F-Secure Labs

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

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

Protection around the clock

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


CONTENTS

ABSTRACT 3

2012 Mobile Landscape Calendar 5

EXECUTIVE SUMMARY 6

Figure 1: Number of Android Samples Received, Q3 2012 8

LATEST THREATS IN THE LAST THREE MONTHS 9

Figure 2: New Mobile Threats Families and Variants Received Per Quarter, 2011-2012 10
Figure 3: Mobile Threats By Platform, 2011-2012 11
Figure 4: Top-20 Mobile Threats By Variant Count Per Platform, 2007-Present 12

Potentially unwanted software 13

Hack-Tool:Android/Penetho.A 14
Hack-Tool:Android/Whapsni.A 14
Monitoring-Tool:Android/AccuTrack.A 14
Monitoring-Tool:Android/Cobbler.A 15
Monitoring-Tool:Android/SMSWatcher.A 16
Riskware:Android/DroidCoupon.A 17
Riskware:Android/Fidall.A, Riskware:iOS/Fidall.A 17
Riskware:Android/SeaWeed.A 18
Figure 5: Mobile Threats By Type, Q3 2012 19

Spyware 20

Adware:Android/AdWo.A 21
Adware:Android/Maxit.A 21
Spyware:SymbOS/Fafespy.A 21
Figure 6: Profit- vs Not Profit-Motivated Threats Per Quarter, 2011-2012 22
Figure 7: Profit- vs Not Profit-Motivated Threats By Platform, Q3 2012 22
Malware

Trojan:Android/AckPosts.A  
Trojan:Android/AppleService.A  
Trojan:Android/DropDialer.A  
Trojan:Android/FireLeaker.A  
Trojan:Android/FJCon.A  
Trojan:Android/IconoSys.A  
Trojan:Android/LuckyCat.A  
Trojan:Android/Maistealer.A  
Trojan:Android/MarketPay.A  
Trojan:Android/NandroBox.A  
Trojan:Android/PopWeb.A  
Trojan:Android/SmsSend.A, and variant B and C  
Trojan:Android/SmsZombie.A  
Trojan:Android/Sumzand.A, and variant B  
Trojan:Android/Vdloader.A  
Trojan:Android/Vidro.A  
Trojan:Blackberry/Zitmo.A  
Trojan:SymbOS/FakePatch.A  
Trojan:SymbOS/Foliur.A  
Trojan:SymbOS/HRU.A  
Trojan:SymbOS/Impler.A  
Trojan:SymbOS/KillTrust.A  
Trojan:SymbOS/Nokan.A, and variant B  
Trojan:SymbOS/PlugGamer.A  
Trojan:SymbOS/Ropitor.A  
Trojan:SymbOS/Shilespy.A  
Trojan-Downloader:Android/Morepak.A  
Trojan-Spy:WinCE/FinSpy.A, Trojan-Spy:iOS/FinSpy.A, 
Trojan-Spy:SymbOS/FinSpy.A, Monitoring-Tool:Android/FinSpy.C

New variants of already known families

Figure 8: Top-10 Android Detection Hits, Q3 2012
Figure 9: Breakdown of Heuristic Detection, Q3 2012
Table 1: Top Android Malware, Riskware and Spyware, Q3 2012
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

NOTE: The threat statistics used in the calendar 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.
Despite Android’s dominance in the mobile threat landscape, the Symbian malware scene is far from dead. 21 new families and variants were discovered in the third quarter of 2012, a 17% increase compared to the second quarter.

A typical Symbian malware is a trojan that mimics a system update or a legitimate application. The object-capability model used in Symbian devices presents some loopholes that can be exploited. For example, the same set of capabilities required by a legitimate action game may be similar to that required by an application that can download and install new software from the Internet. A malware author can capitalize on these similar capabilities to present a malware as a harmless, coveted program that sneakily carries out its activities without arousing the user’s suspicion.

Most of the Symbian malware originates in China and are distributed for the purpose of making a profit. Most of these (for example, Fakepatch.A and Foliur.A) are involved in SMS-sending activities. The SMS messages are usually sent to premium rate numbers or those associated with SMS-based services. Malware authors and distributors can easily turn an infection into profit by taking advantage of a ‘built-in’ billing mechanism for these SMS services; the malware simply sends out SMS messages that silently sign up the device owner for a premium subscription service, incurring charges the user’s account.

Another profit-generating method involve the malware emulating a user’s behaviour and enabling WAP services on the device, which are then billed through the mobile service operator. These malware, such as PlugGamer.A, are capable of acting as scripted bots, silently playing a regular, albeit simple browser-based online game over the WAP service.

Despite the continuing activity on the Symbian malware scene, the Symbian platform itself saw a significant blow to its future, as Nokia confirmed in September that the once popular operating system has now been put in “maintenance mode”, with the only major update this year being a refresh or feature pack that was rolled out in August to certain devices running the current Nokia (formerly Symbian) Belle release.

Market-wise, shipment of Symbian smartphones reportedly fell by 62.9% in Q2 and Symbian now accounts for only 4.4% of the global smartphone market. Despite the lack of activity in platform development and use however, Symbian malware is still likely to be active for some time to come as many users, particularly in developing countries, continue to use existing Symbian-based handsets.

As expected, Android malware continues to dominate the mobile threat landscape with a whopping 51,447 unique samples detected in the third quarter (see Figure 1 on page 8). The increase in samples occurred even after Google introduced Bouncer, an additional layer of security on the Android Play Store - the renamed Android Market - that scans new and existing apps and developer accounts for malicious activity. Google has claimed that this additional security resulted in a 40% drop in malicious apps being offered. Though researchers have demonstrated in technology conferences that Bouncer protection could be circumvented, it seems somewhat unlikely that this could be the reason for the increase in malicious samples.
The surge may better be attributed as a natural consequence of the continued high growth in Android smartphone adoption this quarter, particularly in regions such as China and Russia. In fact, in Q2, China officially surpassed the United States as the largest market for smartphones, with Android handsets accounting 81% of that market.

These expanding markets have also been notable for the proliferation of less-secure third-party apps markets, which are popular with users for various reasons. This factor may also account for the increasing number of malicious samples seen this quarter.

Of this number, we discovered 42 new families and new variants of existing families. Unlike the driveby malware found earlier this year (see the Q2 Mobile Threat Report), the majority of the new Android threats seen this quarter have been designed to generate profit from SMS sending activities or by harvesting information found on the infected device.

Platform-wise, the other notable event this quarter is the release of the 4.1 update, dubbed Jellybean, which included a number of exploit mitigation features as part of an ongoing effort to improve security on the platform.

OTHERS

The third quarter also saw a new variant of Zitmo (mobile version of the Zeus malware) that targets Blackberry devices. An earlier variant was discovered back in 2010, and used JAD file format. The new one is now using COD file format but its purpose remains the same, which is to steal the mobile Transaction Authentication Number (mTAN) sent by banks to their customers. The mTAN is sent via an SMS message and is used to validate an online transaction. Without the number, the transaction cannot be completed. The Zitmo malware intercepts the SMS messages containing mTans and forwards them to a remote server.

Aside from Zitmo for Blackberry, the FinSpy trojan was the other notable discovery in the third quarter of 2012. This trojan was made available on multiple mobile platforms - Android, Symbian, iOS, and Windows Mobile. FinSpy can take screenshots of an infected device, record keyboard strokes, intercept Skype communications, track device location, and monitor SMS and call activities on the device.

FinSpy is the mobile version of FinFisher, a trojan commercially produced by a UK-based software company and marketed as a surveillance product for desktop computers. There has been reports of FinFisher being used against citizens of Egypt, Bahrain, and Turkmenistan. Due to its alleged role in political espionage, the trojan has been of concern to non-governmental organizations such as Privacy International.

Apart from the unusual case of FinSpy, the only other notable case on the iOS platform this quarter was Fidall, an app that essentially sends contacts from the device to a remote server, then sends spam SMS messages to the contacts with a download link for the application. The app is also available on Android.

As a final note, the iOS platform itself was also updated this quarter to iOS 6, which included fixes for many (reportedly 197) vulnerabilities found, the majority of them related to the Webkit web browsing component.
FIGURE 1: NUMBER OF ANDROID SAMPLES RECEIVED, Q3 2012

NOTE: The threat statistics used in Figure 1 are made up of the number of unique Android application package files (APKs).
LATEST
THREATS IN
THE LAST
THREE
MONTHS
**Figure 2: New Mobile Threats Families and Variants Received 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.
FIGURE 3: MOBILE THREATS BY PLATFORM, 2011–2012

**NOTE:** The threat statistics used in Figure 3 are based on the number 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-20 MOBILE THREATS BY VARIANT COUNT PER PLATFORM, 2007-PRESENT

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.
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/Penetho.A**

Penetho.A is a penetration testing application that utilizes a well-known vulnerability in the Thomson/Speedtouch router. It generates a password for the WiFi router using the Service Set Identification (SSID).

![Penetho.A's icon (left), and WiFi confirmation (right)](image)

**Hack-Tool: Android/Whapsni.A**

Whapsni.A is a tool that can sniff out WhatsApp packets over a shared network. For example, when connected to a shared WiFi, it may be able to intercept WhatsApp chat data packets being sent to and from other devices connected to the network. These packets may contain private information, enabling Whapsni.A to read private messages and view contact information associated with the WhatsApp account on those devices.

**NOTE:** For additional reading on WhatsApp's security issues, please refer to the article ‘WhatsApp is broken, really broken’ ([http://www.fileperms.org/whatsapp-is-broken-really-broken/](http://www.fileperms.org/whatsapp-is-broken-really-broken/)).

**Monitoring-Tool: Android/AccuTrack.A**

AccuTrack.A is an application that tracks down the GPS location of the device on which it was installed. While not malicious in itself, it introduces a potential risk for misuse with malicious intent.
Cobbler.A allows a user to define specific SMS messages that can later be used to perform these actions from a remote location:

- Wipe the SD card’s contents
- Wipe everything found on the device
- Retrieve the device’s location
Monitors and Tool-Android/SMSSWatcher.A

SMSSWatcher.A is a commercial monitoring tool advertised as being for parents who are interested in monitoring their children’s SMS activities.
Riskware:Android/DroidCoupon.A

When DroidCoupon.A is installed on a device, users risk having their device information leaked to unauthorized parties. The application may leak the following information:

- International Mobile Equipment Identity (IMEI) number
- International Mobile Subscriber Identity (IMSI) number
- Package version
- Package name
- Channel

Screenshots of DroidCoupon.A

Riskware:Android/Fidall.A, Riskware:iOS/Fidall.A

Distributed under the name Find and Call, this program first requests the user to register by providing their email address. It then searches for e-mails, addresses, and phone numbers from the user’s contact list. This information is then synced with a remote server. Once synced, the server will send an SMS message containing a link to download the application to the contacts—essentially, SMS spam. The SMS messages reportedly contains the user’s phone number in the ‘From’ field.
Another issue concerning Fidall.A is that the data transmitted between the device and the remote server is in plain text, which easily exposes the content if intercepted by another party.

The app is also fully capable of syncing with the contacts from the user’s e-mail, Facebook, and Skype accounts. The app’s website also reportedly allowed users enter their social network and online payment merchant details.

At the time of writing, both the Apple App Store and Google Play Store have removed the app. This incident marks the first time the Apple App Store has had to remove a trojan from its market.

## Riskware:Android/SeaWeed.A

Once installed, SeaWeed.A initiates an application purchase by sending out an SMS message with the content ‘341#102366#34101’ to the number 1065880004. It then monitors all incoming messages, looking for a specific reply. Once the replying message arrived, it will intercept this message and display the content as a dialog box. This dialog box essentially asks the user to confirm the purchase; without the confirmation, the transaction will not proceed. Additionally, SeaWeed.A forwards the device’s IMSI number and other important details to a remote server.
NOTE: The threat statistics used in Figure 5 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.
Adware: Android/AdWo.A

AdWo.A is an advertising module that displays intrusive ads and collects private information, such as the device’s IMEI number.

Adware: Android/Maxit.A

Maxit.A is an SMS-based marketing module that provides SMS advertisements and other extra services. An application containing this module will gather the following information from the device it was installed on:

- International Mobile Equipment Identity (IMEI) number
- International Mobile Subscriber Identity (IMSI) number
- Phone number
- Operating system version
- Operator name
- Operator code
- Operator ISO
- SIM country code
- SIM operator
- SIM serial number
- SDK version
- SDK number
- Device release date
- Device model
- Device manufacturer
- Device product
- Device brand
- Device language setting

The gathered information is then stored in a location that is accessible to the application developer, as provided by the advertising service.

Spyware: SymbOS/Fafespy.A

Fafespy.A is a spyware application developed by Killer Mobile.
**Figure 6: Profit- vs Not Profit-Motivated Threats Per Quarter, 2011-2012**

<table>
<thead>
<tr>
<th>Quarter</th>
<th>Profit-Motivated</th>
<th>Not Profit-Motivated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1 2011</td>
<td>13</td>
<td>6</td>
</tr>
<tr>
<td>Q2 2011</td>
<td>18</td>
<td>20</td>
</tr>
<tr>
<td>Q3 2011</td>
<td>39</td>
<td>37</td>
</tr>
<tr>
<td>Q4 2011</td>
<td>29</td>
<td>33</td>
</tr>
<tr>
<td>Q1 2012</td>
<td>35</td>
<td>17</td>
</tr>
<tr>
<td>Q2 2012</td>
<td>37</td>
<td>22</td>
</tr>
<tr>
<td>Q3 2012</td>
<td>28</td>
<td>39</td>
</tr>
</tbody>
</table>

**Figure 7: Profit- vs Not Profit-Motivated Threats by Platform, Q3 2012**

- **Android**
  - Profit-Motivated: 20
  - Not Profit-Motivated: 22

- **Blackberry**
  - Profit-Motivated: 1
  - Not Profit-Motivated: 0

- **iOS**
  - Profit-Motivated: 0
  - Not Profit-Motivated: 2

- **Windows Mobile**
  - Profit-Motivated: 1
  - Not Profit-Motivated: 0

- **Symbian**
  - Profit-Motivated: 14
  - Not Profit-Motivated: 7

**Note:** The threat statistics used in Figure 6 and 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.
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/AckPosts.A

AckPosts.A collects information from the contact list, and forwards the details to a remote address.

Trojan: Android/AppService.A

AppService.A is distributed via a trojanized application, where it is repackaged in another application that seems legitimate. When executed, it collects user information and details on other installed application on the device. This information is then forwarded to a remote server.

AppService.A also connects to two other remote servers, from which it downloads other malicious applications to be installed on the infected device.

Trojan: Android/DropDialer.A

During installation, DropDialer.A displays a message asking the user to agree to certain terms and conditions.
This action will trigger an SMS message to be sent to 3170. After that, the user is presented with an option to switch the screensaver to a theme based on the video game Grand Theft Auto 4. Different themes are also available, as indicated by the package names.

Trojan:Android/FireLeaker.A

FireLeaker.A accesses contacts information on the device on which it was installed. It later collects and forwards these details to a remote server.

Trojan:Android/FjCon.A

FjCon.A is signed with a key trusted by common custom ROM builds, allowing it to obtain permissions that are usually not needed in typical applications. For example, the INSTALL_PACKAGES and DELETE_PACKAGES allows it to remotely install an application or package onto the device without the user noticing.

FjCon.A also monitors SMS messages, looking specifically for those coming from 10658166. Messages with these contents in the body will be blocked:

- 83589523
- 客服
- 资费
- 1.00 元
• 2.00元
• 元/条
• 元/次
• 1元
• 2元
• 网游

Snippet of code that instructs FjCon.A to install applications onto the device

Trojan: Android/IconoSys.A

IconoSys.A is distributed under various application names—My Pony’s Birthday Countdown, My Twitter Pics, Blonde Jokes, SMS Wish, etc.—but all leads to the same registration page.
During the registration, users are asked to provide several information which may be leaked to other unintended recipients. The information that users provide include:

- Device manufacturer
- Device model
- Email address
- International Mobile Equipment Identity (IMEI) number
- Package version
- Phone number
- User’s age
- User’s gender
- User’s name

**Trojan:Android/LoveSpy.A**

LoveSpy.A is a program that claims to be an anti-virus application, but is actually a spying tool. It monitors SMS and call activities on the device and later forwards the log to a remote server. Logged information include:

- Content of SMS
- Date of call or SMS
- Duration of call
- GPS location
- International Mobile Equipment Identity (IMEI) number
- Name
- Phone number
- Type of call
Since it receives commands via SMS, LoveSpy.A will intercept these messages, as displaying them to the user bring attention to its suspicious activities. It specifically looks for those that begin with the following strings, as they translate to certain actions:

- SCL – send call log
- IME – send device’s IMEI number
- REG – register device through the application
- SML – send SMS log
- CMB – make a call back to the sender’s number
- SYCP – send user’s location
- SYFP – send user’s location

**Trojan: Android/LuckyCat.A**

LuckyCat.A may be connected to an advanced persistent threat (APT) campaign that shares the same name. The LuckyCat campaign targets the Indian and Japanese military research institutions; Chinese hackers were believed to be responsible behind this campaign.
LuckyCat.A exhibits remote access trojan (RAT) capabilities, and connects to a command and control (C&C) server that will further instruct the malware to perform these actions:

- Browse directory in the device
- Download file from the device
- Upload file to the device
- Send information to the C&C server

**NOTE:** For additional reading on the Luckycat APT campaign, please refer to the article titled ‘Luckycat’ APT Campaign Building Android Malware (http://www.darkreading.com/mobile-security/167901113/security/attacks-breaches/240004623/luckycat-apt-campaign-building-android-malware.html).

**Trojan: Android/Maistealer.A**

Maistealer.A collects the user’s contact names and their email addresses. This information is stored in /sdcard/addresscap/list.log, and later uploaded to a remote site.

**Trojan: Android/MarketPay.A**

MarketPay.A is distributed via a trojanized application, using a package named com.mediamoz.gotq.apk. When installed on a device, it automatically places orders to purchase applications from the Chinese mobile market (10086.cn) without the user’s consent.

This malware also collects the device’s associated phone number and IMEI number, and forwards this information to a remote server.
Trojan:Android/NandroBox.A

When launched, NandroBox.A displays a page that notifies the user of a list of terms and conditions. Once the user has clicked Confirm, it sends out the device’s IMEI number and other information to a remote site in XML format.

![Screenhots of NandroBox.A](image)

Next, it sends an SMS message to 1065800815747, with content that follows this format: XXX, game_id, version, 0, channel. To cover its tracks, the malware will intercept all messages from the aforementioned number.

![Details for the SMS message that NandroBox.A is instructed to send](image)

Trojan:Android/PopWeb.A

PopWeb.A harvests device information, and forwards the them to a remote location. Harvested information includes:

- Email
- Location
- Phone number
- SIM serial number
- WiFi MAC address

Trojan:Android/SmsSend.A, and variant B and C

SmsSend.A is a version of another malware called OpFake. It reaps profit by sending the message ‘gf bigfun 281 fnuXW9Ey5’ to these numbers: 9993, 9994, and 9995.

SmsSend.C operates in the same way SmsSend.A does, but uses a different display image, message content and recipient numbers. When executed, it displays images of nude women and sends out the message ‘galve 328 SjhFaG1IK’ to the following numbers: 6008, 6006, 6152, and 6952.
**Trojan: Android/SmsZombie.A**

SmsZombie.A drops a malicious component to a live wallpaper application on the device, featuring various images of women. The malware then creates a file named phone.xml and proceeds to collect user information and banking-related data that can be found on the device. The collected data are later sent via an SMS message to the number 13093632006.

**Trojan: Android/Sumzand.A, and variant B**

During execution, Sumzand.A displays an image of a battery power meter that appears to gauge the battery performance.
In the background, what actually happens is that Sumzand.A is collecting details such as phone numbers from the contact list, and forward them to a remote server. These numbers may later be used in SMS spam campaign or sold to other interested parties.

**Trojan:Android/Vdloader.A**

Vdloader.A collects device information such as the IMEI and IMSI number and forwards the details to a remote address. It is also capable of downloading and installing APK files, and sending out SMS messages.

**Trojan:Android/Vidro.A**

Vidro.A presents the user with a list of terms and conditions during the installation process. Once the user clicks Yes to these conditions, it connects to and downloads content from a remote site.

It will also connect to another remote address, and try to update itself. This will trigger an SMS message with the content "PAY 1d489fa9-4a8e-4877-ab0d-6a56830ed8b0" to be sent to 72908.
**Trojan:Blackberry/Zitmo.A**

Back in 2010, we reported about a Zitmo (mobile version of the Zeus malware) attack on Blackberry devices. Now there is a new variant, which uses the COD file format. Its purpose remains the same—it monitors incoming SMS messages for those containing a mobile Transaction Authentication Number (mTan), which are sent by banks to their customers in order to complete an online banking transaction. The malware instead forwards the SMS messages to a remote server.

**NOTE:** The previous Zitmo attack on Blackberry devices were reported in the blog post titled ‘Zeus Variants Targeting Mobile Banking’ (http://www.f-secure.com/weblog/archives/00002037.html).

**Trojan:SymbOS/FakePatch.A**

FakePatch.A profits by sending SMS messages to premium rate numbers and leaving the user to pay for the charges incurred. It also terminates any antivirus-related processes to avoid detection.

**Trojan:SymbOS/Foliur.A**

Once installed, Foliur.A proceeds to download and install new programs onto the device. Aside from that, its other activities include sending out SMS messages to premium rate numbers and killing off anti-virus processes to avoid detection.

**Trojan:SymbOS/HRU.A**

To protect itself, HRU.A kills off any process belonging to a security product. If the user attempts to uninstall it, the program terminates its own installer process to prevent uninstallation. HRU.A’s activities are triggered by an Ogg Vorbis recognizer.

**Trojan:SymbOS/Impler.A**

Impler.A is a program that contains references to several online games. It quietly downloads and installs new programs onto the device without the user’s consent. When the user attempts to uninstall Impler.A, it will kill off the installer process to block the uninstallation.

**Trojan:SymbOS/KillTrust.A**

KillTrust.A temporarily modifies the system settings so that it can install untrusted programs onto the device without the user noticing. It will also kill off the installer process and some other processes.

---

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

**Ogg Vorbis:** A non-proprietary audio compression format used to store and play digital music.
Trojan:SymbOS/Nokan.A, and variant B
Nokan.A downloads and installs other programs onto the device without the user’s consent. It also terminates the installer process when an attempt to uninstall the application is made.

Trojan:SymbOS/PlugGamer.A
PlugGamer.A contains a lot of similarities with the AndroGamer malware first seen in Q2 2012. It downloads and installs new programs onto the device, and forwards the device information to a remote server.

Trojan:SymbOS/Ropitor.A
Ropitor.A downloads configuration files and software from a remote host and silently installs them onto the device. It is also capable of removing software from the device based on the downloaded configuration files.

Trojan:SymbOS/Shilespy.A
Once installed on a device, Shilespy.A performs the following activities:

- Connects to a remote host
- Monitors and sends out SMS messages
- Installs new software onto the device
- Dials and sends DTMF commands over the voice line

Trojan-Downloader:Android/Morepak.A
Morepak.A is packaged inside a trojanized application and includes an advertising component. Once installed, it connects to a remote location, then proceeds to download malicious files onto the device.

DTMF: Dual-Tone Multi-Frequency signaling, used for telecommunication signaling between a phone and the switching center.

FinSpy.A is the mobile version of the FinFisher surveillance software, a commercial trojan manufactured by the UK-based security company Gamma International. This threat was released on multiple platforms—Android, iOS, Symbian and Windows Mobile. It is used to remotely monitor the device and is capable of performing these tasks:

- Taking screenshots
- Recording keyboard strokes
- Intercepting Skype communications
- Tracking a device’s location
- Monitoring SMS messages and phone calls

**NOTE:** For additional reading on FinFisher, please refer to (https://www.privacyinternational.org/finfisherreport/).
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.

» Monitoring-Tool:Android/FinSpy.C
» Riskware:Android/PremiumSMS.E
» Spyware:SymbOS/Flexispy.M
» Trojan:Android/EuropaSMS.C
» Trojan:Android/FakeInst.P, and variant Q and R
» Trojan:Android/FakeLogo.D
» Trojan:Android/FakeUpdates.B
» Trojan:Android/GameX.B
» Trojan:Android/GoldDream.C
» Trojan:Android/OpFake.J
» Trojan:SymbOS/AndroGamer.C
» Trojan:SymbOS/KensoyK.B
» Trojan:SymbOS/MapUp.D
» Trojan:SymbOS/MulGamer.B
» Trojan:SymbOS/RandomTrack.B
» Trojan:SymbOS/SivCaller.B, and variant C
» Trojan:SymbOS/Zhaomiao.H
Figure 8: Top-10 Android Detection Hits, Q3 2012

Figure 9: Breakdown of Heuristic Detection, Q3 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 Android Malware, Riskware and Spyware, Q3 2012**

**Top-30 Malware**

<table>
<thead>
<tr>
<th>Detection</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trojan:Android/Boxer.C</td>
<td>12471</td>
</tr>
<tr>
<td>Trojan:Android/RuFailedSMS.A</td>
<td>2289</td>
</tr>
<tr>
<td>Trojan:Android/FakeInst.L</td>
<td>1221</td>
</tr>
<tr>
<td>Trojan:Android/Kmin.A</td>
<td>1103</td>
</tr>
<tr>
<td>Trojan:Android/Kmin.C</td>
<td>1047</td>
</tr>
<tr>
<td>Trojan:Android/FakeInst.E</td>
<td>937</td>
</tr>
<tr>
<td>Trojan:Android/OpFake.E</td>
<td>672</td>
</tr>
<tr>
<td>Trojan:Android/JiFake.F</td>
<td>604</td>
</tr>
<tr>
<td>Trojan:Android/SMStado.A</td>
<td>550</td>
</tr>
<tr>
<td>Trojan:Android/FakeInst.A</td>
<td>418</td>
</tr>
<tr>
<td>Trojan:Android/Ginmaster.B</td>
<td>363</td>
</tr>
<tr>
<td>Trojan:Android/GoldDream.C</td>
<td>336</td>
</tr>
<tr>
<td>Trojan:Android/FakeInst.K</td>
<td>336</td>
</tr>
<tr>
<td>Trojan:Android/DroidKungFu.C</td>
<td>316</td>
</tr>
<tr>
<td>Trojan:Android/OpFake.F</td>
<td>313</td>
</tr>
<tr>
<td>Trojan:Android/FakeNotify.A</td>
<td>265</td>
</tr>
<tr>
<td>Trojan:Android/BaseBridge.A</td>
<td>235</td>
</tr>
<tr>
<td>Trojan:Android/Ginmaster.D</td>
<td>193</td>
</tr>
<tr>
<td>Trojan:Android/Ginmaster.C</td>
<td>153</td>
</tr>
<tr>
<td>Trojan:Android/AutoSPSubscribe.A</td>
<td>140</td>
</tr>
<tr>
<td>Trojan:Android/Ginmaster.A</td>
<td>118</td>
</tr>
<tr>
<td>Trojan:Android/DroidKungFu.F</td>
<td>116</td>
</tr>
<tr>
<td>Trojan:Android/BaseBridge.D</td>
<td>91</td>
</tr>
<tr>
<td>Trojan:Android/Geinimi.D</td>
<td>84</td>
</tr>
<tr>
<td>Trojan:Android/FjCon.A **</td>
<td>82</td>
</tr>
<tr>
<td>Trojan:Android/Frogonal.A</td>
<td>79</td>
</tr>
<tr>
<td>Trojan:Android/FakeBattScar.B</td>
<td>78</td>
</tr>
<tr>
<td>Trojan:Android/Kmin.B</td>
<td>76</td>
</tr>
<tr>
<td>Trojan:Android/DroidDream.D</td>
<td>74</td>
</tr>
<tr>
<td>Trojan:Android/FakeBattScar.A</td>
<td>64</td>
</tr>
</tbody>
</table>

**Top-30 Riskware and Spyware**

<table>
<thead>
<tr>
<th>Detection</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adware:Android/Ropin.A</td>
<td>6867</td>
</tr>
<tr>
<td>Application:Android/Counterclank.A</td>
<td>2936</td>
</tr>
<tr>
<td>Adware:Android/AdWo.A **</td>
<td>2265</td>
</tr>
<tr>
<td>Adware:Android/Gappusin.A</td>
<td>2023</td>
</tr>
<tr>
<td>Application:Android/FakeApp.C</td>
<td>409</td>
</tr>
<tr>
<td>Spyware:Android/EWalls.A</td>
<td>84</td>
</tr>
<tr>
<td>Riskware:Android/Boxer.D</td>
<td>75</td>
</tr>
<tr>
<td>Exploit:Android/DroidRooter.B</td>
<td>63</td>
</tr>
<tr>
<td>Exploit:Android/DroidRooter.A</td>
<td>60</td>
</tr>
<tr>
<td>Riskware:Android/MobileTX.A</td>
<td>36</td>
</tr>
<tr>
<td>Spyware:Android/SndApps.A</td>
<td>32</td>
</tr>
<tr>
<td>Monitoring-Tool:Android/SpyTrack.B</td>
<td>25</td>
</tr>
<tr>
<td>Application:Android/Steveware.A</td>
<td>24</td>
</tr>
<tr>
<td>Monitoring-Tool:Android/MobileSpy.C</td>
<td>21</td>
</tr>
<tr>
<td>Hack-Tool:Android/DroidRooter.H</td>
<td>20</td>
</tr>
<tr>
<td>Exploit:Android/DroidRooter.C</td>
<td>17</td>
</tr>
<tr>
<td>Hack-Tool:Android/DroidRooter.A</td>
<td>15</td>
</tr>
<tr>
<td>Monitoring-Tool:Android/Spyoo.A</td>
<td>15</td>
</tr>
<tr>
<td>Exploit:Android/GBFM.A</td>
<td>14</td>
</tr>
<tr>
<td>Monitoring-Tool:Android/MobileMonitor.A</td>
<td>13</td>
</tr>
<tr>
<td>Adware:Android/Mobsqueeze.A</td>
<td>11</td>
</tr>
<tr>
<td>Exploit:Android/DroidRooter.E</td>
<td>9</td>
</tr>
<tr>
<td>Hack-Tool:Android/TattooHack.A</td>
<td>9</td>
</tr>
<tr>
<td>Monitoring-Tool:Android/MobileTracker.A</td>
<td>9</td>
</tr>
<tr>
<td>Monitoring-Tool:Android/KidLogger.B</td>
<td>7</td>
</tr>
<tr>
<td>Monitoring-Tool:Android/SpyBubble.B</td>
<td>7</td>
</tr>
<tr>
<td>Riskware:Android/QPlus.A</td>
<td>6</td>
</tr>
<tr>
<td>Monitoring-Tool:Android/MobiSmSpy.A</td>
<td>6</td>
</tr>
<tr>
<td>Hack-Tool:Android/DroidRooter.E</td>
<td>5</td>
</tr>
</tbody>
</table>

**Note**: The threat statistics used in Table 1 are made up of the number of unique Android application package files (APKs).
F-SECURE MOBILE SECURITY

F-Secure Mobile Security effectively protects your mobile device, smartphone or tablet, from all common mobile threats. It guards against loss and theft, protects your children online with powerful parental control functions, keeps your device free of malware and lets you browse the web safely.

Find out more:
http://www.f-secure.com/web/home_global/mobile-security

Purchase F-Secure Mobile Security:
https://shop.f-secure.com/cgi-bin/shop/?ID=FSMAV