The Joker malware once again bypassed Google's security, spreading strongly on the Play Store

The Joker malware has been around since 2017, but Google has so far struggled to detect and stop it.

Security researchers at Check Point have just discovered that the Joker malware is spreading on Android devices. Joker often lurks in legitimate applications and then silently signs up for high-cost services without the user's knowledge.

The Joker has been repeatedly deleted from the Play Store several times, but it soon finds a way to return. This time, it hides the malicious DEX executable code inside the application as a Base64 encoded string. Once hacked into the victim's device, the strings will be decoded and then launched.

The Joker malware has been around since 2017 and is very sophisticated
After receiving a warning from Check Point, Google removed 11 applications containing Joker malware from the Play Store on April 30, 2020.

"It is difficult to detect the Joker malware even though Google has invested heavily in Play Store protection measures , " said Check Point expert Aviran Hazum, who discovered Joker's new intrusion methods. *"Although Google has removed applications containing Joker from the Play Store, we think this malicious code will be able to return in the future."*

First discovered in 2017, Joker is a well known and popular Android malware. In addition to scams and self-registration of expensive services, Joker can also steal information such as SMS, contacts and device information.

Last year, Joker-related campaigns reached a peak when a number of security units such as CSIS Security Group, Trend Micro, Dr.Wed and Kaspersky discovered a series of malicious applications. In addition, Joker is

constantly finding unique ways to exploit vulnerabilities in Play Store's security testing method.

To hide their true nature, the guys behind the Joker used a variety of methods including chain security to avoid detection tools, buy fake reviews to attract users to download. application. The most sophisticated technique is versioning, bringing the Play Store a clean, quality application to attract users to download, then silently update more malware.

Below is a list of applications infected with the new Joker malware, the application name is in the 2nd column, behind the com .

sha256	Package Name
db43287d1a5ed249c4376ff6eb4a5ae65c63ceade7100229555aebf4a13cebf7	com.imagecompress.android
d54dd3ccfc4f0ed5fa6f3449f8ddc37a5eff2a176590e627f9bc92933da32926	com.contact.withme.texts
5ada05f5c6bbabb5474338084565893afa624e0115f494e1c91f48111cbe99f3	com.hmvoice.friendsms
2a12084a4195239e67e783888003a6433631359498a6b08941d695c65c05ecc4	com.relax.relaxation.androidsms
96f269fa0d70fdb338f0f6cabf9748f6182b44eb1342c7dca2d4de85472bf789	com.cheery.message.sendsms
0d9a5dc012078ef41ae9112554cefbc4d88133f1e40a4c4d52decf41b54fc830	com.cheery.message.sendsms
2dba603773fee05232a9d21cbf6690c97172496f3bde2b456d687d920b160404	com.peason.lovinglovemessage
46a5fb5d44e126bc9758a57e9c80e013cac31b3b57d98eae66e898a264251f47	com.file.recovefiles
f6c37577afa37d085fb68fe365e1076363821d241fe48be1a27ae5edd2a35e4d	com.LPlocker.lockapps
044514ed2aeb7c0f90e7a9daf60c1562dc21114f29276136036d878ce8f652ca	com.remindme.alram
f90acfa650db3e859a2862033ea1536e2d7a9ff5020b18b19f2b5dfd8dd323b3	com.training.memorygame

List of applications infected with Joker malware new version
You should check if your device has any of these installed. If so, immediately remove and check the transaction history for any suspicious payment.

You finished reading the article "**The Joker malware once again bypassed Google's security, spreading strongly on the Play Store**" 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.