

Cybercriminals infiltrate Android markets



Long-term AV-Comparatives investigation reveals
over 7,000 dangerous apps in third-party Android
stores

Language: English

Last revision: 26th August 2013

www.av-comparatives.org

Cybercriminals target Android platforms

Long-term AV-Comparatives investigation reveals over 7,000 dangerous apps in third-party Android stores

Innsbruck, Austria – August 26, 2013

A long-term investigation performed by AV-Comparatives confirms an increasing risk of malicious code affecting Android smartphones via third-party app markets. The research, conducted between November 2012 and May 2013 on 20 major third-party Android stores, found 7,175 malware and greyware programs. Most of these were hosted in Chinese-based markets. At the other end of the scale, the lowest malware presence was found in European markets.

At the time of the survey, a large volume of mobile malware/greyware was discovered in popular Chinese Android app stores. All of the App stores in this survey address mostly the mainland Chinese market.

The research revealed that the fastest-growing smartphone application market is affecting mainly the Asiatic region. Nearly 95% of the malware/greyware apps were found in Asian stores.

The investigations' findings suggest that the dramatic numbers of malicious apps present on the Asian market are closely linked to this market's booming activity. From this point of view, European and US markets can be considered secondary targets, as they are entering a stage where growth is steady. Still, at the individual user level, there is no way of indicating safe and unsafe markets, as threats are globally distributed and a single malicious app is enough to compromise a platform.

The investigation took into account greyware along with malware. This falls into the grey area between clean and malicious apps, posing a potential risk. Most common greyware examples are adware and spyware.

We informed the app stores about the findings of the investigation and some of them have already removed the critical apps from their servers, although others ignored our warnings. Overall, the number of malicious applications on the Internet is increasing very rapidly.

While the mobile app stores try to limit the number of harmful apps by implementing certain regulations, some malicious/unwanted apps still escape filtering. The increasing popularity of

smartphones in general, combined with the growth of the Android market share, means that Android-based systems are an increasingly popular target for cybercriminals.

AV-Comparatives stress the importance of building user-awareness of Internet security, and continue to produce reports promoting a safer online environment. The institute has also recently released AVC UnDroid, a free online service that boosts smartphone security by checking for unsafe apps.

Free registration allows Android users to submit suspicious .apk files (Android app installers) for analysis. A detailed report on the app will be provided, highlighting any risks found by the service.

Users of the service will be able to see statistics for the apps submitted, including the number of clean vs. malicious apps submitted, how many apps contain adware, and the most common malware families submitted.

App Store	Malicious Apps found	Greyware Apps found
AndroidDrawer	1	0
Anzhi	1637	1056
ApkTop	8	22
AppChina	32	232
CoolAPK	16	28
DCN	22	49
EoeMarket	867	400
F-Droid	0	0
Freeware4Android	39	15
FreewareLovers	6	7
Gfan	479	648
GooAPK	55	100
HighAPK	5	2
Mobango	42	29
Mumayi	130	465
Nduoa	17	102
PandaApp	24	13
Pdassi	1	0
SlideMe	88	28
Xiashichang	309	201
	3778	3397
		7175

Table 1: number of malicious Android apps and Greyware found in third-party Appstores between November 2012 and May 2013.

Copyright and Disclaimer

This publication is Copyright © 2013 by AV-Comparatives e.V. ®. Any use of the results, etc. in whole or in part, is ONLY permitted if the explicit written agreement of the management board of AV-Comparatives e.V., is given prior to any publication. AV-Comparatives e.V. and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives e.V. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data. AV-Comparatives e.V. is a registered Austrian Non-Profit-Organization.

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives (August 2013)