G Data

Mobile MalwareReport

Half-Year Report
July – December 2013

G Data SecurityLabs

G Data. Security Made in Germany.

Contents

At a glance

- The number of activated Android mobile devices has surpassed one billion.[10]
- According to Gartner, the number of Android mobile devices purchased worldwide in the past year was over 877 million smartphones and tablets. This represents an increase of over 70% compared to 2013. The analysts calculate over a billion newly-purchased Android devices per year to 2015 and a market share of 50%.

- Malware for Android: The number of new mobile malware samples increased again in the second half of 2013, with 672,940 new malware instances compared to 526,818 in the previous half year.
- Rates of increase in 2013: Compared to the first half of 2013, this represents an increase in the number of new malware instances of 30%.
- Comparison with previous year: A comparison of the total number of new malware instances in 2012 and 2013 shows an increase of 460%.

- The number of backdoors has increased slightly (+5.7%) – this indicates that more and more smartphones are being integrated into botnets.
- Malicious apps that are given the designation "Android.Application" and hence belong to the group of potentially unwanted programs (PUPs) represent a great share of the overall landscape of new files (40.4%). This includes malware with diverse malware functions.
- Hacker tools are a conspicuous type of Android.Application in this regard. These apps are frequently used for ambiguous purposes – as a legitimate system test, or as spyware if they fall into the wrong hands.

Outlook:

- It can be expected that attackers will create and distribute fewer and fewer SMS malware programs, as the security mechanisms against such threats are becoming more and more efficient. Data theft and the development and distribution of malware such as ransomware are gaining in significance.
- As monetary profit remains the number one goal for attackers, attacks on cryptocurrencies such as Bitcoin might come into play in the future, especially where digital wallets are located on mobile devices.
- Smartphones are increasingly being misused to access company networks. Cross-platform infections between PCs and mobile devices are increasing in both directions.
- The "Internet of Things" is increasingly finding its way into everyday life, and the Android platform is frequently being used as an operating system for this. Hence large-scale attacks against these devices are merely a matter of time.
- We are expecting the first attacks on smart TVs in the coming year.

Android malware: share of PUPs increasing significantly

The malware count for Android is based on the evaluation of the number of new malware programs.[1] In the second half of 2013, a total of 672,940 new malicious instances were detected in the G Data SecurityLabs. This represents an increase of almost 30% compared to the first half of 2013 (526,818[2]). However, we have not seen the projected tripling in the number of new mobile malware programs. On average, G Data SecurityLabs received 3,657 new malware files every day!

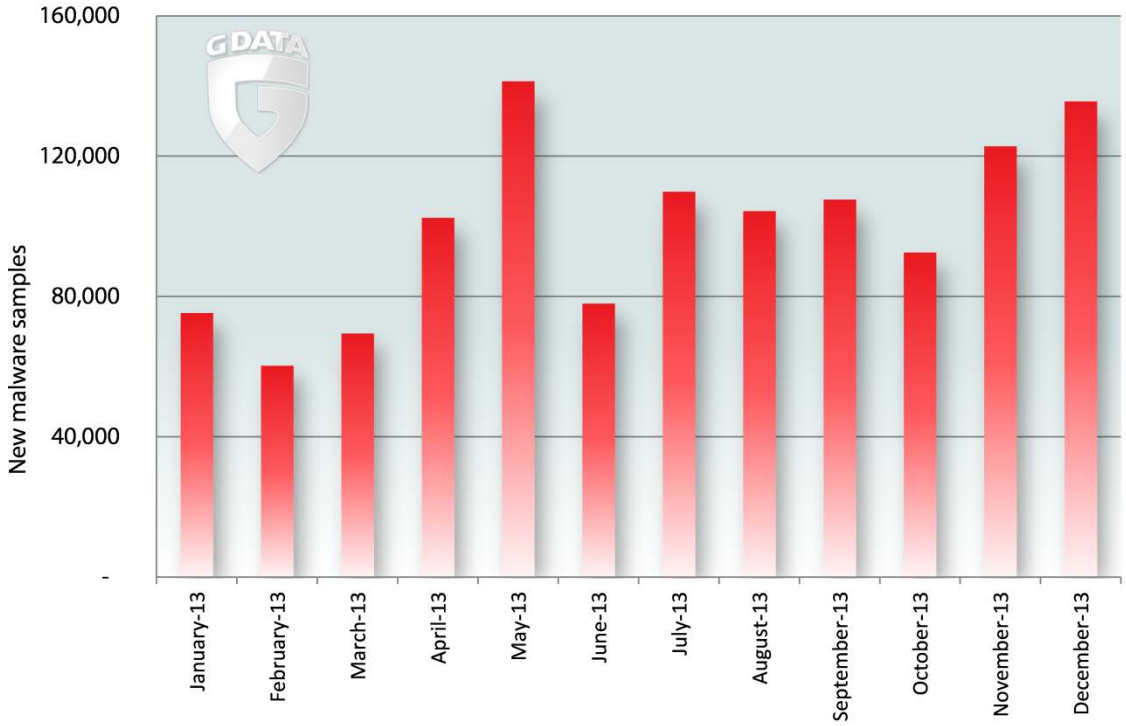


Figure 1: *Spread of new malware instances that can be allocated to the year 2013.*

The individual files are allocated to specific families based on the properties of the malicious code[3]. 312,438 of the new malware files could be clearly assigned to malware families[4], as illustrated in Figure 2. Within the families, 2,859 different malware variants could be determined. These variants are based on 581 different malware families. In the last six month period, the experts recorded 176 new families. Table 1 shows a list of the most productive families, that is, the families with the most variants.

Family	# variants
Trojan.Agent	586
Trojan.SMSSend	171
Backdoor.GingerMaster	159
Trojan.SMSAgent	96
Trojan.Boxer	80

Table 1: *List of Android malware families with the most variants in H2 2013.*

[1] Android malware can be identified based on several files. The installation package (APK) contains numerous files including such things as the code and properties. With this method of counting, detections of APK and their respective components are summarised as one malicious file, even if there are several files in our library.

[2] The retrospective figures for this half of the year are higher than in previously published reports. In some cases, G Data's SecurityLabs receive collections of files with a large number of new malicious files collected over an extended period of time and these sometimes contain older files, which are then assigned to the respective month.

[3] The count of signatures and variants is based on the signatures from G Data protection solutions for mobile products.

[4] Of 672,940 samples, 360,502 samples were identified as "potentially unwanted programs" or as having generic signatures, and are therefore not counted unambiguously as malware.

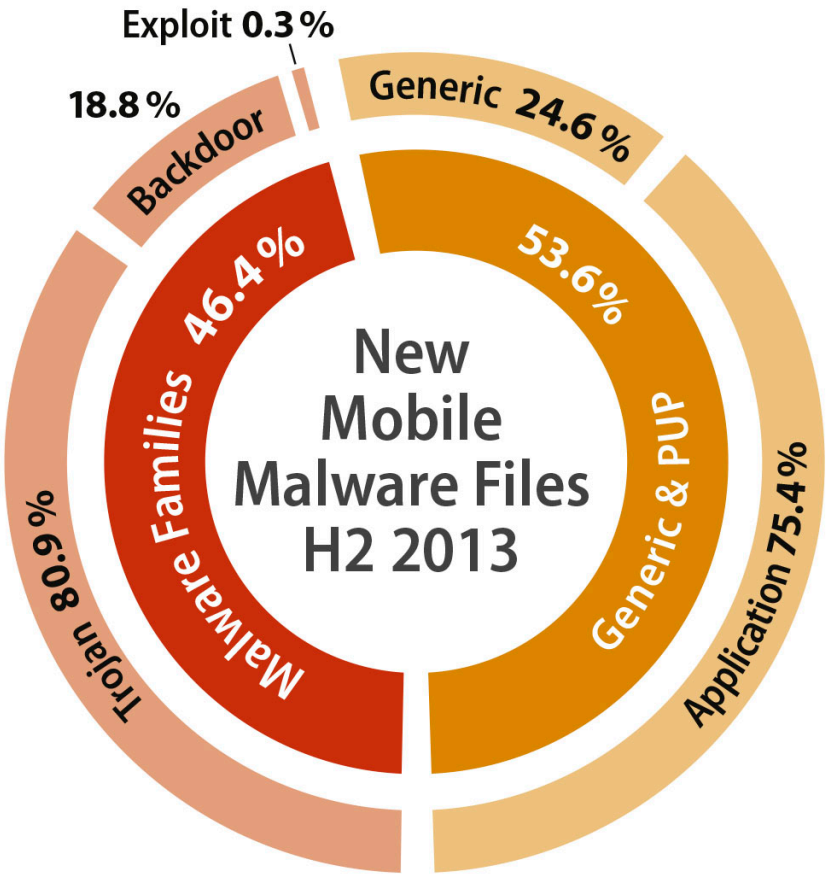


Figure 2: *Composition of new mobile malware instances from H2 2013 in percent.*

The inner circle describes the distribution of new malware in files that could be classified in malware families and those files that were detected as generic, as well as files recognised as potentially unwanted programs (PUP for short). The outer circle illustrates the respective assignment of types as performed using the signatures of G Data MobileSecurity products.

In general, the ratios in the second half of the year have not changed much: classification into malware families and generic detections and PUPs[5] is more or less equal, even though "Generic & PUPs" make up more than half this time.[6]

[5] PUPs are not conventional malware programs. Malware generally refers to software intended to damage the infected device or to steal information that can be used to carry out criminal activities such as identity theft or fraud, without the consent of the user. However, it is not always straightforward to draw a clear line between malware and other nuisances such as adware or PUPs. In the most frequent instances, they change browser settings (browser hijackers), display unwanted advertising (adware), spy on the user in the background (spyware) and sometimes embed themselves deep in the system. However, the programs are not malicious in the stricter sense. Many people actually want to use the functions of the software – hence the name "Potentially" Unwanted Programs.

[6] By optimizing the process of malware designation, it has been possible to allocate more generic detections to clearly appropriate sectors. Hence the big increase in the proportion of Android.Application in the "Generic & PUPs" sector.

Android.Application consists of versatile programs

The PUP sector (designated as Android.Application) makes up a considerable proportion: 40.4% of new samples were recognised as Android.Application. This detection group includes, for example, apps such as the fake Adobe Flash Player apps discovered in early 2014, which went hunting for victims in the Google Play Store.[7]

Furthermore, apps designated as copycats are also counted in this category – these are copies of perfectly normal applications that contain potentially unwanted add-ons, such as display advertisements or the requirement of additional permissions. The attackers use "binders" to create such copies of apps with add-ons, as was reported in the last Mobile Malware Report.[8]

Even though, after its installation, the app operates normally and the user therefore does not immediately delete it from the system, the fraudsters generally do not provide any updates for these apps. Hence the user remains at an app status that might contain security vulnerabilities and/or must do without the benefit of optimisations from the developers. Consequently, experts at the G Data SecurityLabs are still expressly urging users only to download apps from the original providers.

Special case: hacking tools

Another type of app designated as Android.Application is hacking tools, such as programs for monitoring networks.

However, the use of these programs is ambivalent, as they can be used for both legitimate, well-meaning purposes as well as for spying and monitoring. Many of the pentesting tools[9] come from the science sector and were developed for research purposes. However, they have subsequently been misused for fraudulent activities. Knowledge regarding security holes and software vulnerabilities that has been and is being acquired using hacker and pentesting tools consequently represents basic knowledge for malware authors as well.

[7] G Data SecurityBlog: http://blog.gdatasoftware.com/blog/article/worth-looking-again-fake-flash-player-apps-in-google-play-store.html
[8] G Data Mobile MalwareReport H1 2013: http://www.gdata.de/rdk/dl-en-mmwr
[9] Pentesting is an abbreviation for "penetration testing" and describes tests on computers or networks to find security vulnerabilities. During the testing, methods are used to penetrate the system in the way that an attacker would.

Trends

The enthusiasm of smartphone users for the Android platform is unabated – in early September 2013, Google's Sundar Pichai, SVP for Android, Chrome and Apps, reported that the number of activated Android devices had broken through the significant barrier of one billion.[10]

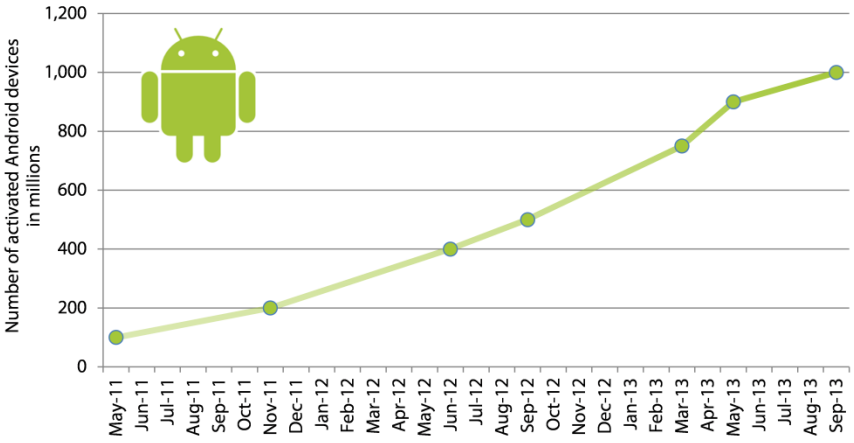
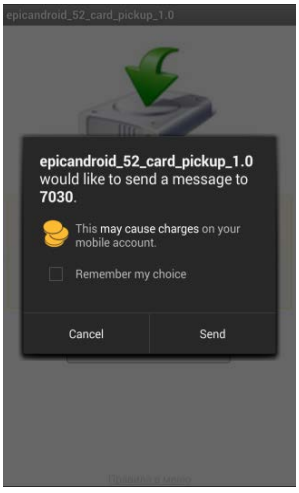


Figure 3: *Number of activated Android devices.*

With the rapid increase in user numbers comes of course an increase in the interest of cyber criminals in making a profit from the platform. To do so, a vast range of attack vectors such as deception tactics is used, as always. Since concentrating on SMS malware is no longer the number one factor, new threat scenarios and sources of income will be created.

SMS malware gradually disappearing



Screenshot 1: *Android warns the user against sending premium SMS.*

Android mobile devices with the operating system version 4 are increasingly gaining market shares, and consequently the security against SMS malware is increasing too. The display of app permissions has been carelessly ignored by many users and information on chargeable permissions is skipped over all too quickly – even though Google has highlighted the messages in conspicuous colours in the new Android versions and given them coin icons.[11]

However, since version 4.2 the operating system has integrated features such as a premium SMS filter. It not only warns the user during installation, but also displays a special screen prior to such SMS messages being sent that provides intervention options.

One important innovation in Android KitKat (version 4.4) is the fact that only the SMS app selected by default is permitted to handle messages – sending, deleting etc.[12] This makes it harder to send messages without the user noticing, and means it is not generally possible to intercept and delete incoming SMS messages so as to conceal subscription agreements or mTAN receipt, for example.

[10] https://plus.google.com/+SundarPichai/posts/NeBW7AjT1QM
[11] See Screenshot 1
[12] http://android-developers.blogspot.de/2013/10/getting-your-sms-apps-ready-for-kitkat.html

In February 2013, the proportion of Android mobile devices using version 4.2 was 1.4%. In November 2013, Android 4.2 and 4.3 accounted for 15.8%, and in December 2013, versions 4.2 to 4.4 combined amounted to 18.2% – the trend is clearly on the up!

This means that the attackers are refining their scams or having to adapt to other business areas, since fast cash through SMS fraud will no longer be the scam with the best cost/benefit ratio. Data theft and the development and distribution of ransomware, among other things, are going to gain in significance.

Cryptocurrencies – digital cash sure to come into focus

Clearly the best known cryptocurrency is Bitcoin, but the list of popular providers is constantly growing longer and payments with these currencies are becoming commonplace on the Internet – including, or perhaps especially, in black market transactions. The much-discussed anonymity is highly valued by users, as is the independence from central institutions such as banks.

However, the currency is based on digital data and has no physical counterpart such as a piece of precious metal. Consequently, storage of the currency data is also purely digital and this storage data, especially the private crypto keys of the users and the wallets, are increasingly becoming the target of cyber attackers. Because of the hype surrounding cryptocurrencies in recent weeks and months, numerous new users are jumping onto the bandwagon and using apps on their mobile devices, in which the wallets are stored. If the attackers can get their hands on these digital wallets, they can rake in the money they contain directly and no longer need to go round the houses via money mules or other intermediaries.

Experts at the G Data SecurityLabs expect that, in future, Android malware will be geared towards stealing relevant data for cryptocurrencies from mobile devices.

Cross-platform malware on the up

Since the introduction of the mTAN function, mobile devices have been playing an important role in the online banking sphere, and for this reason this specialised area has been increasingly targeted by attackers.[13] Infected PCs frequently lure mobile device users into downloading and installing supposed security apps from the Internet, which then intercept mTANs and the like. The good news for users is that, even though downloading the apps might happen automatically, the user must initiate the installation manually – these are drive-by downloads, but not drive-by infections.

We have previously seen automated infections from mobile devices to PCs: for example, an infected mobile device may contain a command to download Windows malware and store it in the memory, then run it on the PC via the autorun function when the mobile is connected to a computer.[14]

It is now expected that PC malware will increasingly install infected .apk files on mobile devices when they are connected. If an Android device is in debug mode when it is connected to the PC, installation via the PC can be automatic, with no query or user interaction involved.

[13] G Data SecurityBlog: http://blog.gdatasoftware.com/blog/article/apparent-security-certificate-turns-out-to-be-android-malware.html
[14] G Data SecurityBlog: http://blog.gdatasoftware.com/blog/article/android-malware-infects-windows-pcs-with-spy-bot.html

Other things of interest

- As parts of botnets, mobile devices might increasingly be used as tools for DDoS attacks and misused.
- The “Internet of Things” is being based more and more on the Android operating system and hence offers more specific attack vectors, primarily in a domestic setting – intelligent refrigerators, heating appliances that can be operated via the Internet, multimedia TVs, game consoles and much more. Everything is networked and, for reasons of convenience, can generally be accessed from outside of the home as well. Much more value is being placed on the development of new functions and features than on implementing security functions.