1.2 Percent of Google Play Store is Thief-Ware, Study Shows

More than 1 percent of some 420,646 apps are stolen from other developers and re-engineered for illicit gains, according to a new Bitdefender survey on Google Play. The study shows that applications uploaded by 2,140 verified developers are over 90% identical (library code aside) to the work of other developers on the official Android Store.

To be considered a copy, the two software pieces need to share more than 90 percent of the code without including the library code – the bits of code that can be legally used by multiple developers. For instance, an advertising SDK is a library code, or a piece of code that can be used in more apps to show ads.

“These duplicates or repackaged applications should not be mistaken with different versions of an app,” said Bitdefender Chief Security Strategist Cătălin Cosoi. “Here, it’s about a publisher who takes an application, reverse-engineers its code, adds aggressive advertising SDKs or other beacons, then repackages and distributes it as his own.”

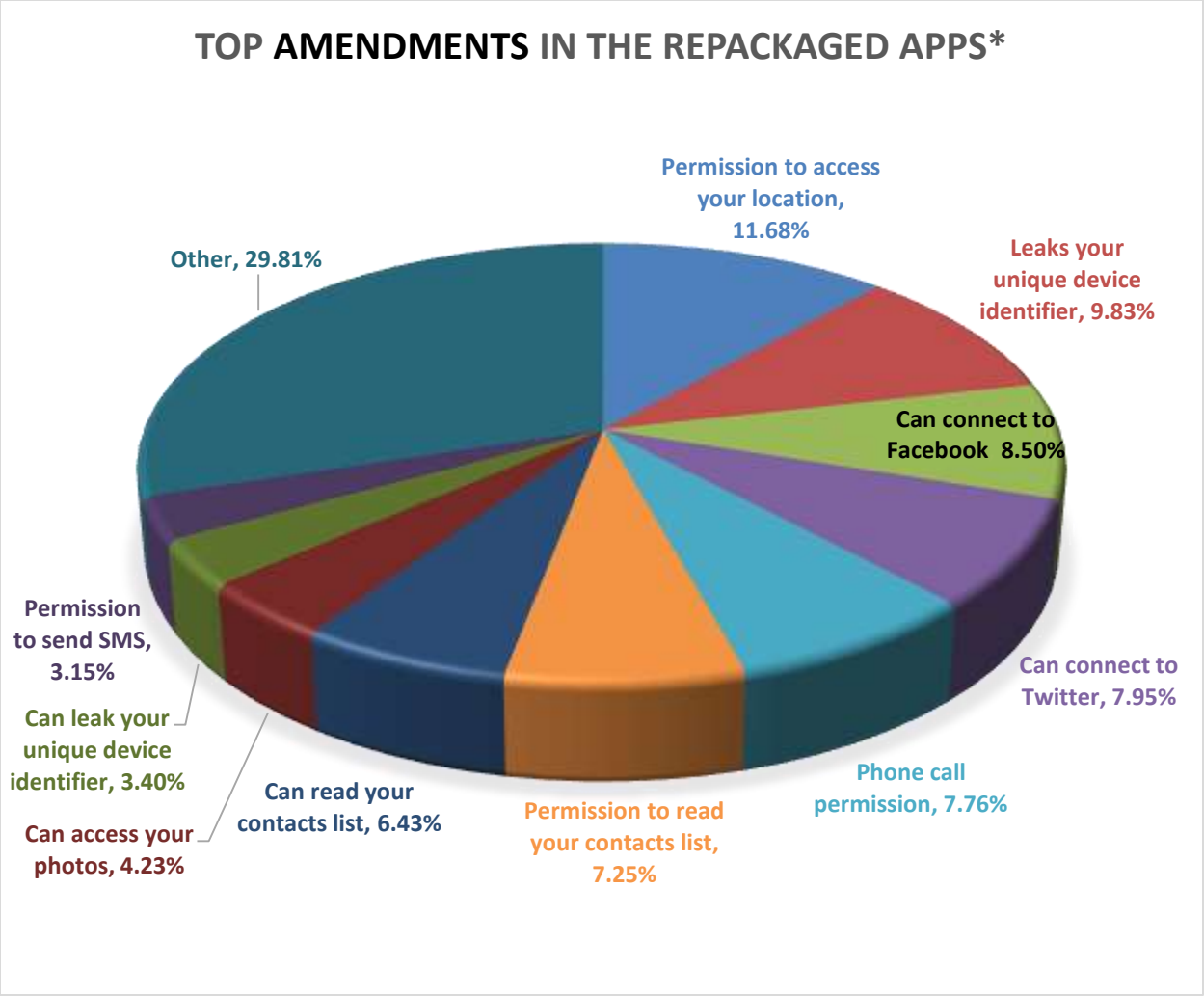
Out of the 420,646 applications analyzed, more than 5077 APKs have been copies of other apps in Google Play. Some came with extra modules that radically modify the way the application behaves on the device it is installed on. Some of these applications contain additional modules that are used to access location, to leak the device ID or to connect to social media platforms such as Facebook and Twitter.

Reverse-engineering and APKs

By design, Android applications can be disassembled, modified and reassembled to provide new functionalities. This way an attacker can easily rip an APK off the Play Store, turn it into program code and modify it as.

Most modifications add a new Advertising SDK in the repackaged app or change the Advertiser ID from the original app so revenue obtained through ad platforms gets diverted from the original developer to the individual who plagiarizes their work.

Other modifications add extra advertising modules to collect more data from the user than the initial developer planned. Moreover, if a developer only collects UDIDs and e-mail addresses initially, a plagiarized application can be extended to place home-screen icons, spam the notification bar and so on to maximize the hijacker’s revenue.



*actions that were not asked in the original app, but are present in the repackaged version.

The above graphic shows what publishers choose to sneak into repackaged apps. Some 7.76 percent of amendments to the repackaged apps could allow an unauthorized party to make phone calls from the mobile device, and 7.25 percent allow someone to read the call history. While some apps may legitimately need to access some data in the phone and explicitly ask for the owner's permission, others access this kind of info without explicitly needing it to perform adequately. Permissions that allow apps to send SMSs sum up to 3.15 percent, while some apps may even read the contact lists and access the photos in the handset.

After these modifications have been made to the original application, the plagiarist sets up a publisher profile with Google Play, uploads the modified APKs and waits for users to install the application.

Airpush, Apperhand, InMobi, Leadbolt and Jumptap are the most frequently used advertising SDKs (listed in order of frequency) that were found in the analyzed repackaged apps, the Bitdefender study revealed.

Instead of spending thousands or hundreds of thousands of dollars developing, testing and marketing a great application to monetize, plagiarists take the road that is less time-costly and less resource intensive by simply hijacking a successful application at the original developer's expenses.

Theft damages both consumers and developers alike

Social media mobile apps such as Facebook and Twitter draw hundreds of millions of installs – and the attention of plagiarists. We found some duplicates of the original apps that offer exactly the same functions as the original except colors and background. Due to the popularity of the original apps, Facebook and the Twitter copycats also enjoy great popularity, with 10,000 to 50,000 installs each.

Some other plagiarists make money by adding an extra advertising SDK to the original code and repackage it into a brand new app. This way the fraudulent developer redirects gain from the developers of the original applications to his own pocket, which impacts the return on investment and may even discourage a small developer from releasing new versions of the application.

This type of theft also impacts the end consumer: while a legit developer tries to protect the reputation of its work and balances ad revenue with the amount of intrusion into the customers' private life, plagiarists may be less scrupulous and try to profile the users and their devices. Moreover, the client of a repackaged app receives no updates or support from the plagiarist developers.

Incalculable loss of business

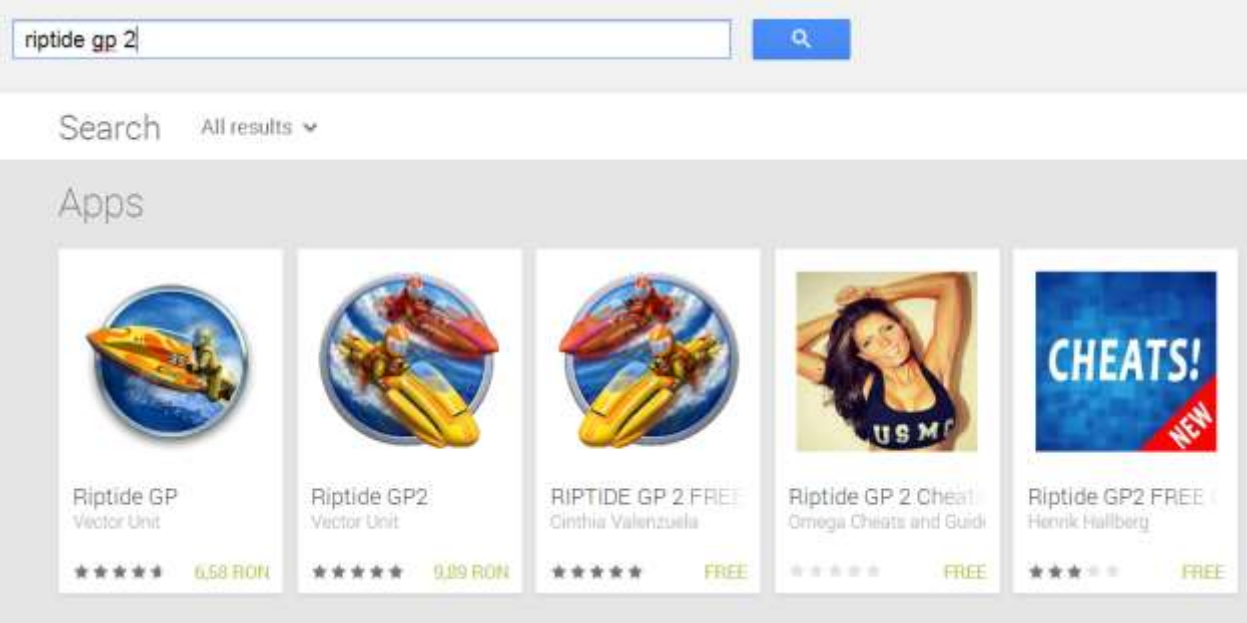
The real financial impact of plagiarism on the developer is difficult to compute, as all cases of intellectual property infringement. However, it appears the revenue the plagiarists collect from hijacking applications is enough of a motivation to keep them in the game: as this practice is not tolerated by Google Play, detection automatically results in the termination of the associated developer account.

Since a developer account costs a one-time fee of $25, plagiarists have to constantly spend money in creating new accounts that will distribute the counterfeit application until these get reported and terminated again. However, these accounts are suspended almost daily, adding to the plagiarist's monthly expenses – expenses that are undoubtedly covered by the fraudulent money they get – or otherwise the business would not be profitable at all.

Case study

After profiling the repackaged versions of Riptide GP2 Vector Unit game, Bitdefender identified that the copies let ad networks access, collect and send some sensitive data.

The original application costs around $3. In a week, four different copies of it surfaced in Google Play. Three vanished immediately, but a fourth is still in store.



Unlike the original app, the repackaged games were distributed free of charge.

Application	Installs	Revenue
Repackaged #1	**100-500**	**$200-$1,000**
Repackaged #2	**1,000-5,000**	**$2,000-$10,000**
Repackaged #3	**1,000-5,000**	**$2,000-$10,000**
Repackaged #4	**1,000-5,000**	**$2,000-$10,000**
Total	**3,100-15,500**	**$6,200-$31,000**

If we consider only these four instances and their download/install rates, and presume that all those that downloaded the copies bought the original app, the developer of the original code might end up losing between 3,100 and 15, 500 clients and some $6,200 and $31,000.

The information sent remotely is comprised of the unique device ID and the exact location of the user. The repackaged apps also automatically add icons on the device home screen, pop unsolicited ads in the notification bar and opens unwanted webpages in browsers.

Android users are advised to exercise extreme caution when installing apps and to always check for what permissions they require. Installing a mobile security solution, such as Bitdefender Mobile Security, that detects virulent adware helps users keep their data secured. Bitdefender also recommends Clueful for

Android, a free app that offers an expert opinion on how apps treat your privacy once you install them on your handset.

This article is based on the technical information provided courtesy of Bitdefender Clueful Team.

Note: All product and company names mentioned herein are for identification purposes only and are the property of, and may be trademarks of, their respective owners.