MOBILE THREAT REPORT Q1 2014

This Mobile Threat Report is based on mobile application data gathered during the period of 1st January to 31st March 2014. The collected samples and data are scanned by multiple internal analysis systems, as well as undergoing in-depth investigation by F-Secure Labs' Threat Research Analysts.

Previous Mobile Threat Reports can be found at: F-Secure Labs/Threat Reports

FOUND IN THE WORLD

F-Secure Labs found or received hundreds of thousands of mobile app samples in Q1 2014, from sites like the Google Play Store, third-party app stores, developer forums, user submissions and other sources. To identify threats, we analyze each app received for malicious code. If we find any, the app is grouped into ***families*** based on similarities in the code and behavior. Unique samples in a family are known as ***variants***.

NEW FAMILIES & VARIANTS

In Q1 2014, we found *275* new threat families (or new variants of known families) that run on Android.

We also found *1* new threat family each on iPhone and Symbian.

275 Android

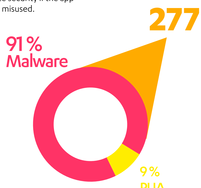
1 iPhone

1 Symbian

277

BY CATEGORY

We categorized 91% of these new families or threats as Malware as they posed a significant security risk to the user's device and/or information. The rest were classed as Potentially Unwanted Apps (PUA) as they could inadvertently introduce risks to the user's privacy or device security if the app were misused.



WHAT DOES IT DO?

Trojans are currently the most common type of mobile malware. Most of the Trojans we saw in Q1 2014 engaged in one (if not more) of the following activities:

SMS sending
Silently send SMS messages to premium-rate numbers or SMS-based subscription services.

File or app downloading
Download and install unsolicited files or apps onto the device.

Location tracking
Silently track the device's GPS location and/or audio or video to monitor the user.

Fake app scanning
Pretend to be a mobile antivirus solution but has no useful functionality.

Link clicking
Silently keep connecting to websites in order to inflate the site's visit counters.

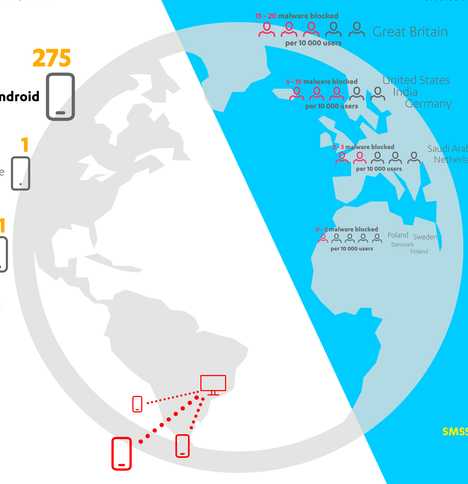
Banking fraud
Silently monitor and divert banking-related SMS messages.

Data stealing
Steal personal material such as files, contacts, photos, and other private details.

Fee charging
Charge a "fee" for use/update/installation of a legitimate (and usually free) app.

SEEN BY USERS

Compared to PC-based threats, the number of mobile malware is miniscule. Even so, in Q1 2014, users of F-Secure's Mobile Security for Android® solution sent a steady stream of reports of malware detected and blocked on their devices to our cloud-based telemetry systems.

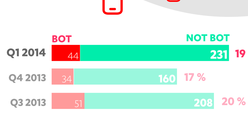


REPORTING HOTSPOTS

In Q1 2014, more users in Great Britain reported malware activity being discovered and blocked on their Android device than in any other country, by a wide margin. Users in the United States, India, Germany, Saudi Arabia and the Netherlands also reported a notable level of malware being detected and blocked. Other countries were excluded due to lack of statistically valid data.

TOP 10 ANDROID MALWARE

Though there are hundreds of malware families, most users only see a handful of common threats, as the Top 10 Android malware families reported in Q1 2014 combined make up 76% of all Android threats seen in this period. Of these Top 10, 45% of the reports were for threats in the Fakeinst family, followed by smssend variants and 8 other families.



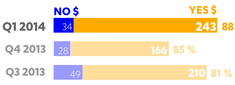
BOTNET-LINKED

19 % of these new families or variants secretly connected over the Internet to a remote Command & Control (C&C) server. Devices that connect to an unauthorized remote server this way are known as bots; a group of such devices is known as a botnet.

These apps can receive instructions dictated by an attacker operating the C&C server, instructing the app to perform actions such as installing programs, collecting information and sending SMS messages.

PROFIT-MOTIVATED

88 % of the new families or variants seen included some way for the attacker to make money off the user that unwittingly installs the app - for example, silently sending SMS messages to a premium-rate number or charging a 'fee' for a free program.



THREAT LANDSCAPE SUMMARY

Mobile malware development in Q1 2014 continues to focus exclusively on the Android platform, continuing the inexorable trend we've seen in the last couple years. Of all the mobile app samples we collected during this period, almost 14 % were malicious Android apps (with the rest being determined as PUAs or clean).

The vast majority of the malicious Android samples we analyzed were Trojans of one kind or another. Even though most of these don't technically fall in the families explicitly focused on **SMS-sending** (e.g., SMSSender), almost 83% of the Trojans performed surreptitious SMS-sending anyway, making it by far the most common objectionable activity. One interesting development related to this is the introduction of a notification prompt for SMS messages sent to premium-rate numbers in the 4.2 (Jelly Bean) update for the Android operating system. The user is given the option to allow or block this action - a change likely to put a major crimp in an SMS-sending Trojan's operation.

Trojans involved in silent downloads, data theft and banking fraud were the next most common, as combined they account for almost 10 % of all malicious samples. One new but notable type of Trojan activity we're starting to see more of recently is fee-charging, which involves repackaging an app (usually already available for free) and then redistributing it with an added 'fee' attached, as was the case with **Trojan:Android/FakeFlash.C**.

Apart from Trojans, **Backdoors** were the second most common malware type, accounting for 5 % of the malicious samples from this quarter. Other types of malware seen - **Exploits**, **Worms** and so on - made up under 5% combined. The low volume of non-Trojan samples is rather made up for by the technical interest of those few that did emerge. The sole new exploit reported was the Pileup vulnerabilities announced by university researchers [1] and involved malware gaining privilege escalations during a system upgrade, while the newly found Dendroid toolkit [6], which we categorize as a Backdoor, is being touted to malware authors looking to automate creation of Remote Access Trojans (RATs) that can evade Google Play Store security. If the toolkit does gain widespread use among malware purveyors, app market security may become more critical than before.

One measure we've previously used to roughly gauge app market security is to compare the number of malware we received from a given app store against the total number of samples from the same source. By that measure, the highest rate of malicious samples we saw came from four services that mainly cater to users in mainland China: Mumayi (7 %), Wandoujia (5 %), Anzhi and Baidu (both 3%). In contrast, only 0.1 % of the samples we received from Google's Play Store were identified as malicious.

HIGHLIGHTS THIS QUARTER

ON ANDROID

With 99% of the new threats that emerged in Q1 2014 designed to run on the Android operating system (OS), it's not surprising the most interesting mobile malware technical developments involved this platform. Here are a few noteworthy advances seen in Android malware in the last few months:

WINDOWS TROJAN HOPS ON ANDROID [1]

A banking-trojan named **Droidpak** that targets Windows PCs also tries to install a mobile banking-trojan on any Android devices connected via USB to the infected machine. Depending on the variant, we detect the mobile banking-trojan used as **Trojan-Spy:Android/Smforw.H** or **Trojan:Android/Gepew.A** or **.B**).

FIRST TOR TROJAN [2]

Trojan:Android/Torsm.A is the first trojan on this platform to leverage the open-source Orbot client for the popular Tor anonymizing network to communicate with its C&C server, making it difficult (if not impossible) for researchers and law enforcement to track and shut down the C&C.

FIRST CRYPTOMINER [3]

Trojan:Android/CoinMiner.A is distributed in a repackaged application. When installed, it essentially hijacks the device to silently mine virtual currency (such as Litecoin) for the malware author. Apart from any data charges incurred, the constant use of the device's hardware may also affect its battery life and eventual lifespan.

FIRST BOOTKIT [4]

Trojan:Android/Oldboot.A is believed to be Android's first bootkit, or malware that affects the earliest stages of the device's bootup routine, making it extremely difficult to detect or remove. The malware is thought to have spread in modified firmware updates, with most infections reportedly seen in China.

PILEUP EXPLOIT [5]

Researchers reported vulnerabilities in the Android OS (collectively called **Pileup** flaws) that could allow an installed malware to silently upgrade its permissions during a system update (essentially, "privilege escalation through updating").

ON IPHONE & SYMBIAN

Though most malware authors concentrated on creating new apps that run on Android, a few unusual souls apparently also tried their hand at making new malware to run on the iPhone and Symbian platforms. These two threats were the only new, non-Android malware we saw in Q1 2014.

TROJAN:IPHONEOS/ADTHIEF.A

A security researcher first reported finding a suspicious library used in a popular framework for app development. When installed and run on a jailbroken iPhone, the malware hijacked various advertising modules in installed apps to display its own advertisements. iPhones that have not been jailbroken aren't affected.

TROJAN:SYMBOS/SMSJEC.B

Though this trojan is unusual for appearing on the Symbian platform when most malware development is focused on other, more booming operating systems, the trojan itself is unremarkable. When active, the malware will silently send SMS messages.

BREACHING APP STORES

Malware authors constantly search for ways to bypass the security measures used by app stores to ensure only clean, legitimate apps are offered. Sometimes, they succeed in getting in (though usually only for a while).

The Google Play Store is currently the largest - and certainly the most scrutinized - official app site catering to the international market. As such, when malware make it into this market, it has the potential to reach a much larger audience. Of course, that makes this store a particularly lucrative target for malware pushers.

During the Q1 2014 period, these malware were available for a short period in the Play Store. All these threats have since been removed.

Trojan:Android/FakeFlash.C

Trojan-Spy:Android/Wabek.A

DENDROID TOOLKIT [6]

Backdoor:Android/Dendroid.A is a toolkit for creating Remote Access Trojans (RAT) that allow an attacker to create trojans that can remotely access an infected device's audio and video functions. It also creates trojans that can evade Google Play Store security.

SOURCES

1. Symantec; Flora Liu; *Windows Malware Attempts to Infect Android Devices*; published 23 Jan 2014; http://www.symantec.com/connect/blogs/windows-malware-attempts-infect-android-devices
2. Securelist; Roman Unuchek; *The first Tor Trojan for Android*; published 25 February 2014; https://www.securelist.com/en/blog/8184/The_first_Tor_Trojan_for_Android
3. Trend Micro blog; Veo Zhang; *Mobile Malware Mines Dogecoins and Litecoins for Bitcoin Payout*; published 25 March 2014; http://blog.trendmicro.com/trendlabs-security-intelligence/mobile-malware-mines-dogecoins-and-litecoins-for-bitcoin-payout/
4. ZDNet; Lian Yung; *Modded firmware may harbour world's first Android bootkit*; published 28 January 2014; http://www.zdnet.com/modded-firmware-may-harbour-worlds-first-android-bootkit-7000025665/
5. Malwarebytes Unpacked; Joshua Cannell; *Research Paper Shows Upgrading Android Could Upgrade Malware*; published 20 March 2014; http://blog.malwarebytes.org/mobile-2/2014/03/research-paper-shows-upgrading-android-could-upgrade-malware/
6. Ars Technica; Dan Goodin; *Malware designed to take over cameras and record audio enters Google Play*; published 8 Mar 2014; http://arstechnica.com/security/2014/03/malware-designed-to-take-over-cameras-and-record-audio-enters-google-play/

WHAT YOU CAN DO

Lock your device
Despite concern about online-based attacks, the easiest way for malware to get on a device is still for someone to secretly manually install it. Protect your device's physical security first. Locking it 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.

Use anti-theft protection
Anti-theft protection gives you the ability to remotely wipe the data on your device, including on removable media, if you think the device is irretrievable. Some anti-theft solutions also include features like location mapping or ringing the alarm, for when you're trying to locate the device.

Set up message barring
If your Android device isn't using OS version 4.2 (Jellybean), consider requesting a call or SMS barring service (also known as 'premium-rate blocking') from your operator to prevent unwanted outgoing calls or messages. This is especially handy for parents who want to keep their children's devices from racking up unexpected charges.

Download only from trusted sources
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.

Scrutinize permission requests
Whether you're downloading from the Play Store or other sources, check the app's list of requested permissions. Does it ask for Internet connection, to save files to external storage, or to be allowed to send SMS messages? Check the developer's site to see why the permissions are needed and look at reviews for feedback from other users.

Scan downloaded apps
If you're downloading an app from another source, use a reputable mobile antivirus to scan it before installing. You can think of this as a check on its 'silent' behavior - it's unstated but allowed actions. If you're comfortable with the verdict from the mobile antivirus, then you can elect to install the app.

F-SECURE products that can help:

MOBILE SECURITY
Mobile protection for online banking and browsing, parental control, app scanning, and more. Now also includes **Application Privacy** to highlight apps which affect your privacy and the permissions they use.

KEY
Secure your log-in details with strong encryption. Keep access simple with a single master password. Make it accessible anywhere by saving it on your device and synching to your cloud account.

APP PERMISSIONS
See all the permissions requested by all apps installed on your device in one handy, helpful screen. Identify which apps cost you money , which access your private data or which impact the battery life.

FREEDOME
Keep your connection private with Virtual Private Network (VPN) encryption. Stay protected against tracking, malicious sites and malware while online.

F-Secure