

Auto-launching HiddAd on Google Play Store

 blogs.quickheal.com/auto-launching-hiddad-on-google-play-store-found-in-more-than-6-million-downloads/

July 28, 2022



HiddenAd or **HiddAd** are icon-hiding adware applications. The prime motive of HiddAd is to generate revenue through aggressive advertisements. As long as HiddAd remains on the device, it will generate revenue for the malware author. To make uninstalling difficult, malware authors hide the application's icon from the application drawer. They also use different deceptive techniques to make uninstallation less intuitive to the users.

HiddAd is not a new thing for the Google Play Store. We have seen many such malware applications on the Google Play Store in the last 3-4 years.

- In May 2018, researchers found 38 HiddAd applications on the Google Play Store disguised as games and education applications. These applications were found to be displaying ads and redirecting users to install another application. For hiding the application icon, these applications used ***setComponentEnabledSettings*** API. These applications have added another layer of deception by using **different names on the Google Play Store and different application names after installation**. This name change made it even more difficult for the users to identify the app and remove it from their devices.

- In the same month, another researcher found the HiddAd application on Google Play Store that was **forcing users into leaving 5-star ratings** in order to remove ads from the app. This is to increase its reach, as a good rating was intended to increase its download probability. In June 2018, a HiddAd application bike racing game was found, making uninstallation difficult by using **device admin permission**.

2019 is known as the year of HiddAds, as many such applications were reported in that year.

- In the month of Feb 2019, 40 HiddAds were reported to be **using social media to spread**.
- In August, 85 Photography and Gaming applications **recorded timestamps and started showing ads 30 minutes after the first launch**.
- In September 2019, 25 new HiddAds were reported **using configuration files to hide their icon**.
- Similarly, in Oct, another 15 applications were reported that used **deceptive application icons and names that resemble a system application**.

We observed similar cases in the year 2020 related to the HiddAd applications. In Feb 2021, the updated version of the Barcode scanner application with 10 million downloads was found to be HiddAd.

Quick heal researchers also contributed to this HiddAds by reporting and removing several HiddAds from Google Play Store.

- In [August 2018](#), we found 8 HiddAd applications on Google Play Store which were using application names such as Google Play Service or Google Play Store and icons of genuine apps such as Google Play Store, default Android icon, or YouTube.
- In [September 2019](#), we reported 29 HiddAds with 10 million+ downloads using different techniques to hide their code.
- In [March 2020](#), Quick Heal researchers reported another 15 HiddAds to Google.

Recently we found 14 such applications on Google Play Store. The download count of all these applications is more than 6 million. These applications are HiddAd malware and execute themselves without user interaction. We have denoted them by naming them “**Autolauncher HiddAds**.” Fig.1 shows icons of malicious applications.

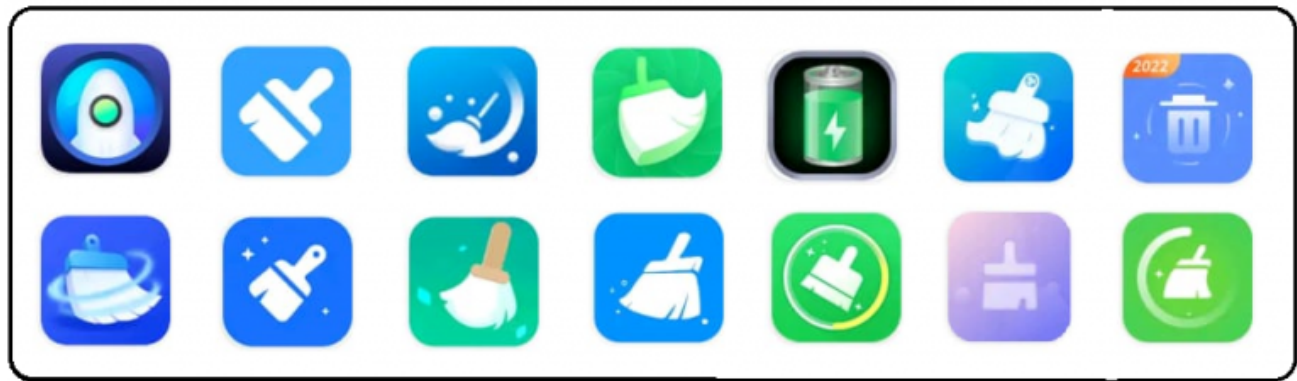


Fig.1 Application icon

Now let's have a look into one of these applications.

Application Name: Windy Clean

MD5: 2e4649e88bd9ae39d66b92f473fae8e9

As soon as we installed the application, it immediately started its activity. We didn't have to take any action as we did not even click on its icon to run the application. It hides its icon from the application drawer and starts displaying overlapping pop-up advertisements. Fig. 2 shows pop ads shown by malicious applications.

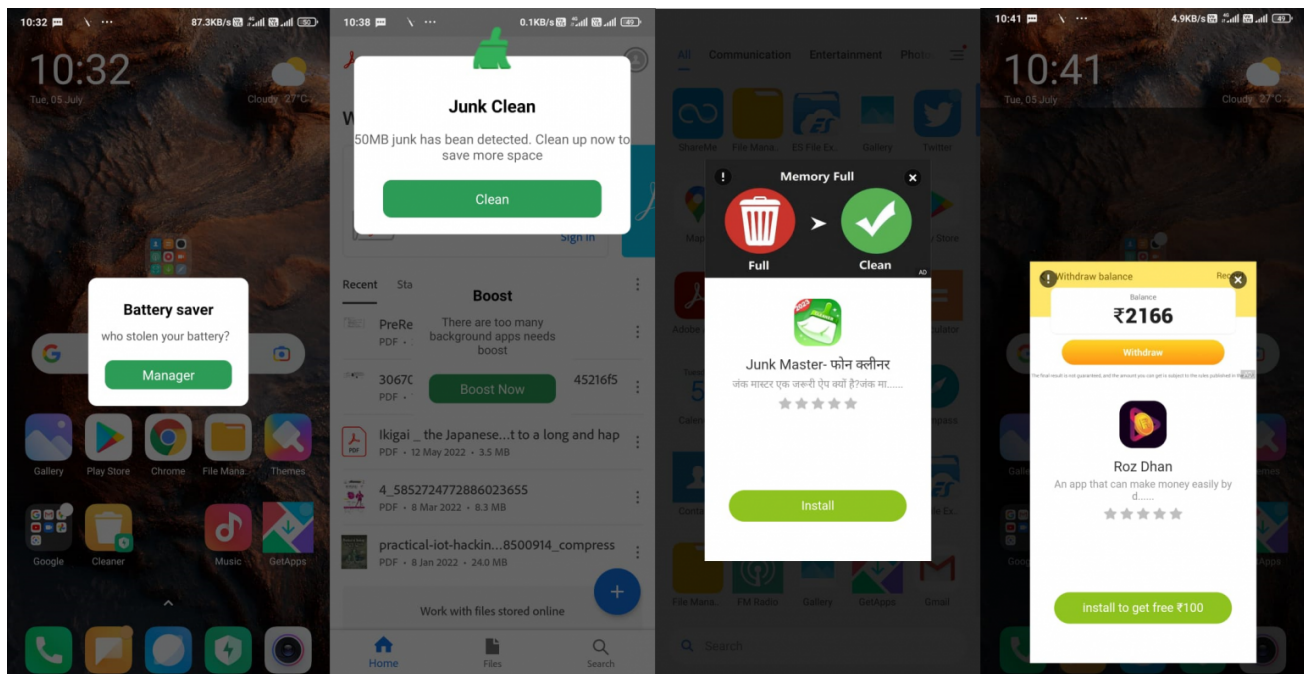


Fig.2 Malware application showing ads

In the background, as soon as the installation is completed application requests the advertising server. It sends information about OS, phone, etc. In response, it gets encrypted info about the advertisement.

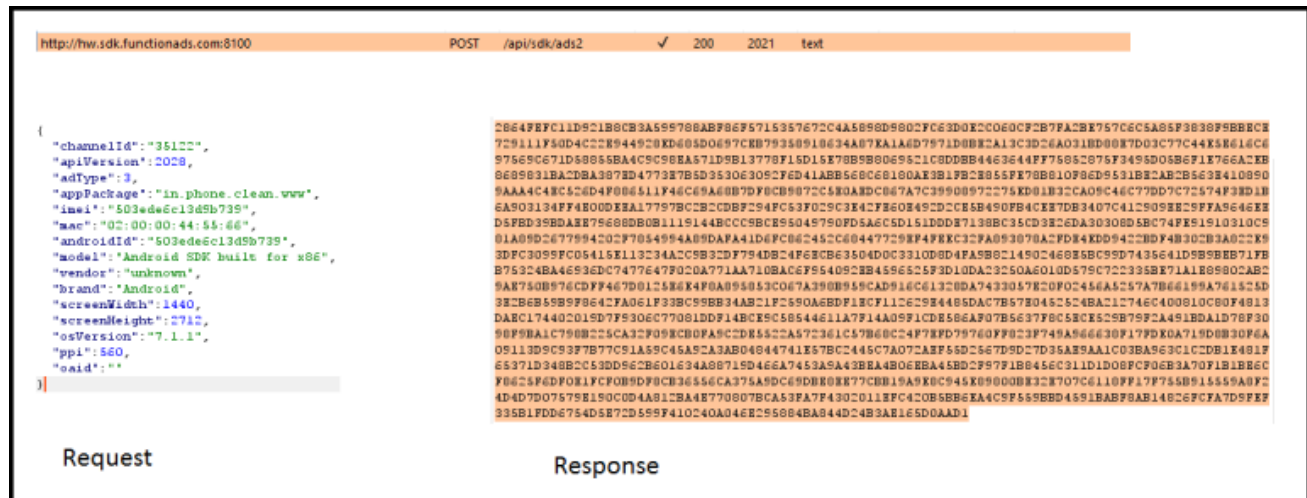


Fig.3 Malware makes this request as it is installed

This application uses a broadcast receiver to execute the code on various system broadcasts: –

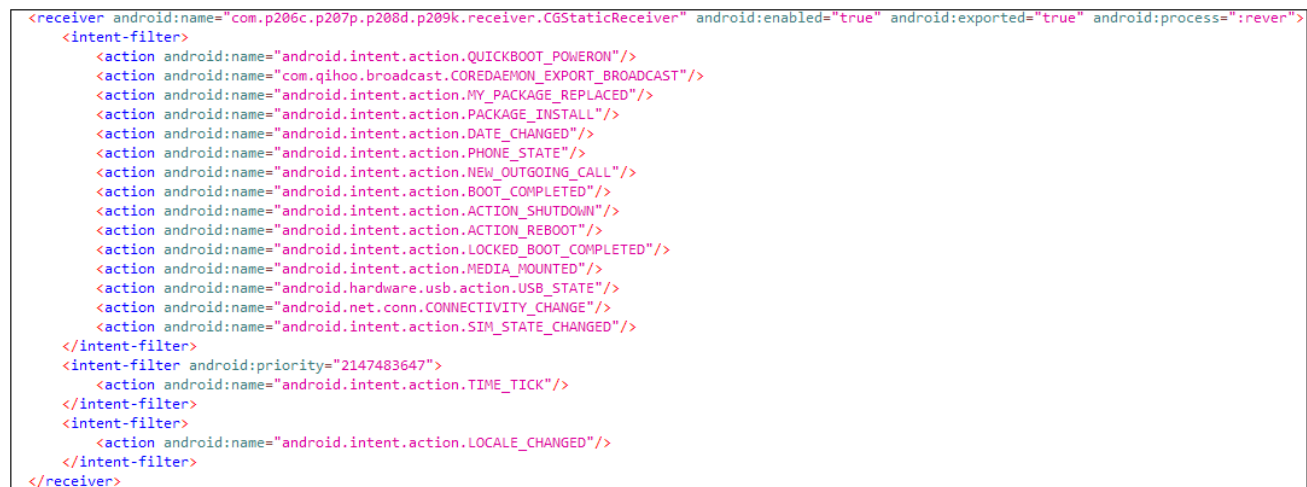


Fig. 4 Broadcast Receiver's intent filter

These applications show aggressive ads overlapping other applications, which can be very annoying for the users who install them. Some users have expressed their anger by writing bad reviews about the application.

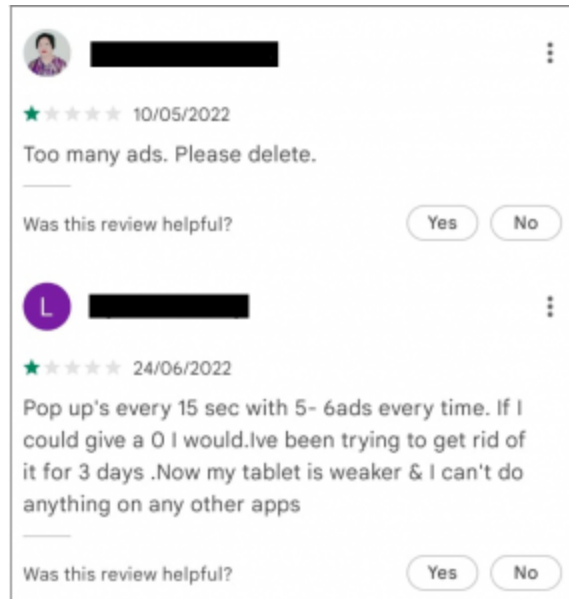


Fig.5 Users expressing their anger

As illustrated in the following table, all these applications are reported from the Tools category. They claim to provide free android cleanup and enhancement programs, phone acceleration, CPU cooling, garbage cleaner, battery saver, virus scanning, etc. They use these claims to reach out to more users and increase the download count. Each application is published from a different developer account, but all of them have a similar code structure and malicious behavior. Most of these applications were recently released on Google Play Store.

Application Name	Developer	Downloads	Published date
Windy Clean	Dale A McConnell	500k	15-Jun-2022
Meteor Clean	Abigail R London	100k	20-Jun-2022
Concise Clean	Zhou Yajun	100k	23-Jun-2022
Universe Clean	Shen Huangying	100k	21-Jun-2022
Carpet Clean	fouesenouerds	500k	9-Jun-2022
Strong Clean	Xia Hang	500k	7-Jun-2022
Multifunction Clean	Tang di	500k	15-Jun-2022
EasyCleaner	PeiGao Zhang	100k	14-Mar-2022
space clean	Lv Yuqing	100k	23-May-2022
Super Clean	李湘	500k	23-Mar-2022
Junk Cleaner	葛洪武	1M+	26 April 2022
Power Doctor	Exhibition snow	500k	23 April 2022
Keep Clean	Aurore Wisozk	1M+	19-May-2022
Fingertip Cleaner	Fan Jianwu	500k	11-May-2022

Fig. 6 Application information

IOC List:

Quick Heal Security Labs detects these apps with variants of Android.Hiddad:-

Application Name	Package Name	MD5
Windy Clean	in.phone.clean.www	2e4649e88bd9ae39d66b92f473fae8e9
Meteor Clean	org.ssl.wind.clean	ee427dab4d66c13e4f090a154c3331e8
Concise Clean	hk.stem.concise.wer	cd2d14efcf57cde8cf3d8e68ea9595e4
Universe Clean	hk.lamp.clean.univ	4901fc40b0b8d61634c6cfdb37281fa1
Carpet Clean	og.crp.cln.zda	5bf1efd95bff6b0013992d01485e382b
Strong Clean	in.memory.sys.clean	56a0406f927bcd2714e6c6ca04ed275b
Multifunction Clean	in.mult.stt.clean	0912ac77f1878e1cf4128674b111959b
EasyCleaner	come.easy.clean.ipz	20de51fa5a5da601df2e5d4ef5d0dffd
space clean	org.sst.space.ace	flflcaa7cdeef9fc2f4ab05f4e00caa5
Super Clean	com.super.clean.zaz	2fd6a0432f7e148d02d5123c6fl8344d
Junk Cleaner	cn.junk.clean.plp	bb8e40a18dd9fbe117bea9f38d926e0a
Power Doctor	com.power.doctor.mrb	3374cb25b3570cf9f0f5c520d7edf4ea
Keep Clean	org.clean.sys.lunch	0fbb1b2ce43aa153cef026397a5f583d
Fingertip Cleaner	com.fingertip.clean.cvb	d278aca87ddf71ac84286e281c14c2d5

Conclusion:

The above-mentioned malware applications behave differently than the other malware we reported earlier. Automatically launching applications without user interaction is a dangerous weapon that can be misused to harm the user's device and data. We may see more malware applications using such techniques in the future. Quick Heal's Security Lab continuously checks applications from Google Play Store for such malware.

The application ensures to bombard you with pop-up advertisements. If you have the Hiddad adware on your devices, we recommend you to remove it immediately.

Tips to keep you safe from such malware applications:

- You should not fall for claims made by application developers.
- You should read reviews as it may give some idea about the application's working.
- Try to limit yourself to known apps from known developers and keep only those apps on mobile that are really required.
- Use a reliable mobile antivirus (like Quick Heal Total Security) that can prevent fake, malicious apps, adware, etc., from getting installed on your phone.



Digvijay Mane

