TRUST IN
GERMAN
SICHERHEIT

MOBILE MALWARE REPORT

THREAT REPORT: H2/2014

CONTENTS

Whitepaper MMWR EN 03-2015 • 0015200315

TRUST IN GERMAN SICHERHEIT

AT A GLANCE

MARKET SHARE FOR ANDROID-SMARTPHONES AND -TABLETS

- 1.301 billion smartphones were purchased globally in 2014 according to market analysts – 702 million in the second half of the year alone.[1] During this period, the smartphone market share for Android stood at 81 percent on average.[2] In terms of processor, 569 million of the smartphones purchased had an Android operating system installed, as did a total of 91.6 million Android tablets purchased.[3]

MALWARE NUMBERS FOR ANDROID DEVICES

Definitive malware numbers for Android devices: G DATA security experts identified and analysed 796,993 new malware samples in the second half of the year. This represents an increase of 6.1 percent (751,136) compared to the first half of the year. In total, over 1.5 million new Android malware programs were investigated by G DATA experts in 2014. This represents an increase in new Android malware instances of almost 30 percent compared to 2013 as a whole.

THIRD PARTY MARKETS FOR ANDROID APPS

- Third-party markets for Android apps: European and American providers come out better compared to markets in China or Russia. Up to a quarter of some app markets in China are infected with malware and PUPs (Potentially Unwanted Programs).

PRE-INSTALLED SPYWARE

- G DATA security experts have again discovered a smartphone from a renowned provider with a permanently installed digital spy on it. The malware hides in a fake app and sends data to third parties.

[1] http://www.idc.com/getdoc.jsp?containerId=prUS25407215
[2] http://blogs.strategyanalytics.com/WSS/post/2015/01/29/Android-Shipped-1-Billion-Smartphones-Worldwide-in-2014.aspx
[3] http://www.strategyanalytics.com/default.aspx?mod=pressreleaseviewer&a0=5617 , http://www.strategyanalytics.com/default.aspx?mod=pressreleaseviewer&a0=5640

Whitepaper MMWR EN 03-2015 • 0015200315

FORECASTS AND TRENDS

ABSOLUTE NUMBER OF NEW MALWARE INSTANCES EXPLODES

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

ADVERTISE, SPY, MANIPULATE: ADWARE BECOMING MORE REFINED

- Adware is annoying for many users. This category is becoming more and more refined. Current cases on computers indicate that SSL encryption is being rendered ineffective by adware. Cyber criminals can exploit this to spy on sensitive data, such as that used for online banking or on social networks. The security experts expect that this trend will spread to mobile devices as well.

USERS INCREASINGLY RELYING ON ENCRYPTION

- Awareness of security and privacy has grown following the revelations regarding spying and cyber crime. Encryption is increasingly becoming the standard. Users can easily secure and encrypt their data, especially on Android devices. Android already offers a function in the settings for securing all the data on the internal and external memories against access.

CROSS-PLATFORM MALWARE: THE KEY TO THE COMPANY NETWORK

- In 2015, multi-target malware (malware that can be used both on PCs and on mobile devices) is being used more frequently by cyber criminals to gain access to company networks. Cross-platform infections will increase significantly, in the opinion of G DATA.

"QUANTIFIED SELF" DATA MUCH SOUGHT-AFTER BY CRIMINALS

- Fitness apps and accessories are popular on smartphones. Personal data ("quantified self") is being recorded and analysed more and more often. G DATA security experts are concerned that data theft in this area will increase.

SPECIAL MALWARE TARGETS BANK DATA

- 2015 will be characterised by special malware that targets bank and financial data. In 2014, around a third of all bank customers used their mobile device for online banking transactions – and the trend is increasing.[4] Cyber criminals are relying on fake or manipulated banking apps that specifically target this development.

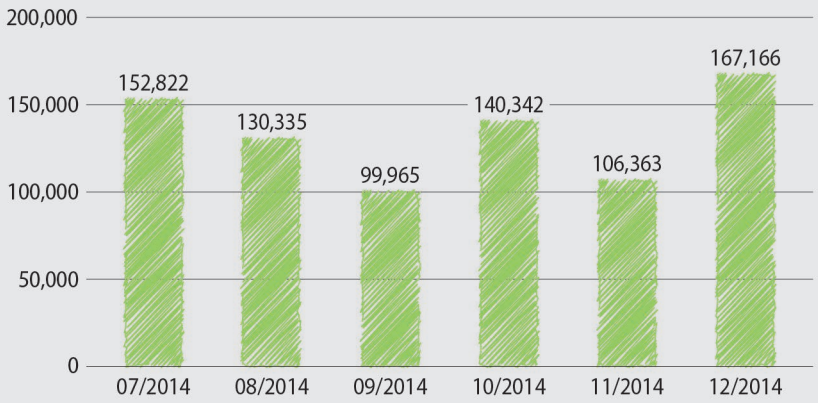
[4] http://www.statista.com/statistics/380803/online-banking-penetration-in-the-eu/

TRUST IN GERMAN SICHERHEIT

CURRENT SITUATION: 4,500 NEW ANDROID MALWARE INSTANCES EVERY DAY

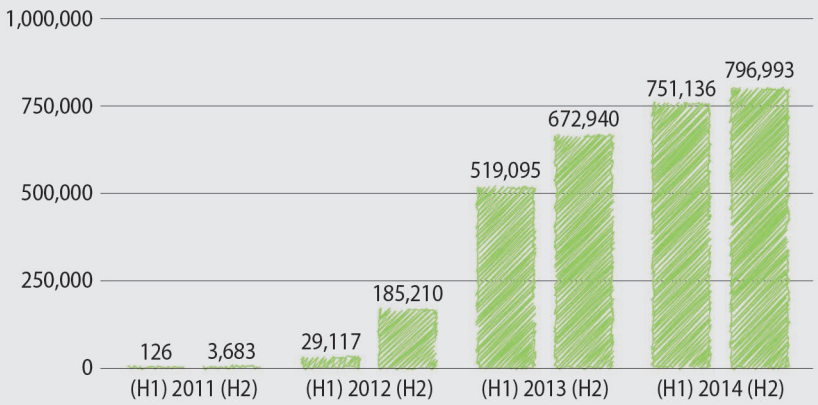
During the second half of 2014, G DATA security experts recorded 796,993 new malware types. On average, the experts discovered almost 4,500 new Android malware files every day in the second half of the year. This represents an increase of 6.1 percent (751,136) compared to the first half of the year. Consequently the number of new malware program types has risen by 18 percent compared to the second half of 2013 (672,940). In 2014 as a whole, the security experts identified 1,584,129 new Android malware samples. This represents an increase in new mobile malware instances of almost 33 percent compared to 2013 (1,192,035).

NEW ANDROID MALWARE SAMPLES IN 2014 / MONTHLY (H2)



Source: G DATA Software AG

ANDROID MALWARE SAMPLES / HALF-YEARLY



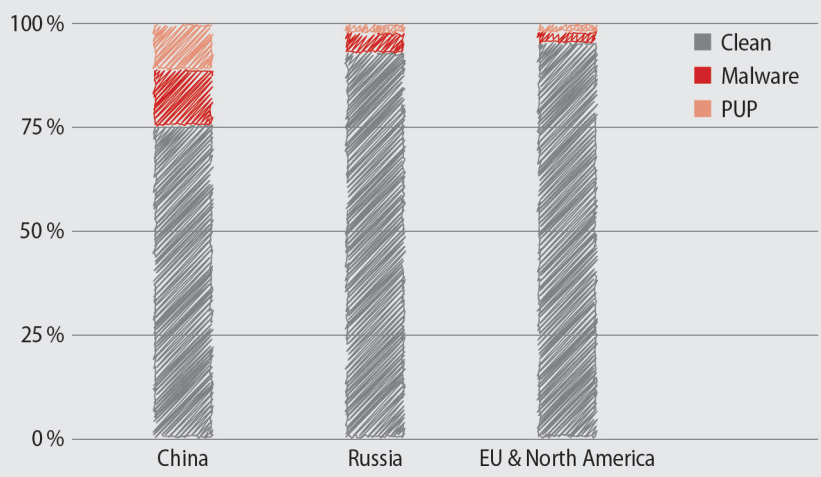
Source: G DATA Software AG

THIRD-PARTY APP STORES

In the second quarter of 2014, the Android operating system reached a global market share on smartphones of almost 85 percent.[5] Malware programmers try to exploit this trend and specifically develop malware for the Google operating system. The prospect of high financial profits for comparatively little outlay is highest here.

Unlike iOS or Windows Phone, Android is an open source operating system. Because of this freedom, numerous app stores run by third-party providers have arisen alongside the Google Play store. Google automatically scans all of the apps used in its own store for suspicious content. Such analysis often does not take place in alternative app stores. Many third-party providers are very imprecise, or do not even bother, when it comes to checking whether applications are infected with malware. To be able to use an alternative app market place, users must allow the installation of applications from sources other than the Play store in the Android device's settings. This disables the central protective function for Android and enables malware to find its way onto the mobile device. Malware authors are then able to lure Android users into their trap. Frequently, cheap versions of apps that are actually expensive, or apparently important system updates are used to try to induce smartphone owners to disable the protective function on their device. Users who still want to use a third-party provider's store should look into its trustworthiness beforehand.

ANDROID MALWARE ALLOCATION IN 3RD PARTY MARKETS



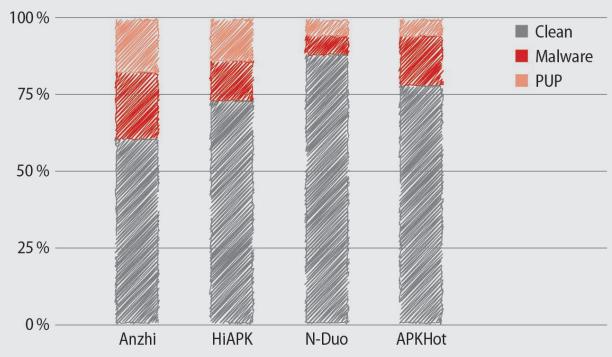
Source: G DATA Software AG

[5] http://www.idc.com/getdoc.jsp?containerId=prUS25037214

CHINESE APP MARKETS COMMONLY DISTRIBUTE MALWARE

G DATA security experts have found malware or potentially unwanted programs (PUPs) such as adware or riskware in just 3.4 percent of applications offered in American and European app stores. In many app stores in the Chinese market place, over 25 percent of applications are infected – 13 percent alone with malware.

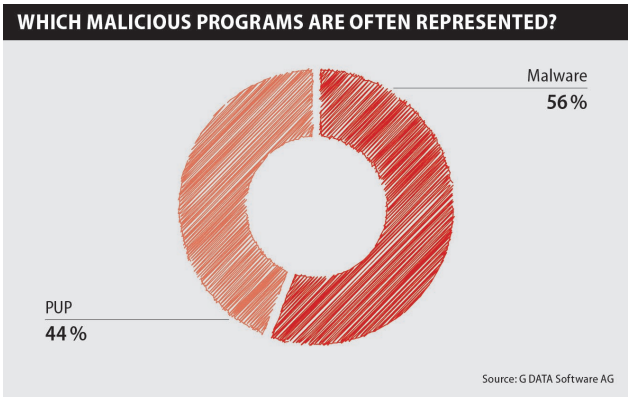
ANDROID MALWARE IN CHINESE 3RD PARTY MARKETS



WHICH MALWARE IS DOMINANT IN APP MARKETS?

Over half (56 percent) of the malware identified consists of Trojans or other malware. Malware here is an umbrella term for various types of malicious software. These include exploits, Trojans and backdoors.

WHICH MALICIOUS PROGRAMS ARE OFTEN REPRESENTED?



44 percent of the other malware falls into the PUP category. Adware and riskware are examples of PUPs. Adware means programs that have advertising content and use dishonest methods to display this to the user. These apps are not necessarily malicious, but they are still a nuisance for the user. Riskware, on the other hand, is potentially dangerous software. Installing such apps can lead to damage to the device. Apps in this category may even be legitimate apps that have vulnerabilities or have been compromised.

SECURITY IN APP STORES NEEDS TO BE MORE IN FOCUS

Few app markets run by third-party providers are currently checked with antivirus scanners. The available statistics are based on known malware. The security experts believe that the actual number is higher. To guarantee security in these markets as well, they need to be continually monitored and analysed.

Whitepaper MMWR EN 03-2015 • 0015200315

YET ANOTHER SMARTPHONE WITH MALWARE IN THE FIRMWARE

In spring 2014, G DATA security experts discovered pre-installed malware on a smartphone for the first time. The device, purchased under the name Star N9500[6], had a comprehensive spyware program built in at the factory itself. Now the experts have come across another device with firmware infected with malware. Some versions of the Xaomi Mi4 came with a pre-installed Trojan. The devices concerned were supplied with German menus and could be purchased in certain online shops. G DATA security experts therefore suspect that an intermediate dealer is behind this scam, installing the manipulated firmware on the devices.

MALWARE HIDING IN MANIPULATED TWITTER APP

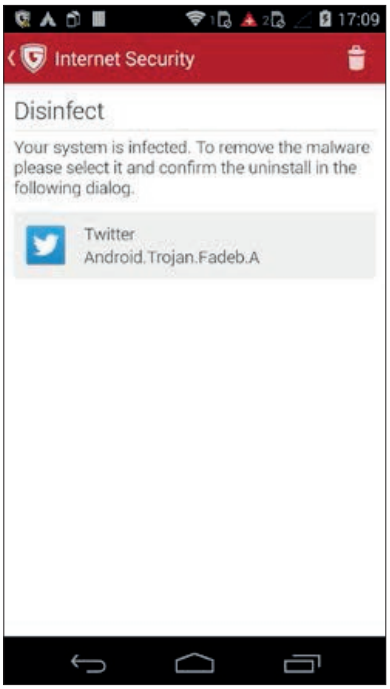
The malware was hiding in a manipulated Twitter app. Unlike the original app, the fake version demanded more rights. Besides accessing the call list, the app tries to track running programs and install and remove applications independently. This means that criminals can access personal data without being noticed, eavesdrop on conversations, read SMS and emails, or remotely control the camera and microphone. The malware can also subsequently install other apps without being noticed. Furthermore the malware sends information about the smartphone, the operating system being used, the language version and location data to anonymous servers. This means that the options for attackers are unlimited.

SENSITIVE USER DATA SENT TO ANONYMOUS SERVERS

In their analysis, the security experts were able to determine that the data was being sent to Asia. Because it is integrated into the device's firmware, the malware has extensive permissions and can install other applications without the user noticing. The Trojan uninstalls unwelcome apps if necessary. It is not possible to remove the manipulated app and the spyware since they are integrated into the firmware.

PREDICTION COMES TRUE

When they discovered the Star N9500, G DATA security experts predicted that the smartphone with pre-installed spyware on it would not remain an isolated case. The Xaomi device has reinforced this belief. But the case is not yet closed. The analysts are investigating yet more devices that have been supplied with similar firmware.



G DATA INTERNET SECURITY FOR ANDROID detects the manipulated Twitter app.

[6] https://blog.gdatasoftware.com/blog/article/android-smartphone-shipped-with-spyware.html

Whitepaper MMWR EN 03-2015 • 0015200315