MOBILE THREAT REPORT

JANUARY-MARCH 2013

F-Secure

F-Secure Labs

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

At any given moment, F-Secure Response Labs staff is on top of the worldwide security situation, ensuring that sudden virus and malware outbreaks are dealt with promptly and effectively.

Protection around the clock

Response Labs' work is assisted by a host of automatic systems that track worldwide threat 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.

CONTENTS

METHODOLOGY

THIS REPORT IS BASED ON MOBILE APPLICATION DATA GATHERED DURING THE PERIOD OF 1ST JANUARY TO 31ST MARCH 2013 FROM A VARIETY OF SOURCES INCLUDING, AMONG OTHERS, THE OFFICIAL ANDROID PLAY STORE AND APPLE APP STORE, THIRD-PARTY MOBILE APPLICATION SITES, AND ANONYMIZED DATA FROM F-SECURE MOBILE SECURITY CUSTOMERS. THE COLLECTED SAMPLES AND DATA ARE SCANNED BY MULTIPLE INTERNAL ANALYSIS SYSTEMS, AS WELL AS BY F-SECURE LABS' THREAT RESEARCH ANALYSTS.

CATEGORIZING MOBILE THREATS

F-Secure Labs classifies mobile threats into two categories based on their potential for damaging the user's device or data: Malware and Potentially Unwanted Application (PUA). The programs can be further divided based on how they behave.

Unlike PC-based threats, mobile malware have shown relatively little diversity thus far. Worms (Bluetooth-worms in particular) were once relatively common in the mobile threat landscape of the early 2000, but in the last few years, the vast majority of mobile threats F-Secure Labs have encountered have been trojans.

The following list provides a brief summary of the various types of mobile threats seen up until Q1 2013:

MALWARE	Software that performs actions which pose a significant security risk to the user's system and/or information. The type of behavior the program engages in is used to further identify it as one of the following types:	
	Backdoor	A program that provides unauthorized remote access to the device.
	Trojan	A program that deliberately performs harmful actions such as stealing data, hijacking device resources, interfering with the user's control of the device, etc. Beneficial functionality, if any exists, is intended as a decoy or distraction to draw attention away from the malicious payload. Trojans may be further subdivided by the type of action they take — trojan-downloader, trojan-dropper, trojan-spy, etc.
	Worm	A program that creates exact or similar standalone copies of itself. The copies can be on the device and/or connected or removable media. A notable subset of worms send copies of themselves over a Bluetooth connection, i.e., Bluetooth-worm.
PUA	For mobile applications, this term encompasses the Spyware and Riskware categories used for PC-based threats and is used to classify legitimate programs that may be considered undesirable or intrusive by a user if used in a questionable manner, or may inadvertently introduce risk.	
	Spyware	A program that collects data about the user's behavior patterns, such as Web browsing history and site preferences, and stores the data locally or remotely.
	Trackware	A program that gathers data that could be used to identify a user or a device to a third party, for example, an app that provides device location services as theft protection.
	Adware	A program that displays advertising content. Adware may also track the user's behavior patterns to better target the advertising content to be displayed.

LATEST THREATS IN THE LAST THREE MONTHS

EXECUTIVE SUMMARY

While the raw amount of Android malware continues to rise significantly, it is the increased commoditization of those malware that is the more worrying trend. The Android malware ecosystem is beginning to resemble to that which surrounds Windows, where highly specialized suppliers provide commoditized malware services. Two key examples of this trend surfaced in the first quarter of 2013 in the form of "Stels" and "Perkele" malware. Besides commoditization, targeted attacks and spam operations involving Android malware are also making strides in the mobile threat scene.

"The Android malware ecosystem is beginning to resemble that which surrounds Windows..."

COMMODITIZATION

In the fourth quarter of 2012, an Android trojan known as "Stels" (detected by F-Secure Mobile Security as Trojan:Android/SmsSpy.K) was distributed via Russian language mobile software portals. It targeted Android users in Russia to fall prey to its premium rate SMS fraud. But in Q1 2013, Stels switched its operation to adopt a spam module and shifted some of its distribution to a well-known botnet called Cutwail. The Cutwail botnet has long been involved in baiting victims and leading them towards sites hosting the infamous Blackhole exploit kit.

Stels' new distribution method uses Internal Revenue Services (IRS)-themed spam, targeting recipients living in the US, which is linked to Android-aware servers. If the spam recipient clicks on a Cutwail link from an Android device, he will be directed to a webpage asking him to "update the Flash Player software"—this is a typical modus operandi for Windows malware. By installing the so-called "Flash Player," the victim unknowingly grants the trojan the permission to make phone calls. Stels will capitalize on this permission to reap profit by placing long-lined (a.k.a. short-stopped) calls while the device owner is asleep.

Another instance of commoditization that surfaced in Q1 2013 came in the form of "Perkele" (page 17)—a mobile banking trojan component designed to be used in conjunction with Windows banking trojans such as Zeus. Such SMS spy components, which are used to circumvent two-factor authentication schemes, are nothing new. They have been used by 'high-end' Zeus variants for years already. But in those earlier cases, it was the high-end Zeus operators who commissioned the work from the component developers.

In the case of Perkele, an independent developer is bringing his component to the crimeware marketplace and offering his distribution to smaller 'low-end' Zeus gangs. This signals the shift to malware as a service—Zeus-in-the-mobile (Zitmo) for the masses. Now anybody running a Zeus botnet can find affordable options for Zitmo. Perkele has been found to target banks located in various countries, including Italy, Thailand, and Australia. For each bank, its appearance is customized to imitate the banks' branding style to make its case more convincing. And Perkele's vendors will happily customize the Zitmo's user interface for dozens more.

TARGETED ATTACKS

In addition to increasing commoditization of Android malware, Q1 2013 has also seen interesting developments concerning targeted attacks. Targeted attacks have long been a staple of Windows malware; now it is creeping into Android malware's territory. In March, an Android trojan was discovered being sent from a Tibetan activist's

compromised email and distributed to other high profile human rights activists. Highly targeted attacks against such activists is nothing new; they have long been the target of even the small amount of existing Mac malware. This "Chuli" (page 14) attack further validates the idea that no operating system is entirely safe—there is no security through obscurity. Now that it has been demonstrated that Android malware is targeting human rights activists, it is only a matter of time before such trojans will be used against countries and governments.

"...it is only a matter of time before such trojans will be used against countries and governments"

Another example of Android malware being used in a targeted attack is "SmSilence" (page 18), which has been discovered in South Korea using the guise of "coupons" for a popular coffeehouse chain. If the so-called coupon app is installed, the malware will check if the phone number has a South Korean country code (+82). If the condition is met, SmSilence will harvest information from the device and forward the details to a server located in Hong Kong[1].

419 SCAMS

Advanced fee fraud is one of the oldest scams in the book. You would probably find "419 scams" slotted somewhere in your emails' spam folders. Previously distributed via emails and SMS messages, malware authors are now utilizing mobile apps to propagate their scams.

In Q1 2013, fake "job offer" (page 16) Android apps have been discovered circulating in India. The apps claim to provide a means for the user to submit their curriculum vitae (CV) for consideration. At the end of the process, the apps request that the user submit a "process fee." Unfortunately, the job for which the victim is applying is not real; but the financial loss is.

Most, if not all, approaches taken by Android malware have been seen before on a different platform, i.e., Windows. In a way, Android is experiencing the same fate as Windows where its huge market share works in both good and bad ways. Such popularity certainly translates well in terms of sales, but it also appeals to the maliciously-minded crowds. Malware authors see plenty of opportunities yet to be explored on the relatively new and growing platform. And they are drawing inspiration from Windows malware's approaches, which is why we are now seeing trends such as commoditization of malware services, targeted attacks and 419 scams popping up in the mobile threat scene.

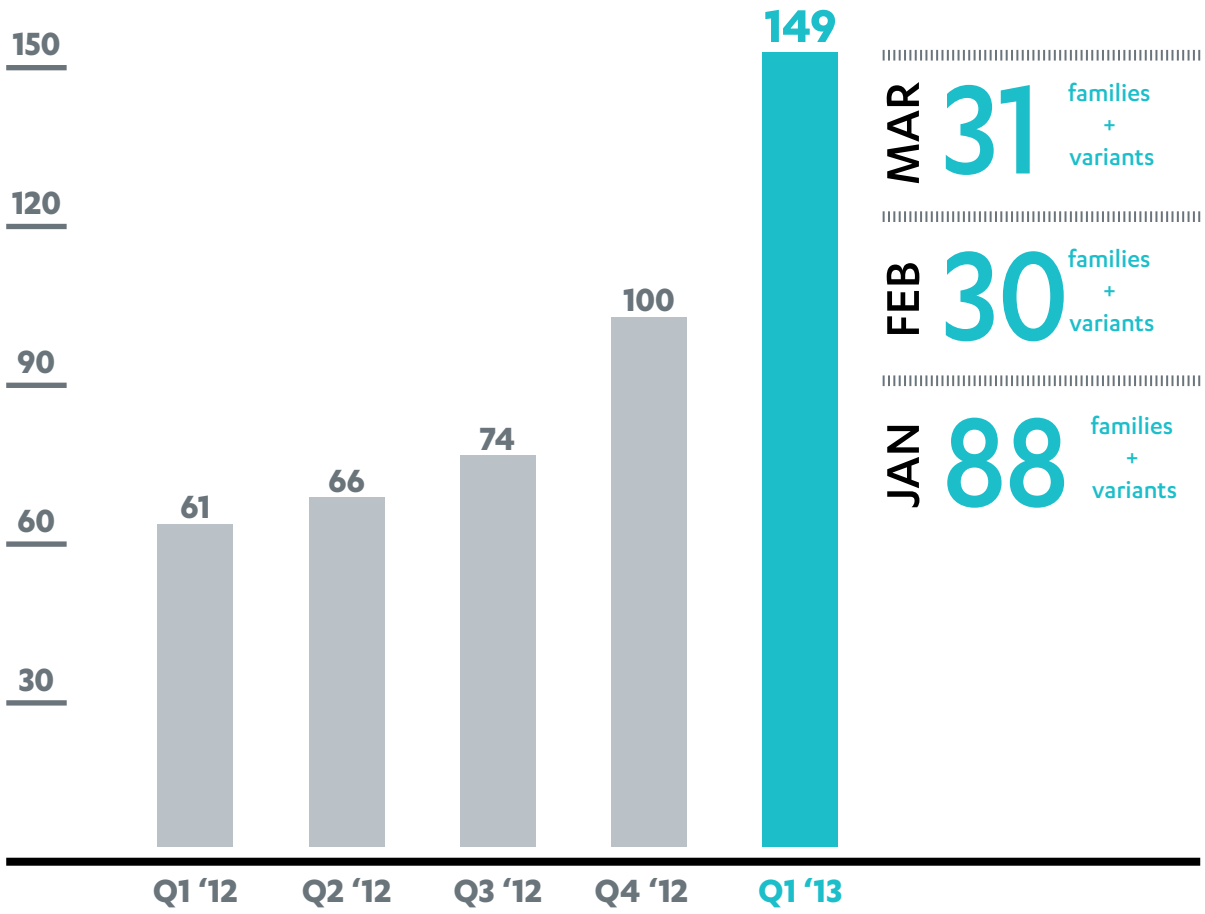
DETECTIONS

Stels – Trojan:Android/SmsSpy.K
Perkele – Trojan:Android/PerkeSecuApp.A
Chuli – Trojan:Android/Chuli.A
SmSilence – Trojan:Android/SmSilence.A
FakeJobOffer – Trojan:Android/FakeJobOffer.A

SOURCE

[1] F-Secure Weblog; Sean Sullivan; *South Korea, Starbucks, and Android/Smsilence*; published 10 April 2013; https://www.f-secure.com/weblog/archives/00002540.html

FIGURE 1: NEW MOBILE THREAT FAMILIES AND VARIANTS, Q1 2013



TOTAL THREAT COUNT

149

families + variants

54

new families (+ different variants)

95

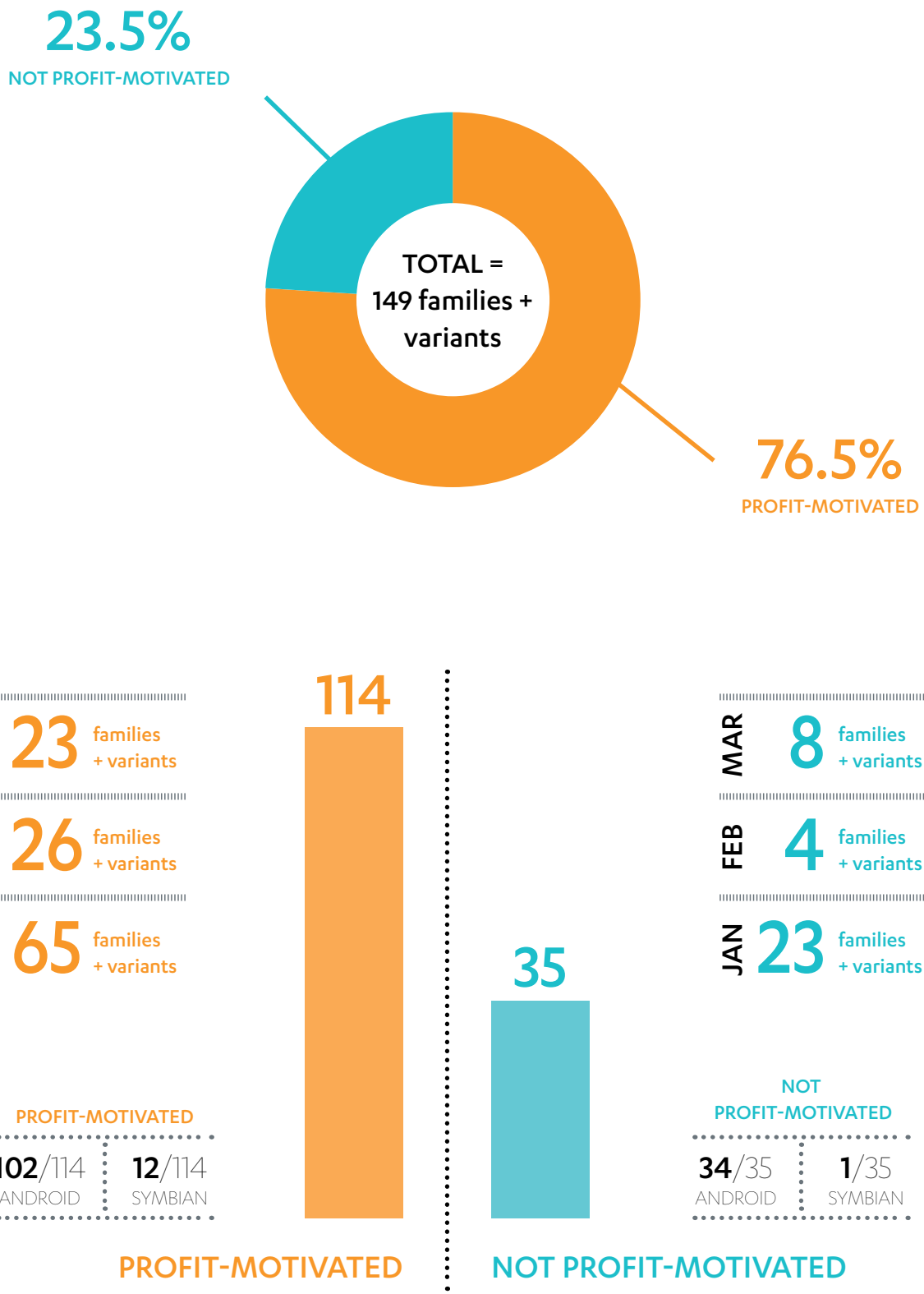
new variants of existing families

136/149
ANDROID

13/149
SYMBIAN

0/149
OTHERS (Blackberry, iOS, Windows Mobile)

FIGURE 2: MOBILE THREATS MOTIVATED BY PROFIT, Q1 2013



ADWARE

If you have ever downloaded a free app, chances are you have encountered an adware, a program that displays advertising content through an advertising module. Some may also track the user's behavior patterns to better target which advertising content to be presented to that user. Free apps are often adware, or are distributed with them, because it provides a way for the developer to offset the development cost through advertising revenue, hence the term 'ad-supported.'

Most adware programs are not malicious in intent. Annoying perhaps, but certainly harmless. They are just displaying advertisements—not that much different from being shown commercials while watching your favorite television show. Unfortunately, there is a fraction of adware that crosses to the malicious side.

When an adware leads the user to a malicious site, it is now categorized as malicious. Since adware is often bundled with other apps, tricky situations arises when the main application is clean but the adware is not. To make matters more complicated, the adware content may also be tailored to the user based on regions. For example, a user in Finland may be presented with an ad that is different from the one presented to a user in Brazil. One may be clean, but the other one could be malicious. Besides, the ad module could be changed easily from day to day. A malicious ad module that appears today might be replaced with a clean one tomorrow. Because of these factors, it is hard to accurately categorize an adware as entirely clean or malicious.

And then, there are some adware that fall in a gray area. They abide the rules and do nothing wrong, yet they may use sneaky tactics to convert the ads into sales revenue. Let's take a look at apps that are offered for free but rely on in-app purchases as a source of revenue. By legal definition, they are doing nothing wrong. Users are not being forced to make a purchase if they don't wish to. Before proceeding with a purchase transaction, the users are presented with a dialog box to confirm the purchase in case that they accidentally clicked on the purchase button.

However, when the same tactic is used in apps targeted to small children, it raises some ethical issues. Mobile devices, which comprises smartphones and tablets, are this era's babysitter. There is a market for children's apps; most parents willingly download apps requested by their children, especially if the app is free. Small children may not understand that they are paying real money to make purchases in a game and the parents may make a mistake by not setting up password prompt for each purchase or download made on the device. These are the conditions—children's naivety, parents' trust, unsecured device settings, etc.—that some adware may manipulate in order to generate sales revenue from in-app purchases.

An adware is, generally, a simple program whose function is to display advertisements; but it can be a surprisingly difficult program to rate from a security point of view. Based on the (often externally provided) advertising content, the program can be considered clean, malicious, or somewhere in between. And as this content changes, the security of an app can change from time to time, or differ by region. Clearly identifying a program that displays advertising content as Adware, however, means users can at least be aware that such an element is present in an app so that they can exercise judgment when necessary.

NOTEWORTHY THREATS

>> Backdoor:Android/Damon.A
>> Trojan:Android/Chuli.A
>> Trojan:Android/Exprespam.A
>> Trojan:Android/FakeJobOffer.A
>> Trojan:Android/PerkeSecuApp.A
>> Trojan:Android/Smsilence.A
>> Trojan:Android/Ssucl.A, and variants B and C
>> Trojan:Android/Tetus.A

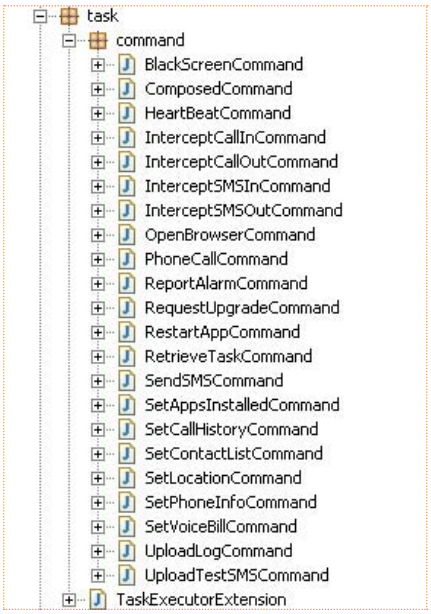
Backdoor:Android/Damon.A

Damon.A is a backdoor program that circulates in a third party Android app market in China. It is dropped onto a device by a downloader program of the same name, which was injected into a clean application to mask its malicious identity.

Damon.A allows the attacker to take control of the device and perform these activities from a remote location:

- Collect device information
  - » Call logs
  - » Contacts
  - » International Mobile Equipment Identity (IMEI) number
  - » International Mobile Subscriber Identity (IMSI) number
  - » Locations
- Intercept phone calls
- Intercept SMS messages
- Make phone calls
- Send logs to attacker
- Send out SMS messages
- Restart itself
- Upgrade itself
- Visit website

F-Secure detects the backdoor component as Backdoor:Android/Damon.A and the downloader as Trojan-Downloader:Android/Damon.A.



List of commands found in a Damon sample

DATE DISCOVERED:
March 2013

COUNTRY DISCOVERED:
China

ACTIVITIES:
Collect device information
Intercept phone calls
Intercept SMS messages
Direct users to a website

CONNECTS TO C&C SERVER:
Yes

PROFIT MOTIVATED:
Yes

Trojan:Android/Chuli.A

Chuli.A is an information stealing trojan that was used in a targeted attack involving a Tibetan activist and several other high-profile human rights activists.

Chuli.A arrives onto a device via an installer named 'WUCs Conference.apk' and is installed as an application named Conference. When launched, it displays a string of text addressing several organizations.

Chuli.A's icon (left) and message (right)

In the background however, Chuli.A connects to a command and control (C&C) server at the IP address 64.78.161.133 to report the infection. It also collects device information and forwards the details to the server if instructed to do so via an SMS message. Collected information include:

- Contacts data
- GPS coordinates
- Phone call logs
- Stored SMS messages

DATE DISCOVERED:
March 2013

ACTIVITIES:
Collect device information
Display activism messages

CONNECTS TO C&C SERVER:
Yes

PROFIT MOTIVATED:
Yes

Trojan:Android/Exprespam.A

Exprespam.A is a trojan that harvests personal information from an infected device. It has been circulating in the unofficial Android app market and targets Android users in Japan. During the installation process, it requests for permissions which will essentially allow it to access or view these items:

- Accounts listed in the Account Service
- Internet
- Phone state
- User's contacts data

Exprespam.A places an icon on the main application menu. When clicked to launch, it will display a message.

Exprespam.A's icon (left) and displayed message (right)

Meanwhile in the background, it collects information such as phone numbers and contact details (i.e. names and email addresses) stored on the device. The collected information is later forwarded to a remote server, http://ftuk[...]obat.com/.

DATE DISCOVERED:
January 2013

COUNTRY DISCOVERED:
Japan

ACTIVITIES:
Collect user and device information
Upload information to a server

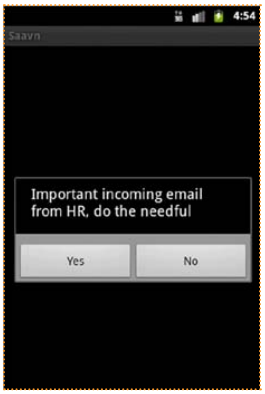
CONNECTS TO C&C SERVER:
Yes

PROFIT MOTIVATED:
Yes

Trojan:Android/FakeJobOffer.A

FakeJobOffer.A is a trojan used is propagating a job offer scam. It targets users in India and is distributed in a third party Android app market, where it is repackaged into legitimate Bollywood related applications such as Saavn and YouBolly.

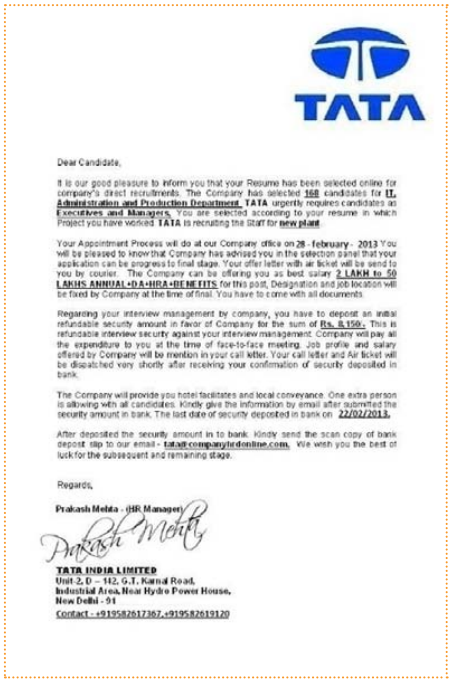
Once installed, FakeJobOffer.A waits for the device to be rebooted to activate its malicious components. It then notifies the user about an incoming email from the Human Resource department, and proceeds to visit a website *(http://ge.tt/api/1/files/4TcQx7Z/0/blob/x675)* on the device's browser.



Email notification

The link directs the user to an image file of a job offer letter, informing that the user has been considered for a position at TATA Group, an Indian multinational conglomerate company. To arrange for a job interview, the user must first pay a refundable security deposit. The victim, obviously, will never get refunded as there is no job interview or even a job in the first place. It is all a scam.

This type of scam is neither new nor complicated. Similar offers have been circulating via emails (see image below) and SMS messages since 2010 in India, but this incident marks the first time that such a scam is carried out through a trojanized Android application.



TATA

Dear Candidate,

It is our good pleasure to inform you that your Resume has been selected online for company's direct recruitments. The Company has selected 168 candidates for IT, Administration and Production Department. TATA urgently requires candidates as Executives and Managers. You are selected according to your resume in which Project you have worked. TATA is recruiting the Staff for new plant.

Your Appointment Process will do at our Company office on 28 - February - 2013 You will be pleased to know that Company has advised you in the selection panel that your application can be progress to final stage. Your offer letter with air ticket will be send to you by courier. The Company can be offering you as best salary 2 LAKH to 50 LAKHS ANNUAL+DA+HRA+BENEFITS for this post, Designation and job location will be fixed by Company at the time of final. You have to come with all documents.

Regarding your interview management by company, you have to deposit an initial refundable security amount in favor of Company for the sum of Rs. 8,150/- This is refundable interview security against your interview management. Company will pay all the expenditure to you at the time of face-to-face meeting. Job profile and salary offered by Company will be mention in your call letter. Your call letter and Air ticket will be dispatched very shortly after receiving your confirmation of security deposited in bank.

The Company will provide you hotel facilitates and local conveyance. One extra person is allowing with all candidates. Kindly give the information by email after submitted the security amount in bank. The last date of security deposited in bank on 22/02/2013.

After deposited the security amount in to bank. Kindly send the scan copy of bank deposit slip to our email - tatajfcompanyitdonline.com. We wish you the best of luck for the subsequent and remaining stage.

Regards,

Prakash Mehta - (HR Manager)

TATA INDIA LIMITED
Unit-2, D – 142, G.T. Karnal Road,
Industrial Area, Near Hydro Power House,
New Delhi - 91
Contact - +919582617367,+919582619120

Fake offer letter, providing the instructions to set up an interview

DATE DISCOVERED:
March 2013

COUNTRY DISCOVERED:
India

ACTIVITIES:
Spread out a job offer scam
Direct user to a suspicious website

CONNECTS TO C&C SERVER:
No

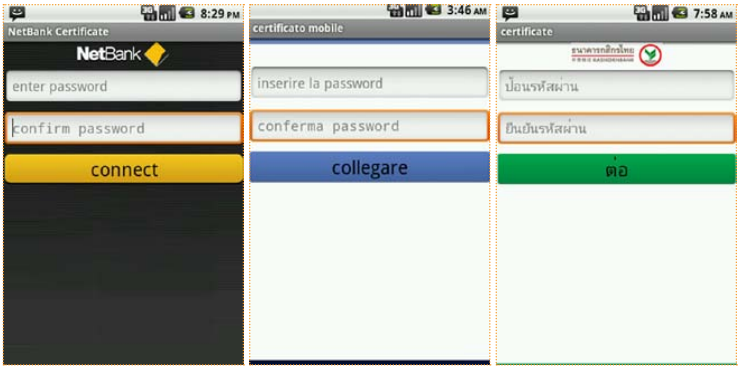
PROFIT MOTIVATED:
Yes

Trojan:Android/PerkeSecuApp.A

PerkeSecuApp.A is a banking trojan that steals confidential data that banks send to customers to validate an online transaction. It monitors incoming SMS messages, looking specifically for those originating from the bank and containing the mobile Transaction Authentication Number (mTAN). Banks typically relies on mTAN as the second part of a two-factor authentication method. This number is sent via an SMS message to the customers, and must be entered to proceed with a transaction.

PerkeSecuApp.A is just one part of the whole operation. It complements the computer-based component that compromises websites using code injection. When users visit compromised banking sites, they will be asked to provide their phone numbers in order to receive a so-called security application from the banks. Users will receive an SMS message containing a link to download the application. Once installed, PerkeSecuApp.A will display or perform a fake operation while silently intercepting SMS messages in the background.

Unlike Zitmo and other banking trojans, PerkeSecuApp.A does not forward the intercepted messages to a remote server or to a URL link but sends out plain SMS messages to a specific number instead.



PerkeSecuApp.A disguised as banking applications

DATE DISCOVERED:
March 2013

COUNTRY DISCOVERED:
Russia

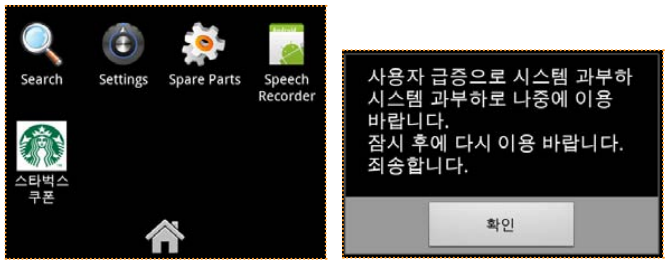
ACTIVITIES:
Monitor incoming SMS messages
Steal mTANs

CONNECTS TO C&C SERVER:
Yes

PROFIT MOTIVATED:
Yes

Trojan:Android/SmSilence.A

SmSilence.A is an SMS spying trojan that was discovered in a third-party Android app market in South Korea. It infiltrates a device by pretending to be an app associated with the products served by a famous coffeehouse chain, Starbucks. This is merely a disguise as it is not actually endorsed by nor affiliated with Starbucks.



SmSilence.A's icon (left) and error notification message (right)

Once installed, SmSilence.A uses an image file named 'Starbugs.png' for its icon, featuring the well-recognized Starbucks logo. When the user clicks on this icon to launch the app, an error notification message will pop up. At the same time, in the background, SmSilence.A is quietly creating a new service to enable its SMS monitoring activities. This service is set up to use the maximum priority value (1000) so that it will be the first one to see any incoming messages.

After creating the service, SmSilence.A will notify about the infection on the device to a URL, http://[...].com/Android_SMS/[...]/installing.php. It uses the HTTP POST method to send the following message—"mobile=<number>"—where <number> respectively indicates the phone number registered to the device.

SmSilence.A is only interested in SMS messages that originated from numbers beginning with "+82" which is the country code for South Korea, as evidenced by the following code found in the analyzed sample:

```
if(paramIntent.getAction().equals("android.provider.Telephony.SMS_
RECEIVED"))
   this.myNumber = ((TelephonyManager)paramContext.
   getSystemService("phone")).getLine1Number();
   if (this.myNumber.substring(0,3).equals("+82"))
```

Code found in an analyzed sample of SmSilence.A

It then proceeds to collect the messages' content and the senders' phone numbers, and forwards the gathered information to a remote location, http://[...].com/Android_SMS/[...]/receiving.php. Any notification of these messages will be blocked, leaving the users unaware that they are receiving messages in the inbox.

DATE DISCOVERED:
February 2013

COUNTRY DISCOVERED:
South Korea

ACTIVITIES:
Intercept incoming SMS messages
Harvest SMS contents and phone numbers
Forward information to a server

CONNECTS TO C&C SERVER:
No

PROFIT MOTIVATED:
Yes

Trojan-Spy:Android/Sscul.A, and variants B and C

Ssucl is a family of trojans found in a third party Android app market. It claims to be a utility application called DroidCleaner or SuperClean that can improve a device's performance. But when installed, it does nothing useful.

Ssucl's main operation revolves around information theft. It communicates with a command and control (C&C) server and receives instructions to carry out further actions. These actions vary between variants and include:

- Upload files, contact data, photos, GPS coordinates, device information (IMEI number, IP address, list of installed application, etc.), and SMS content to the server
- Send or delete SMS messages
- Change the ringer mode to silent or normal
- Set up call forwarding by inputting the code **21* *phonenumber*#, where *phonenumber* is the number to which the calls will be forwarded
- Turn the WiFi on or off
- Launch other applications on the device
- Steal Android or Dropbox login credentials
- Download AutoRun malware onto the device's memory card

Ssucl has been found to be in contact with these two servers:

- http://claco/[...]/kicks-ass.net
- http://claco./[...]/hopto.org

The first part of the URLs is similar to Claudio c, the name used to sign Ssucl's certificate. This similarity may be a hint pointing to the author's name.

Additionally, Ssucl tries to infect the Windows computer linked to device by taking advantage of the AutoRun feature. When infecting a device, Ssucl will copy a Windows executable to the memory card that will automatically run when the device is connected to the computer as an external USB storage device. This Windows component is also a spying trojan; it connects to the same C&C servers as its Android counterpart.

A mobile malware attempting to infect a Windows computer is not a new finding. The CardTrap family of Symbian trojans used the same method —taking advantage of the AutoRun feature to infect memory cards— back in 2005. But this is the first instance where the method is used by an Android malware. However, the AutoRun infection method used by Ssucl is quite crude and does not work on the newer version of Windows or on older versions if the AutoRun feature has been disabled.

DATE DISCOVERED:
February 2013

ACTIVITIES:
Collect user and device information
Alter device setting
Steal login credentials
Infect connected Windows machine

CONNECTS TO C&C SERVER:
Yes

PROFIT MOTIVATED:
Yes

Trojan:Android/Tetus.A

Tetus.A is an information stealing trojan disguised as a fun, social application or a helper tool. It is distributed via a third party Android app market, and may use the following package file names:

- com.appsmediaworld.fitpal
- com.appengines.fastphone
- com.mobilityplus.friendly
- com.coolmasterz.flirt
- com.droidmojo.celebstalker
- com.droidmojo.awesomejokes
- com.stephbrigg5.batteryimprove
- com.supersocialmob.allfriends
- com.nogginfunsite.zgames

Tetus.A spies on incoming SMS messages. Once an event handler is successfully set, it will notify one of these command and control (C&C) servers:

- http://[...]/android/[...]/tetulus.com
- http://[...]/android-gaming-zone/[...]/.com

Whenever a new SMS message arrives, Tetus.A will turn the content into one long string (replacing space with '_') and forward it to the C&C server. The server recognizes different infected devices by the International Mobile Equipment Identity (IMEI) number.

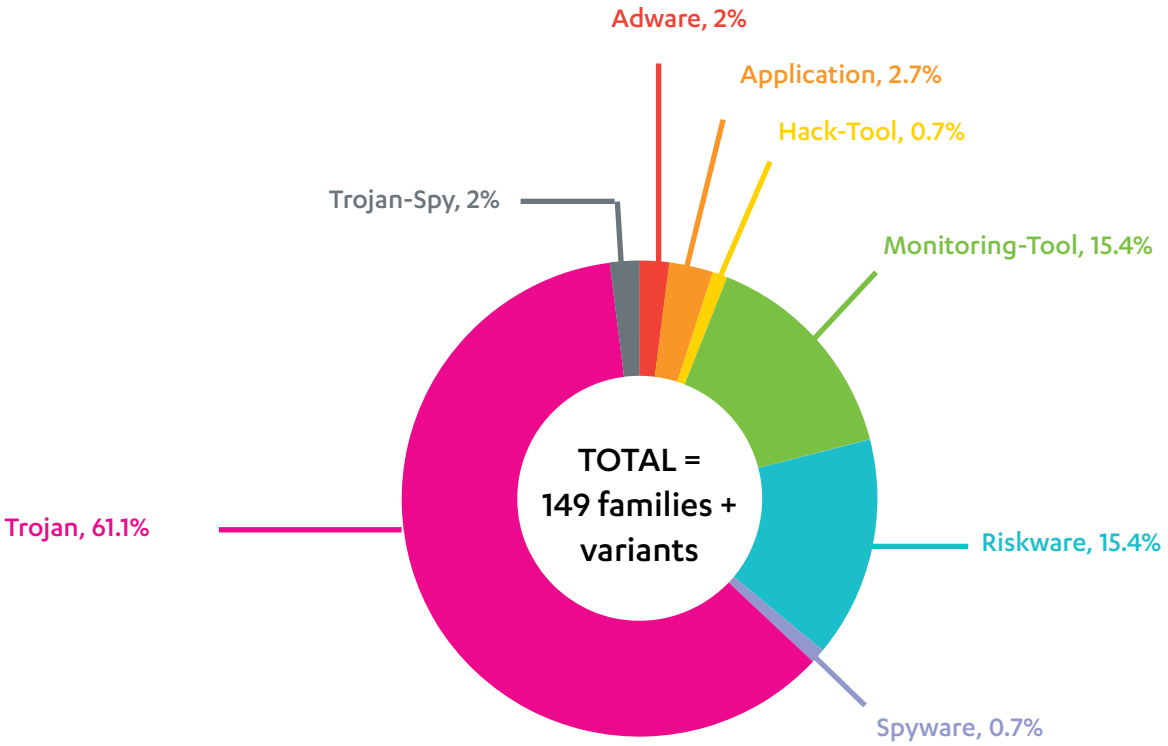
DATE DISCOVERED:
January 2013

ACTIVITIES:
Collect SMS content
Forward information to C&C servers

CONNECTS TO C&C SERVER:
Yes

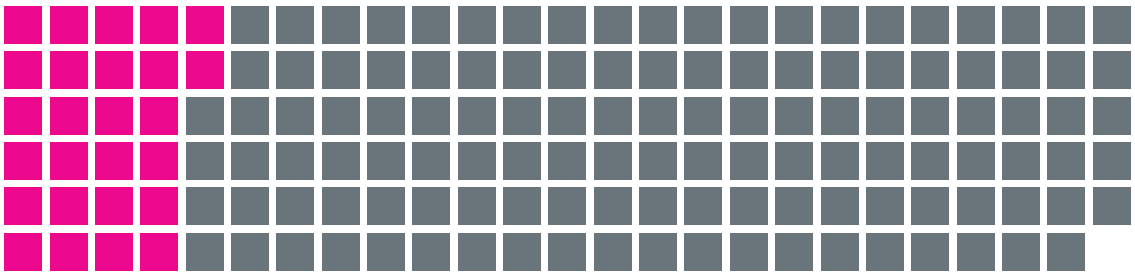
PROFIT MOTIVATED:
Yes

FIGURE 3: MOBILE THREATS BY TYPE, Q1 2013



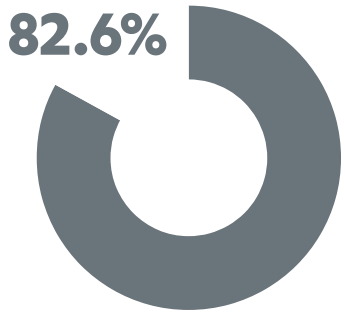
	ANDROID	SYMBIAN
ADWARE	3/149	0/149
APPLICATION	4/149	0/149
HACK-TOOL	1/149	0/149
MONITORING-TOOL	23/149	0/149
RISKWARE	23/149	0/149
SPYWARE	1/149	0/149
TROJAN	78/149	13/149
TROJAN-SPY	3/149	0/149

FIGURE 4: MOBILE THREATS CONNECTED TO C&C SERVERS, Q1 2013



26/149
CONNECTED TO C&C SERVERS

123/149
NOT CONNECTED TO C&C SERVERS



JAN	FEB	MAR
11	7	8

families + variants

JAN	FEB	MAR
77	23	23

families + variants

26/26	0/26
ANDROID	SYMBIAN

110/123	13/123
ANDROID	SYMBIAN

FULL LIST OF DISCOVERED THREATS

TABLE 1: NEW MOBILE THREAT FAMILIES, Q1 2013

CATEGORY	TYPE	DETECTION
PUS	Application	Application:Android/Dcoman.A
		Application:Android/FatatKr.A
	Hack-Tool	Hack-Tool:Android/Kiser.A
	Monitoring-Tool	Monitoring-Tool:Android/Adrsmscon.A
		Monitoring-Tool:Android/AlienFc.A
		Monitoring-Tool:Android/Anforen.A
		Monitoring-Tool:Android/Ansmcon.A
		Monitoring-Tool:Android/CellSpy.A
		Monitoring-Tool:Android/Fauxcopy.A
		Monitoring-Tool:Android/FierceEagle.A
		Monitoring-Tool:Android/Gambler.A
		Monitoring-Tool:Android/Jackq.A
		Monitoring-Tool:Android/Lgxin.A
		Monitoring-Tool:Android/Liey.A
		Monitoring-Tool:Android/Locmg.A
		Monitoring-Tool:Android/RemoteCommander.A
		Monitoring-Tool:Android/SilentTracker.A
		Monitoring-Tool:Android/Smscomm.A
		Monitoring-Tool:Android/StealthCell.A
		Monitoring-Tool:Android/StealthCell.B*
	Riskware	Riskware:Android/Adflood.A
		Riskware:Android/Gamex.A
		Riskware:Android/RediAssi.A
SPYWARE	Adware	Adware:Android/Hamob.A
		Adware:Android/Mulad.A
		Adware:Android/Webim.A

continue >>

CATEGORY	TYPE	DETECTION
MALWARE	Trojan	Trojan:Android/Bacsta.A
		Trojan:Android/Chuli.A
		Trojan:Android/Damon.A
		Trojan:Android/Exprespam.A
		Trojan:Android/FakeJobOffer.A
		Trojan:Android/Fsm.A
		Trojan:Android/Gemni.A
		Trojan:Android/Hrmis.A
		Trojan:Android/Huxre.A
		Trojan:Android/LiveWall.A
		Trojan:Android/Loozfon.A
		Trojan:Android/MobKong.A
		Trojan:Android/PerkeSecuApp.A
		Trojan:Android/SmSilence.A
		Trojan:Android/SystemSecurity.A
		Trojan:Android/Tascudap.A
		Trojan:Android/Tetus.A
		Trojan:Android/Tucysms.A
		Trojan:Android/Zitmo.A
		Trojan:Symbian/Boisted.A
		Trojan:Symbian/Drytion.A
		Trojan:Symbian/Larka.A
		Trojan:Symbian/Senog.A
		Trojan:Symbian/Yolkk.A
		Trojan:Symbian/Yolkk.B*
	Trojan-Spy	Trojan-Spy:Android/Ssucl.A
		Trojan-Spy:Android/Ssucl.B*
		Trojan-Spy:Android/Ssucl.C*
		TOTAL = 50 new families + 4 variants of new familiies

* A variant of a new family discovered in Q1 2013

TABLE 2: NEW VARIANTS OF EXISTING FAMILIES, Q1 2013

FAMILY	DETECTION	VARIANT	COUNT
AndSpy	Monitoring-Tool:Android/AndSpy.[variant]	B	1
AutoSPSubscribe	Trojan:Android/AutoSPSubscribe.[variant]	B	1
BaseBridge	Trojan:Android/BaseBridge.[variant]	O	1
DroidKungFu	Trojan:Android/DroidKungFu.[variant]	K, L, M, N	4
FakeApp	Application:Android/FakeApp.[variant]	D	1
FakeInst	Trojan:Android/FakeInst.[variant]	Z, AA, AB, AC, AD, AE, AF, AG, AH, AI, AJ, AK, AL, AM, AN, AO, AP, AQ, AR, AS, AT, AU, AV, AX, AY, AZ, BA, BB, BC	29
Gamex	Riskware:Android/Gamex.[variant] Trojan:Android/Gamex.[variant]	C, D, E, F, G,	5
Gamexx	Trojan:Android/Gamexx.[variant]	P	1
GinMaster	Trojan:Android/GinMaster.[variant]	K, L, M, N, P, Q, R, S	8
GoldDream	Trojan:Android/GoldDream.[variant]	E	1
GoneSixty	Spyware:Android/GoneSixty.[variant]	B	1
Impler	Trojan:SymbOS/Impler.[variant]	B	1
InfoStealer	Trojan:Android/InfoStealer.[variant]	B	1
MobileMonitor	Monitoring-Tool:Android/MobileMonitor.[variant]	B	1
MobileSpy	Monitoring-Tool:Android/MobileSpy.[variant]	F, G	2
Nickispy	Trojan:Android/Nickispy.[variant]	D	1
OpFake	Trojan:Android/OpFake.[variant]	P	1
PlugGamer	Trojan:SymbOS/PlugGamer.[variant]	B	1
PremiumSMS	Riskware:Android/PremiumSMS.[variant]	AA, AB, AC, AD, AE, AF, AG, AH, AI, AJ, AK, AL, AM, AN, AO	15
SeaWeed	Riskware:Android/SeaWeed.[variant]	B	1
Shilespy	Trojan:SymbOS/Shilespy.[variant]	B, C	2
SmsBomber	Application:Android/SmsBomber.[variant]	C	1
SmsReg	Riskware:Android/SmsReg.[variant]	C, D, E	3
SmsSend	Trojan:Android/SmsSend.[variant]	H, I, J, M, O	5
SmsSpy	Trojan:Android/SmsSpy.[variant]	J	1
SpyHasb	Monitoring-Tool:Android/SpyHasb.[variant]	B	1
Spyoo	Monitoring-Tool:Android/Spyoo.[variant]	B	1
Temai	Trojan:Android/Temai.[variant]	B	1
Tunsu	Trojan:SymbOS/Tunsu.[variant]	B	1
Zhaomiao	Trojan:SymbOS/Zhaomiao.[variant]	I, J	2
			TOTAL = 95 variants

Protecting the Irreplaceable

F-Secure