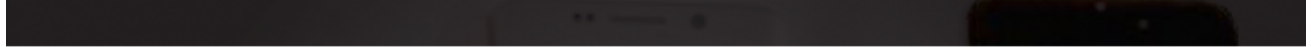


Quick Heal reports 29 malicious apps with 10 million+ downloads on Google Play Store

 blogs.quickheal.com/quick-heal-reports-29-malicious-apps-10-million-downloads-google-play-store/

September 24, 2019



Quick Heal Security Labs reported 29 malicious apps found on Google Play Store, which have a collective download count of more than 10 Millions. Google was quick enough to remove these malicious apps from Play Store immediately. One of the Apps from this set, named “**Multiapp multiple accounts simultaneously**” has crossed 5 million installs already.

Fig. 1– Malicious HiddAd Apps from Google Play Store

From this set of 29 malicious Apps, 24 are from HiddAd category. The HiddAd Apps hide their icon after first launch and create shortcut on Home Screen. Clear purpose of this action is that users should not be able to uninstall it by just dragging the icon. When users launch the App through the shortcut, these apps show full screen ads on device screen. Few of these Apps can show adds even when the device is in idle state and the App is not in active use. Most of these Apps are of Photography category and are similar to previous HiddAds found on Google Play Store. Fig. 1 shows screenshots of malicious HiddAd Apps from Google Play Store.

The remaining 5 Apps from above list are of Adware category and would generally get into your Android phones through advertisements. Users see many advertisements every-time they visit social media sites like YouTube, Facebook, etc. which promote different mobile applications. Many a times, these promoted mobile applications boast about a lot of unbelievable functionalities like X-Ray scanning. We came across few advertisements of

some interesting Android Apps which claim to offer functionality of X-ray scanning. When we explored the App further, we found out that two such apps have crossed 1 million + downloads already.

Here is a screenshot of such an advertisement we came across on YouTube, prompting users to download one of the magnifier application –

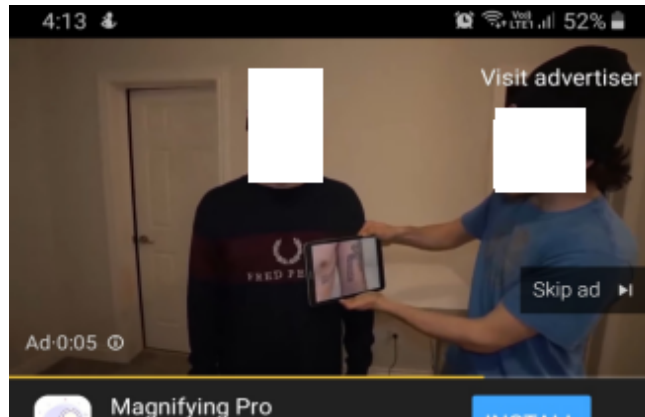


Fig. 2 – Advertisement screenshot from YouTube

In this Advertisement, it claims that it can scan human body like X-ray scanning machine. But obviously, this app doesn't have any such functionality. We can guess that many users are tricked into downloading this App and they end up with annoying advertisements. During our analysis, we found around 5 applications with similar functionalities.

Analysis of HiddAd malware Apps:

HiddAd malware App hides its icon after installation and its first launch. It creates shortcut on Home Screen. We analyzed one of these HiddAd malware App in detail. It directly uses *setComponentEnabledSetting* method to hide its own icon, without any obfuscation. This is little different from most of the HiddAd malware which we analyzed earlier and they were using some obfuscation techniques to evade detections.

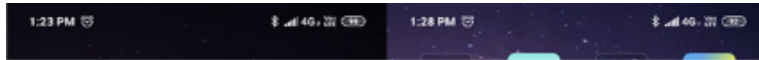


Fig. 3 – Screenshot of HiddAd activity

This HiddAd App has following code to decide when to show Ads. The function name itself tells its purpose. The following code snippet clearly shows that App installation time is saved in one variable and then depending on that value, it decides the exact time to show Ads.

Fig. 4 – code to decide Ad display time

In one of these Apps, named “First camera HD”, malware author has used a different technique. In this apk, there is an encrypted file present in its “assets” directory. This file gets decrypted at runtime and it creates odex file (Optimized dex file) in “data\data\com.first.app.camera.spitel\files\podex\odexdir”.

Later it deletes this created odex file runtime. We analyzed this file by fetching it from our emulator and found that it has similar code. Below code snippet shows how it decrypts and create odex file –

```
securename5 = "0000011111";

File secureDataFile = new File(new StringBuilder(String.valueOf(Appfiledir)).append("/").append(securename5).toString());
if (!secureDataFile.exists() || secureDataFile.length() == 0) {
    SafeUnzipFile(apkzf, "assets/" + securename5, secureDataFile, 0);
}

DeleteFile(new StringBuilder(String.valueOf(Appfiledir)).append("/").append(securename5).toString());
```

Fig. 5 – odex file creation

Quick Heal Total Security for Mobile detects these applications as **Android.Hiddad.A**

Analysis of Adware Apps:

These Apps pretend to offer a functionality of magnifying the view, but in reality these Apps just show heavy Advertisement on user's mobile, eventually draining phone battery and causing heavy data usage and productivity loss.

Right after the launch, these applications open camera and show various options like flash-light, gallery, etc. But when user chooses an option, these apps start full-screen Ads, with no option to close or skip. Initially there is no way to close these Ads and it takes considerable time to show Close Ad button. These Ads are continuous and annoying. Even if user gets a chance to close one Ad, it will again open another Ad immediately and won't allow to use the real application functionalities.

Fig. 6 – Screenshots of Adware activity

From the user reviews, it seems that user is trapped/lured in installing these Apps.

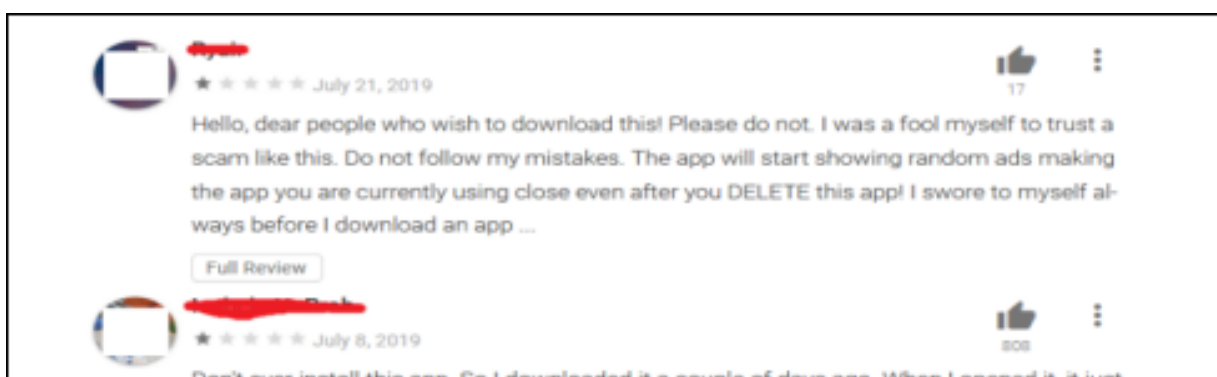


Fig. 7 – User reviews

Quick Heal Total Security for Mobile detects these applications under the Adware category as **Android.Magnify.A (Adware)**

Application name	Package name	Download count	Category	Ratings
------------------	--------------	----------------	----------	---------

Fig. 8 – IOCs

Threat actors are continuously trying to find new ways to enter into the user's device and earn money through advertisements. So, user should not fall prey for this and should not install any random mobile application coming from social platforms blindly. Rather, user should check App Developer's information and reviews before downloading any app.

Tips to stay safe from Android malware:

- Check an app's description before you download it.
- Check the app developer's name and their website. If the name sounds strange or odd, you have all the reasons to suspect it.
- Go through the reviews and ratings of the app. But, note that these can also be faked.
- Avoid downloading apps from third-party app stores.
- Always keep 'Unknown Sources' disabled. Enabling this option allows installation of apps from unknown sources.
- Most importantly, verify app permissions before installing any app even from official stores such as Google Play.
- Use a reliable mobile antivirus (like Quick Heal Total Security), that can prevent fake, malicious apps, adware, etc. from getting installed on your phone.

- Limit yourself to known apps from known developers and keep only those apps on mobile that are really needed.

Although Quick Heal's Security Lab is constantly on the lookout for malicious activities happening against Mobile Devices, prevention is always better than cure. Our modern world has absolutely brought mobile devices at the forefront of how we conduct our day to day lives.

Communication, e-commerce, entertainment, logistics, even office work is all being conducted today via mobile devices. Evidently then, any type of breach to mobile devices personally used will bring life to a standstill, create panic and cause extreme inconvenience. To avoid this unpleasant scenario leverage on Quick Heal's enterprise-grade [Total Mobile Device Protection for Android](#) product, and safeguard your valuable mobile devices.



Digvijay Mane

Copyright © 2025 Quick Heal. All rights reserved.