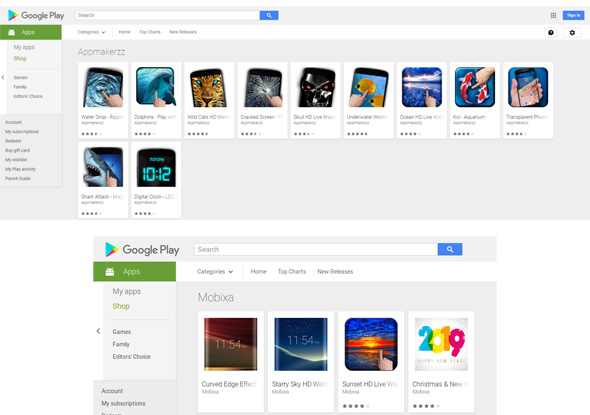
**Android Wallpaper Apps Found Running Ad Fraud Scheme**

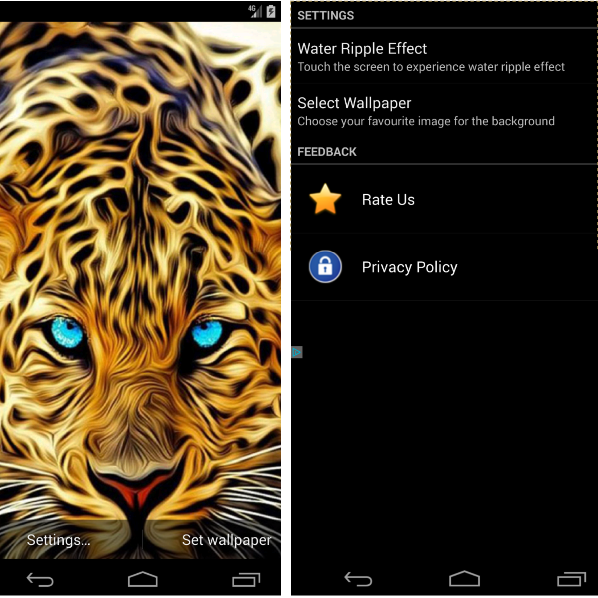
We detected 15 wallpaper apps available in Google Play Market committing click ad fraud. The said apps have been collectively downloaded from Google Play more than 222,200 times at the time of writing, and our telemetry showed Italy, Taiwan, the United States, Germany and Indonesia with the most infections recorded.



*Figure 1. Mobile apps available for download in Google Play Market.*

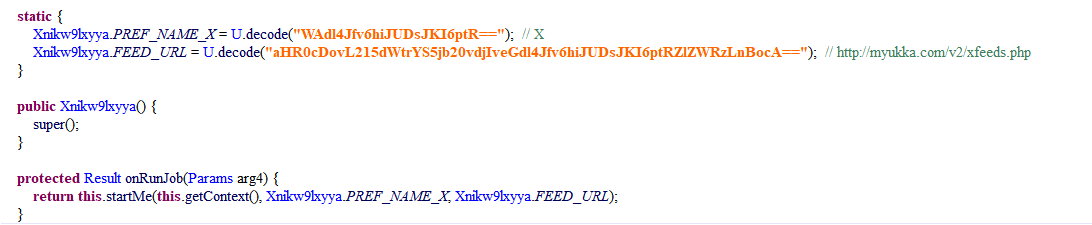
***Behavior***

The apps were designed with enticing icons that promise beautiful mobile wallpapers. The apps themselves also have high user reviews and good comments, but we highly suspect that these reviews are fake and meant to project credibility to users.



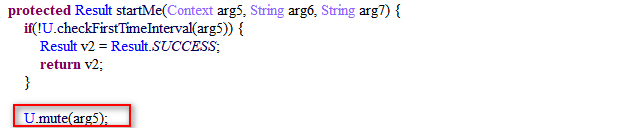
*Figure 2. Wild Cats HD Wallpaper app has been downloaded more than 10,000 times. Review of the app was ranked 4.8 on Google Play.*

Once downloaded, the apps decode the command and control (C&C) server address for the configuration.



*Figure 3. C&C server address decoded and run.*

The entire process is muted to hide the activity from the user. An HTTP GET request is communicated to the C&C for a JSON-formatted list once the app is launched.



*Figure 4. The entire process is muted.*



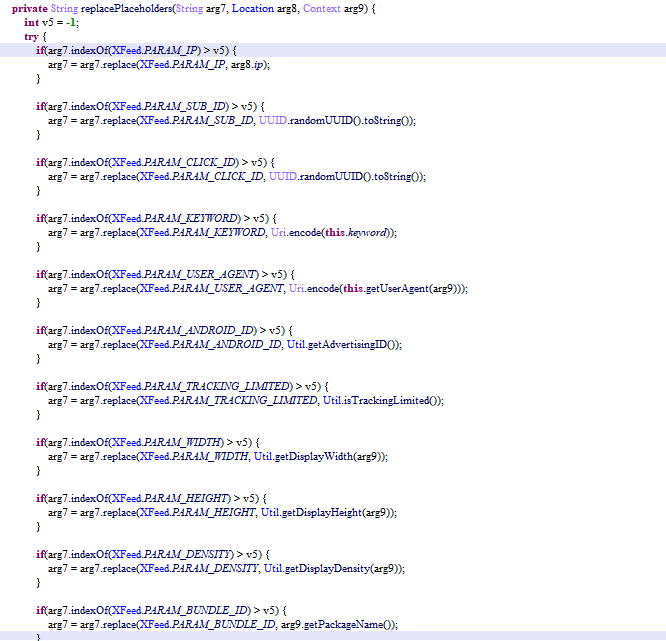
*Figure 5. C&C server response.*

When the feed runs, each initialized feed and object includes a *fallback\_URL*, *type*, *UA*, *URL*, *referer*, *x\_requested\_with*, and keywords.



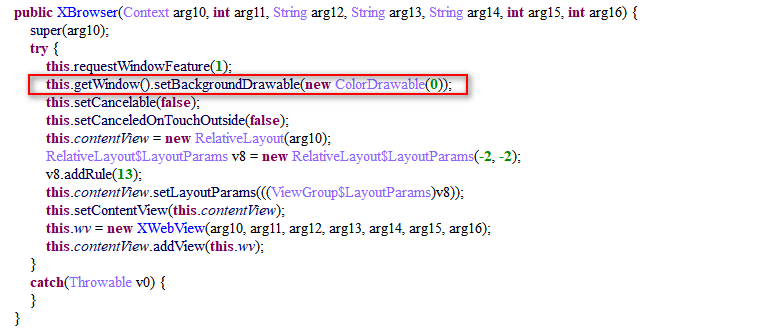
*Figure 6. Initialized feed list.*

The apps then get the advertising ID from Google Play Services, and replace some parameters such as the URL, ANDROID\_ID with the advertising ID, replace BUNDLE\_ID with the fraudulent app’s package name, replace IP with the infected device’s current IP, and more. After replacement, the URL is loaded according to the type.



*Figure 7. Constructing a fraudulent fallback\_URL.*

While loading the URL, the browser background will be set to transparent.



*Figure 8. Background set to transparent.*

After the URL loads, the apps begin to simulate clicks on the ad page.



*Figure 9. Simulating fake ad clicks.*

The cybercriminals profit through the parameters’ value replacement. IDs provided by Google Play for Android developers such as the advertising ID, advertiser ID and device ID are anonymous identifiers specific to users to monetize their apps. The app replaces ANDROID\_ID, BUNDLE\_ID, IP, USER\_AGENT with the ad ID, the app’s package name, current IP, and the user agent of the current browser. These are all in the *fallback\_URL* from the configuration file, creating a fraudulent *fallback\_URL* for fake clicks. For example, the original would be:

[http://pub.mobday.com/api/ads\_api.php?ver=1.2&pubid=1022&adspace=1007&advid={ANDROID\_ID}&bundle={BUNDLE\_ID}&ip={IP}&ua={USER\_AGENT}&cb=5c1236f316e45](http://pub.mobday.com/api/ads_api.php?ver=1.2&pubid=1022&adspace=1007&advid=%7bANDROID_ID%7d&bundle=%7bBUNDLE_ID%7d&ip=%7bIP%7d&ua=%7bUSER_AGENT%7d&cb=5c1236f316e45)

This will be replaced with:

[http://pub.mobday.com/api/ads\_api.php?ver=1.2&pubid=1022&adspace=1007&advid=260903559217b3a8&bundle=com.amz.wildcats&ip= 203.90.248.163&ua=Mozilla/5.0 (Linux; Android 6.0.1; MuMu Build/V417IR; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/52.0.2743.100 Mobile Safari/537.36&cb=5c1236f316e45](http://pub.mobday.com/api/ads_api.php?ver=1.2&pubid=1022&adspace=1007&advid=%7bANDROID_ID%7d&bundle=%7bBUNDLE_ID%7d&ip=%7bIP%7d&ua=%7bUSER_AGENT%7d&cb=5c1236f316e45)

***Trend Micro Solutions***

Google has already removed all identified malicious apps. Users have to be vigilant and be cautious of the apps they download, as cybercriminals will continue manipulating app features to profit and attack. Mobile devices have to be protected with a comprehensive security structure and program against mobile malware.

[Trend Micro Mobile Security](https://www.trendmicro.com/en_us/forHome/products/mobile-security.html?_ga=2.144631986.642837046.1542587339-1577535324.1526018629) detects this threat, and [Trend Micro Mobile Security Personal Edition](https://play.google.com/store/apps/details?id=com.trendmicro.tmmspersonal.apac) and [Mobile Security Solutions](http://www.trendmicro.com/us/enterprise/product-security/mobile-security/) defends devices from all related threats. [Trend Micro’s Mobile App Reputation Service](https://mars.trendmicro.com/) (MARS) covers Android and iOS threats using leading sandbox and machine learning technologies to protect users against malware, zero-day and known exploits, privacy leaks, and application vulnerability.

***Indicators of Compromise***

|  |  |  |
| --- | --- | --- |
| **PackageName** | **SHA256** | **Installs (as of 12/14/2018)** |
| com.amz.wildcats | 0995b52a9a12cf31ae19c360d56ca1a20d784eecc9b018514dbf01446f4ad36e | 10,000+ |
| com.amz.underwaterworld | 1f6907b2e8f7fa7597a28b2e7133325fcddb3e4f9e1c3cbad82afaa82bf3c57e | 5,000+ |
| com.appmakerz.dclock | b098d0ee0766558dff37761358d250a7b648c1de1556bd0345564b74a6db848c | 50,000+ |
| com.appmakerz.shark | fbcc2c9ddc69c0f272f80051987b5ed911cd112ef6e26709b54e67cae7ce1fb6 | 50,000+ |
| com.appmakerz.xphone | aec79ed8cb779474a058e89bd4f1a55a534d439af5d48751867300a885d50182 | 10,000+ |
| com.appmakerz.dolphins | 48d7ebf7fd65cb317e52c5d331d193bfaf3f48590b8f598292be88f26dc8464e | 10,000+ |
| com.appmakerz.ocean | 034aa9f3ceeb74acf38c0f4036bb0e89339759ed73de009207c7036eb25e14a5 | 10,000+ |
| com.appmakerz.waterdrop | 8d643500319bd9e4eb2007ac43613bf53943b65dff25ee933d5450ecc11402b8 | 10,000+ |
| com.appmakerz.koi | 8f16246b9afc1dfb89ca8b60f1b097584b94034e0de6496bbc28e58d667c4af5 | 10,000+ |
| com.appmakerz.crackedscreen | a2ef230d3b091c0571bb0c96b456c17f94a176a2861281b6ff0b56e789e17b64 | 50,000+ |
| com.amz.skull | ee6ef277ea9d8478965452e10c0c01cd7a4d13c1cd23e9ee8d2668a715f7a6b5 | 5,000+ |
| com.mobixa.curvededges | fa8f9d3415bc38b679204f2c8fd983e12298e014007f2a18f7501e3c1d3d1910 | 100+ |
| com.mobixa.starrysky | bf016cf1142b17c5a088a80feb88fb10ab9be05c20133931b7190e352a1f1b08 | 100+ |
| com.mobixa.sunset | bc8237bf6a9b25e71bb55c0841c1ee6ef443835bf172666a680f74badadf34f8 | 1,000+ |
| com.mobixa.christmas | d34598835b28a6ad070dd0986b0bbc336c8ba7cac9a9a22d6b3c6a99049242a6 | 1,000+ |

C&C Server

http[:]//myukka.com/v2/xfeeds.php

http[:]//198.1.125.77/tracking/config.php