What is Malware Joker? How to fight Malware Joker?

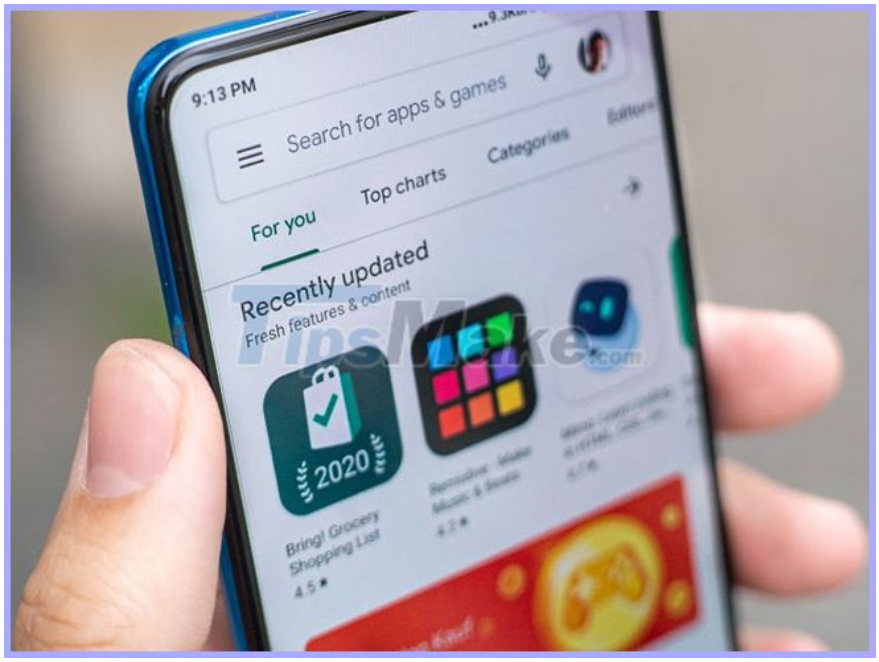
Joker malware is another threat to your privacy and sensitive information. Recently, it attacked Android mobile devices globally, resulting in the need to remove some applications from the Google Play Store.

If you want to keep your device safe, you'll need to know what **Joker malware** is and how it works.

What is the Joker malware?

This phishing malware is called Joker, because it hides behind the mask of an authentication application and targets unknown users. You can also see the Joker malware called Bread, both are the same.

Google first encountered this threat in 2017 and it is still an ongoing problem. The hackers behind the Joker malware are constantly trying to manipulate the Google Play Store security holes, allowing the malware to be disguised without being detected.



The hackers behind the Joker malware are constantly trying to manipulate the Google Play Store security holes
The authors of Joker have some methods to get infected applications to bypass security protocols in the Play Store. In fact, they even created an app version without malware, uploaded it to the Google Play Store, and then installed the malware on the victim's device by hiding it in the form of malware. an application update.

When you install an application that is infected with the Joker malware, it will register a paid option without your permission. To make matters worse, the Joker malware can hold your contacts, SMS messages and device information. It is very difficult to get money back after being a victim of this scam, so it is very important to prevent this malware infection before it happens.

How does Malware Joker work?

Joker malware-infected applications do not automatically request your personal information. This malware is much more sneaky than that, making it even more difficult for you to realize you've become a victim.

The first type of Joker malware relied heavily on SMS fraud. By sending an SMS to a premium number from your phone, the Joker malware will register or make payments without your knowledge. Because these premium services and subscription packages are often partnered with mobile carriers, you should often see unexpected charges on your mobile phone bill.

In early 2019, Google tightened restrictions on applications that require users to access call logs or SMS messages. As a result of this policy change, many Joker infected apps were discovered and then removed from the Play Store. Deploying Google Play Protect has also helped keep Android devices safe.

Despite Google's efforts, the Joker malware still exists. Check Point's research has found a new type of Joker malware, which has also done the same cheating act as before. Instead of cheating SMS, it now uses an old trick commonly found in Windows malware.

Once installed on the device, the Joker malware downloaded the executable DEX file from the command and control server. This code is used to secretly register the premium option. It then proceeds to prevent registration confirmation messages from appearing on the victim's phone.

To do this, the Joker malware takes advantage of the **Notification Listener** , an Android feature that allows apps to access notifications on the device. Malware hijacks the Notification Listener, allowing it to interfere with push notifications.

The latest version of the Joker malware bypasses Google security using a clever technique. According to Check Point, currently, the new variant has hidden the malicious DEX file inside the application as Base64 encoded strings, ready to be decoded and loaded.

This means that when the app is placed on the Play Store, there will be no sign of malware. Only when a user actually downloads the application does the malware 'show up'.

How to protect yourself from malware Joker

Google has recently removed 11 applications containing Joker malware from the Play Store. If you have any of the following, uninstall them immediately:

1. Compress Image (com.imagecompress.android)
2. Contact Message (com.contact.withme.texts)
3. Friend SMS (com.hmvoice.friendsms)
4. Relaxation Message (com.relax.relaxation.androidsms)
5. Cheery Message - listed two times (com.cheery.message.sendsms)

6. Loving Message (com.peason.lovinglovemessage)
7. File Recovery (com.file.recovefiles)
8. App Locker (com.LPlocker.lockapps)
9. Remind Alarm (com.remindme.alram)
10. Memory Game (com.training.memorygame)

Although most of these malicious apps act as alternative messaging apps, others include image compressors, reminder alarms, wallpaper apps, and so on. If any of these Which sounds familiar to you, check your credit card bill and mobile phone. Any "weird looking" transaction or registration could be a sign of the Joker malware.

Joker-infected applications look legitimate
Because Joker-infected apps look legitimate, you'll need to take some additional precautions when downloading apps.

You should also remember that many Joker-infected apps have fake user reviews on the Play Store. These positive reviews build trust and entice people to download the app.

Fortunately, it is quite easy to detect fake reviews. If you see any duplicate reviews under an app, the reviews are likely to be fake. The same thing happens for general reviews that don't mention the app name.

Besides knowing how to identify an unsafe application on the Play Store, you can also protect yourself by installing a trusted security application on your device. You might not think you need an Android antivirus app, but it can certainly be useful against Joker malware.

Finally, you should only install apps that you truly trust. Do some additional research on any apps you want to download. If you see any signs of fraud, stay away from it at all costs.