SIMPLY SECURE

G DATA MOBILE MALWARE REPORT

THREAT REPORT: Q2/2015

Whitepaper Mobile Malware Report US 07-2015 - 1816010915

CONTENTS

Whitepaper Mobile Malware Report US 07-2015 • 1816010915

AT A GLANCE

- The global market share of Android smartphones and tablets was almost 64 percent in the second quarter of 2015. This represents an increase of three percent compared to the first quarter. In the USA around 48 percent of users use a mobile device with an Android operating system.[1]
- Rapid increase in absolute malware figures for Android devices: During the second quarter of 2015, G DATA security experts analysed 560,671 new malware samples. This is an increase of 27 percent compared to the first quarter of 2015.
- New record: In the half-yearly comparison, the one million mark for new Android malware samples within a six-month period was surpassed for the first time since the Mobile Malware Report has been published. In the first half of 2015, G DATA experts discovered 1,000,938 new malware files. Compared to the second half of 2014, that is an increase of 25 percent.
- Apps that conceal functions and monitor users are blocked in G DATA security solutions. But according to which criteria are they evaluated? The experts explain their method using the example of an app with hidden monitoring functions.
- Last year, the Star N9500 smartphone with built-in spyware functions caused an uproar. G DATA security experts have discovered evidence on well over 26 devices that indicates similar functions. The experts suspect middlemen are behind this, who have changed the firmware so that they can potentially steal user data and make money through advertising.

FORECASTS AND TRENDS

OVER TWO MILLION NEW ANDROID MALWARE SAMPLES IN 2015

The G DATA security experts expect well over two million new malware sample for the Android operating system for 2015 as a whole – a new record. This means that the number of new malware samples will have doubled within two years.

QUALITY OF ANDROID MALWARE RISES

The IT company Hacking Team programs high quality malware for intelligence services and governments. After a cyber attack on the company, corporate data and source code for an Android malware sample were published. G DATA security experts expect cyber criminals to exploit this easily accessible knowledge base and publish large numbers of more mature Android malware.

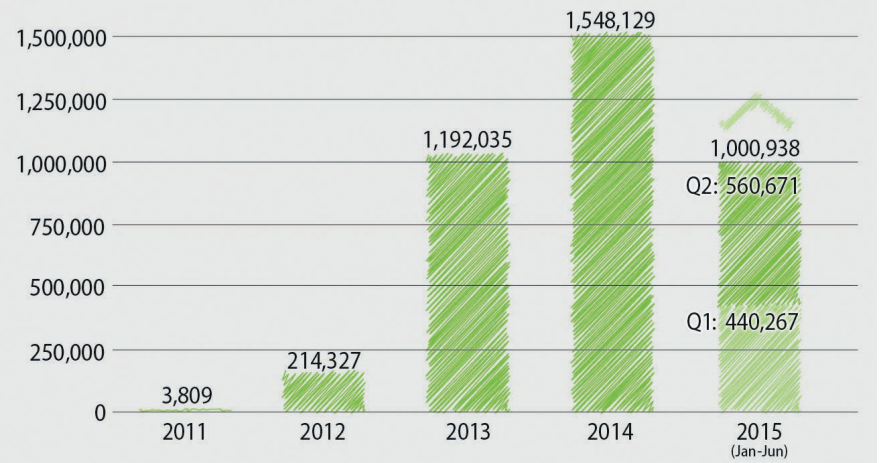
[1] Statcounter: http://gs.statcounter.com/

CURRENT SITUATION: 6,100 NEW ANDROID MALWARE INSTANCES EVERY DAY

The number of new Android malware instances has grown enormously again, as the forecast from the first quarter has confirmed. During the second quarter of 2015, G DATA security experts analysed 560,671 new malware samples. This represents an increase of over 27 percent compared to the first quarter of 2015 (Q1/2015). On average the experts discovered over 6,100 new Android malware instances per day in Q2/2015 – almost 1,200 per day more than in Q1/2015. The analysts identify a new malware sample every 14 seconds on average.

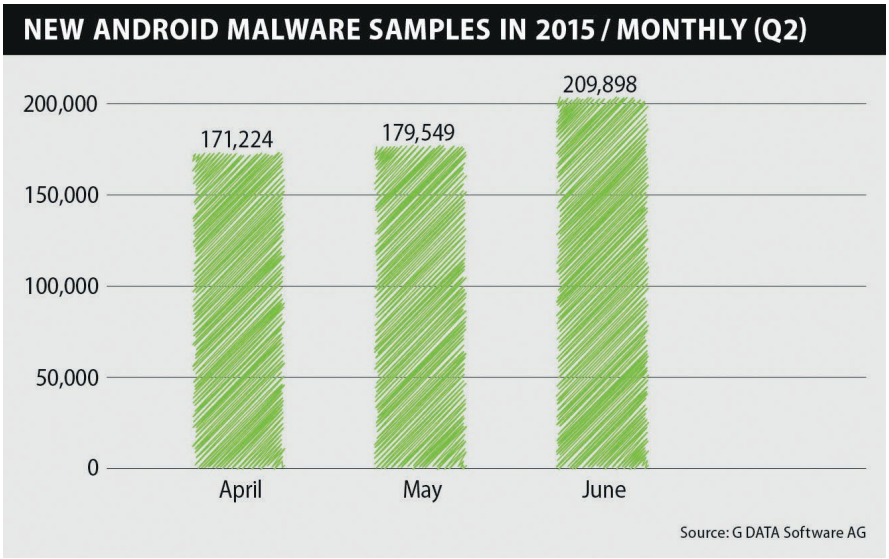
The enormous increase in new Android malware samples in the first six months of 2015 represents a new record. For the first time, G DATA security experts discovered over a million new Android malware instances in a six month period. The analysts are expecting significantly more than two million new Android malware samples for 2015 as a whole.

NEW ANDROID MALWARE SAMPLES



The retrospective figures in this report are higher than in previously published reports. In some cases, G DATA receives collections of files with a large number of new malware files collected over an extended period of time and these sometimes contain older files, which are then assigned to the respective month.

NEW ANDROID MALWARE SAMPLES IN 2015 / MONTHLY (Q2)



MONITORING APPS ON MOBILE DEVICES

In the Mobile Malware Report for the first quarter of 2015, G DATA security experts demonstrated the significance of the adware threat on Android mobile devices. Besides adware, a large number of other apps are categorized as PUP (Potentially Unwanted Programs). In this report we look at the area of monitoring. These programs are not malware in the traditional sense. Rather, another individual uses them to secretly monitor the smartphone owner and collect the data. For example, parents can monitor their children and see who the child is contacting or where they are right now. There a numerous usage options.

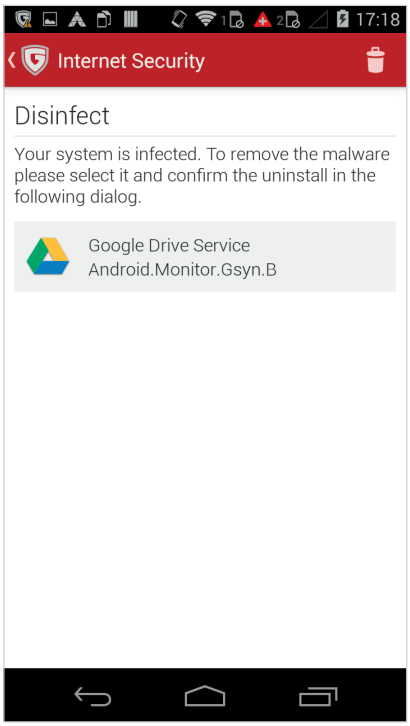
Monitoring malware hides itself. Permissions can only be reviewed during the installation or if the user finds the app. However, even legitimate apps often request permissions that go beyond the actual activity of the application. Hence it is not always obvious to users that there is an app with monitoring functions on their smartphone. For this reason, G DATA security experts categorise such programs as PUPs. G DATA security solutions detect the applications.

DISGUISED GOOGLE DRIVE APP WITH MONITORING FUNCTION

Android.Monitor.Gsyn.B is an app categorised as a monitor that pretends to be the Google Drive app. Users assume that they have the original Google Drive app as the icon and the app identifier are similar to the original program. However, in this case the app contains just monitoring functions.

According to providers, the disguised app can steal a wide range of data and execute functions without the user knowing:

- Listening in to telephone conversations
- Viewing and copy contacts
- Asking for location data
- Taking and copying images
- Recording conversations using the microphone
- Sending and reading SMS/MMS
- Disabling AV software and other apps
- Listening in to chats via messaging services (WhatsApp, Skype, Viber, Facebook, Google+, etc.)
- Reading the browser history



PRE-INSTALLED MALWARE ON SMARTPHONES

Since the discovery of pre-installed malware on a smartphone in spring 2014, G DATA security experts have found more and more models on which the presence of malware in the firmware can be proven. But where does the malware come from and who is installing it? The G DATA security experts are certain that the manufacturers are not the perpetrators in the majority of cases. Renowned companies will not risk their reputation by distributing malware in the firmware.

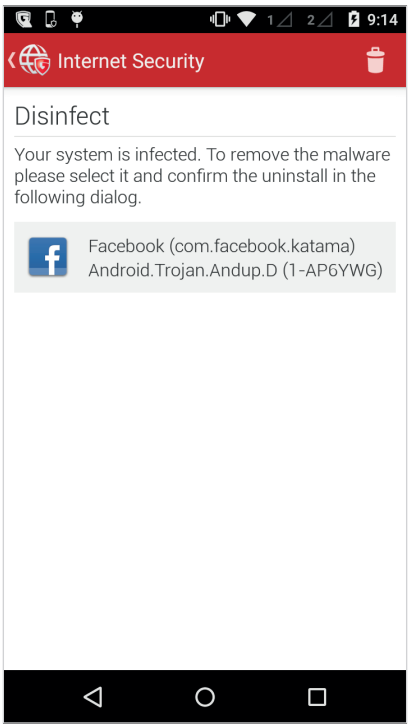
The G DATA experts therefore suspect middlemen of being the perpetrators. In addition to the revenue gained from selling on the mobile device, they try to make additional financial gains from stolen user data and enforced advertising.

HOW IS THE MALWARE HIDDEN?

In the analysed cases, the malware is usually hidden in a legitimate app which is manipulated to contain malware as an add-on. The malware hides alongside the usual functions in the app. Users do not notice these add-on functions as the majority of the processes run in the background.

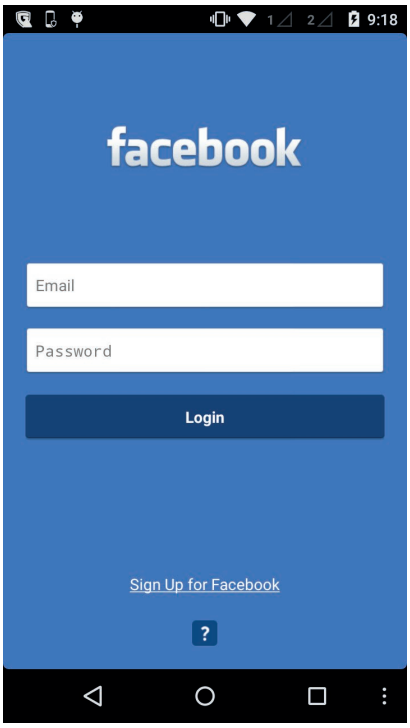
EXAMPLE: MANIPULATED FACEBOOK APP

A common method is to manipulate a legitimate, popular app such as the Facebook app. All of the usual Facebook functions are available in the manipulated version. Users do not notice the surreptitious



access, but the range of functions is expanded by the attached malware, enabling third parties to access the entire device without asking for the user's consent. The permissions have already been approved by the owner prior to commissioning the device. Hence the user only notices the malicious app when he installs a security solution such as G DATA INTERNET SECURITY FOR ANDROID. As soon as the security software has been installed, it immediately sounds an alarm. In this example, the G DATA security solution identifies the malware as Android.Trojan.Andup.D. Uninstalling is often not possible as the app is one of the fixed installation applications in the firmware. The G DATA security experts advise afflicted users to contact the vendor of the mobile device.

The secret add-on functions are wide-ranging. In this example, the app can access the Internet, read and send SMS, subsequently install apps, see, store and amend call data and data about the smartphone, access the contact list, obtain location data and monitor app updates. These permissions enable extensive misuse: location detection, listening to and recording telephone calls or conversations, making purchases, bank fraud or sending premium SMS. The possibilities are almost endless.



In almost every variant that the G DATA security experts have analysed, the app has been poorly programmed and harbours an enormous security risk. Sensitive data are largely sent unencrypted or with a hardcoded key that can be

easily decrypted. Thus, even other attackers can steal data or take control of the malware.

In addition, none of the examined samples checks in advance whether it exchanges data with the correct server. In this case Man-in-the-middle-attacks could be easily implemented.

```
<uses-permission android:name="android.permission.INTERNET" />
<uses-permission android:name="android.permission.READ_SMS" />
<uses-permission android:name="android.permission.RECEIVE_SMS" />
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.READ_PHONE_STATE" />
<uses-permission android:name="android.permission.SEND_SMS" />
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
<uses-permission android:name="android.permission.CHANGE_COMPONENT_ENABLED_STATE" />
<uses-permission android:name="android.permission.MODIFY_PHONE_STATE" />
<uses-permission android:name="android.permission.READ_CONTACTS" />
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
<uses-permission android:name="android.permission.ACCESS_MOCK_LOCATION" />
<uses-permission android:name="android.permission.CONTROL_LOCATION_UPDATES" />
<uses-permission android:name="android.permission.ACCESS_LOCATION_EXTRA_COMMANDS" />
```

The app can access the Internet, read and send SMS, subsequently install apps, see, store and amend call data and data about the smartphone, access the contact list, obtain location data and monitor app updates.

WHICH DEVICES ARE INVOLVED?

The experts were able to prove the presence of a manipulated pre-installed app on three mobile devices in factory condition. Besides the Star N9500, which has been under investigation since 2014, the Star N8000 and IceFox Razor are involved as well.

Through feedback from G DATA INTERNET SECURITY FOR ANDROID, support calls and results from other security researchers, the experts have identified further instances in which evidence of pre-installed malware on the devices is suspected. In these cases, G DATA security experts suspect that middlemen are behind the manipulation of single devices, like models from Huawei or Lenovo. The experts believe that there is a much higher undetected number.

INFECTED MODELS (EXCERPT)

- Xiaomi MI3
- Huawei G510
- Lenovo S860
- Alps A24
- Alps 809T
- Alps H9001
- Alps 2206
- Alps PrimuxZeta
- Alps N3
- Alps ZP100
- Alps 709
- Alps GQ2002
- Alps N9389
- Andorid P8
- ConCorde SmartPhone6500
- DJC touchtalk
- ITOUCH
- NoName S806i
- SESONN N9500
- SESONN P8
- Xido X1111