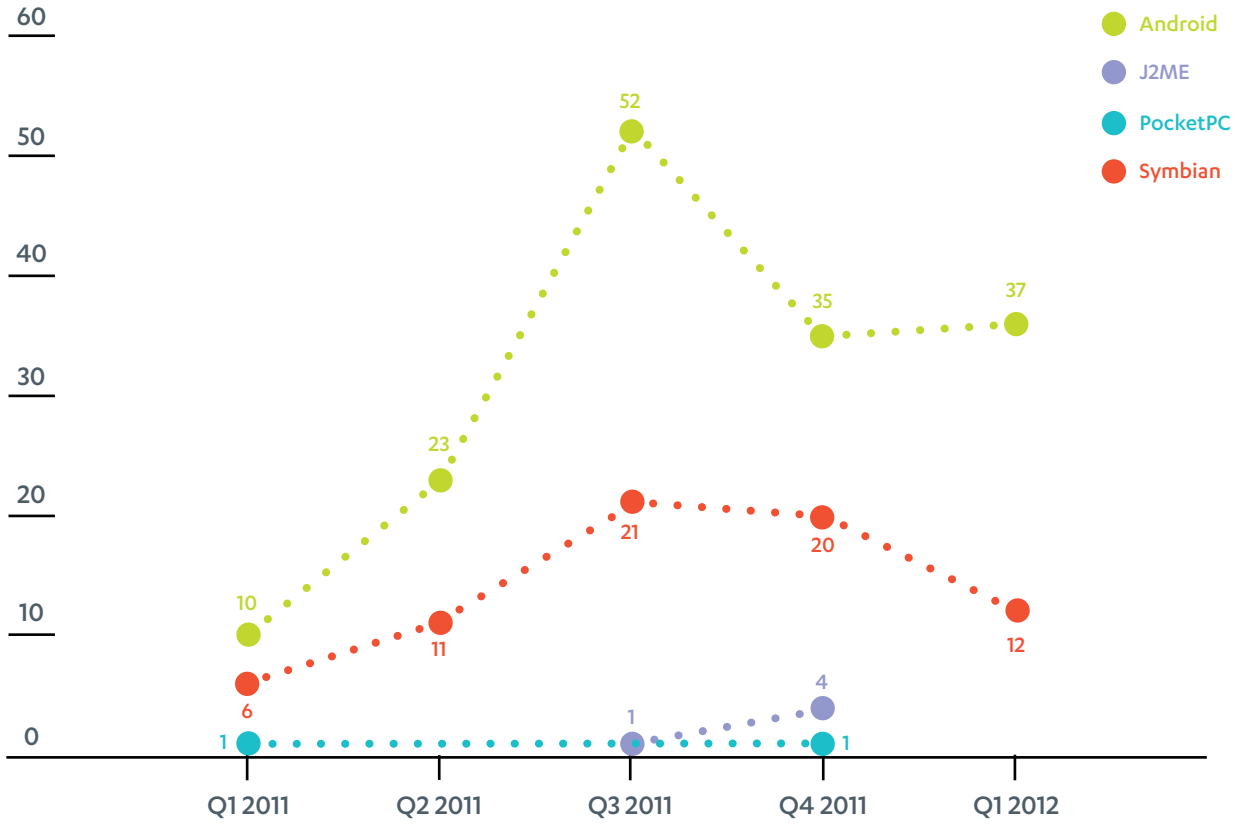


FIGURE 4: NEW FAMILY OR VARIANT RECEIVED PER QUARTER, 2011-2012

NOTE: The threat statistics used in **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.

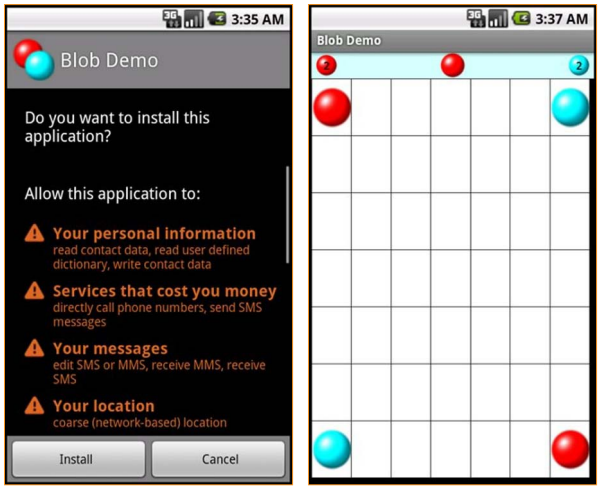
Malware

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.

Trojan:Android/Binder.B

Upon installation, Binder.B requests for permissions that will allow it to access contact data, SMS messages and location of the device.



Binder.B pretending to be an application called Blob Demo, and requesting some permissions

It collects the following device information:

- SIM serial number
- IMSI (International Mobile Subscriber Identity) number
- IMEI (International Mobile Equipment Identity) number
- Phone number

It then connects to a remote server, and receives further command to perform the following missions:

- Send SMS messages to certain number for N times
- Download and install APKs from given URL

The applications that Binder.B are intructed to install are as follows:

- com.taobao.mobile.dipei
- com.tencent.qqpimsecure
- com.renren.mobile.android
- com.kandian.hdtogoapp
- com.uc.browser
- com.tencent.mtt

```
private void installAPK()
{
  copyAPK("android_dipei_1.4.0.apk");
  copyAPK("QQSecure2.0_(Android)_Build289(1).apk");
  copyAPK("Renren_Android_3.0.2.7.20110510.apk");
  copyAPK("KSHDToGo-v0.1.48-1.6-20110526_youyoucun3.apk");
  copyAPK("UCBrowser_V7.8.1.96_Android_pf139_bi800_(Build11060915).apk");
  copyAPK("QQBrowser2.0(Android)_Build0095_60058.apk");
  installApk("com.taobao.mobile.dipei", "android_dipei_1.4.0.apk");
  installApk("com.tencent.qqpimsecure", "QQSecure2.0_(Android)_Build289(1).apk");
  installApk("com.renren.mobile.android", "Renren_Android_3.0.2.7.20110510.apk");
  installApk("com.kandian.hdtogoapp", "KSHDToGo-v0.1.48-1.6-20110526_youyoucun3.apk");
  installApk("com.uc.browser", "UCBrowser_V7.8.1.96_Android_pf139_bi800_(Build11060915).apk");
  installApk("com.tencent.mtt", "QQBrowser2.0(Android)_Build0095_60058.apk");
}
```

Binder.B is programmed to install selected APKs onto the device

Any message that contains these keywords in the content will be blocked:

- 83589523
- 83589523
- 客服电话 (“Customer service phone number”)
- 元/条 (“dollar /one message”)
- 元/次 (“dollar /time”)
- 本次1元 (“one time 1 dollar”)
- 本次2元 (“one time 2 dollar”)

Trojan:Android/Boxer.G

Boxer.G pretends to be an installer for a legitimate application, but is actually an SMS-sending Trojan. It sends out SMS messages to premium numbers, and collects profit from the charges being billed to the user’s account.

These are the premium numbers that Boxer.G sends out SMS messages to:

- 2855
- 7151
- 9151

Trojan:Android/DroidDream.G, and variant H

Similar to the previous variants, the G and H variants of DroidDream also collect and send information about the compromised device to a remote server. Collected details are:

- IMEI number
- IMSI number
- Device model
- Contact information
- Inbox and outbox SMS messages

These Trojans are also capable of sending SMS messages to every contact listed in the device, as well as creating messages in the inbox that appear to be coming from one of the listed contacts.

Trojan:Android/FakeAngry.A

FakeAngry.A comes in a malicious package, 'com.i22.angrybirds,' found in a trojanized application (com.katecca.screenofflock).

It gathers information from the compromised device, and sends the information to a remote location. Listed below are the details collected by FakeAngry.A:

- Device ID
- IMEI number
- IMSI number
- SDK version
- SIM serial number
- Subscriber ID

Trojan:Android/FakeRegSMS.A, and variant B

The FakeRegSMS Trojans are fake installers that install no real application on the device, but collect profit from signing up the user for a subscription based service.

During installation, the Trojans request for permissions that will allow the following actions:

- Modifying SD card contents
- Sending out SMS messages
- Reading the device's information

In the latter variant, the Trojan utilizes a pseudo-cryptic technique to conceal information in a PNG image file. The same image is used as the icon, and it becomes visible during and after the installation.

Permissions requested by FakeRegSMS.B, and the icon image used to hide data

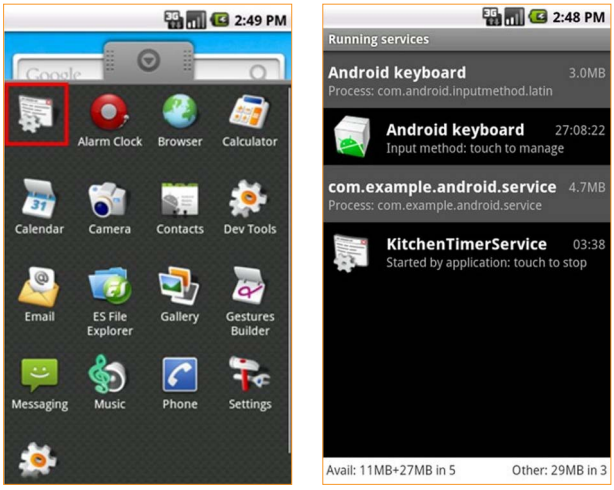
RELATED LABS WEBLOG POST

Android malware employs steganography? Not quite...

http://www.f-secure.com/weblog/archives/00002305.html

Trojan:Android/FakeTimer.A

FakeTimer.A installs a service named 'KitchenTimerService' onto the device, and accesses a website containing adult or pornographic contents.



FakeTimer.A installing 'KitchenTimerService' onto the device

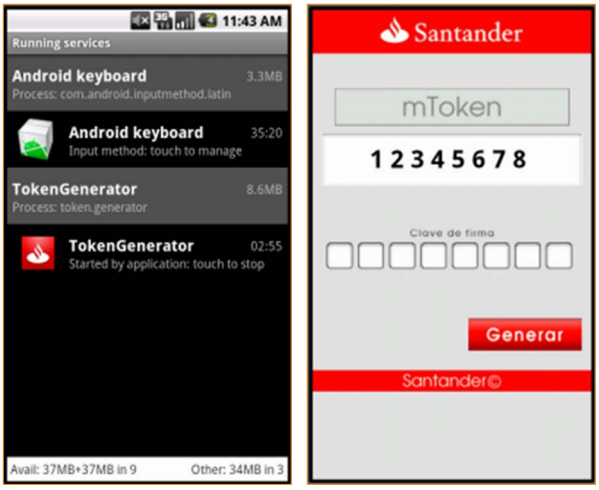
It retrieves the following information, which it later forwards to a remote server.

- **Phone number**
- **Device ID**

Trojan:Android/FakeToken.A

FakeToken.A pretends to be a mobile token generator, but is actually a Mobile Transaction Authentication Number (mTAN) interceptor. When installed, it intercepts SMS messages and looks for the mTAN, which it later forwards to a remote location or to a user.

mTAN: A number that is generated by a bank and sent to a user's mobile device to validate an online transaction. The user must enter this number before proceeding with the transaction.



FakeToken.A pretending to be a token generator

The Trojan installs a service that may start the following event:

- SMS_RECEIVED, upon receiving an SMS message
- PHONE_STATE, upon detecting a change in the device's state such as lock or standby mode to active mode
- BOOT_COMPLETED, upon completing device booting

It also keeps an XML configuration file, which contains the details on where to send the intercepted SMS messages.

```
<setingsSet>
      <catchSmsList class="java.util.ArrayList"/>
      <deleteSmsList class="java.util.ArrayList"/>
      <number>79021121067</number>
      <version>1.0</version>
      <smsPrefix>santander</smsPrefix>
      <sendSmsResultList class="java.util.ArrayList"/>
      <serverList class="java.util.ArrayList">
            <string>http://[redacted]hop.ru/[redacted].php</string>
            <string>http://[redacted]best.com/[redacted].php</string>
      </serverList>
      <serverPrefix>qe4faf23r4e2</serverPrefix>
      <sid>sid_1</sid>
      <period>43200</period>
      <timeConnection>1334662815611</timeConnection>
      <sendInitSms>false</sendInitSms>
</settingsSet>
```

XML configuration file containing details for sending SMS messages

Additionally, it may also forward the following information to a remote location:

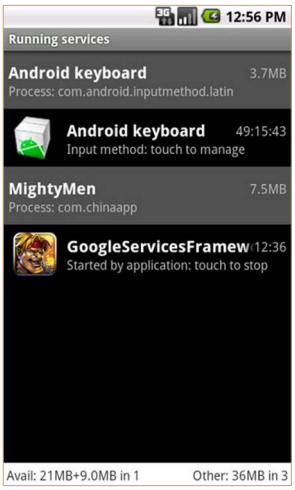
- IMEI number
- IMSI number
- Device model
- Phone number
- SID (System Identification Number) code

Trojan:Android/FakeUpdates.A

Once installed, FakeUpdates.A silently starts a service named 'GoogleServicesFramework' in the background.

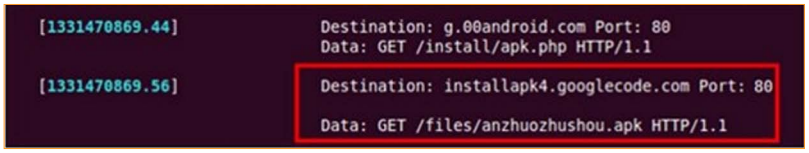
It connects to a remote server, and posts the following information:

- IMEI number
- IMSI number
- Operating system version
- Device model



FakeUpdates.A silently starting the 'GoogleServicesFramework' service

The Trojan also decrypts URLs that are stored at another remote location. From the location, it obtains a list of applications. These applications are later downloaded and stored in the download folder in the SD card.



FakeUpdate.A trying to download an application from the list

Downloaded applications are stored in the download folder in the SD card

Trojan:Android/FakeVoice.A

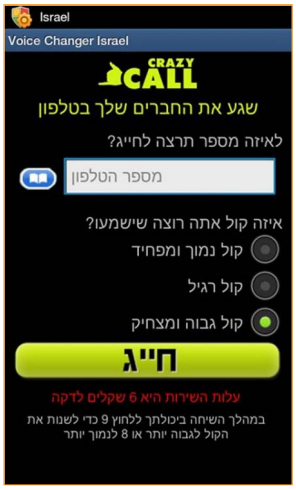
FakeVoice.A is a Trojan that promotes itself as a voice changing application to users in Israel. Upon execution, it prompts the following questions:

- What number do you want to dial?
- Which sound do you want to be heard in?
  - » Low and scary voice
  - » Normal voice
  - » High funny voice

The service would cost 6 NIS/minute. During the call, users can press '9' to change the voice to a higher pitch or press '8' for lower pitch.

NIS: Denotes Israeli New Shekel, the currency of the State of Israel.

In addition to the charged service, FakeVoice.A also makes a call to 01240900720674, which is a premium service number in Romania.



FakeVoice.A requesting user to enter a number to dial, and select a voice option

Trojan:Android/Kituri.A

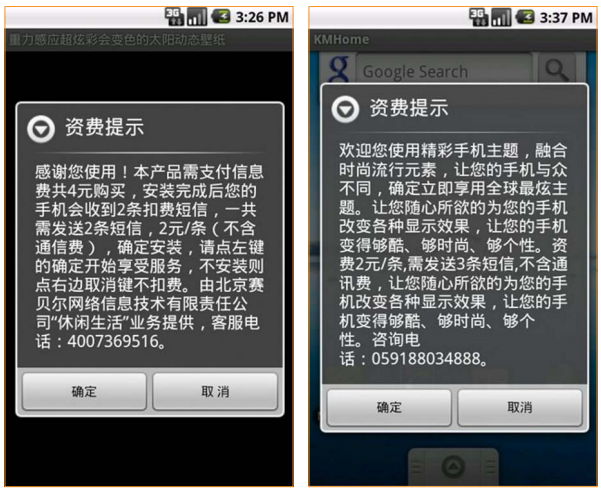
Upon execution, Kituri.A displays a 'User Agreement' to distract users from noticing suspicious activities that take place in the background.

The Trojan sends the device's IMEI number to a remote server. It also connects to a remote location to obtain a list of premium numbers to which it will send SMS messages to.

Kituri.A displaying the 'User Agreement'

Trojan:Android/Kmin.B, and variant C

Upon execution, the Kmin Trojans prompt a message asking whether the user would like to install a certain application, which would incur some charges to the user's bill.



Kmin.B and Kmin.C asking whether user wants to install a charged application

However, even if the user declines to install this application, the Trojan still proceeds to performing one of these malicious actions:

- Sending IMEI and phone number to a remote server
- Sending SMS messages to a premium number, 10669500718
- Downloading and installing another application
- Running services in the background

QUOTE OF THE QUARTER

ONE OF THE MORE INTERESTING MOBILE PHONE MALWARE TRENDS WE'VE SEEN IN RECENT MONTHS IS THE GROWTH OF TROJANS THAT "DELIVER ON THEIR PROMISES". IN THE PAST, MOST OF THE PROFIT DRIVEN TROJANS AIMED AT MOBILE PHONE USERS PROVIDED A DECOY ERROR MESSAGE AND ATTEMPTED TO CONVINCE THE USER THAT INSTALLATION OF THE SO-CALLED "FREE BROWSER" (TYPICALLY FOR SYMBIAN OR WINDOWS MOBILE) HAD FAILED. MANY FOLKS WOULD THEN DO A WEB SEARCH FOR THE ERROR MESSAGE, EITHER BECAUSE THEY WERE SUSPICIOUS OR BECAUSE THEY WANTED TO TROUBLESHOOT THE PROBLEM, AND AT THAT POINT, THEY OFTEN DISCOVERED THAT THE ERROR MESSAGE WAS FAKE AND THAT THEY HAD COMPROMISED THE SECURITY OF THEIR PHONE.

TODAY WHAT WE'RE SEEING ARE MALICIOUS ANDROID APPLICATIONS THAT HAVE BUNDLED LEGITIMATE APPS SUCH AS ROVIO'S ANGRY BIRDS SPACE. FIRST THE MALICIOUS "WRAPPER" TRICKS AND MANIPULATES THE USER INTO GRANTING PERMISSIONS THAT ALLOW THE MALWARE TO SUBSCRIBE TO PREMIUM RATE SERVICES. BUT THEN... THE MALWARE ACTUALLY DOES INSTALL A WORKING COPY OF THE PROMISED GAME. AT THIS POINT, THERE IS LITTLE TO BE SUSPICIOUS OF AND NOTHING TO TROUBLESHOOT. THE USER GETS THE GAME THAT HE WAS PROMISED.

WITH THIS NEW PARADIGM, IT REMAINS TO BE SEEN JUST HOW LONG IT TAKES VICTIMS TO ACTUALLY REALIZE THAT THEY'VE BEEN VICTIMIZED.

-SEAN SULLIVAN,

SECURITY ADVISOR, F-SECURE LABS

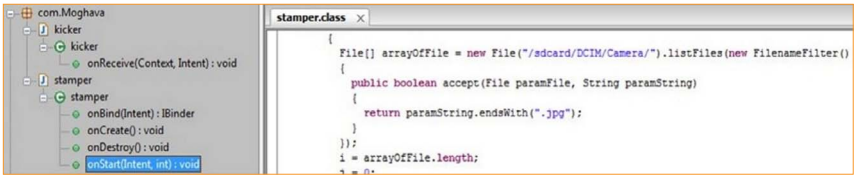
@FSLabsAdvisor

> "TODAY WHAT WE'RE SEEING ARE MALICIOUS ANDROID APPLICATIONS THAT HAVE BUNDLED LEGITIMATE APPS SUCH AS ROVIO'S ANGRY BIRDS SPACE"

Trojan:Android/Moghava.A

Moghava.A is a Trojanized application that was circulating in third party websites. Unlike most Android malware, it is not designed for monetary profit but rather for political ridicule.

Moghava.A's malicious activity is triggered off whenever the device boots up, and continues to go on for a certain time interval. When the device boots up, it activates a service named 'stamper.' This service waits for five minutes before proceeding to search for JPEG image files stored in the memory card, looking in the /sdcard/DCIM/Camera/ location in particular because that is where pictures taken from the device's camera are stored.



Moghava.A searching for JPEG image files at /sdcard/DCIM/Camera

For every found image file, it will superimpose another image on top of the original one. This routine will be repeated over and over in every five minutes, which effectively increases the size of the image file , and consumes the free space in the memory card.

Below is an example showing the image before and after modification:

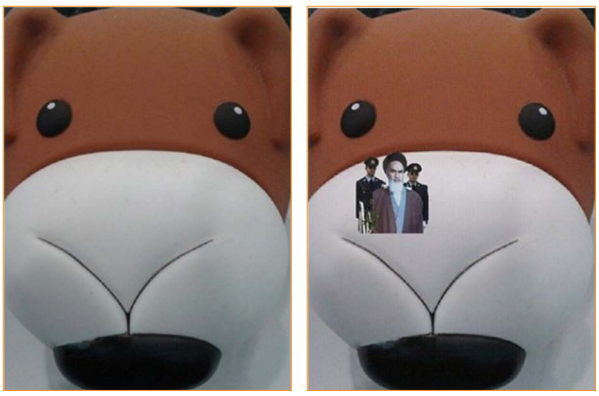


Image before (left) and after (right) the superimpose

Trojan:Android/Nyearleak.A

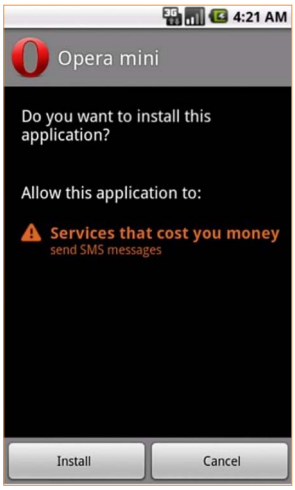
Nyearleak.A is a Trojan that disguises as a wallpaper application using the 2012 New Year celebration as a theme, while secretly collecting and sending out the following information from the device:

- Device ID
- Google account
- Email address
- Installed packages

Nyearleak.A disguising as a New Year themed wallpaper

Trojan:Android/OpFake.D

The Opfake Trojan was first discovered in Symbian and Windows Mobile devices, but now has made its way to the Android platform.



OpFake.D requesting for the permission to send SMS messages

RELATED LABS WEBLOG POST

Trojan:Android/OpFake.D Still Encodes Its Config File

http://www.f-secure.com/weblog/archives/00002306.html

Similar to its counterpart on other platforms, Opfake.D also masquerades as an Opera mini application. During installation, it only requests for one permission, which is to send out SMS messages.

When OpFake.D is launched, it sends out SMS messages to certain numbers. The messages' contents and telephone numbers are stored in an encoded file named 'config.xml' but can be decoded using base64 decoding.

```
[Sent SMS]
----------
        Number: 2332
        Message: 5+656tm-339-a43
        Number: 7250
        Message: 5+656tm-339-a43
        Number: 7099
        Message: 5+656tm-339-a43
```

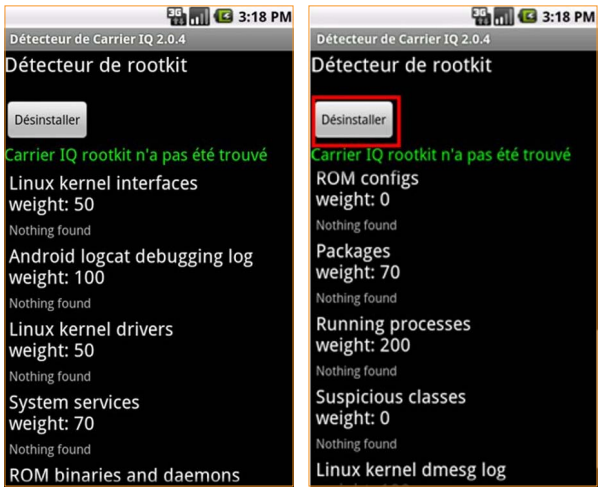
The content of the SMS messages, and the recipient number

Trojan:Android/Qicsomos.A

Qicsomos.A promotes itself as an application called 'Détecteur de Carrier IQ,' a French term that translates to Carrier IQ Detector. It claims to detect and remove a controversial application, Carrier IQ, from the device.

In 2011, Carrier IQ was a source of some concern for security researchers and privacy advocates, as the application was alleged to have been silently installed by telecom operators onto their customer's devices and used to gather information, including data usage and location details.

Qicsomos.A essentially takes advantage of fears raised by this issue to trick users into installing it.

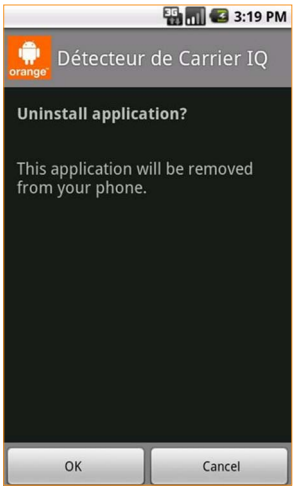


Qicsomos.A presenting the 'Desinstaller' (Uninstall) button

When user clicks the 'Désinstaller' (Uninstall) button, it will send out four SMS messages to the number 81168, containing these texts:

- AT37
- MC49
- SP99
- SP93

The malware then asks for the permission to uninstall itself.



Qicsomos.A asking whether the user wants to uninstall the application

NOTE: For additional details on Carrier IQ, please refer to 'Carrier IQ: What it is, what it isn't, and what you need to know' (http://www.engadget.com/2011/12/01/carrier-iq-what-it-is-what-it-isnt-and-what-you-need-to/)

Trojan:Android/RuFailedSMS.A

RuFailedSMS.A was found in third-party Android markets, targeting users in Russia, Belarus, Kazakhstan, and Azerbaijan. It pretends to be the installers for a range of applications, some of which are listed below:

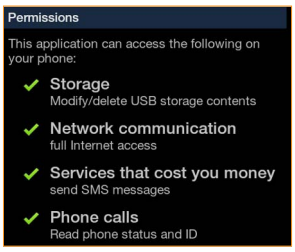
- Add_It_Up
- Advanced_Launcher_Lite
- AmazingMaze_supLitesup
- Analog_Clock_Collection
- Animal_Sudoku
- AnySoftKeyboard
- AnySoftKeyboard_Slovak_Language_Pack
- AppInventor_Toggle
- Arrow_Caz
- Astronomical_Flashlight
- BentoCam!

RELATED LABS WEBLOG POST

Failed Android Premium Rate SMS Trojan

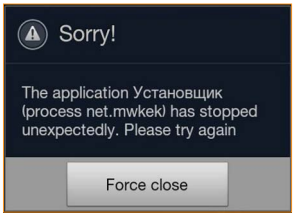
http://www.f-secure.com/weblog/archives/00002289.html

- Bimaru_-_Battleship_Sudoku
- BlackJack
- Carve_a_Pumpkin_supLitesup
- Chinese_Chess
- Christmas_Ringtones
- Coloring_pages
- Contact_Finder_supLitesup
- Converter
- Countdown_Widget
- Crayon_Ball
- Cyan_aHome_Theme



Permissions requested by RuFailedSMS.A

Upon installation, RuFailedSMS.A requests for permissions that would allow it to access Internet and send SMS messages among others. It was designed to reap profit from sending out SMS messages to premium numbers, but because of a glitch in its code, it fails to execute the malicious routine.



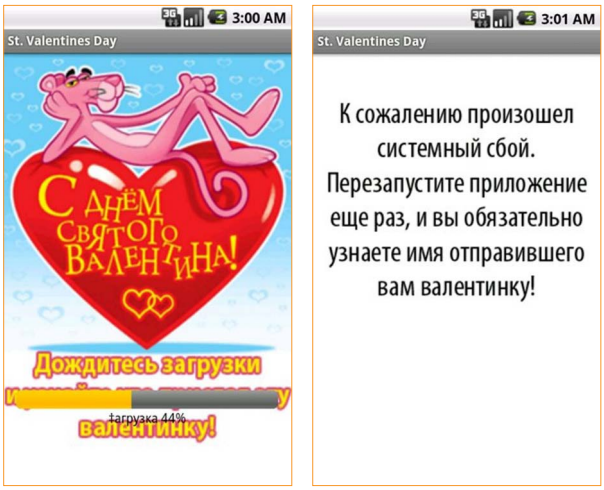
RuFailedSMS.A failing to complete its routine, and crashes instead

Trojan:Android/Saiva.A

Saiva.A was discovered around Valentine's Day, and is another malware that derives profit from SMS-sending activities. Upon execution, it displays a fake progress bar.

It pretends to be amidst downloading a task, but is actually sending out SMS messages containing the text "rb9816" to the number "5370." After that, it displays a fake message in Russian, supposedly notifying about a system failure. The exact message, translated to English, is as follows:

> **"Unfortunately there was a system failure. Restart the application again and you would find out the name of the person sending you the Valentine"**



Fake progress bar and failure message displayed by Saiva.A

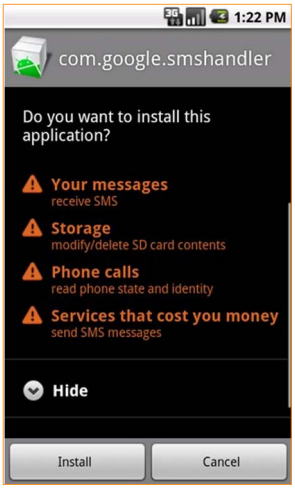
Trojan:Android/SMSFisher.A

SMSFisher.A contains a malicious package named 'fish.' Upon execution, it silently sends out SMS messages without the user's consent. To hide its track, this Trojan represses the system from prompting the notification about the SMS charge by aborting the broadcast of messages that contain or start with "+86" or "10."

Trojan:Android/SMSHandler.A

SMSHandler.A arrives in a package named 'com.google.smshandler.' During installation, it requests for permissions to access SMS messages, phone calls, and storage contents.

Once installed, it does not place any icon on the screen to avoid being noticed by the device's user. Its suspicious SMS-sending activity takes place when the device is being rebooted.

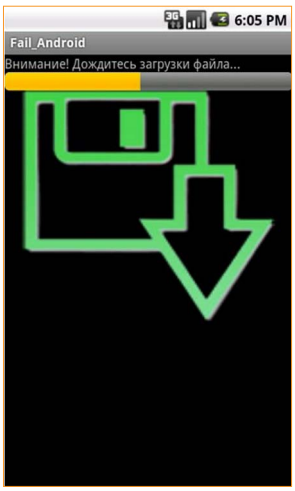


Permissions requested by SMSHandler.A

Trojan:Android/SMSLoader.A

SMSLoader.A arrives as an application named 'Fail_Android.' Upon execution, it displays a progress bar to indicate that a file is being downloaded, along with a message that is read as:

> "Attention! Wait for download file..."



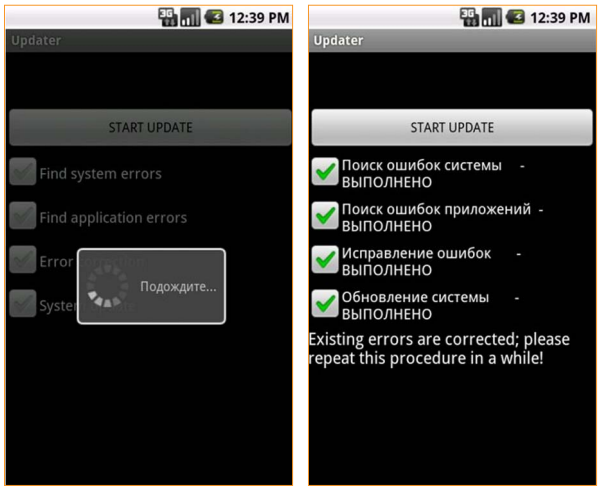
Fake progress bar and message displayed by SMSLoader.A

This Trojan silently sends out SMS messages with the content "5+125 7-14-654-13233359428100" to the following premium numbers:

- 5373
- 7250
- 7099

Trojan:Android/SMStealer.A

SMStealer.A pretends to be an "Updater" application, claiming to locate and correct errors in the device's system and applications.



SMStealer.A claiming to locate and correct errors in the system

But its real activity is connecting to a remote location, and sending out the following information:

- IMEI number
- Device ID and operator
- Inbox and outbox SMS messages

Trojan:Android/SpyService.A

After installation, SpyService.A does not place any significant icon on the home screen to hide its presence from the device user. It silently accesses the following details from the compromised device:

- IMEI number
- IMSI number
- SIM serial number
- Phone number
- Device model
- Network operator
- SMS messages

Trojan-Downloader:Android/RootSmart.A

RootSmart.A disguises itself as '系统快捷设置' (Quick System Settings).

RootSmart.A disguising as 'Quick System Settings'

Upon starting up, it connects to a command and control (C&C) server, forwarding the following information:

- IMEI number
- IMSI number
- Operating system version
- Package name

Next, it connects to a remote location to obtain the GingerBreak root exploit needed to gain root permission on the compromised device. From the location, RootSmart.A downloads a file named 'shells.zip,' which contains three components:

- **Exploit – GingerBreak root exploit (Detected as Exploit:Android/Droidrooter.F)**
- **Install script – bash script to install root shell in system directory**
- **Installapp script – bash script to install other malicious applications**

Additionally, the Trojan also downloads other malicious applications from the C&C server, and silently installs these applications onto the compromised device.

NOTE: For additional details on the GingerBreak exploit, please refer to 'Android Botnet Exploits Gingerbread Root Access' (http://www.informationweek.com/news/security/mobile/232600576)

TABLE 1: MOBILE THREAT STATISTICS BY PLATFORM, 2004-2011

	2004	2005	2006	2007	2008	2009	2010	2011	TOTAL
Android							9	120	129
iOS						2			2
J2ME			2		2	7	2	5	18
PocketPC	1		1	2	7	8	19	2	40
Symbian	24	124	188	44	19	21	50	58	528
	25	124	191	46	28	38	80	185	717

TABLE 2: MOBILE THREAT STATISTICS BY TYPE, 2004-2011

	2004	2005	2006	2007	2008	2009	2010	2011	TOTAL
Adware									-
Application								5	5
Backdoor							3		3
Garbage			8						8
Hack-Tool							4	8	12
Monitoring-Tool							1	15	16
Riskware			1		1	8	1	10	21
Spyware			5	15	6		2	5	33
Trojan	11	105	160	23	13	24	47	141	524
Trojan-Downloader								1	1
Virus	14	19	17	6					56
Worm				2	8	6	22		38
	25	124	191	46	28	38	80	185	717

NOTE: The threat statistics used in **Table 1** and **Table 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.

Trojan:SymbOS/Farewell.A

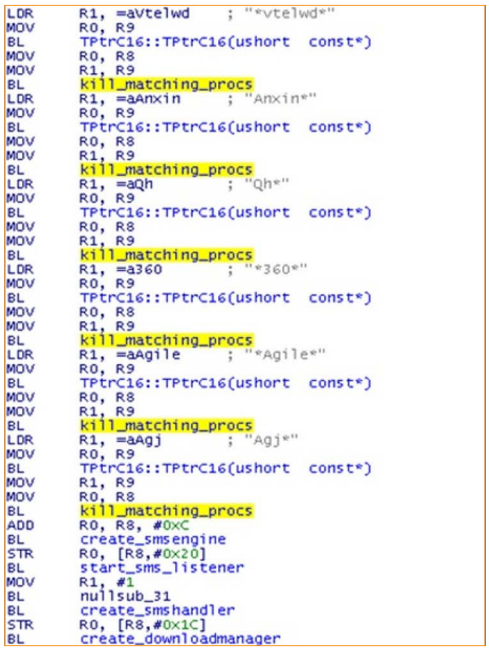
Farewell.A is programmed to terminate application processes with unique identifiers (UIDs) belonging to anti-virus vendors. Upon installation, it executes its first binary, which sends out an SMS message containing the text "I get home" to the number '13709586492.' When it is being uninstalled, the first binary is once again executed, sending a "Goodbye" message to the same recipient number.

Farewell.A's installer also contains a launch point that will execute another binary in the package when the device is booted. This second executable downloads a configuration from a remote server, and proceeds to send out SMS messages. Further network connections are made by using the regular HTTP stack and raw TCP sockets. But for some reason, if the device is locked, any process that has "360" in its name will be killed off before any network connection can be made.

Farewell.A saying 'Goodbye'

Trojan:SymbOS/SivCaller.A

SivCaller.A is a Trojan that downloads and installs new components into the compromised device, without needing any user intervention. When the main executable is launched, it kills processes that belong to anti-virus products. It also modifies bookmarks in the web browser, and intercepts incoming SMS messages before they are placed in the inbox.

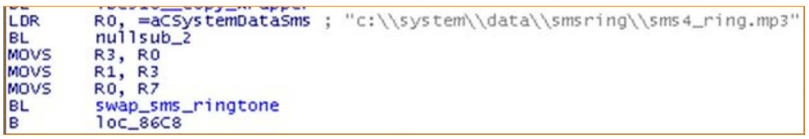


SivCaller.A is programmed to kill processes that belong to anti-virus products

Trojan:SymbOS/SilentPusher.A

SilentPusher.A is a Trojan that sends out and monitors SMS messages. To prevent user from noticing its SMS sending activity, it represses the message notifications from showing up.
This is done by changing the SMS ringtone to a silent MP3 included in the installer package, and by killing the message notification service (ncnlist.exe).

SilentPusher.A killing message notification service in order to repress notification



SilentPusher.A changing the SMS ringtone to a silent MP3 file

However, the action of repressing the message notifications is only performed when SilentPusher.A is waiting for its own messages, most likely confirmation messages from premium services. Normal message notifications are restored afterwards.

Aside from sending SMS messages, other activities that SilentPusher.A carries out include killing processes that belong to anti-virus vendors, harvesting IMEI and IMSI numbers, and connecting to various remote servers over the Internet connection.

```
LDR     R1, =aAgilemoncon ; "AgileMonCon"
MOV     R0, SP
BLX     TPtrC16::TPtrC16(ushort  const*)
MOVS    R0, R5
MOV     R1, SP
BL      kill_matching_processes
LDR     R1, =aAgileserver ; "AgileServer"
MOV     R0, SP
BLX     TPtrC16::TPtrC16(ushort  const*)
MOVS    R0, R5
MOV     R1, SP
BL      kill_matching_processes
LDR     R1, =aQh360keeper ; "Qh360Keeper"
MOV     R0, SP
BLX     TPtrC16::TPtrC16(ushort  const*)
MOVS    R0, R5
MOV     R1, SP
BL      kill_matching_processes
LDR     R1, =aQh360safesvr ; "Qh360SafeSvr"
MOV     R0, SP
BLX     TPtrC16::TPtrC16(ushort  const*)
MOVS    R0, R5
MOV     R1, SP
BL      kill_matching_processes
LDR     R1, =aMcleanerserver ; "MCleanerServer"
MOV     R0, SP
BLX     TPtrC16::TPtrC16(ushort  const*)
MOVS    R0, R5
MOV     R1, SP
BL      kill_matching_processes
```

SilentPusher.A is programmed to kill processes that belong to anti-virus products

Trojan:SymbOS/Yorservi.A, and variants B and D

The first variant, Yorservi.A, connects to several remote hosts using raw TCP sockets. It then silently downloads and installs some components, without the device user's consent.

The second variant, Yorservi.B, contains an uninstallation feature. When it is being uninstalled from a device, it instantly kills the uninstallation process. Its other capabilities include monitoring calls, reading call logs, and reading and sending SMS messages.

Yorservi.D, the other variant, is programmed to kill the 'connmon.exe' service to prevent user from noticing that network connections have been created. It has a scrambled configuration file which contains a list of unique identifiers (UIDs). This variant also starts new processes, and downloads and installs new software silently.

```
27 00 00 00 59 00 30 00  52 00 69 00 6F 00 69 00  '...Y.0.R.i.o.i.
6A 00 5B 00 63 00 52 00  5F 00 64 00 69 00 6A 00  j.[.c.R._.d.i.j.
57 00 62 00 62 00 52 00  48 00 5B 00 5D 00 5F 00  W.b.b.R.H.[.]._.
69 00 6A 00 68 00 6F 00  52 00 27 00 26 00 27 00  i.j.h.o.R.'.&.'.
28 00 2C 00 58 00 58 00  58 00 24 00 68 00 5B 00  (.,.X.X.X.$.h.[.
5D 00 00 00 16 00 00 00  59 00 30 00 52 00 69 00  ].......Y.0.R.i.
```

Scrambled file name in Yorservi.D

```
00000000 33 31 31 32 62 38 60 64-31 33 31 31 33 34 38 32  3112b8`d13113482
00000010 39 30 33 31 31 33 67 39-65 33 30 33 31 31 32 31  903113g9e3031121
00000020 33 32 37 30 33 31 31 31-64 64 65 36 30 33 31 31  32703111dde60311
00000030 31 64 64 65 33 30 33 31-31 33 63 31 35 35 30 33  1dde303113c15503
00000040 31 31 33 34 39 38 38 30-33 31 31 33 37 34 60 31  11349880311374`1
```

Scrambled configuration (Yorservi.D)

```
00000000 32 30 30 31 61 37 61 63-30 32 30 30 32 33 37 31  2001a7ac02002371
00000010 38 66 32 30 30 32 66 38-64 32 66 32 30 30 31 30  8f2002f8d2f20010
00000020 32 31 36 66 32 30 30 30-63 63 64 35 66 32 30 30  216f2000ccd5f200
00000030 30 63 63 64 32 66 32 30-30 32 62 30 34 34 66 32  0ccd2f2002b044f2
00000040 30 30 32 33 38 37 37 66-32 30 30 32 36 33 61 30  0023877f200263a0
```

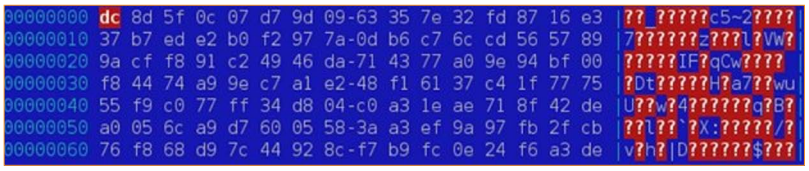
Unscrambled configuration (Yorservi.D)

Trojan:SymbOS/Zhaomiao

Trojans in the Zhaomiao family have been around since last year, but recent analysis discovered that some variants have been employing similar keys to decrypt their configuration files.

Samples from the Zhaomiao family contain an encrypted configuration file; it can be decrypted using the DES key 'DDH#X%LT' which is hardcoded in the malicious bytecode. Once decrypted, the file reveals a list of fast-flux sites.

Fast-flux: A technique of abusing the Domain Name System (DNS) to protect an IP address from being identified. Often used by cybercriminals to hide their activities from being tracked down.



Encrypted configuration file found in Zhaomiao samples

Decrypted file revealing a list of sites

This same decryption key was spotted in a number of samples, which are later detected as Trojan:SymbOS/Zhaomiao.E. However, Zhaomiao.B was also found to use this key to decrypt a local configuration file.

Encrypted configuration file found in other Zhaomiao samples

Decrypted file revealing a list of sites

Another DES key, 'DOW#MD%D,' was also found to be commonly used by the Zhaomiao family. In one instance, it was used by Zhaomiao.E to decrypt the local configuration file.

Encrypted configuration file found in another Zhaomiao samples

```
<ConnectProtect>
  <ConnectProtectProduct>
    <HandledProduct uid="2000AB0E" property="64578" launchfile="NetQin_Anti_Virus_
    <HandledProduct uid="20009031" property="62703" launchfile="C:\System\Apps\New
    <HandledProduct uid="20009031" property="62704" launchfile="C:\System\Apps\New
    <HandledProduct uid="20009031" property="62705" launchfile="C:\System\Apps\New
    <HandledProduct uid="2002588F" property="58964" launchfile="NetQin_PhoneGuard_
    <HandledProduct uid="2002659F" property="57864" launchfile="NetQin_PhoneGuard_
    <HandledProduct uid="20026D57" property="44564"/>
    <HandledProduct uid="20026E4F" property="54246"/>
    <HandledProduct uid="20027EFB" property="34682"/>
    <HandledProduct uid="20028AFC" property="17463"/>
    <HandledProduct uid="20028B0B" property="23793"/>
    <HandledProduct uid="2001CFC5" property="48937"/>
    <HandledProduct uid="20025936" property="15695"/>
    <HandledProduct uid="20029966" property="36723"/>
    <HandledProduct uid="2002996A" property="36724"/>
  </ConnectProtectProduct>
  <JudgeProperty value="56496"/>
</ConnectProtect>
```

File decrypted using similar DES key

In the same Symbian sample, the key used to decrypt the configuration data is similar to that used by Trojan:Android/DroidDream.B. In the Symbian sample, the key decrypts a configuration data downloaded from a remote host; in DroidDream.B, the key is used to decrypt a local configuration file.

```
; Attributes: bp-based frame

update_config

plaintext_storage= -0x28
ciphertext_tptr8= -0x24
context_obj= -0x10

MOV     R12, SP
STMFD   SP!, {R11,R12,LR,PC}
SUB     R11, R12, #4
SUB     SP, SP, #0x20
STR     R0, [R11,#-0x10] ; store and load context object
LDR     R3, [R11,#-0x10]
LDR     R3, [R3,#0x10]
SUB     R0, R11, #-ciphertext_tptr8
LDR     R1, [R3,#0x18]  ; get ciphertext buffer from context
BL      HBufC8::Des(void)
LDR     R0, =aDdhxLt_5  ; "DDH#X%LT"
BL      prep_key
SUB     R3, R11, #-ciphertext_tptr8
MOV     R1, R3
BL      des_decrypt
STR     R0, [R11,#plaintext_storage]
LDR     R0, [R11,#plaintext_storage]
BL      CleanupStack::PushL(void *)
LDR     R3, [R11,#context_obj]
LDR     R3, [R3,#0x10]
LDR     R0, [R3,#0x1C]
BL      combine_plaintext
LDR     R3, [R11,#context_obj]
LDR     R0, [R3,#0x20]
LDR     R1, [R11,#plaintext_storage]
BL      parse_xml
LDR     R0, [R11,#plaintext_storage]
BL      cleanupstack_popanddestroy
LDR     R0, [R11,#context_obj]
BL      save_config
SUB     SP, R11, #0xC
LDMFD   SP, {R11,SP,PC}
; End of function update_config
```

Found connection between Zhaomiao and DroidDream.B

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.

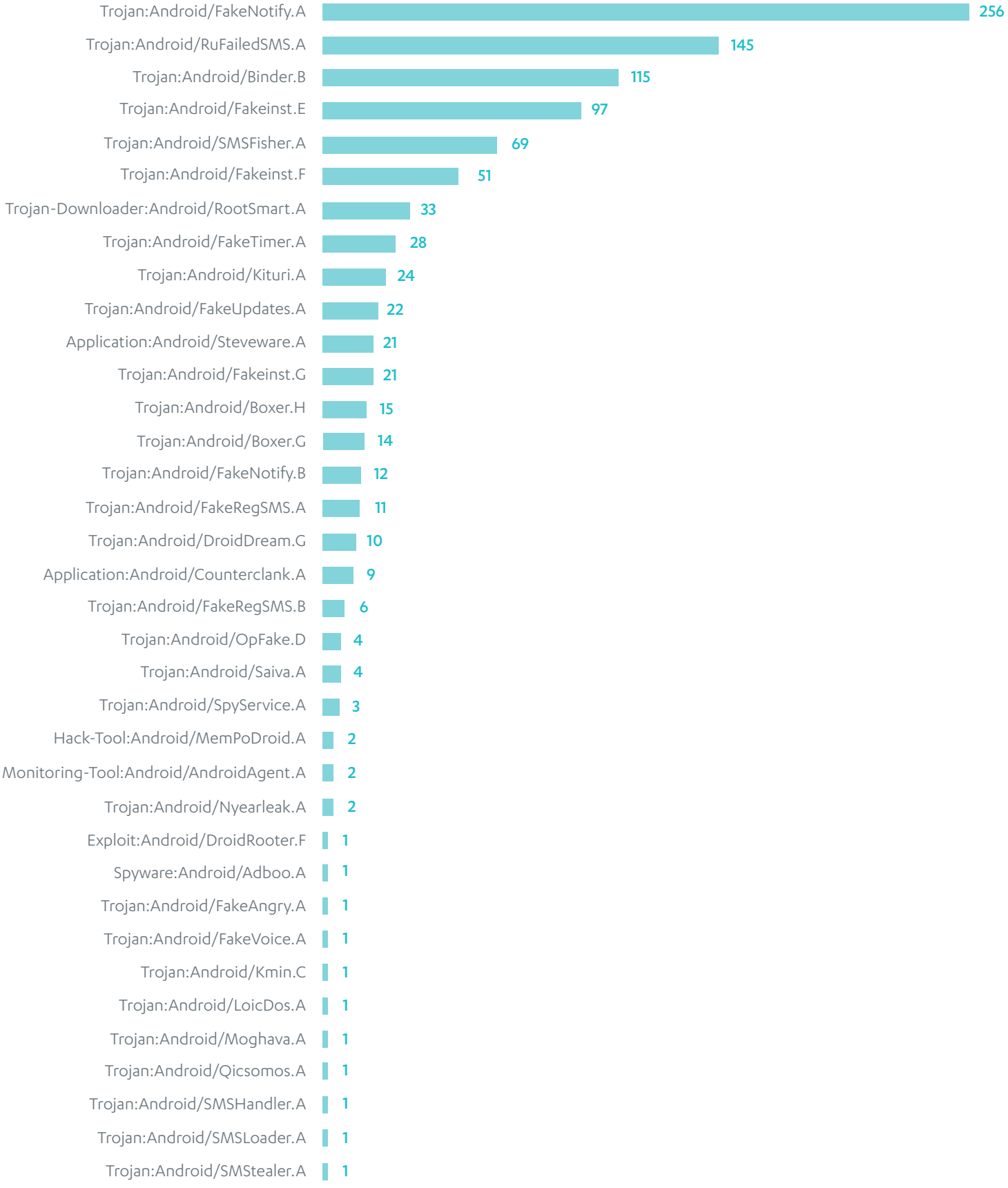
- Trojan:Android/Boxer.H
- Trojan:Android/DroidDream.G
- Trojan:Android/DroidKungFu.H
- Trojan:Android/Fakeinst.E, and variant F and G

TABLE 3: DETECTION COUNT FOR ANDROID SAMPLES RECEIVED IN Q1 2012

DETECTION	COUNT
Heuristics	828
Application:Android/Counterclank.A	9
Application:Android/Steveware.A	21
Exploit:Android/DroidRooter.F	1
Hack-Tool:Android/LoicDos.A	1
Hack-Tool:Android/MemPoDroid.A	2
Monitoring-Tool:Android/AndroidAgent.A	2
Spyware:Android/Adboo.A	1
Trojan:Android/Binder.B	115
Trojan:Android/Boxer.G	14
Trojan:Android/Boxer.H	15
Trojan:Android/DroidDream.G	10
Trojan:Android/DroidKungFu.H	2
Trojan:Android/FakeAngry.A	1
Trojan:Android/FakeNotify.A **	256
Trojan:Android/FakeNotify.B **	12
Trojan:Android/FakeRegSMS.A	11
Trojan:Android/FakeRegSMS.B	6
Trojan:Android/FakeTimer.A	28
Trojan:Android/FakeUpdates.A	22
Trojan:Android/FakeVoice.A	1
Trojan:Android/Fakeinst.E	97
Trojan:Android/Fakeinst.F	51
Trojan:Android/Fakeinst.G	21
Trojan:Android/Kituri.A	24
Trojan:Android/Kmin.C	1
Trojan:Android/Moghava.A	1
Trojan:Android/Nyearleak.A	2
Trojan:Android/OpFake.D	4
Trojan:Android/Qicsomos.A	1
Trojan:Android/RuFailedSMS.A	145
Trojan:Android/Saiva.A	4
Trojan:Android/SMSFisher.A	69
Trojan:Android/SMSHandler.A	1
Trojan:Android/SMSLoader.A	1
Trojan:Android/SMStealer.A	1
Trojan:Android/SpyService.A	3
Trojan:Android/Stiniter.A	4
Trojan-Downloader:Android/RootSmart.A	33

** This variant was discovered in late Q4 2011.

FIGURE 5: ANDROID SAMPLES RECEIVED IN Q1 2012, SORTED BY DETECTION COUNT



Protecting the Irreplaceable

Document made public since: 11 May 2012

F-Secure