MOBILE THREAT REPORT

JULY-SEPTEMBER 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 are 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

MOBILE THREAT LANDSCAPE

In the mobile threat landscape, malware authors continue to concentrate on the Android platform. This should not come as a surprise considering that Android holds 79.3% of the total market share[1] in mobile phones and tablet devices. Out of the 259 new threat families and new variants of existing families discovered in Q3 2013, 252 were Android threats while the other 7 were Symbian (**Figure 1,** page 5). No malware has been yet to be recorded in 2013 on the other platforms (Blackberry, iOS, Windows Phone).

The majority of these threats fall under the 'malicious program' or Malware category, with trojans making up the largest percentage of the samples (**Figure 2,** page 6). The rest are deemed as 'potentially unwanted applications' or PUA, where the program may be considered undesirable or intrusive if used in a questionable manner, or may inadvertently introduce privacy or security risks.

"The majority of these threats fall under the 'malicious program' or Malware category, with trojans making up the largest percentage..."

Based on the statistics recorded by our internal systems and telemetry data, another trend we've seen this quarter is the increasing growth of profit-motivated threats (**Figure 3,** page 6), which typically make monetary profit by sending premium-rate SMS messages from infected devices, without the users consent. This rise could be attributed to the continued growth in large SMS-sending trojan families such as FakeInst, OpFake, PremiumSms and SmsSend, whose developers keep churning out new variants each quarter.

DEVELOPMENTS THIS QUARTER

Identifying Pincer's creator

In early April this year, we reported on Pincer[2], an Android malware that connects to a command-and-control or C&C server (**Figure 4,** page 6) and serves one component of a system used to defeat two-factor authentication for online banking transactions. In August, security researcher Brian Krebs reportedly tracked down and identified the author of this trojan as a programmer in a Russian app development company, who had apparently create Pincer for an unidentified client as a freelance side project[3].

Creating malware gets easier

In Q1 2013, we reported on the Perkele toolkit used to generate Android trojans for monitoring and forwarding SMS messages containing mTANs[4,5]. In July, there were reports of a new toolkit (aka 'binders') that simplifies the process of inserting malicious code into legitimate Android apps. The binder, named 'Androrat APK binder,' is used to insert an existing remote access tool (RAT) known as AndroRAT, into a 'carrier' app, trojanizing it[6].

Once the carrier app is installed onto a device, the implanted AndroRAT allows an attacker to remotely control it and among other things, monitor and make calls and messages, activate the camera and microphone, and access stored files.

"Masterkey" vulnerability

In July, security researchers publicly announced the discovery of a vulnerability in cryptographic signature verification for Android apps that, if exploited, would allow

an attacker to modify a legitimate app's code without affecting its cryptographic signature[7] — essentially keeping the tampering from being detected during verification. Shortly after the announcement, researchers were able to find samples of such modified apps being distributed[8,9]. A few days later, Chinese security researchers announced discovery of a similar vulnerability, though in this case the issue revolved around how the verification process handled a mismatch between signed and unsigned integers.

Google was reportedly notified of the 'Masterkey' issue earlier in the year, and at the time of the announcement had fixed the issue in the Android open source codebase[10]. Patches for the subsequent 'signed integer verification' vulnerability were also released shortly after the announcement. Users would however still need to wait for a firmware update from their device manufacturer in order to receive the patched code. In the meantime, basic security precautions are generally sufficient to avoid encountering.

"... attackers can simply bypass the store's built-in security by using advertisement modules as the attack vector to lure users onto external sites ..."

More details on page 9

ANDROID AND SYMBIAN NEWS

Android

When Google introduced security measures to the Google Play app store, it helped to keep malicious apps out of the store but it doesn't entirely eradicate the risks. For instance, the measures are ineffective in blocking malicious advertisements in apps - as in the case of **FakeDefender**, attackers can simply bypass the store's built-in security by using advertisement modules as the attack vector to lure users onto external sites where they can be scammed or infected.

More details on page 8

Besides, some threats are beyond the scope of Google Play's security measures, as is the case with the **Masterkey** exploit. Because of a security hole (referred to in the press as the 'Masterkey' vulnerability) in the Android operating system, malicious programs could still sneak into the store while hiding inside legitimate applications.

Symbian

While Android has been soaring high, Symbian is suffering the opposite fate. Its ecosystem is being driven down and the growing pressure from the recently announced Nokia Devices & Services acquisition by Microsoft is no doubt speeding up the process. On 4th October 2013, Nokia Developer News blog announced that developers will no longer be able to publish new content or update existing content on the Nokia Store, beginning on 1st January 2014[11].

The Symbian Signed program will also come to an end on the same date. Since all Symbian 3rd Edition and later versions require that applications be signed, no one can publish new versions of their installation files after January 2014. As of this moment, there is no explicit public statement on what is going to happen to express signing or other third party signing services. If they are also not available, it really means the end of life for Symbian.

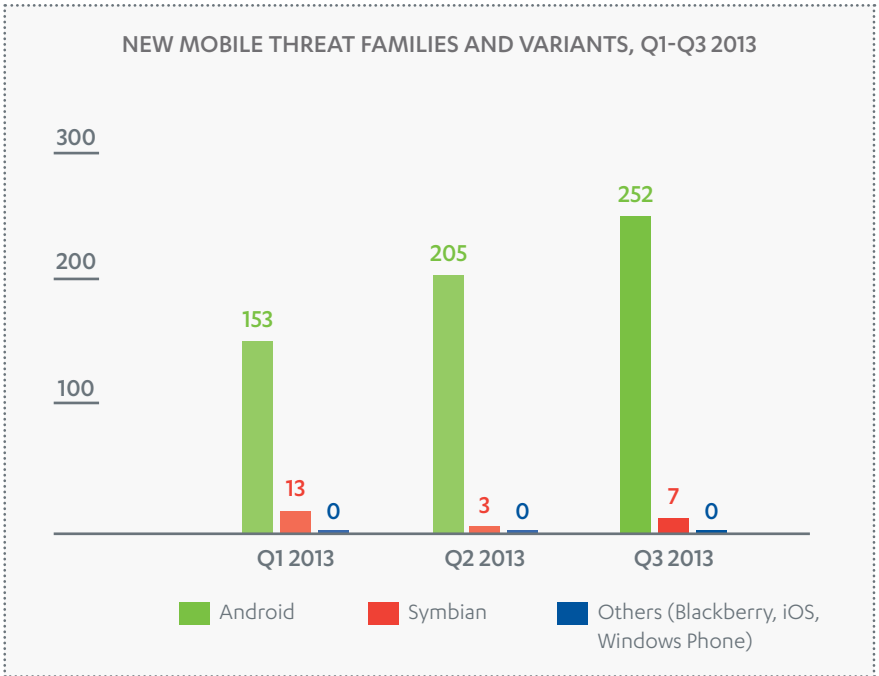


Figure 1: New families and new variants of existing families discovered on different platforms from Q1 to Q3 2013.

Sources: See page 15

Mobile Malware Statistics, Q3 2013

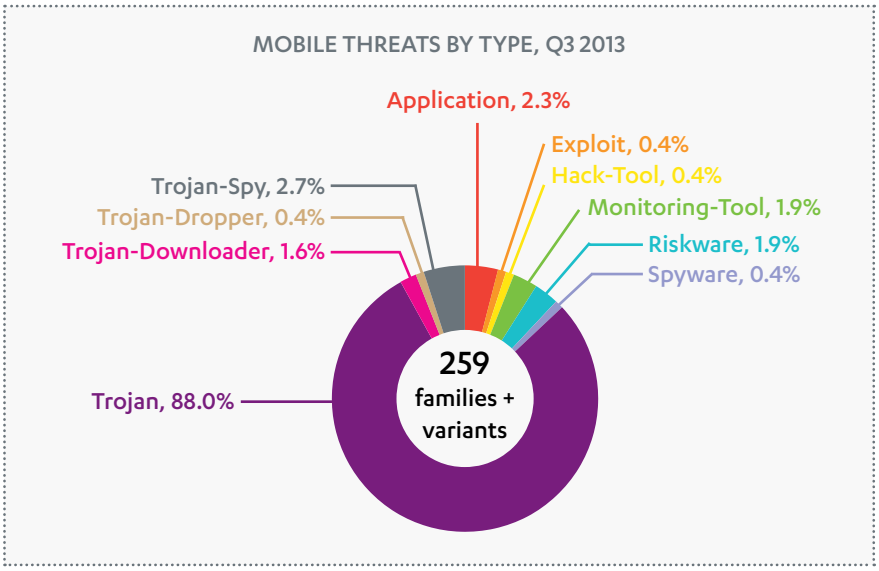


Figure 2: New mobile threats families and variants discovered in Q3 2013, broken down into types.

NOTE: No new adware families or variants were discovered in Q3 2013; new families or variants of other PUA types (e.g., Spyware, Riskware) were recorded during this same period.

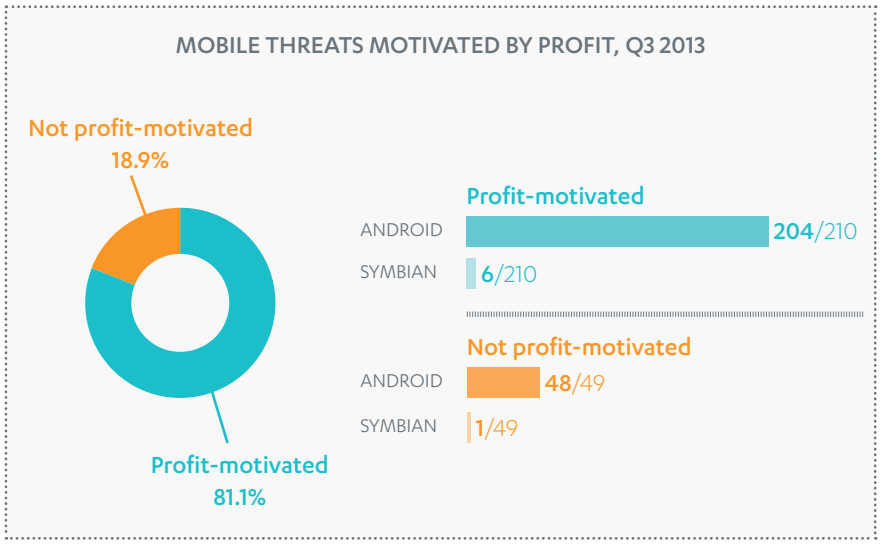


Figure 3: Comparison between new threats discovered in Q3 2013 that are profit-motivated versus non-profit-motivated ones.

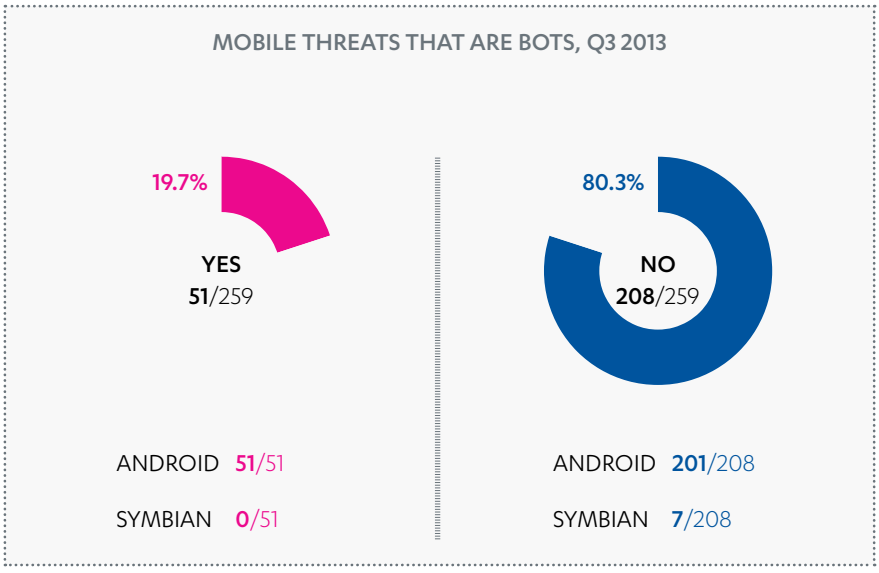


Figure 4: Comparison between new threats discovered in Q3 2013 that connected to C&C servers versus those that did not.

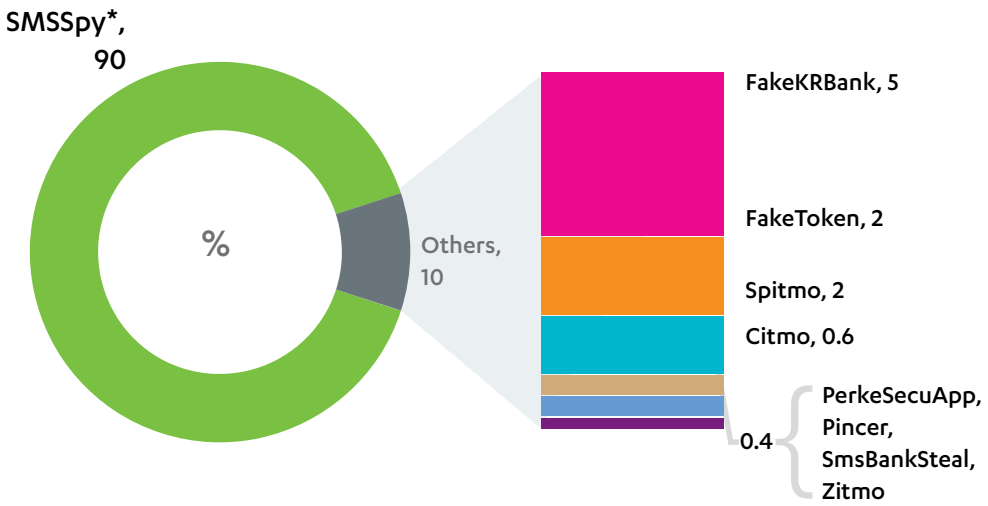
THREATS HIGHLIGHTS

The state of mobile malware is becoming more interesting as mobile phones and tablets become the preferred media consumption device for most users. The current trend for malware development has been to follow and target the most widely used operating system or platform.

One critical factor driving mobile malware development has been the growing use of mobile devices as a security check, usually as a form of secondary or two-factor authentication for user credentials or online transactions. The most common manifestation of this is the **mTAN (mobile Transaction Authentication Number)** authentication used by during online banking transactions by some banks as an added extra level of security. Malware authors are currently able to circumvent this extra level of protection by creating a mobile program or application that explicitly intercepts the SMS messages used to validate these transactions - thus the birth of **mobile Banking Trojans**.

The most common of these are still just a component of a more complex system, as they must function in tandem with a separate desktop-based banking malware that does the actual monetary theft. Interestingly, though mobile banking trojans still form a relatively small chunk of the overall count in our mobile malware sample collection, we do see a growing trend in the number of banking trojans.

MOBILE BANKING TROJANS BY PERCENTAGE, BASED ON PROTECTION NETWORK COUNT



More generally, another trend to highlight for this quarter is the further evolution of Android malware in terms of complexity and environment. An example is the evolution of a simple premium-SMS sending app that has developed its own 'ecosystem' on evolving into an SDK that supports an affiliated premium subscription number, somewhat like the way legitimate advertising modules are associated with affiliated ad networks - but nastier. As an SDK, it can be easily integrated into an app. The change means that two things can happen - it can be used solely for its 'traditional' premium-SMS subscribing routine, or the SDK can be unwittingly used by legitimate developers unaware of the impact of its behavior. Following the steps of previously reported malware Badnews, this quarter this was seen in **SxJolly.A**. Though not new, **Obad.A** also showed more development this quarter with regards to its ecosystem.

Classic Trojan-clicker behavior, more commonly seen in PC malware, reappeared in **Uten.A**, though the same principles were already seen in Adrd.A[1] in 2011. Delving further into specific malware, the public disclosure of the 'Masterkey' vulnerability this quarter showed the most potential for use in real malware, and sure enough was quickly followed by the discovery of in-the-wild malware exploiting this loophole. On the Symbian front, the only new threat of note was **Kleaq.A** - though even then, its malicious routines are not unusual for Symbian malware. And finally, in terms of spying-malware, the most notable development was **Tramp.A's** utilization of the Google Cloud Messaging (GCM).

***SMSSpy**
SMSSply differs from other malware families in that it doesn't contain variants 'descended' from a single identifiable code. Instead, SMSSpy groups mobile threats that share specific similarities in behavior related to SMS message monitoring. This may include threats that could also be identified as belonging to other families, such as Stels, Pincer or Zitmo.

Sources: See page 15

THREATS HIGHLIGHTS

COUNT OF KNOWN UNIQUE SAMPLES*
The count of unique samples for a particular variant of family found in our file collections. This number is used to provide a meaningful idea of how large a given malware family may be.

PROTECTION NETWORK COUNT**
The number of the times a client installation of F-Secure's Mobile Security reported blocking an attempt to install malware onto the protected device to our cloud-based telemetry systems during Q3 2013.

EXPLOIT:ANDROID/MASTERKEY.A

Count of known unique samples*: 101

Distribution
Seen in third-party app markets targeting Chinese users.

Summary
This malware takes advantage of the Masterkey vulnerability in Android, which allows attackers to make changes to an app's code without affecting the cryptographic signature used to check the legitimacy of an app.

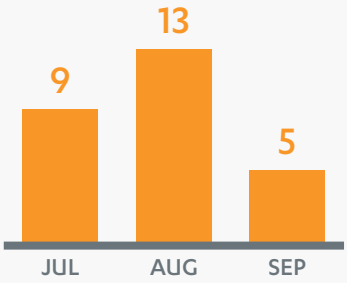
FEBRUARY
Bluebox Security responsibly discloses Masterkey vulnerability to Google

3 JULY
Bluebox Security publicly discloses Masterkey vulnerability [2]

10 JULY
Similar vulnerability related to verification of signed integers found by Chinese security researchers [3]

1 AUGUST
Masterkey vulnerability presented at BlackHat conference [4]

Protection Network Count**



JULY | **AUGUST** | **SEPTEMBER**

10 JULY
Proof-of-Concept (POC) Masterkey sample received

11 JULY
Proof-of-Concept (POC) for signed integer verification sample received

11 JULY
Non-POC, non-malicious Masterkey sample encountered. App code altered to display a message onscreen and include cheat cods in configuration files

26 JULY
Our Protection Network identifies a POC Masterkey exploit app circulating, disguised as a mobile banking app

7 AUGUST
30 apps found on third-party app market in China containing Masterkey exploit, including one banking app. On installation, apps will contact remote server for commands

Sources: See page 15

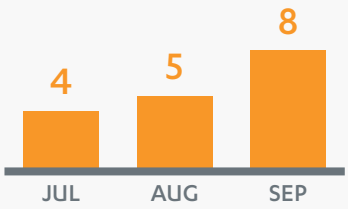
TROJAN:ANDROID/FAKEDEFENDER.A

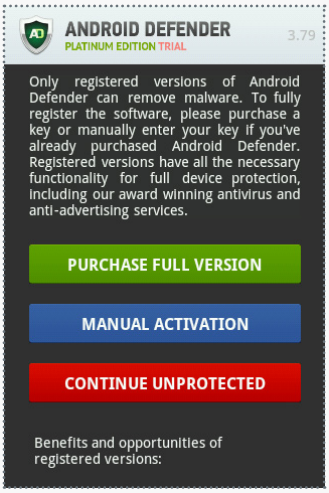
Count of known unique samples*: 34

Distribution
Seen advertised in third-party advertisements displayed on mobile devices.

Summary
Similar to rogue anti-spyware programs found on PCs, FakeDefender is a rogue anti-spyware program for the mobile device. The program does not provide the scanning or malware removal functionalities as claimed.

Protection Network Count**

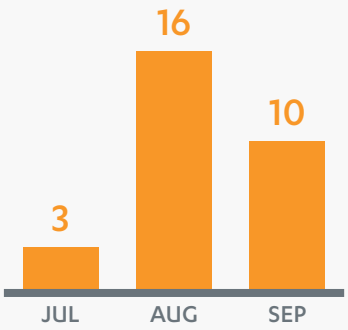




TROJAN:ANDROID/OBAD.A

Count of known unique samples*: 14

Protection Network Count**



Distribution
Obad variants were observed being advertised on a malicious website while browsing on an Android device, and is likely to arrive on a client's device via a mobile drive-by-download.

Summary
Once installed on the device, Obad variants gain administrator privileges and uses an exploit to break through the Android operating system's security layer. Obad collects and sends the following details about the device to a remote C&C server: the Media Access Control (MAC) address and IMEI, the operator name, the time and root access. The C&C server is also able to issue commands to the installed application, including to send SMS messages, make the device act as a proxy or a remote shell, launch a URL in the mobile browser, download and install additional components, get the Contact list as well as further details of a specific installed app and send a file via Bluetooth.

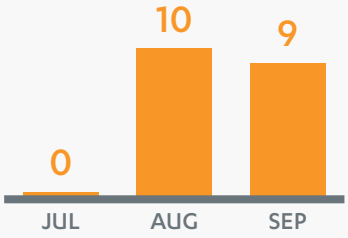
TROJAN:ANDROID/SXJOLLY.A

Count of known unique samples*: 19

Distribution
Seen in third-party app markets targeting Russian users.

Summary
A Bot capable of receiving commands to send SMS messages or subscribe the device to a premium-SMS service, and change or update its C&C server.

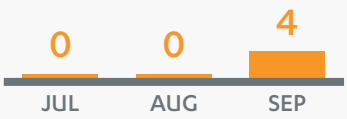
Protection Network Count**



TROJAN:ANDROID/TRAMP.A

Count of known unique samples: 31

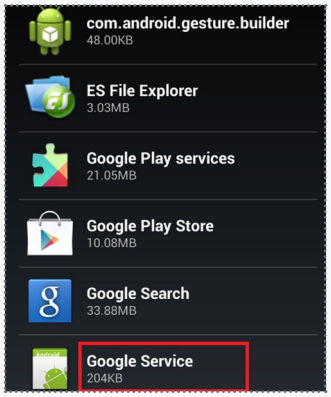
Protection Network Count**



Distribution
Unknown

Summary
Generally this malware monitors the user's SMS messages and steals the following details from user's phone: phone numbers, carrier and SMS. An interesting aspect of this malware is that it can receive the following commands through Google Cloud Messaging (GCM):

- Send message
- Block call
- Get current location
- Observe
- Contact



The Tramp sample we analyzed was also equipped with the androidvncserver native binary. Though this particular sample did not utilize the binary, it does raise the possibility that they could later add commands to execute files, especially as the VNC server would give an attacker full control over the phone. This VNC server application is publicly shared at http://code.google.com/p/android-vnc-server/.

The other interesting thing is that the malware doesn't create any shortcut to the application, so the presence of the app on the device is very difficult to spot. It most likely waits for device reboot or an SMS before it activates and runs its routines.

TROJAN:ANDROID/UTEN.A

Protection Network Count**

Count of known unique samples: 192

Distribution
This malware is a repackaged and trojanized app based on a game available in Google Play and believed to be spread in various third party app markets.

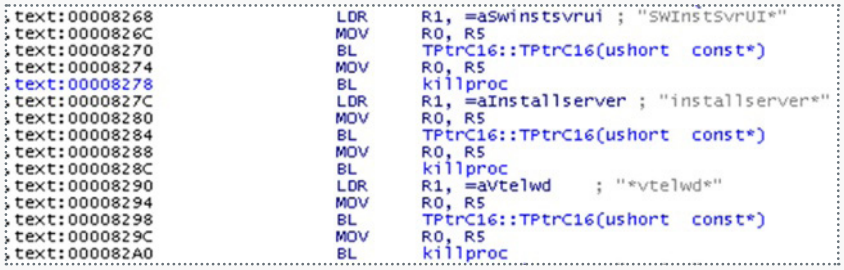
Summary
The malware disguises itself as "Umeng" SDK library, a mobile analytic platform used by developers. The original application that was trojanized to create this appears to be a legitimate gaming app available on the official Google Play Market.

Upon installation of this malware, affected devices are silently subscribed to a premium-SMS service, then SMS messages are sent to the service. Uten is also capable of intercepting SMS originating from certain numbers to avert user suspicion. It also performs click-fraud by emulating the user clicking on certain advertisements in the background – all at the expense of the user's precious bandwidth.

TROJAN:SYMBOS/KLEAQ.A

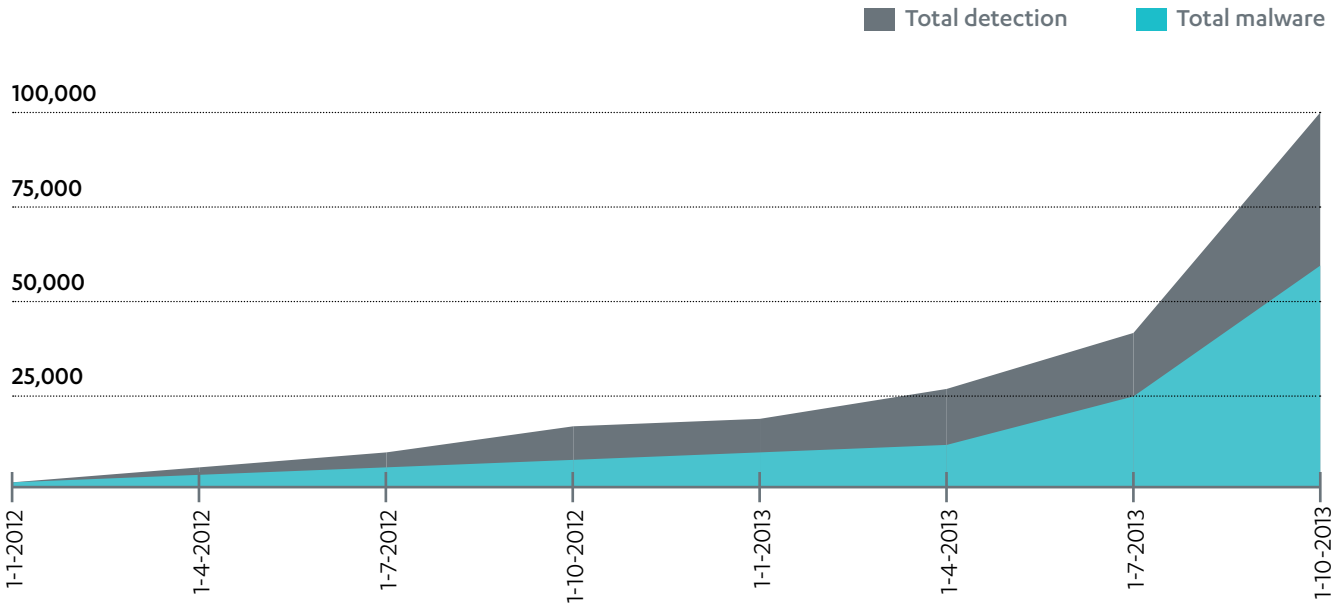
Distribution
Unknown

Summary
This malware's installation package contains two executables, one of which is responsible for downloading and installing the real payload silently, while the other executable kills any uninstallation attempts by terminating relevant processes. Typically, the kill list also includes some anti-virus vendors' processes and network connection status indicators.

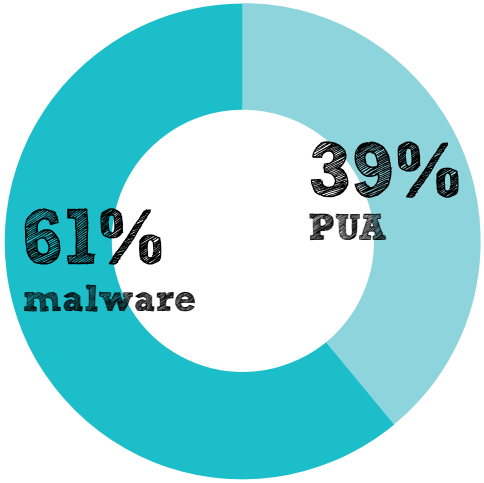


Android Malware Statistics

TOTAL MALWARE COUNT AGAINST TOTAL DETECTION COUNT FOR ANDROID THREATS, 2012-2013



ANDROID THREATS BY CATEGORY, Q3 2013



TOP-15 ANDROID MALWARE RECEIVED AND IDENTIFIED IN Q3 2013

DETECTION	COUNT
Trojan:Android/FakeInst	90,252
Trojan:Android/GinMaster	15,853
Trojan:Android/OpFake	11,319
Suspicious:Android/Malware	7,245
Trojan:Android/SmsSend	7,062
Trojan:Android/Vdloader	4,111
Trojan:Android/Boxer	2,590
Trojan-Downloader:Android/Boqx	2,210
Trojan:Android/SmsSpy	2,099
Suspicious:Android/GinMaster	1,857
Trojan:Android/Downloader	1,734
Trojan:Android/Mseg	1,709
Trojan:Android/Vidro	789
Trojan:Android/Temai	657
Trojan:Android/FakeNotify	558

RECOMMENDATIONS: Protecting against mobile malware

Securing the device

Today most people have their email accounts (personal and/or work) and other critical services on their mobile devices. This convenience also means that if your device is lost or stolen, your losses could involve more than just the physical device.

And despite concern about online-based attacks, the easiest way for malware to get on a device is still for someone to manually install it while the device is in their possession. In other words, protect your device's physical security first.

1. Lock the device

Locking your device prevents anyone else from meddling with its settings and installing an app (such as a monitoring-tool or spyware) while it is out of your possession. For the lock to be effective, make sure the password/passcode/pattern is unique, and preferably memorable for you without being easy for someone else to guess.

2. Set up anti-theft protection

Anti-theft protection typically provides you the ability to remotely wipe the data on your phone, including on any memory cards installed, if you decide your phone is irretrievable.

Some anti-theft solutions also include features such as location mapping or sounding the alarm, to help when attempting to locate the device.

Blocking unwanted services

Lucrative profit-generating mechanisms for mobile malware are to silently send premium rate SMS messages, subscribe the user to continuous premium services, or to force the device to call premium-rate numbers. Blocking premium calls or messages is one way to minimize financial losses, even if malware does get installed. This also provides protection against non-malware billing fraud by "operators" who silently subscribe users to premium services and forward billing requests to the user's mobile operator, hoping to have the charges quietly added to the user's bill.

3. Set up call or message barring

Most operators allow users to set up a call or SMS barring service to block the device from sending unwanted calls or messages. Also known as 'premium-rate blocking', this is particularly useful for parents who want to prevent their children's devices from inadvertently incurring unnecessary charges. To set up this service, contact your phone operator for more details. Some services also provide a PIN number or other method that allows the user to selectively remove the barring, if they desire.

Sources: See page 15

When downloading apps

Once your device's physical security has been addressed, you can also take the following steps when downloading an app.

4. Download apps only from the Play Store

By default, Android devices block installation of apps from any source other than the Play Store. You can check to make sure your device only allows Play Store apps by looking in ***Setting > Applications > Unknown sources***. If the checkbox is checked, non-Play Store apps can be installed. Uncheck this.

5. Check the apps' permission requests

Whether you're downloading from the Play Store or other sources, make sure to read the app's list of requested permissions (the ones that typically raise eyebrows due to security or privacy concerns are listed below right).

If the permissions requested seem excessive or unrelated to the app's purpose—for example, a casual game asks to send SMS messages—you can check the developer's references for more details, as reputable developers usually explain why the permissions are needed. If the use appears justified to you, then you may elect to download the app.

- Services that cost you money
  - Make phone calls
  - Send SMS or MMS
- Your location
- Your personal information

Incidentally, apps such as PocketPermissions, LBE Privacy or PermissionDog can be useful guides for explaining the sometimes-obscure permissions. Some also include features to restrict permissions used by installed apps, though such functionality is often intended for advanced users.

6. Scan apps with a mobile antivirus

Once downloaded onto your device, use a reputable mobile antivirus to scan the app. You can think of this as a check on the app's 'silent' behavior—permissable actions that are implied in the app's permissions list (for example, sending the device's details to a remote server) but may cause users concern. If the verdict from the mobile antivirus is acceptable to you, then you can proceed to install the app.

While online

As websites have evolved to cater for visitors browsing from mobile devices, we've also seen malicious sites follow suit[1].

7. Use web browsing protection

To avoid stumbling onto a malicious site while surfing on a mobile device, use web browsing protection (available from most antivirus solutions) to block known harmful sites.

METHODOLOGY

THIS REPORT IS BASED ON MOBILE APPLICATION DATA GATHERED DURING THE PERIOD OF 1ST JULY TO 31ST SEPTEMBER 2013 FROM A VARIETY OF SOURCES INCLUDING, AMONG OTHERS, THE OFFICIAL ANDROID PLAY STORE AND APPLE APP STORE, THIRD-PARTY APP MARKETS AND ANONYMIZED DATA FROM F-SECURE MOBILE SECURITY CUSTOMERS. THE COLLECTED SAMPLES AND DATA ARE SCANNED BY MULTIPLE INTERNAL ANALYSIS SYSTEMS, AS WELL IN-DEPTH INVESTIGATION 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 into *Types* based on their behavior.

The following list provides a brief summary of the criteria used classify mobile threats:

MALWARE	A mobile application that performs actions which pose a significant security risk to the user's system and/or information. Such applications are by default blocked from installation.	
	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	An application or component that may be considered undesirable or intrusive by a user if used in a questionable manner, or may inadvertently introduce privacy or security risks. If the user is aware of and accepts the implied risk(s), they may elect to install and use the application.	
	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 mobile application with an advertisement display functionality that potentially exposes the user to privacy or security risks as well as exhibiting aggressive advertisement behaviors. Privacy concerns involve the collection or leakage of user's or device's personal information such as location, behavior, International Mobile Equipment Identity (IMEI) number, contacts, etc. Aggressive behavior includes changing device settings such as adding home screen shortcuts, browser bookmarks, or icons on the user's device for advertising purposes. Security concerns involve exposure and/or redirection to unsolicited, unverified or questionable applications, websites or contents.

SOURCES

MOBILE THREAT LANDSCAPE (PAGE 4-5)

1. International Data Corporation; *Apple Cedes Market Share in Smartphone Operating System Market as Android Surges and Windows Phone Gains, According to IDC*; published 7 August 2013; http://www.idc.com/getdoc.jsp?containerId=prUS24257413
2. F-Secure Weblog; Sean Sullivan; *Trojan:Android/Pincer.A*; published 5 April 2013; http://www.f-secure.com/weblog/archives/00002538.html
3. Krebs on Security; Brian Krebs; *Who Wrote the Pincer Android Trojan?*; published 27 August 2013; http://krebsonsecurity.com/2013/08/who-wrote-the-pincer-android-trojan/
4. F-Secure Weblog; Sean Sullivan; *Mobile Bot "Perkele Lite" [Android Only]*; published 7 March 2013; http://www.f-secure.com/weblog/archives/00002519.html
5. Krebs on Security; Brian Krebs; *A Closer Look: Perkele Android Malware Kit*; published 19 August 2013; http://krebsonsecurity.com/2013/08/a-closer-look-perkele-android-malware-kit/
6. Symantec; Andrea Lelli; *Remote Access Tool Takes Aim with Android APK Binder*; published 16 July 2013; http://www.symantec.com/connect/blogs/remote-access-tool-takes-aim-android-apk-binder
7. Symantec; *First Malicious Use of 'Master Key' Android Vulnerability Discovered*; published 23 July 2013; http://www.symantec.com/connect/blogs/first-malicious-use-master-key-android-vulnerability-discovered
8. Naked Security; Paul Ducklin; *Android "Master Key" vulnerability - more malware exploits code verification bypass*; published 9 August 2013; http://nakedsecurity.sophos.com/2013/08/09/android-master-key-vulnerability-more-malware-found-exploiting-code-verification-bypass/
9. InfoSecurity; *More Exploits for Android 'MasterKey' Vulnerability Turn Up in the Wild*; published 9 August 2013; http://www.infosecurity-magazine.com/view/33941/more-exploits-for-android-masterkey-vulnerability-turn-up-in-the-wild/
10. Threat Post; Dennis Fisher; *Jeff Forristal on the Android Master-Key Vulnerability*; published 5 August 2013; http://threatpost.com/jeff-forristal-on-the-android-master-key-vulnerability-2/101587
11. Nokia Developer News; Fred Patton; *Changes to supported content types in the Nokia Store*; published 4 October 2013; http://developer.nokia.com/Blogs/News/blog/2013/10/04/changes-to-supported-content-types-in-the-nokia-store/

THREATS HIGHLIGHTS (PAGE 7-11)

1. F-Secure Weblog, *Trojan:Android/Adrd.A,* published 16 February 2011; http://www.f-secure.com/weblog/archives/00002100.html
2. Bluebox Security, Jeff Forristal; *Uncovering Android master key that makes 99% of devices vulnerable,* published 3 July 2013; http://bluebox.com/corporate-blog/bluebox-uncovers-android-master-key/
3. Sina blog, *Android security squad discovered new vulnerabilities,* published 10 July 2013; http://blog.sina.com.cn/s/blog_be6dacae0101bksm.html
4. BlackHat, *Android: One root to own them all,* published 1 August 2013; https://www.blackhat.com/us-13/archives.html#Forristal

RECOMMENDATIONS: PROTECTING AGAINST MOBILE MALWARE (PAGE 13)

1. F-Secure Weblog, Sean Sullivan; *Post-PC Attack Site: Only Interested in Smartphones/Tablets,* published 19 June 2013; http://www.f-secure.com/weblog/archives/00002569.html

Protecting the Irreplaceable

F-Secure