SIMPLY SECURE

G DATA
MOBILE MALWARE REPORT

THREAT REPORT: Q1/2015

SIMPLY SECURE

CONTENTS

Whitepaper Mobile Malware Report EN V2 06-2015 • 2310290615

AT A GLANCE

- The global market share of Android smartphones and tablets used for Internet access exceeded 61 percent in the first quarter of 2015. Over 62 percent of users in Europe used a mobile device with an Android operating system to go online.[1]
- Definitive malware numbers for Android devices: G DATA security experts identified and analysed 440,267 new malware samples in the first quarter of 2015. This represents an increase of 6.4 percent compared to the fourth quarter of 2014 (413,871). The number of malware strains rose by 21 percent compared to the first quarter of 2014 (363,153).
- Financially motivated Android malware makes up around half of the malware analysed (50.3 percent). This type of malware includes banking Trojans, ransomware, SMS Trojans and the like.
- Many apps, especially free ones, rely on the display of advertising, but at what stage should such applications be considered adware? When apps hide themselves in the background, conceal functions from the user or feed legitimate apps with additional advertising networks, the analysts categorise them as PUPs (potentially unwanted program).

FORECASTS AND TRENDS

DEFINITIVE NUMBER OF NEW MALWARE SAMPLES INCREASES SIGNIFICANTLY

G DATA security experts expect a rapid increase in numbers of new malware samples in 2015. A figure of over 2 million new Android malware strains is realistic. Users are ever more frequently using Android devices for everyday Internet usage when banking or shopping online. Cyber criminals make strenuous efforts to get malware into circulation here.

THE INTERNET OF THINGS: MOBILE DEVICES AS A GATEWAY

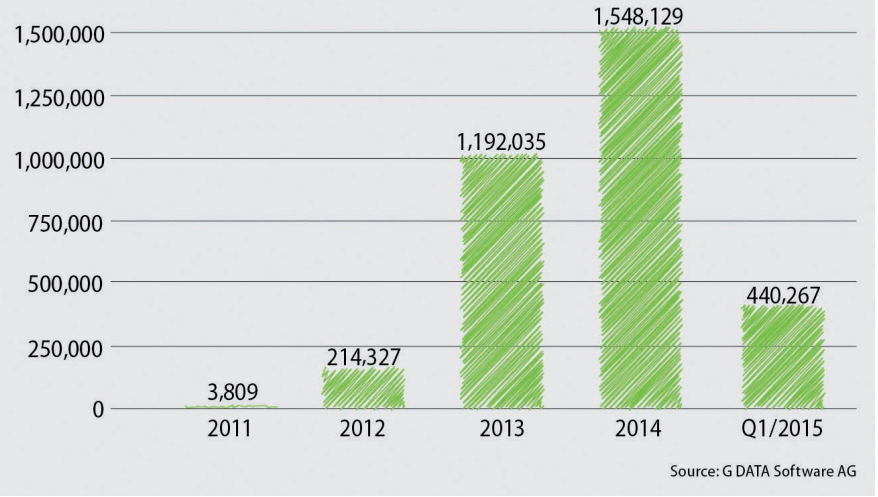
Intelligent devices are frequently prone to attack. Whether these are intelligent cars or routers, researchers are coming across more and more security deficiencies. In many cases, smartphones and tablets are being used to control the devices. G DATA security experts are expecting mobile devices to become the focus of attacks as the propagation of the Internet of Things continues. Examples of this are fitness apps and trackers. All of the data collected can be stolen if it is not properly encrypted.

[1] Statcounter: http://gs.statcounter.com/#mobile_os-ww-monthly-201501-201503

CURRENT SITUATION: 4,900 NEW ANDROID MALWARE SAMPLES EVERY DAY

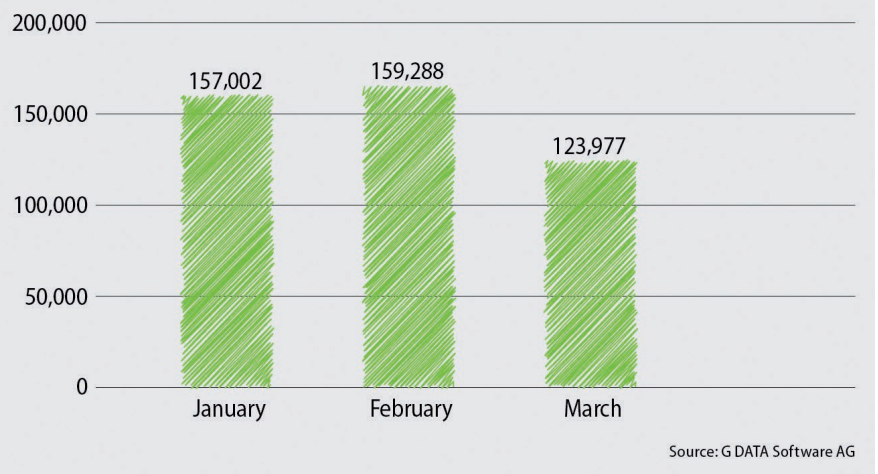
During the first quarter of 2015, G DATA security experts chronicled 440,267 new malware files. This represents an increase of 6.4 percent compared to the fourth quarter of 2014 (413,871). Consequently, the number of new malware programs has risen by 21 percent compared to the first quarter of 2014 (363,153). On average, the experts discovered almost 4,900 new Android malware files every day in the first quarter of 2015, an increase of almost 400 more new malware files per day compared to the second half of 2014. In the first quarter of 2015, the analysts identified a new malware sample every 18 seconds, per hour this makes about 200 new Android malware samples.

NEW ANDROID MALWARE SAMPLES



[2]

NEW ANDROID MALWARE SAMPLES IN 2015 / MONTHLY (Q1)

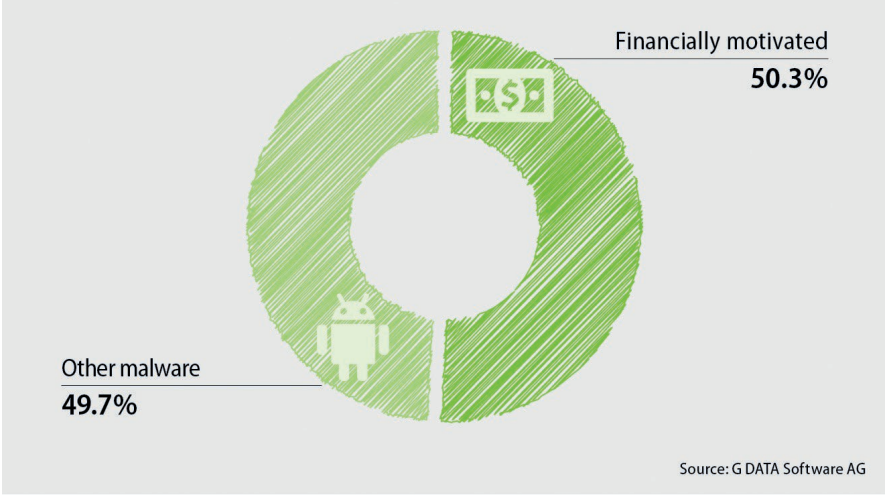


[2] The retroactive figures in this report are higher than those previously published in the reports. In some cases, receives G DATA file collections with a large number of new malicious files from a longer period of time and these sometimes contain older files which are then mapped to the corresponding month.

HALF OF ANDROID MALWARE IS FINANCIALLY MOTIVATED

41 percent of European consumers use a smartphone or tablet for their banking transactions.[3] Conducting financial transactions on a smartphone or tablet is an area of rapid growth – something that cyber criminals have also noticed. For this reason, G DATA security experts have taken a closer look at the new malware files and determined that at least 50 percent of Android malware currently being distributed has a financially motivated origin and includes banking Trojans, SMS Trojans and the like. Counting unknown cases, the number could be even higher, as the experts have only studied malware with a direct financial purpose. If a malware program subsequently installs apps or steals credit card data as an additional process after a payment has been made, the malware does not appear as financially motivated in these statistics.

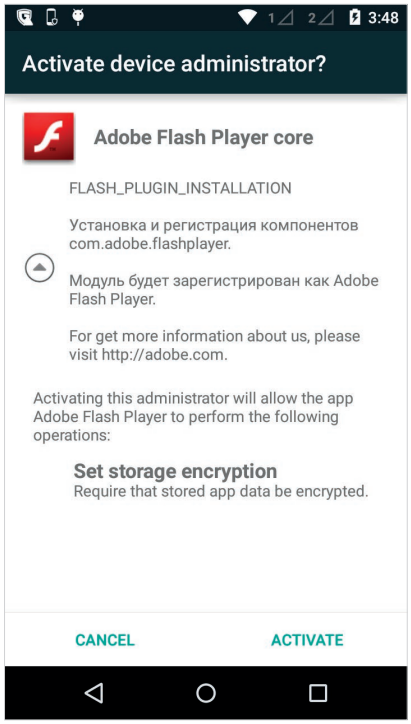
SHARE OF FINANCIALLY MOTIVATED ANDROID MALWARE



The analysed values in these statistics relate to named (non-generic) malware. No potentially unwanted programs (PUPs) have been included in these statistics.

[3] http://www.ezonomics.com/ing_international_survey/mobile_banking_2015

EXAMPLES FOR TROJANS

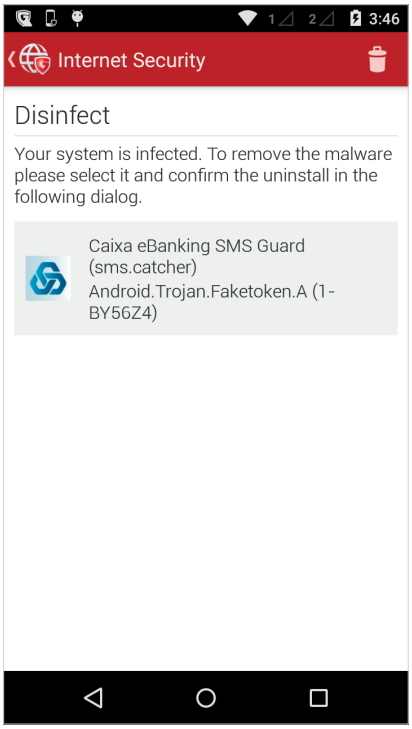


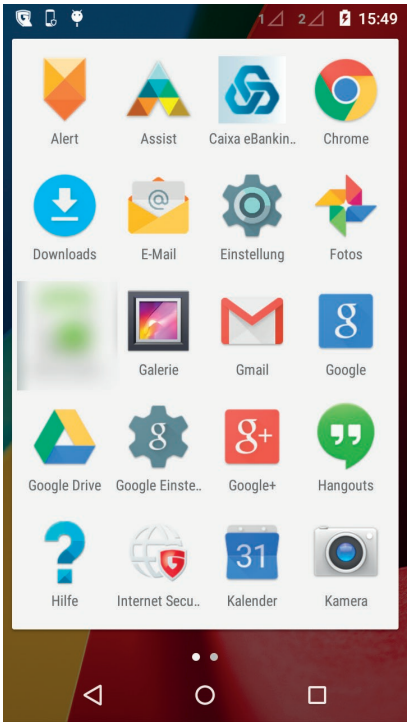
SVPENG TROJAN

The Svpeng Android Trojan is one example of financially motivated malware. Svpeng, which is known to G DATA as "Android.Trojan.Svpeng.A", combines the functionality of a finance malware program with the potential of ransomware. Depending on the variant, the malware steals access data when a banking app is used or encrypts the device to extort a ransom (ransomware).
In the example image, the fraud can be seen from the fact that the descriptions are in Russian. Memory encryption is also requested as a right, entitling the application to encrypt app data. Finally, there is no Flash Player for the Android operating system.

FAKETOKEN TROJAN

The FakeToken banking Trojan (Android.Backdoor.Token.A) is specifically designed to steal mTANs. In doing so, the Android malware disguises itself as one of the applications provided by the user's bank for generating TANs.
A message that asks for the app to be installed is displayed by an attack during an online banking session on the mobile device. If the malicious app is then installed, the cyber criminals use the Trojan to access the victim's account. Attackers can log into the user's account using the stolen access data, intercept mTANs and transfer money to their own accounts. The perpetrators can then use the data for their own purposes.





WHEN DOES ADVERTISING BECOME ADWARE?

The purpose of adware is to display advertising to the user and, through the advertisements, generate financial profit first and foremost, as well as data that, in many cases, can be resold. Adware is displayed not only once, but every time a program is launched or the device is restarted. Adware frequently hides in manipulated or fake apps that are installed from sources other than the Play store.

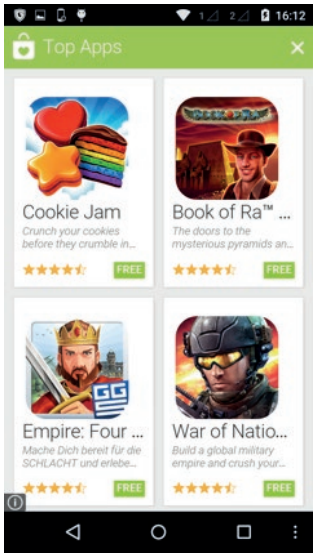
But at what point are apps categorised as adware? G DATA security experts draw a clear line on this question: When apps hide themselves in the background, conceal functions from the user or feed legitimate apps with additional advertising networks, the analysts categorise them as PUPs (potentially unwanted programs) and report this to the user.

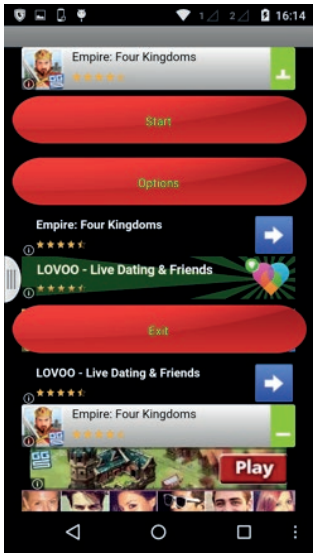
HOW DOES A PUP GET ONTO THE MOBILE DEVICE?

Google declared war on such apps some time ago. Applications must follow specific guidelines – for example, advertising within the app must be declared. Advertising forms that mimic system messages and might deceive or confuse users are forbidden. For example, no advertising can be displayed that emulates the Google Play store. Also forbidden is the placing of shortcuts or icons outside the application. No icons may be used that mimic an existing app in circulation either.

But how can such applications get onto the mobile device? The answer generally lies in alternative app stores or intrusive advertising networks. Copies of paid-for original apps are often available here at a cheaper price or even for free, but they come packed with potentially unwanted add-ons. The guidelines and verification processes are not clearly regulated in many cases, or are simply non-existent. This means that publishers can place and offer adware in these applications.

EXAMPLE ADWARE





The purpose of adware is to display advertising to users and acquire financial profit and data via these adverts. In this example, free copies of well-known apps are purchased via an advertisement that claims to be Google Play. Behind such ads are frequently manipulated apps that contain functions such as spyware or even more adware in addition to their actual functions. This can lead to a real torrent of advertising being dumped onto the user.