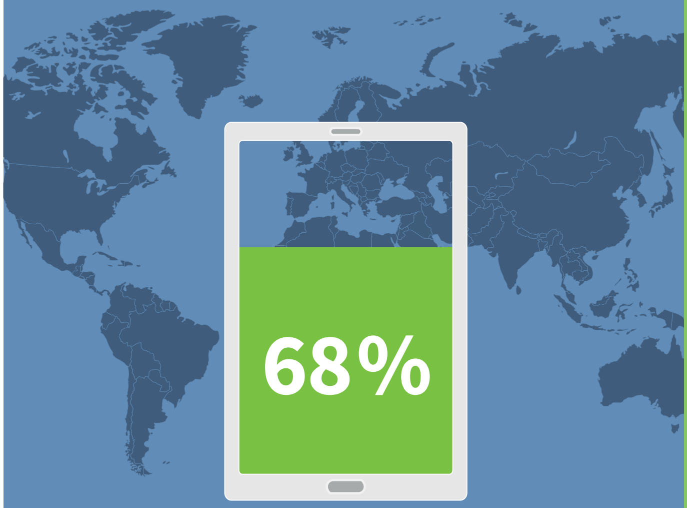
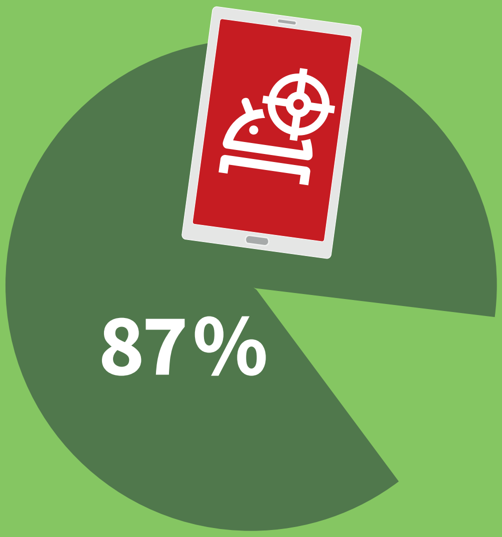
Threat report: H1/2016

SIMPLY SECURE

G DATA
Mobile Malware Report



Worldwide, 68 percent use an Android device



87 percent of all Android users had an outdated version of the operating system installed by June 2016

1,723,265

new Android malware samples in the first half of 2016

Inhalte

At a glance

- In the first half of 2016 the proportion of smartphones with Android operating systems in Europe increased to 66 percent (Q4/2015: 64 percent). Globally, the proportion of mobile devices with Android increased to almost 68 percent (Q4/2015: 66 percent).[1]
- **1,723,265 new Android malware samples** in the first half of 2016 constitute an increase of over 29 percent compared to the second half of 2015 (1,332,839). With over 1.7 million new malware samples, more than half of the result for the whole of 2015 (2,333,777) has already been reached. The expected switch from standard PCs to mobile devices is gaining speed.
- With Android 6.0, encryption of the device's memory is enabled by default. Google wanted to introduce this with version 5.0 already, but was unable to implement it.[2]
- Only 13 percent of Android users that have used the Play Store had Android 6.0 on their devices in June 2016. More than 30 percent were still using version 4.4 („KitKat").[3]
- Drive-by infections for Android have become a serious threat for users. Current G DATA analyses indicate that these infection and attack routes are currently being exploited by cyber criminals..

Outlook

New negative record – over 4 million new Android malware samples

Almost 2.5 million new Android malware samples in 2015 already represents a new record. Nevertheless, G DATA security experts have observed a rapid increase in new malware in the first half of 2016.

The forecast for 2016 correspondingly predicts 4 million new Android malware samples.

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

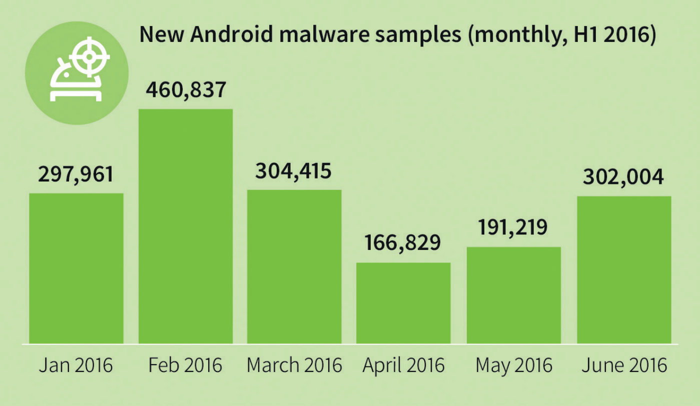
[2] https://security.googleblog.com/2016/04/android-security-2015-annual-report.html

[3] http://developer.android.com/about/dashboards/index.html; version july 2016

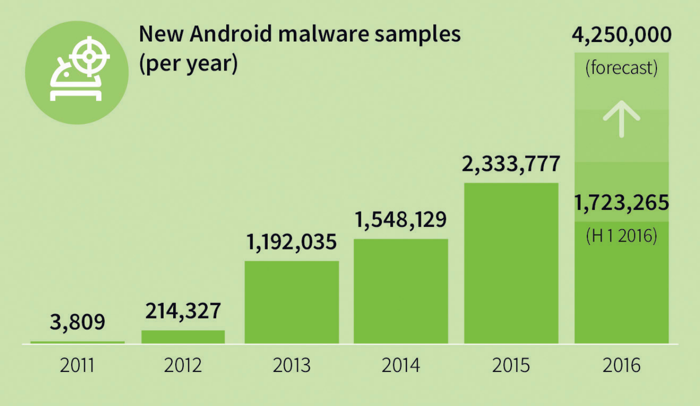
Current situation: 9,468 new Android malware instances every day

G DATA security experts identified 1.723.265 new Android malware samples in the first half of 2016.

This represents an increase of over 29 percent in new detections compared to the second half of 2015 (1.332.839). The experts detected an average of 9,468 new malware samples for the Android operating system per day. This means that the analysts identified a new malware sample **every 9 seconds.**



G DATA security experts have counted a total of more than 7 million malware files for the Android operating system since 2011.



The rapid increase in malware shows that digital life is taking place on mobile devices. Online banking and shopping are increasingly being performed on smartphones and tablets. Cyber criminals are aware of this, too. The attack scenarios are becoming increasingly complex.

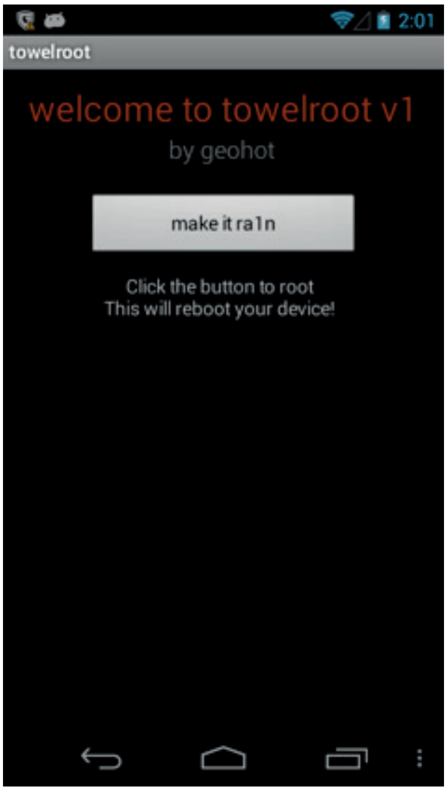
Visiting a manipulated website is all it takes for a successful infection with malware.

Why do rooting apps cause problems for Android?

Through rooting of an Android device, a user receives extensive permissions on the mobile device and gets full access to the entire file system as well as deeply-rooted system functions.

The advantages of rooting are that users can access various system settings and modifications such as uninstalling pre-installed apps.

However, for this reason it also represents a serious threat, as the Android security system is overridden. A security hole in the operating system is often exploited to root the device.



towelroot

welcome to towelroot v1

by geohot

Click the button to root
This will reboot your device!

As has happened previously with Stagefright detection tools, these applications do not necessarily have any malicious intentions. However, they can penetrate the operating system‘s security functions.

They can also be used to gain access to the mobile device. Consequently, the apps can work on the mobile device without restriction and for example steal private data, install other apps or smuggle in malware. The user of the device would not notice a thing.

On the other hand, there are positive-looking new possibilities, such as removing unwanted pre-installed apps or enhanced back-up options.

Towelroot is an app that enables root access to be gained to Android devices. To do this, the application exploits an error in the Linux kernel. However, the app can be manipulated and thus smuggle malware onto the mobile device or set up unwanted services. Users that still want to use an app like this should download it from a trustworthy source and be aware of the security issues.

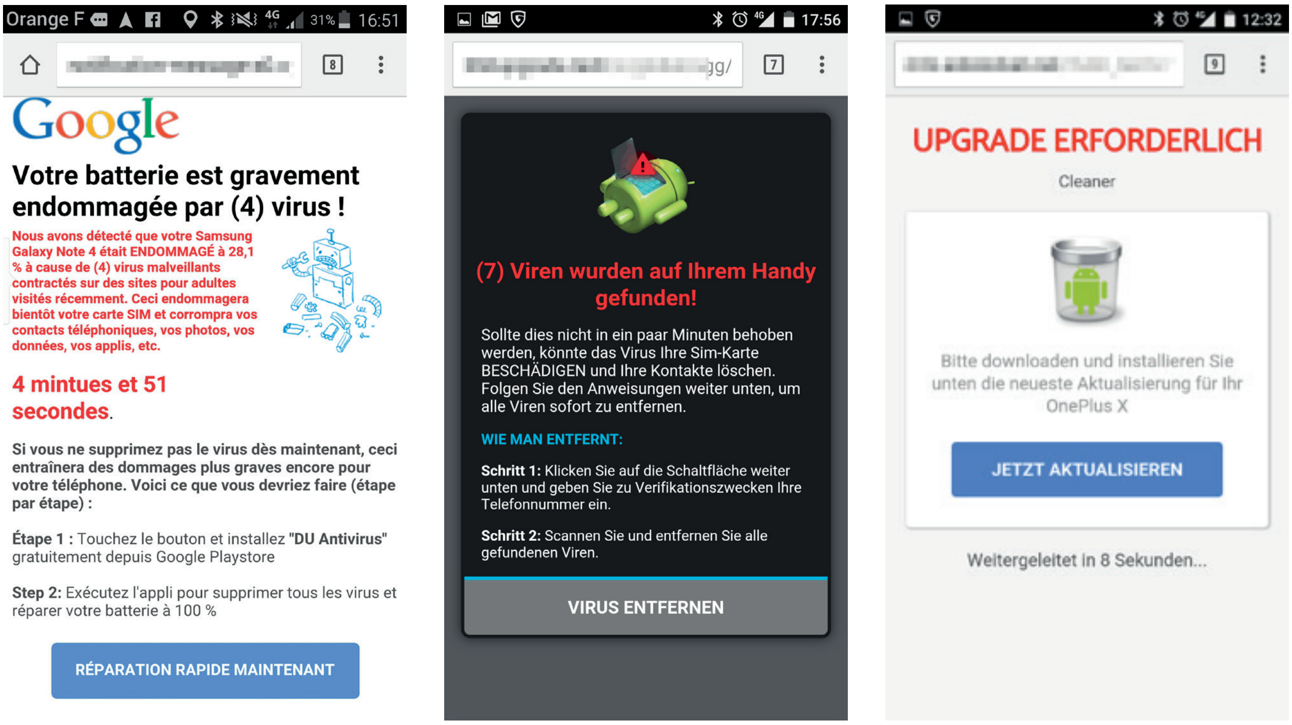
It is due to the fact that the entire Android security framework can be undermined that G DATA security experts categorise these apps as problematic and report them.

Malvertising:
Advertising that deceives virus detection

While surfing on a smartphone or tablet, users may suddenly face a fictitious warning, claiming that the mobile device might be infected with a supposed virus or needs updating. However, users do not need to surf dubious sites to come across those warnings.

Such messages should never be clicked on, but closed using the 'Back' button.

This is an attempt at fraud. There is **no** virus present on the mobile device, so **no** update is needed.



Votre batterie est gravement endommagée par (4) virus !

Nous avons détecté que votre Samsung Galaxy Note 4 était ENDOMMAGÉ à 28,1 % à cause de (4) virus malveillants contractés sur des sites pour adultes visités récemment. Ceci endommagera bientôt votre carte SIM et corrompra vos contacts téléphoniques, vos photos, vos données, vos applis, etc.

4 mintues et 51 secondes.

Si vous ne supprimez pas le virus dès maintenant, ceci entraînera des dommages plus graves encore pour votre téléphone. Voici ce que vous devriez faire (étape par étape) :

Étape 1 : Touchez le bouton et installez **"DU Antivirus"** gratuitement depuis Google Playstore

Step 2: Exécutez l'appli pour supprimer tous les virus et réparer votre batterie à 100 %

RÉPARATION RAPIDE MAINTENANT

(7) Viren wurden auf Ihrem Handy gefunden!

Sollte dies nicht in ein paar Minuten behoben werden, könnte das Virus Ihre Sim-Karte BESCHÄDIGEN und Ihre Kontakte löschen. Folgen Sie den Anweisungen weiter unten, um alle Viren sofort zu entfernen.

WIE MAN ENTFERNT:

Schritt 1: Klicken Sie auf die Schaltfläche weiter unten und geben Sie zu Verifikationszwecken Ihre Telefonnummer ein.

Schritt 2: Scannen Sie und entfernen Sie alle gefundenen Viren.

VIRUS ENTFERNEN

UPGRADE ERFORDERLICH

Cleaner

Bitte downloaden und installieren Sie unten die neueste Aktualisierung für Ihr OnePlus X

JETZT AKTUALISIEREN

Weitergeleitet in 8 Sekunden...

Those three screen shots are examples for fake virus warnings or supposedly mandatory updates. Users should never tap those buttons.

The need for an update is **never** announced via the browser.

In many cases, an .apk file is downloaded if the user clicks on the advert and, as a result, chargeable software for 'battery or storage optimisation', an expensive subscription or malware is installed

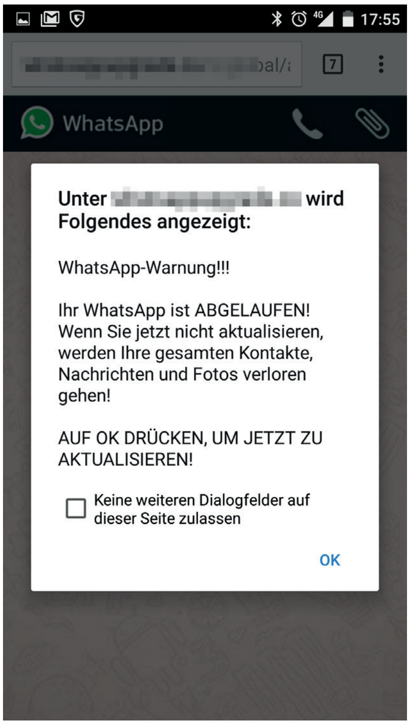
What is Pay Per Install?

Pay Per Install is a popular marketing instrument that enables providers of an app to distribute software and increase download figures. Users are frequently made aware of the app by advertising. The more installations an app achieves, the more visible it will be in the app store, attracting more users to install the app on their device. There are various service providers that have specialised in these marketing methods. This route is absolutely legitimate.

However, in IT security the term Pay Per Install also refers to the fraudulent form of this process as malvertising (a combination of the words Malware and Advertising, describing online advertising that runs malware).

Cyber criminals offer their services in underground forums. In many cases advertising is used and the fraudsters are paid by the number of installations. The advertising is misleading and is intended to confuse users.

Fake virus detections or allegedly available updates for Android are used to compel users to install costly or malicious apps or sign up for expensive subscriptions. In the worst case scenario, the mobile devices could be used for criminal activities after the installation.



Unter [redacted] wird Folgendes angezeigt:

WhatsApp-Warnung!!!

Ihr WhatsApp ist ABGELAUFEN! Wenn Sie jetzt nicht aktualisieren, werden Ihre gesamten Kontakte, Nachrichten und Fotos verloren gehen!

AUF OK DRÜCKEN, UM JETZT ZU AKTUALISIEREN!

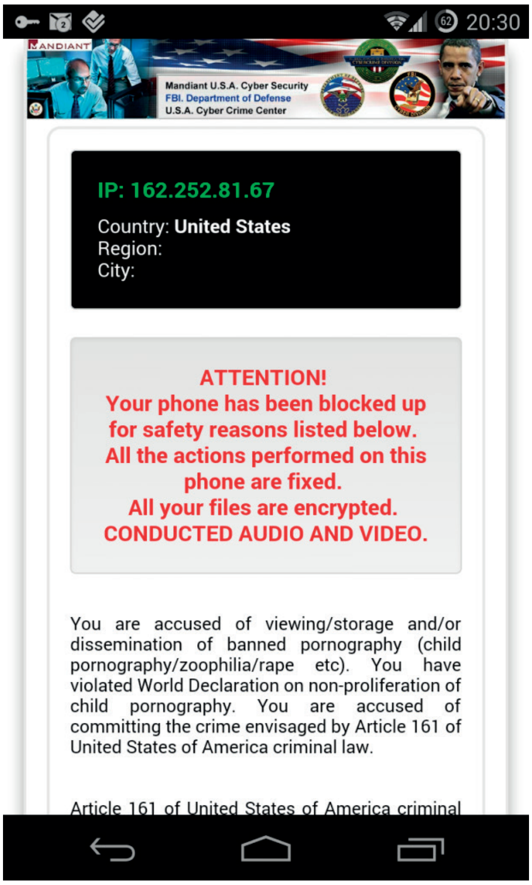
□ Keine weiteren Dialogfelder auf dieser Seite zulassen

Another trick is to display that “WhatsApp has expired”.
The user is threatened with negative consequences if he fails to react immediately.

Drive-by-infection: Attack vector also threatens Android devices

Back in 2015 G DATA security experts forecast that malware for the Android operating system would continue to be developed. The revelations concerning Italian IT company Hacking Team in particular have shown the possibilities of how mobile devices can become infected simply by visiting websites primed with malware. This means that no user interaction is required. Once the malware gets onto the device, the infection happens automatically.

Current analyses by G DATA experts show that drive-by infections are now being used by attackers to infect Android smartphones and tablets as well. Security holes in the Android operating system therefore pose an even more serious threat.



Mandiant U.S.A. Cyber Security
FBI. Department of Defense
U.S.A. Cyber Crime Center

IP: 162.252.81.67

Country: United States
Region:
City:

ATTENTION!
Your phone has been blocked up for safety reasons listed below.
All the actions performed on this phone are fixed.
All your files are encrypted.
CONDUCTED AUDIO AND VIDEO.

You are accused of viewing/storage and/or dissemination of banned pornography (child pornography/zoophilia/rape etc). You have violated World Declaration on non-proliferation of child pornography. You are accused of committing the crime envisaged by Article 161 of United States of America criminal law.

Article 161 of United States of America criminal

The long periods until an update for Android reaches users‘ devices in particular can aggravate the problem further.

How do drive-by infections function?
Online criminals hack web servers and up primed websites there. They then send out spam emails with links to these sites and optimise them for search engines. When users go to the websites or are taken there via advertising, malware can quickly get onto the system without being noticed. The infection takes place without the victim seeing anything – simply by visiting the site.

These attack routes are currently being used to infect users with extortion Trojans known as **ransomware**. As the name suggests, this is a form of malware that demands a ransom from the victim in order to release the data or device.

There are two types of ransomware – screen lockers and crypto-ransomware. Screen lockers lock the display so the user can no longer access the mobile device. Crypto-ransomware encrypts the data on the smartphone or tablet.

Ransomware: Extortion in the digital age

Tips for protection against ransomware:

- A **comprehensive security solution** that provides protection against viruses and other threats.
- **Regular backups** of important documents and data should be carried out.
- Installed apps and the operating system should be kept **up to date** at all times.
- Apps should only be downloaded from the providers' **official stores**, such as Google Play.
- Emails from unknown senders should generally be **deleted** without being read. File attachments and links should also **not be accessed**.
- A ransom should **never be paid**. It indicates willingness to the extortioners and motivates them to try it again.

About G DATA

G DATA Software AG is the antivirus pioneer. Founded in Bochum in 1985, the company developed the first antivirus program more than 30 years ago.

Today, G DATA belongs to the leading providers of internet security solutions and virus protection, with over 400 employees worldwide.

Contact: www.gdatasoftware.com / presse@gdata.de / Phone: +49 234 97 62 - 0

Whitepaper MMWR EN H1 2016 • 0713050816