

# Warning: The Joker malware has infected over 500,000 Huawei Android devices

The Joker, one of the most persistent and dangerous strains of malware targeting Android devices, has just been discovered.

This time, the Joker's target is Huawei-branded Android devices, with an estimated number of infections not less than 500,000 cases.

More than half a million Huawei users are believed to have downloaded apps infected with the Joker malware on the company's official AppGallery app store platform. Security researchers found 10 applications in AppGallery that contain code to connect to a malicious command and control server (C2 server) operated by threat actors. This will allow the configuration and additional components to be received after the malware has successfully infected the victim's system.



## Shade common applications

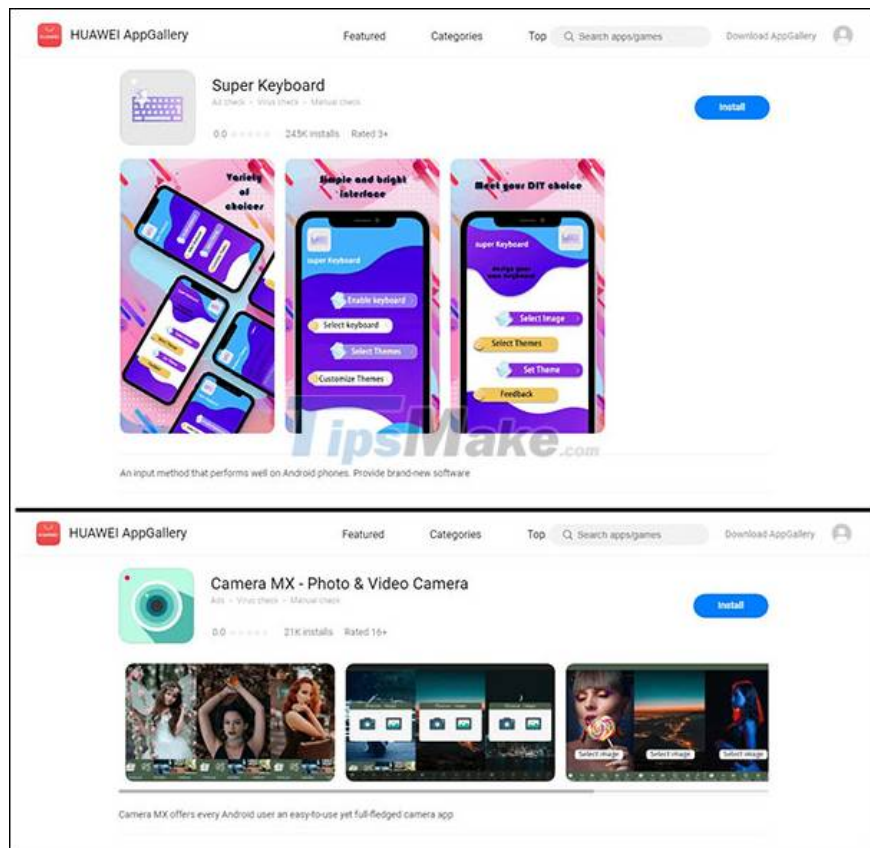
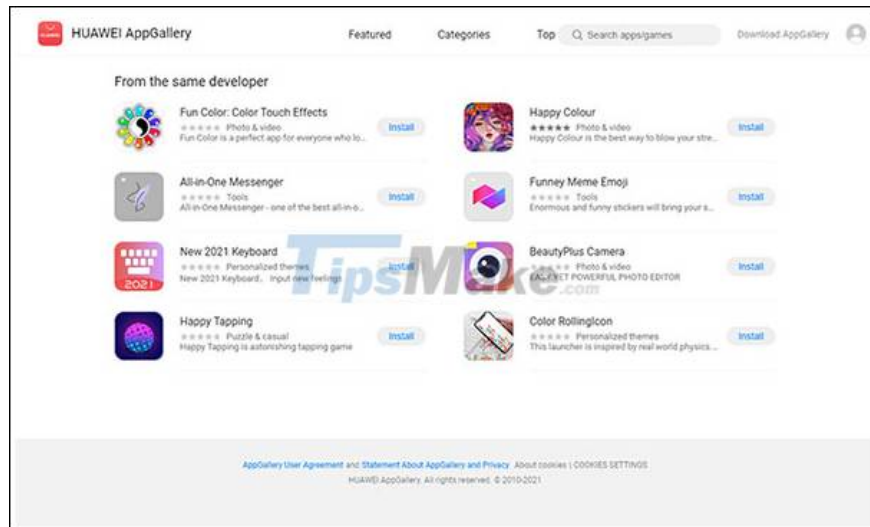
According to a report by security experts Doctor Web, during this campaign, the Joker malware still has most of the dangerous functions that have made its 'name'. For example, when the infection is successful on the target Android device, the malicious code will silently control SMS messages, contacts, device information, and collect some other important personal information such as passwords, The account name as well as some valuable data are being stored on the device.

In particular, the most serious threat posed by this malicious code to victims is the ability to automatically register paid wireless application protocol (WAP) services without the user's permission. The victim only really knew this when he paid the charges, and by then it was too late.

However, in this campaign, the Joker seems to be adding a new malicious feature, which requires access to the notification system on the device. This allows it to block the confirmation code sent by paid subscription services via SMS, leaving the user completely unaware.

According to researchers, the malware can subscribe to up to five services on its own. However, the threat actors behind malicious code operators can modify this limit at any time.

The list of applications containing the Joker malware detected on AppGallery to date includes virtual keyboard, camera app, launcher, online messenger, sticker collection, color software, and games.



Notably, 8 of these come from the same developer (Shanxi Kuailapai Network Technology Co., Ltd.) and 2 from another. According to statistics, these 10 apps have been downloaded by more than 538,000 Huawei users.

The Doctor Web side has informed Huawei and the Chinese company has now removed all 10 of these apps from AppGallery. If you own one of the above apps, you need to immediately uninstall it from your device.

Also, you should double-check your entire transaction history to see if there were any suspicious payments you didn't recognize. Also, make sure to closely check the permissions you grant to every app installed on your Android device.

You finished reading the article "**Warning: The Joker malware has infected over 500,000 Huawei Android devices**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.