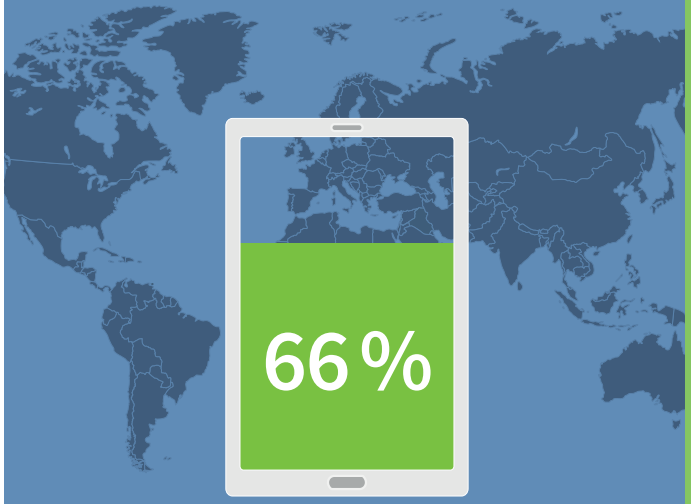
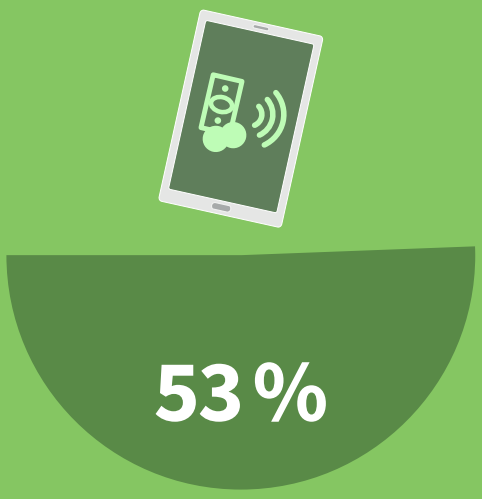
Threat report: Q4/2015

G DATA SIMPLY SECURE

# G DATA Mobile Malware Report




Worldwide, 66 percent use an Android device




53 Percent of European mobile device owners use their smartphone or tablet for online banking (Source: ING DiBa)

**758,133**

new malware samples in the fourth quarter of 2015/2,3 million in 2015 as a whole

SIMPLY SECURE

# Contents



Whitepaper MMWR EN Q4 02-2016 #54889 • 0511190216

# At a glance

- Worldwide, 66 percent of users were using an Android device in the fourth quarter of 2015 (Q3: 67 percent). The market share for Android operating systems has remained constant compared to the third quarter of 2015.[1]
- G DATA security experts identified 758,133 new Android malware files in the fourth quarter of 2015. That is an increase of almost 32 percent compared to the third quarter (574,706). In the second half of 2015, 1,332,839 new malware apps were discovered in total. For 2015 as a whole, a new record of 2,333,777 malware files for the Android operating system alone has been set. This marks an increase of over 50 percent compared to 2014 (1,548,129).
- Android should always be fully up to date. Security holes for Android are being found and exploited by criminals more and more quickly. The revelations concerning the Italian vendor Hacking Team have also underlined the vulnerability of Android.[2] Updating to the current version of Android is therefore fundamental for all users. When buying a new device, G DATA security experts recommend ensuring that the latest version of Android is installed or that an update is available. Supposed bargains in particular turn out to be devices with old versions of Android – and for which there are no longer any updates either.
- Mobile banking Trojans are more complex. More and more people are carrying out their banking transactions on a mobile device. Cyber criminals are upgrading and distributing ever more sophisticated malware in order to specifically target banking customers.

# Outlook

## Evolution of Android malware

G DATA security experts analysed almost 2.5 million new Android malware apps in 2015. The rapid increase underlines the significance of the profit from mobile operating systems – especially Android. Cyber criminals see the future here – and the potential for high financial gains. The switch from PCs to mobile devices will continue in 2016. For this reason, experts expect another significant increase in malware figures.

## The Internet of Things in cyber criminals' sights

Hacked vehicles, fitness wristbands and networks – the Internet of Things is becoming more and more popular, within our own four walls as well as at work. Criminals are stepping up their activities in this area and are specifically looking for security holes in order to exploit them. Numerous consumer devices in the IoT sector are controlled via Android apps. The experts expect the threat to increase in 2016.

[1] http://gs.statcounter.com/

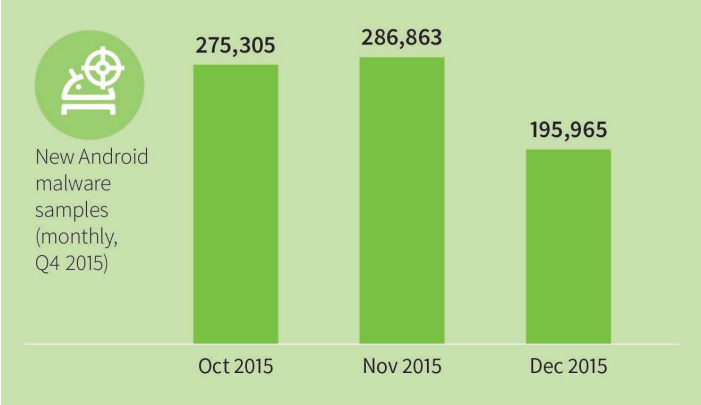
[2] http://www.heise.de/security/meldung/Super-Spion-Android-Ueberwachungssoftware-von-Hacking-Team-nutzt-allerhand-schmutzige-Tricks-2759365.html

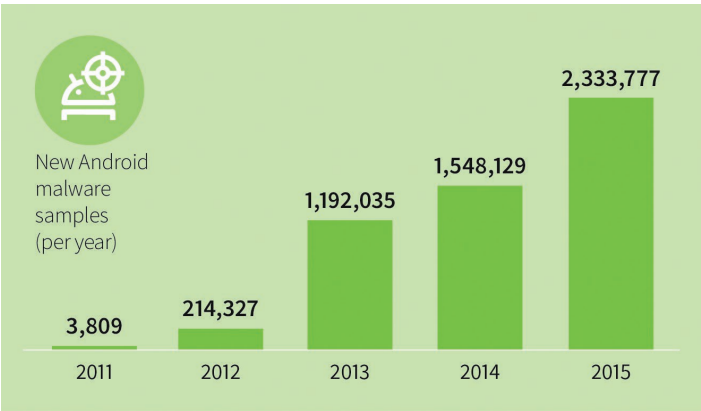
Whitepaper MMWR EN Q4 02-2016 #54889 • 0511190216

# Current situation: Experts identify a new Android malware strain every 11 seconds

The number of new Android malware strains increased significantly in the fourth quarter of 2015. During this period, G DATA analysts counted 758,133 new Android malware instances. This represents an increase of around 32 percent compared to the third quarter (574,706). In the fourth quarter, the experts identified over 8,240 new Android malware apps per day on average – over 1,800 more than in the previous quarter.

For 2015 as a whole, a new record of 2,333,777 new malware files for the Android operating system alone has been set. This is an increase of over 50 percent compared to 2014 (total number 1,548,129).




# What are Stagefright detection tools?

In recent mobile malware reports the G DATA security experts have explained several Categories of Potentially Unwanted Programs (PUP). Also in this report it's back to a range. The topic this time are Detection apps.

The Stagefright[3] security hole caused uproar in July 2015 and represented the worst case scenario for Android users. Up to a billion devices worldwide are thought to have been affected by this vulnerability.

When the malware is run (remote code execution), complete takeover of the device is thought to be possible by simply displaying a Multimedia Messaging Service (MMS). The vulnerability has compelled smartphone manufacturers to change their strategy for security updates for their devices in order to provide users with updates more swiftly.

While this problem with Stagefright exists, numerous apps have appeared that check the mobile device for the security hole. In many cases, these apps also exploit a security hole in Android so they can test the operating system for susceptibility to Stagefright.

[3] https://blog.gdatasoftware.com/blog/article/vulnerability-in-android-media-engine-stagefright.html

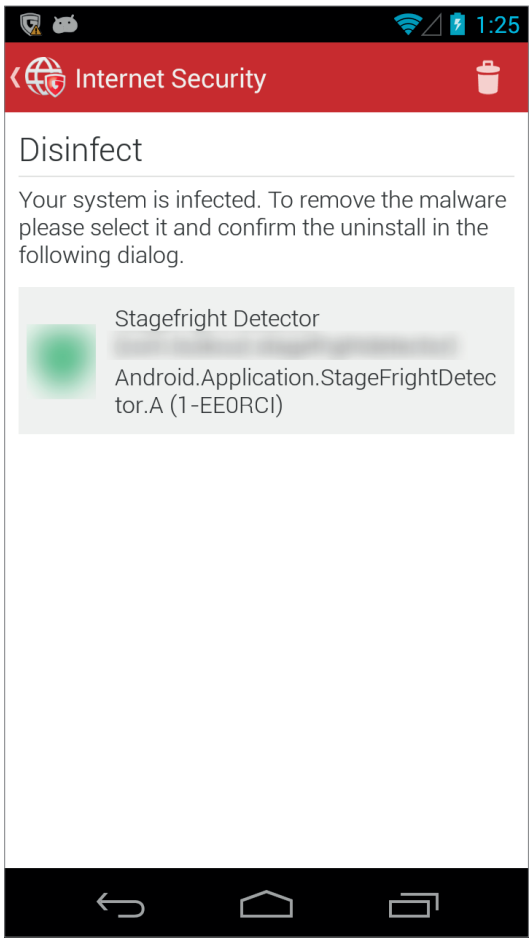
Whitepaper MMWR EN Q4 02-2016 #54889 • 0511190216

Android apps that are reported following detection of „Android.Application.StageFrightDetector.A“ are applications that check whether an Android device is vulnerable to an attack via the security hole.

**What is Stagefright?**

The Stagefright engine is used for recording and playing back audio and video files. There are multiple vulnerabilities in a library in the Android operating system used for displaying media content. Attackers can use these vulnerabilities to exploit audio and video files and run malicious code on the device concerned. This process can take place silently in the background, without the user realising that anything is going on.

The market for Android devices is unimaginably big. There are numerous different software versions. The only available option is for a detector app to actively test the respective device for the security hole. But to do so, an attack must be carried out. Hence the Stagefright detection apps contain the relevant security holes. The Stagefright hole includes not only the potential for attack, but even more. It is unclear whether these apps execute or download malware. Nevertheless, the apps exploit security holes in the mobile device. That is why G DATA security solutions detect the Stagefright Detector apps and declare them to be malicious applications.




**About G DATA**

G DATA Software AG is the antivirus pioneer. Founded in Bochum in 1985, the company developed the first antivirus program 30 years ago. Today, G DATA belongs to the leading providers of internet security solutions and virus protection, with over 400 employees worldwide.

G DATA SIMPLY SECURE

Whitepaper MMWR EN Q4 02-2016 #54889 • 0511190216