New Joker variant hits Google Play with an old trick

By etal

Published: 2020-07-09 · Archived: 2026-04-12 02:11:04 UTC

Research By: Aviran Hazum, Bogdan Melnykov, Israel Wernik

Overview:

Check Point's researchers recently discovered a new variant of the Joker Dropper and Premium Dialer spyware in Google Play. Hiding in seemingly legitimate applications, we found that this updated version of Joker was able to download additional malware to the device, which subscribes the user to premium services without their knowledge or consent.

Figure 1 – Joker application on Google Play

General:

Joker, one of the most prominent types of malware for Android, keeps finding its way into Google's official application market as a result of small changes to its code, which enables it to get past the Play store's security and

vetting barriers. This time, however, the malicious actor behind Joker adopted an old technique from the conventional PC threat landscape and used it in the mobile app world to avoid detection by Google.

To realize the ability of subscribing app users to premium services without their knowledge or consent, the Joker utilized two main components – the Notification Listener service that is part of the original application, and a dynamic dex file loaded from the C&C server to perform the registration of the user to the services.

In an attempt to minimize Joker's fingerprint, the actor behind it hid the dynamically loaded dex file from sight while still ensuring it is able to load – a technique which is well-known to developers of malware for Windows PCs. This new variant now hides the malicious dex file inside the application as Base64 encoded strings, ready to be decoded and loaded.

Technical Analysis:

Originally, the code that was responsible for communicating with the C&C and downloading the dynamic dex file was located inside the main classes.dex file, but now the functionality of the original classes.dex file includes loading the new payload.

Joker triggers the malicious flow from the Activity by creating a new object that communicates with the C&C to check if the campaign was still active. After confirmation, it can then prepare the payload module to be loaded.

Figure 2 – Creation of the malicious object

Figure 3 – malicious object communicates with C&C

Figure 4 – response from C&C server

The first method used to load the dex file was to read it from the manifest file. When inspecting the manifest file, we could see that there was another metadata field that contained a Base64 encoded dex file. So all that was needed was to read the data from the manifest file, decode the payload, and load the new dex file.

Figure 5 – Manifest file containing the Base64 encoded dex

Figure 6 – reading data from manifest

During our research, we have also detected an “in-between” variant, that utilized the technique of hiding the .dex file as Base64 strings – but instead of adding the strings to the Manifest file, the strings were located inside an internal class of the main application. In this case, all that was needed for the malicious code to run was to read the strings, decode them from Base64, and load it with reflection.

Figure 7 – Strings inside main application

Figure 8 – Reading class strings and decode

Figure 9 – Loading the dex file with Reflection

Figure 10 – Decrypting strings

The new payload contained code that the original Joker had in its main dex file – the registration of the NotificationListener service, subscribing the user to premium services, and more. But now, after this change, all that the actor needed in order to hide the entire functionality was to set the C&C server to return “false” on the status code, and none of the malicious activity would occur.

Conclusion:

If you suspect you may have one of these infected apps on your device, here’s what you should do:

- Uninstall the infected application from the device
- Check your mobile and credit-card bills to see if you have been signed up for any subscriptions and unsubscribe if possible
- Install a security solution to prevent future infections

Protect your enterprise and users from sophisticated mobile cyberattacks like Haken or any other ones with SandBlast Mobile. To protect personal devices against attacks, check out ZoneAlarm Mobile Security.

IOC’s:

sha256	**Package Name**
db43287d1a5ed249c4376ff6eb4a5ae65c63ceade7100229555aebf4a13cebf7	com.imagecompress.android
d54dd3ccfc4f0ed5fa6f3449f8ddc37a5eff2a176590e627f9be92933da32926	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
f6c37577afa37d085fb68fe365e1076363821d241fe48be1a27ae5edd2a35c4d	com.LPlocker.lockapps
044514ed2aeb7c0f90e7a9daf60c1562dc21114f29276136036d878ce8f652ca	com.remindme.alram
f90acfa650db3e859a2862033ea1536e2d7a9ff5020b18b19f2b5dfd8dd323b3	com.training.memorygame

Mitre ATT&CK

Source: https://research.checkpoint.com/2020/new-joker-variant-hits-google-play-with-an-old-trick/