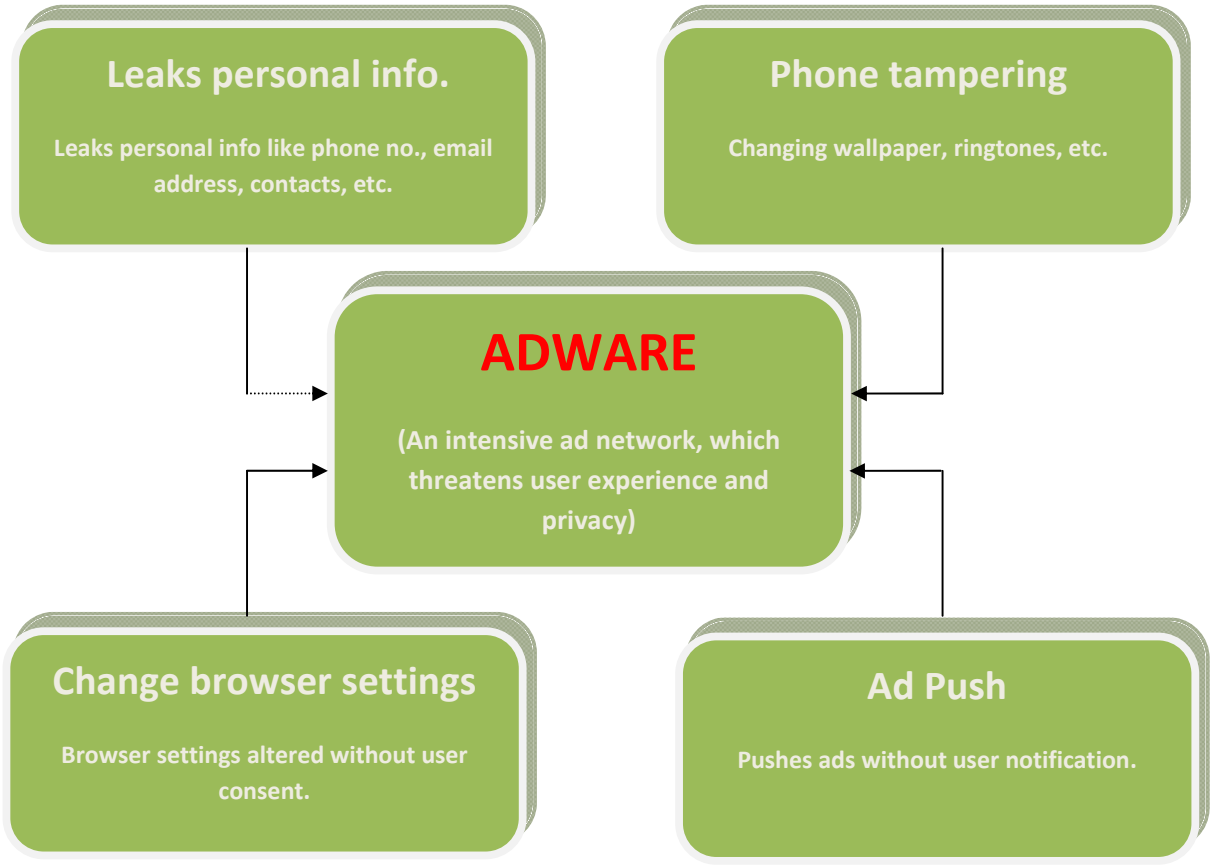
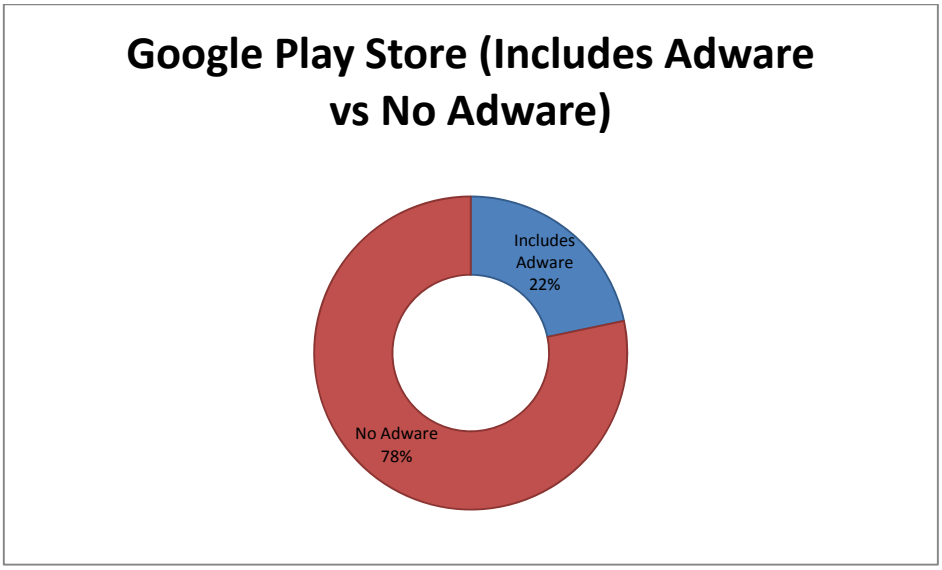
Gap between Google Play and AV vendors on adware classification

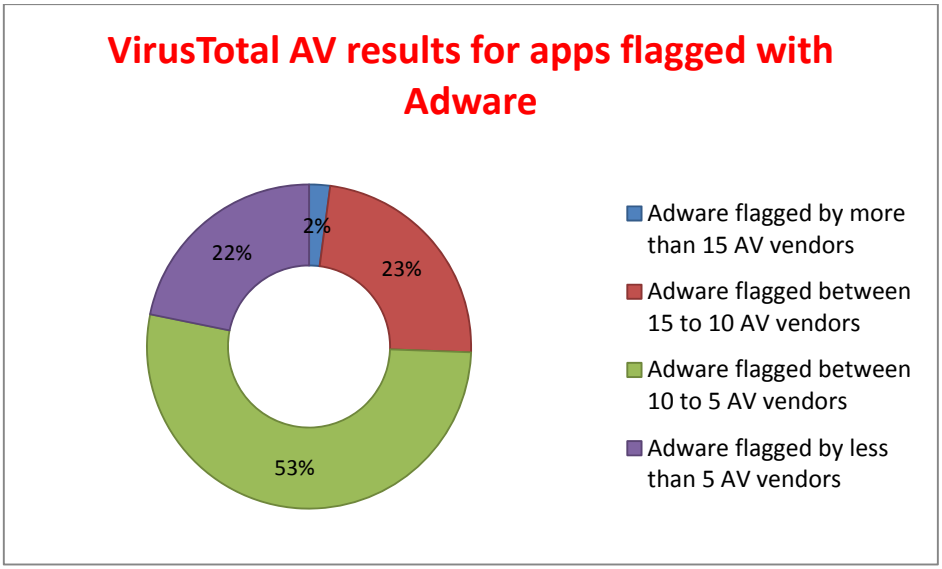
Two critical items impacting mobile use are privacy and a positive user experience. The mobile app market is built on trust. Questionable mobile advertising practices, such as apps employing deceptive adware practices, negatively impact the end user's perception of both privacy and the user experience. Doing things like capturing personal information such as email addresses, device IDs, IMEIs, etc. without properly notifying users and modifying phone settings and desktops without consent, is annoying and unacceptable for mobile users. While the majority of mobile ads are not malicious, they are undesirable for most.



Zscaler regularly analyzes applications in the Google Play store to profile apps and identify those presenting security and privacy risks. By studying this data, we have come up with some interesting statistics concerning the prevalence of 'adware' in apps permitted into the Google Play store. We have tracked the top 300 applications in each category.

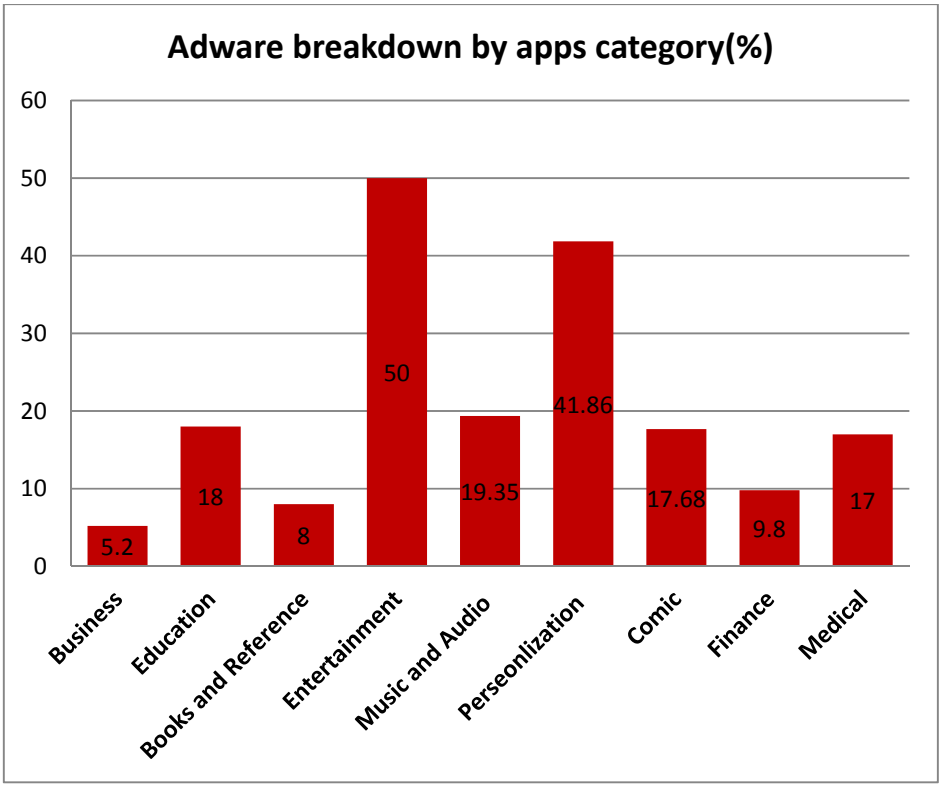


We have found around 1,845 applications which are flagged by one or more AV vendors as including adware. This is a big number. Most of the applications were flagged by AV vendors due to their excessive inclusion of ads and deceptive practices for delivering them, including altering device settings. For example, many AV vendors flag the Airpush API as adware. Despite this fact, there are many apps within the Google Play store that include this API. This illustrates the conflicting interests that Google and the AV vendors have. It is in the best interests of Google to appease advertising companies. Google wants to encourage developers to expand offerings in their app store and developers often profit from free apps through advertising. Paid apps may also include advertising, in which case, Google takes a direct cut from from the app proceeds. Therefore, Google has plenty of incentive to allow apps with aggressive advertising practices. AV vendors on the other hand have no such incentive but are instead under pressure to show that they are adding value by identifying malicious/suspicious/unwanted content. As such, there is a big gap between Google and AV vendors when it comes to adware. Ultimately, end users are stuck in the middle as they are left to decide if they will keep or delete the apps being flagged. Other adware commonly flagged by AV vendors includes leadbolt, airmob, plankton etc.

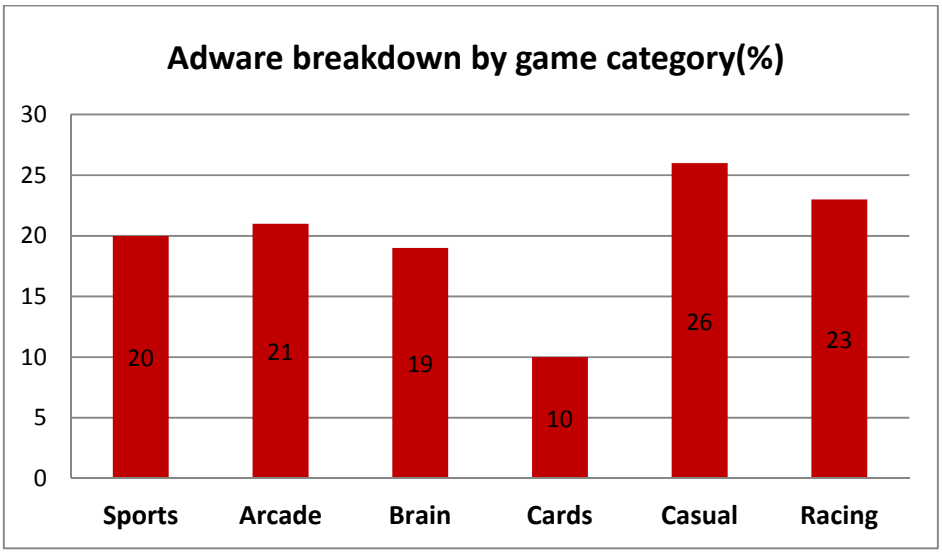


We have collected the following AV data for apps flagged as including adware leveraging VirusTotal:

- Number of apps flagged by fewer than 5 AV vendors: 354
- Number of apps flagged by 5 to 10 AV vendors: 854
- Number of apps flagged by 10 to 15 AV vendors: 381
- Number of apps flagged by more than 15 AV vendors: 34



This above chart shows adware percentage in each app store category.



This above chart shows adware percentages in each game category.

We have only considered the top 300 applications in each category. As such, the statistics include the most popular applications in the Google Play store.

Below is an analysis of a single application flagged as adware on Google Play store :

Application: Windows Live Hotmail PUSH mail

Details

AV results: Flagged by 21 AV vendors

Zscaler static analysis:

Requested application permissions:

- android.permission.READ_SYNC_SETTINGS
- com.android.launcher.permission.UNINSTALL_SHORTCUT
- android.permission.USE_CREDENTIALS
- com.motorola.dlauncher.permission.READ_SETTINGS
- android.permission.ACCESS_COARSE_LOCATION location
- com.motorola.dlauncher.permission.INSTALL_SHORTCUT
- android.permission.READ_SYNC_STATS
- android.permission.WRITE_SYNC_SETTINGS
- android.permission.INTERNET
- com.android.vending.BILLING
- com.lge.launcher.permission.INSTALL_SHORTCUT
- android.permission.SEND_SMS
- com.android.browser.permission.WRITE_HISTORY_BOOKMARKS
- com.android.launcher.permission.INSTALL_SHORTCUT
- com.clearhub.wl.permission.C2D_MESSAGE
- android.permission.WRITE_SMS
- android.permission.ACCESS_NETWORK_STATE
- com.android.browser.permission.READ_HISTORY_BOOKMARKS
- com.htc.launcher.permission.READ_SETTINGS
- android.permission.WRITE_EXTERNAL_STORAGE
- android.permission.ACCESS_FINE_LOCATION location)
- android.permission.RECEIVE_BOOT_COMPLETED
- com.android.launcher.permission.READ_SETTINGS
- android.permission.CALL_PHONE
- android.permission.READ_PHONE_STATE
- com.motorola.launcher.permission.READ_SETTINGS
- android.permission.READ_SMS
- android.permission.VIBRATE
- com.motorola.launcher.permission.INSTALL_SHORTCUT
- com.fede.launcher.permission.READ_SETTINGS
- org.adw.launcher.permission.READ_SETTINGS

- android.permission.ACCESS_WIFI_STATE
- com.lge.launcher.permission.READ_SETTINGS
- android.permission.WAKE_LOCK
- android.permission.READ_CONTACTS
- com.google.android.c2dm.permission.RECEIVE
- android.permission.GET_ACCOUNTS

It can clearly be seen that this application asks for excessive permissions.

By analyzing this app statically, some suspicious privacy related data leakage can be seen :

- Device UDID
- Device IMEI(GSM)/MEID or ESN(CDMA) number
- Device geo-location
- Personal identification information leakage
- Reads contact info.
- SMS activity
- Call activity
- Writes to external storage

Ad related libraries :

- Startapp
- Zestadz
- Admob
- Inmobi
- Airpush
- Mdotm
- Jumptap
- Adwhirl
- Millennialmedia

List of URLs found in source code:

- http://api.airpush.com/api.php
- http://api.airpush.com/model/user/getappinfo.php?packageName=
- http://api.airpush.com/redirect.php?market=
- http://api.airpush.com/testicon.php
- http://api.airpush.com/testmsg2.php
- http://api.airpush.com/v2/api.php
- http://api.airpush.com/v2/api.php?apikey=
- http://cus.adwhirl.com/custom.php?appid=%s&nid=%s&uuid=%s&country_code=%s%s&appver=%d&client=2
- http://met.adwhirl.com/exclick.php?appid=%s&nid=%s&type=%d&uuid=%s&country_code=%s&appver=%d&client=2
- http://met.adwhirl.com/exmet.php?appid=%s&nid=%s&type=%d&uuid=%s&country_code=%s&appver=%d&client=2
- http://cus.adwhirl.com/custom.php?appid=%s&nid=%s&uuid=%s&country_code=%s%s&appver=%d&client=2

As can be seen, the Airpush API is leveraged by this particular application.

Zscaler dynamic analysis:

http://a.applovin.com/ad?placement=com.friendship.quotes.ui.CiteMania&**cpu_speed=4787.82**&**os=4.0.4**&**platform=android**&**model=Nexus+S**&accept=inter_pages,inter_size,custom_size&api_did=&h**udid=378ce8cd300ddae2106ecb3edfb17c89e17e1b1e**&locale=en_US&sdk_version=4.4.0-4.4.0&format=json&total_imps=0&session_imps=0&**network=3g**&sdk_key=6JpJkMwFTFwVz-JemtqwK3soQ6-tsxlJta7Xh8pnGMc5arUpzfeE8Q4hN-vum8UV6xCbBQzdynZ_Ka2hoNG4r-&sources=tpa&size=BANNER&hserial=2f10040ebab09e8887d7c8714eb44f86adc5adb3&**brand=samsung**&**carrier=Android**&app_id=6a5ff889bc4c6910&hphone=4bdd4f929f3a1062253e4e496bafba0bdfb5db75&hanid=ad4aca02186a44b8e31ce35749f3b4737f28c3eb&apps=6a5ff889bc4c6910,febbc860d4d7a2fc,16568adb3f980bfc,0a8e27d912567be3,bfc5013ffc85f778,dbca1157358a2895,27717f5c9c6d559c,fbb138470313edf4,eec390d1aa173f03,e3c4c9788f818fd9,3f816fa6882ad841,2bf5b1f5c88af849,fc991f708b270f04,e2d07cb448d55c1d,a9d65cee7359afc1,12c8b3d835ba9e21,7de8736fbac195c9,6c801094f6504785,e2bc2938862baf48,9c40104f66412490

The URL above illustrates an example of communication sent to the ad network. Advertisers collect such information to develop a profile for the device (and by extension the owner) in order to track the apps that are used so that targeted advertisments can be delivered to the device. The UDID is a unique identifier which can be leveraged to track a specific phone.

Google Play Store apps flagged by more than 15 AV vendors

App Name	VirusTotal result
com.god.lordhanuman.wallpaper	http://www.virustotal.com/file/2f8a1d5bb5dbd66962d30b37a609c7383dd6c9764426f1b8693066e3204e248d/analysis/
zhen.mor.erobik	http://www.virustotal.com/file/983fa56n8e4d88c2ecb4890f5306f8175c5654da64db56cc94396a2a468dddf79/analysis/
com.elift.hdplayer	http://www.virustotal.com/file/61ac5c6e1d65c83a24f0cbd04522cf191dd482f4e4880e834e4eb98857355f15/analysis/
com.nsex.hishar	http://www.virustotal.com/file/35f4710cb074545fe17ce6b2b210c7159384eaec4ee4b77a6f084b28d18d6973/analysis/
prank.xxx.videos.porn.app	http://www.virustotal.com/file/cf1bc23afbdd5b451c883c9e2f728dcf4afc4e110945b45627b04101b9d41552/analysis/
com.mobileriders.sex.workout	http://www.virustotal.com/file/bae10ad31a6a9d9e5131848e1f85d3ad5abc44b9bc0bafad1cbbb958bf65b265/analysis/
com.apptray.dumbbell.workouts	http://www.virustotal.com/file/97bbc480ba361fa483fa4954a52acbcc8c937bd0152d09058fcd7a31a014c69c/analysis/
com.laoyu.ringtone	http://www.virustotal.com/file/aa968157319a85b2c7ee9fe9a405184c5dd1ce0ab5971e13e33422b83bf0cd2e/analysis/
com.huashao.threeD	http://www.virustotal.com/file/885a97cdae23b1c0989cf8b29c01640620504c199e7c1724dcb3b2aaf2ff4344/analysis/
com.wangsong.costwatcher	http://www.virustotal.com/file/cf6b90580b92346c8f1fb9b3558925f1eeae1e8e8fbfac42283388e677a189f6/analysis/
com.huashao.Scary	http://www.virustotal.com/file/6233cb4641c1042a1d8880e4843f1b848fcba567c47a6649cb1d51db04c460ee/analysis/
com.god.lordvishnu.wallpaper	http://www.virustotal.com/file/5fe938ccc2fe4668795f3ea527a0c16b5a9fc7d78d70ee3bd43d18b344bd96db/analysis/
com.god.gurunanak.wallpaper	http://www.virustotal.com/file/f39cb97d259b2e4c9fde915f3792e34a700a74c97b3125c4772984a62e592794/analysis/
zhen.mor.saotyi	http://www.virustotal.com/file/360efd96e5db9ac8683930eb445ac76435b39ac38ef8ed13320207822766f7e5/analysis/
com.experience_game_3d.truck.parking	http://www.virustotal.com/file/2e941c7ff48409c8e139aec0a3db3af84676a2fc6beea7877689eb43cee56363/analysis/
yong.universalplayer	http://www.virustotal.com/file/d6675e3b833c8f4805f99198dc7ba85810d34041e08ceb72314b5b8b3ba32c12/analysis/
com.mine.videoplayer	http://www.virustotal.com/file/d72a0df97250f990d325714c9d9f69a5ec1595b2cad2f80a427cb1c064f7c238/analysis/
bys.widgets.lordvenkateshwara	http://www.virustotal.com/file/4a939c5a1f23ead3cd7a4bda7aebc7ca750fdc50484b110c34bb53f72306c892/analysis/
droids1.prasad.shiv3d	http://www.virustotal.com/file/16f7e29768665a7f66c666f035ce855bcf1e4f2640375cc63b96ddba71fde49b/analysis/
com.muk.durga	http://www.virustotal.com/file/d2196932ad4c343574cf2ef0dd51410a0052638e864c5e7caf1d12ed36f3e775/analysis/
com.muk.hanuman	http://www.virustotal.com/file/fc6cad34884e56a44ffa0de4acfd627113aa47fac80130e4c726486427c54010/analysis/

com.muk.lakshmi	http://www.virustotal.com/file/4ffc0d56ae32d36839b97e5bf4420bfe50b1968104f82f31bcbf3f27e9275c7d/analysis/
com.wind.funnyphoto	http://www.virustotal.com/file/d5d75fd12bc7aae28603f883eb39eacf784a616e16f1395696701581de014638/analysis/
com.outthinking.textonpic	http://www.virustotal.com/file/6a4bebaa2bb21634aab5082362e22ba022eeaa143610aa3d3184dda996eb59ae/analysis/
com.face.warp.deformer.distortion	http://www.virustotal.com/file/936978dce7a042efb7b1aebc6f8ed3b699457ccb6eb161020aae537cbfb836ce/analysis/
com.learn.effectone	http://www.virustotal.com/file/9603b8b2b74b84292e7275eee5311bbb6c959898bec26d438e73dfc9405d6784/analysis/
com.sweetsugar.whatsapplock	http://www.virustotal.com/file/5220608a893ddead034fb8f219ec763dfe9406c52487d13b288e4e81eac67078/analysis/
com.clearhub.wl	http://www.virustotal.com/file/f4e9ba663b5a9b2e95e22925799479c36b9fd55b57ce848ea1b79c6392ea91e5/analysis/

Why this is happening? Why are AV vendors flagging a huge number of applications as adware while Google is freely permitting them into the Google Play store? The excessive use of advertisements can negatively impact customer privacy and result in a negative user experience. On the other hand, advertisements are necessary for app developers looking to earn money when providing free apps. So where should the line be drawn? Google has clearly chosen to be very lenient with aggressive advertising practices, while Apple has taken the opposite approach, as they have shown that they're willing to sacrifice advertising revenue to provide a positive user experience, even restricting the ability of advertisers to track device IDs and MAC addresses.

How do we define adware? We feel that adware exhibits one or more of the following intrusive behaviors without requesting appropriate user consent:

- Harvests excessive personally identifiable information
- Performs unexpected actions in response to ad clicks without appropriate user consent (appropriate user consent entails providing a clear alert in the application that the user can accept or decline before any behavior takes place)
- Collects IMEI numbers, UDIDs or MAC addresses
- Initiating phone calls and SMS messages
- Changing wallpaper and ringtones
- Leaks location information
- Leaks email addresses
- Leaks personal information such as contacts, birthdays, calendar appointments, etc.

Reference : https://www.lookout.com/

We base our own categorization of adware-enabled apps on the aforementioned definition. Hopefully Google and the AV vendors can reach a compromise in this ongoing adware battle as at present, end users are paying the price.