SIMPLY SECURE

G DATA MOBILE MALWARE REPORT

THREAT REPORT: Q3/2015

Whitepaper MMWR EN Q3 12-2015 #53115 • 3313151215

CONTENTS

AT A GLANCE

- The global market share of mobile devices using Android as an operating system was almost 67 percent in the third quarter of 2015. This represents an increase of no less than three percent compared to the second quarter. In Germany, around 68 percent of users were using a mobile device with an Android operating system. This percentage has remained the same.[1]
- Malware figures for Android devices in the third quarter of 2015 remained at a high level. During the third quarter, G DATA security experts identified 574,706 new malware samples. The figures were at a similarly high level in the second quarter (560,671). The number of new Android malware instances increased by 50 percent compared to the same period in the previous year (Q3/2014: 383,122).
- View for 2015 as a whole: up to the third quarter, G DATA security experts have already analysed some 1.6 million new Android malware samples.
- Over 80 percent of Android devices have an outdated operating system in use. Only 20 percent of the smartphones or tablets are using a current version of Android. Often the rollout of security fixes by the manufacturer takes a long time. Known vulnerabilities are be fixed in a timely manner.

FORECASTS AND TRENDS

ANDROID AS A GATEWAY TO THE INTERNET OF THINGS

People and companies are turning to the Internet of Things. From fitness apps to vehicles, more and more devices are being networked together and can be linked to a smartphone or tablet. Such applications and the Android operating system are becoming more and more popular among cyber criminals, as they can offer a route for attack.[2] One well-known example of this is attacking a heating control system via a smartphone.[3]

SMARTPHONES WITH PRE-INSTALLED MALWARE

Following the latest results in the Mobile Malware Report for the second quarter of 2015, G DATA experts are continuing to look into this subject. More and more smartphones and tablets are afflicted with manipulated firmware. New results on this are expected in the coming months.

COMPLEX MALWARE FOR ONLINE BANKING ATTACKS

G DATA security experts expect to see an increase in complex malware that combines Windows and Android attack campaigns on online banking customers. Numerous customers have the option to receive TAN numbers by mobile phone as a secure two-way authentication process. Criminals can use this method to manipulate online banking transactions on the PC and simultaneously steal the accompanying authentication via the mobile device.

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

[2] G DATA Security Evangelist Eddy Willems has published his opinion of the current situation on the Internet of Things in the G DATA SecurityBlog: https://blog.gdata.de/artikel/the-internet-of-things-trouble/

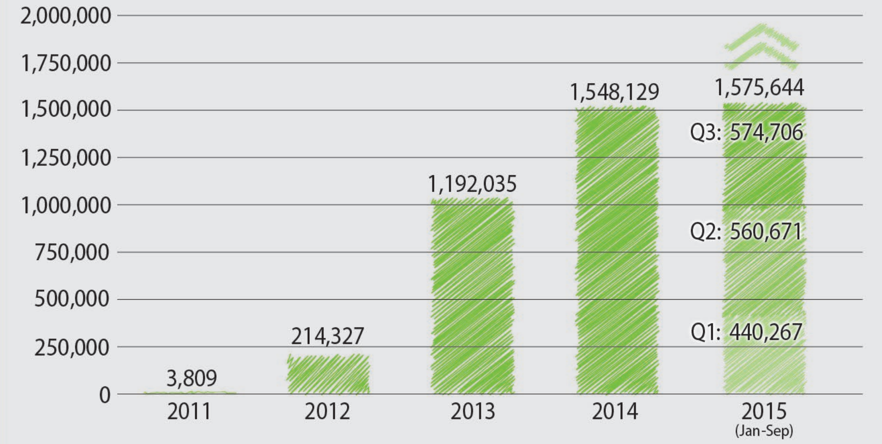
[3] http://www.heise.de/security/meldung/Vaillant-Heizungen-mit-Sicherheits-Leck-1840919.html

CURRENT SITUATION: ALMOST 6,400 NEW ANDROID MALWARE INSTANCES EVERY DAY

During the third quarter of 2015, G DATA security experts analysed 574,706 new malware instances. The volume of new malware has continued to be at a high level and has increased compared to the second quarter of 2015 (560,671). This represents an increase of 50 percent compared to the same period in the previous year. On average, the experts discovered almost 6,400 new Android malware files every day in Q3/2015.

Up to the end of the third quarter of 2015, G DATA experts had discovered over 1.5 million new Android malware samples this year. This means that the analysts have already discovered more malware programs than in the whole of 2014. Significantly more than two million new Android malware samples for 2015 as a whole is looking more and more likely.[4]

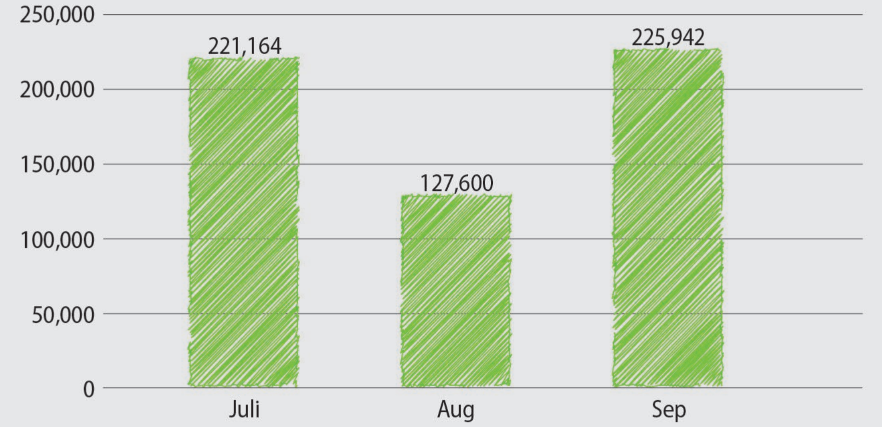
NEW ANDROID MALWARE SAMPLES



Source: G DATA Software AG

[4] 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 (Q3)



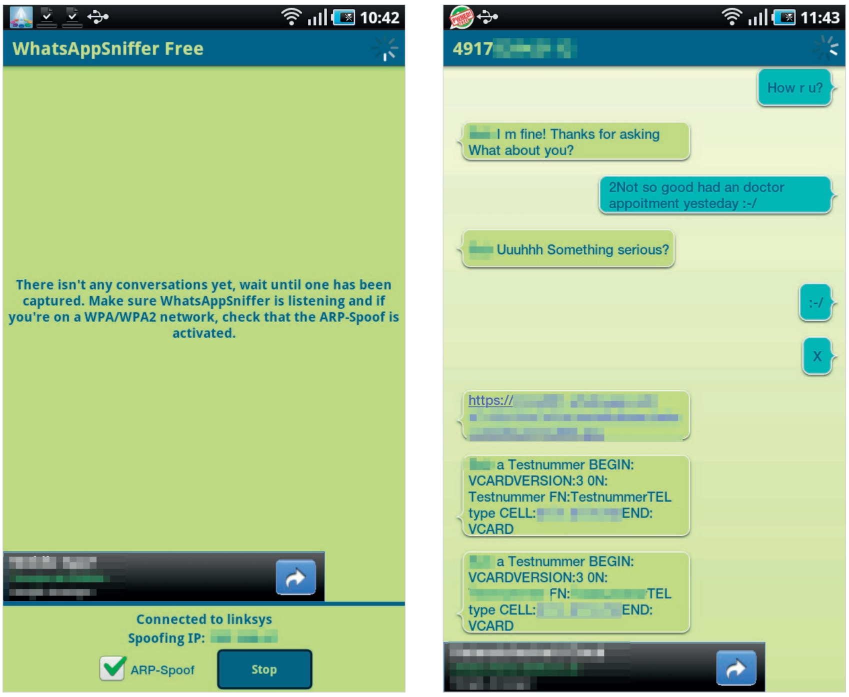
Source: G DATA Software AG

WHAT ARE HACKING TOOLS?

Hacking tools are not found in the Google Play store, but rather in third party markets, which also hide the risk of a malware infection. To use those apps, users must enable installation from unknown sources in the settings of their mobile device.

IT experts use hacking tools to check out networks and computers for vulnerabilities and to prevent successful attacks on networks and devices. However, these apps can also be used to screen third-party mobile devices for potential security holes, infiltrate a WLAN network or monitor data traffic. As such, applications can pose a risk for users and G DATA security experts classify hacking tools as malware.

Such applications can also have criminal law consequences. In the last report, the security experts described monitoring apps that monitor mobile devices. In Europe and the US recently investigating authorities brought a campaign against purchasers of the DroidJack monitoring software. This tool can be used, for example, to steal data such as TAN numbers, send SMS messages, locate the smartphone or eavesdrop on telephone calls.[5]



There isn't any conversations yet, wait until one has been captured. Make sure WhatsAppSniffer is listening and if you're on a WPA/WPA2 network, check that the ARP-Spoof is activated.

[redacted]

Connected to linksys
Spoofing IP: [redacted]

☑ ARP-Spoof

4917[redacted]

How r u?

[redacted] I m fine! Thanks for asking
What about you?

2Not so good had an doctor appoitment yesteday :-/

[redacted] Uuuhhh Something serious?

:-/

X

https://[redacted]

[redacted] a Testnummer BEGIN: VCARDVERSION:3 0N: Testnummer FN:TestnummerTEL type CELL:[redacted] END: VCARD

[redacted] a Testnummer BEGIN: VCARDVERSION:3 0N: [redacted] FN:[redacted]TEL type CELL:[redacted]END: VCARD

[redacted]

Note: The G DATA security experts have decided not to offer a current example of a hacking tool so as not to advertise them

WHATSAPP SNIFFER: READING OTHER PEOPLE'S CHATS

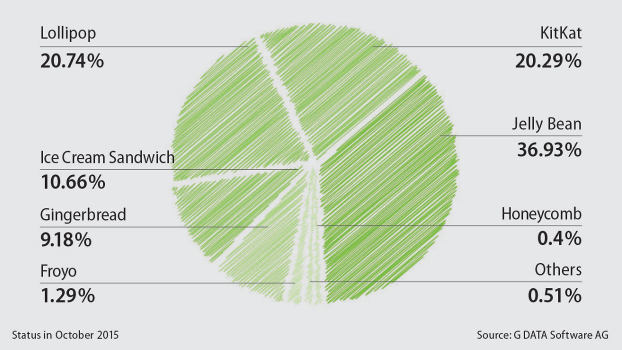
For some time now, the WhatsApp sniffer[6] has been one of the most popular hacking tools for monitoring other people's WhatsApp chats. The application does this by exploiting a security hole in the popular messaging tool. Those who have the app can spy on conversations and data in any chats in real time. To do so, the devices must simply be logged in to a shared network. A public wireless network at an airport or in a hotel offers a never-ending source of opportunity for stealing sensitive data for owners of the monitoring app. Screenshots also show how easy it is to eavesdrop on chats. WhatsApp has now closed the security hole. However, this sniffer is still a very good example of hacking tools and the opportunities that exist for using them.

[5] http://www.infosecurity-magazine.com/news/police-crack-down-droidjack/
[6] https://blog.gdatasoftware.com/blog/article/using-whatsapp-in-wifi-makes-conversations-public.html

OVER 80 PERCENT OF ANDROID USERS HAVE AN OUT-OF-DATE OPERATING SYSTEM

In October 2015, G DATA security experts examined which Android versions are being used on smartphones and tablets with G DATA security solutions installed. The current Android 6 operating system is missing, as the new version was released this October. Only about 20 percent of users have installed an up-to-date operating system (Android 5.0 or higher). Over 80 percent use an outdated operating system that contains known security holes. And almost 12 percent are still using Froyo and Gingerbread, versions that are around five years old. The FBI[7] issued warnings about using Gingerbread over two years ago. Since then, even more security holes have been published, such as Stagefright[8], which affects a wide range of Android versions.

ANDROID OS DISTRIBUTION



Status in October 2015

Source: G DATA Software AG

In October 2015 only about 20 percent of Android users use an – at this time – current Android version.

ANDROID VERSION	DISTRIBUTION (IN PERCENT)
Lollipop	**20.74%**
Android 5.1	6.63%
Android 5.0	14.11%
Kitkat	**20.29%**
Android 4.4	20.29%
Jelly Bean	**36.93%**
Android 4.3	6.35%
Android 4.2	12.75%
Android 4.1	17.83%
Ice Cream Sandwich	**10.66%**
Android 4.0	10.66%
Honeycomb	**0.4%**
Android 3.2	0.4%
Gingerbread	**9.18%**
Android 2.3.3 - 2.3.7	9.18%
Froyo	**1.29%**
Android 2.2	1.29%
Other	0.51%

Android users frequently wait a long time before updating their operating system. When Google publishes an update for the Android operating system, it normally takes weeks or months for providers of mobile devices to modify the versions for their products and make them available to their customers. With older smartphones and tablets, it is often unclear whether the providers have even closed security holes yet. Frequently even the most popular devices are only provided with support in terms of necessary updates for one or two years.

Hence some providers have started to launch monthly update programs for products with an Android operating system. For example, Samsung has launched a mobile security blog where customers can see what updates are available for their device. In doing so the Korean provider has been guided by Microsoft Patchdays, whose

[7] https://publicintelligence.net/dhs-fbi-android-threats/

[8] https://blog.gdata.de/artikel/sicherheitsluecke-in-android-medien-engine-stagefright/

software is fully updated on every second Tuesday of the month. However, unfortunately only a few devices from the last two years are currently receiving these security patches.[9]

Other providers are also planning to offer a similar service in the coming months in order to keep customers better informed and create greater awareness of security updates for mobile devices.

[9] http://security.samsungmobile.com/

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 products set the benchmark worldwide: In the comparison tests of AV-Test, which are carried out twice a year, G DATA has repeatedly achieved the best virus detection of all products. "Stiftung Warentest" has compared IT security solutions eight times in total, starting in 2005. In every single one of these tests, G DATA INTERNET SECURITY demonstrated the best virus detection. The European Community project IPACSO named G DATA the most innovative IT security company of Europe in 2014 and lauded the quick response time to new threats.

G DATA security solutions protect millions of PCs worldwide and are available in over 90 countries – for private users as well as for SMB and large corporations, and as a Managed Service for enterprise customers through the numerous G DATA partners. That is security "Made in Germany".

G DATA SIMPLY SECURE