深度揭露 Anubis 移动银行木马

介绍

Anubis 是古希腊语，原本表示埃及神话中一位与木乃伊制作及死后生活有关的胡狼头死亡之神；然而 2017 年之后，Anubis 成了最流行的 Android 银行木马代名词，已经给全球 300 多家金融机构造成了不少麻烦。

2016 年 12 月 19 日，一个名为 maza-in 的用户在 exploit.in 的恶意软件开发者论坛中分享了一种新的 Android 银行木马 BankBot 的源代码，该木马能够发送和拦截文本消息以及执行覆盖攻击以窃取凭证。

2017 年第四季度开始，maza-in 私下将一种功能更强大的银行木马 Anubis 租给客户，与原始 BankBot 相比，该恶意软件功能得到了大幅增强，增加了现代主流的覆盖技术、设备屏幕记录和流传输、网络代理功能、键盘记录功能以及从受感染设备中窃取文件的功能。

2018 年 12 月 13 日，maza-in 发布版本 Anubis2.5，并宣称重构了整个代码，但实际上只是重新设计了后端的 Web 界面。

2019 年 1 月 16 日，Anubis 代码在地下论坛中泄露（后端代码和未混淆的 APK）。

2019 年 2 月 14 日，首次发现仅针对俄罗斯银行的 Anubis 样本，表明新的运营者出现。

2019 年 2 月 25 日，在地下论坛中出现出现了一些 Anubis 客户的投诉，指出 maza-in 和 Anubis 的技术支持不再回复消息。

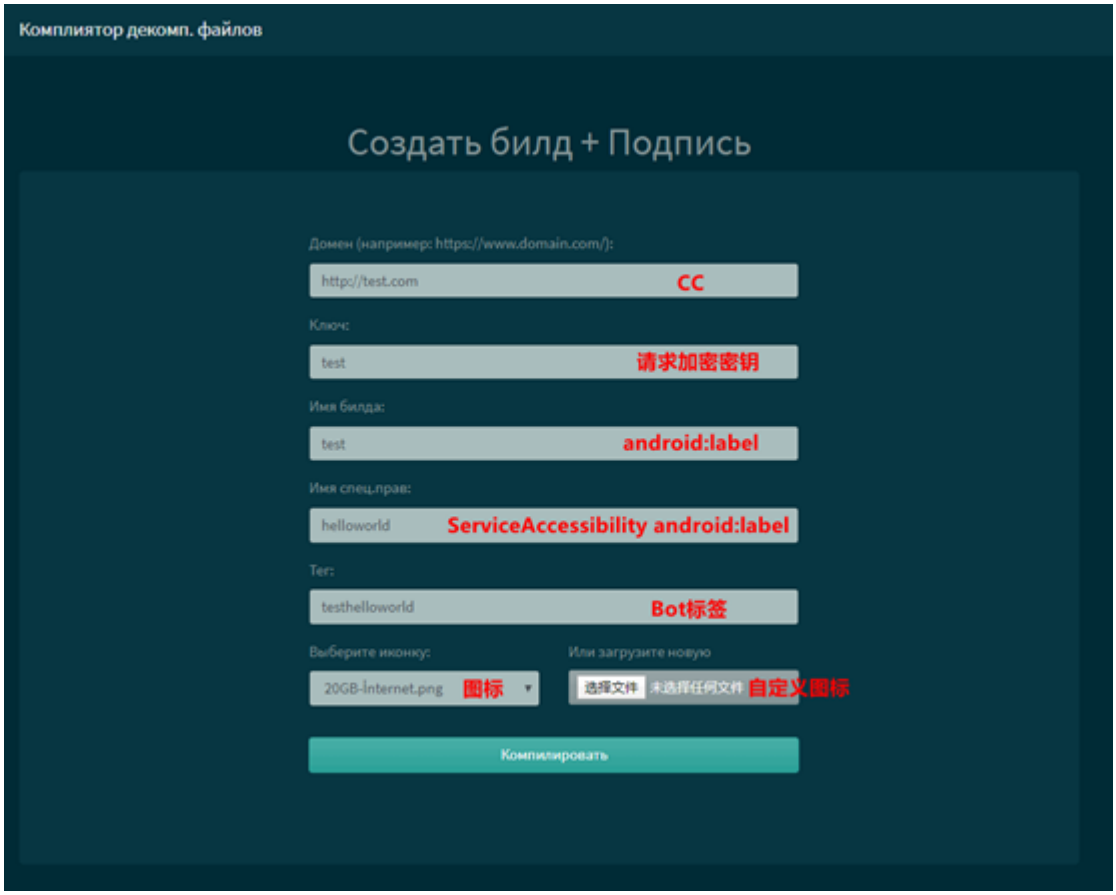
2019 年 3 月 4 日一个地下论坛的管理员传出了 maza-in 被捕的消息。此后多个论坛上禁止使用 maza-in 账户。

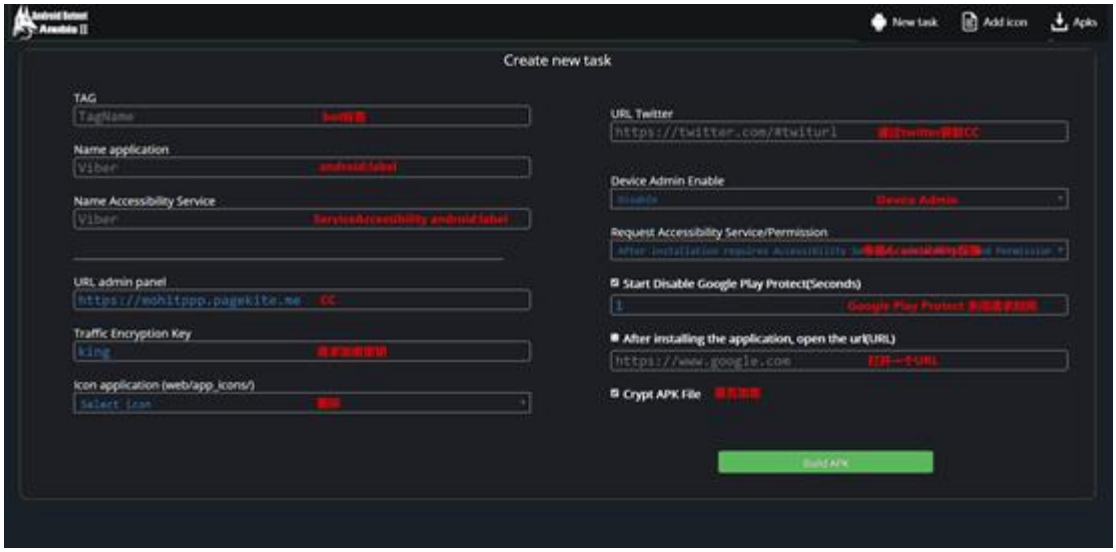
2019 年 3 月中旬，与 maza-in 有过联系的用户 Aldesa 在地下论坛上创建了一个帖子，出售所谓的 Anubis 3 恶意应用，但是该帖子很快被论坛管理员删除。

此后 Anubis 银行木马的正式租赁版本停止更新，但是由于代码泄露，基于 Anubis 的银行木马攻击活动并未消失，而是一直保持着活跃状态。

发现

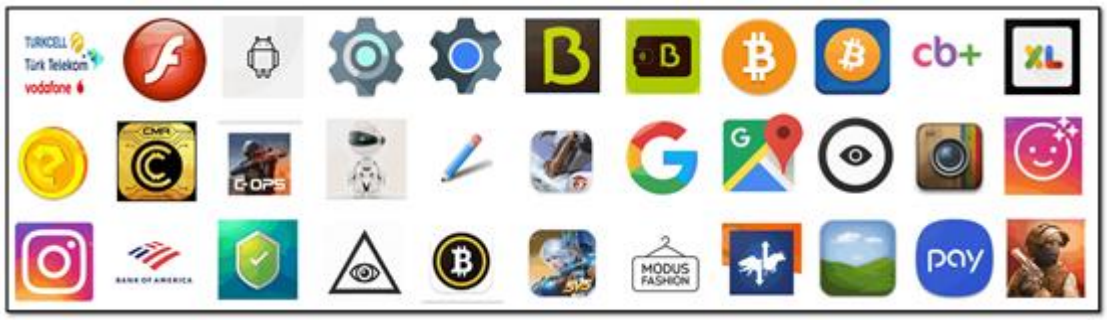
近期，烽火实验室在日常分析中发现了大量 Anubis 银行木马，并且发现多个制作 Anubis 银行木马的网站，这些网站以两种不同的界面展示，并且网站域名指向了同一个 IP，可能为同一个开发者制作。虽然网站在界面展示上有一些区别，但是使用方法基本一致，使用者只需要按照网站提示简单的填写相关配置，即可制作一个自己的 Anubis 银行木马，结合网上泄露的后端代码，即可成为 Anubis 的运营者。



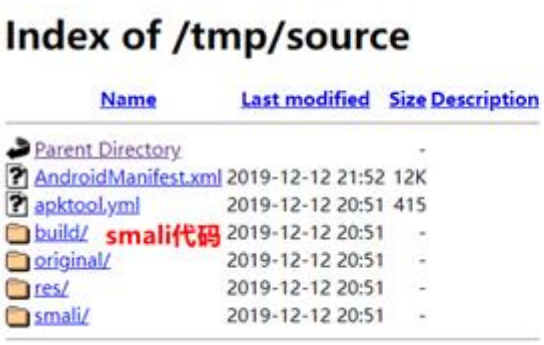


该网站提供了大量的图标进行伪装，预置的图标可以伪装成 Flash 播放器应用程序、系统工具应用、加密货币应用、图像处理应用和游戏

等相关应用。除此之外，该网站还提供了使用自定义图标的功能，用户可以自己选择上传伪装图标，进一步增加了伪装对象的多样性。

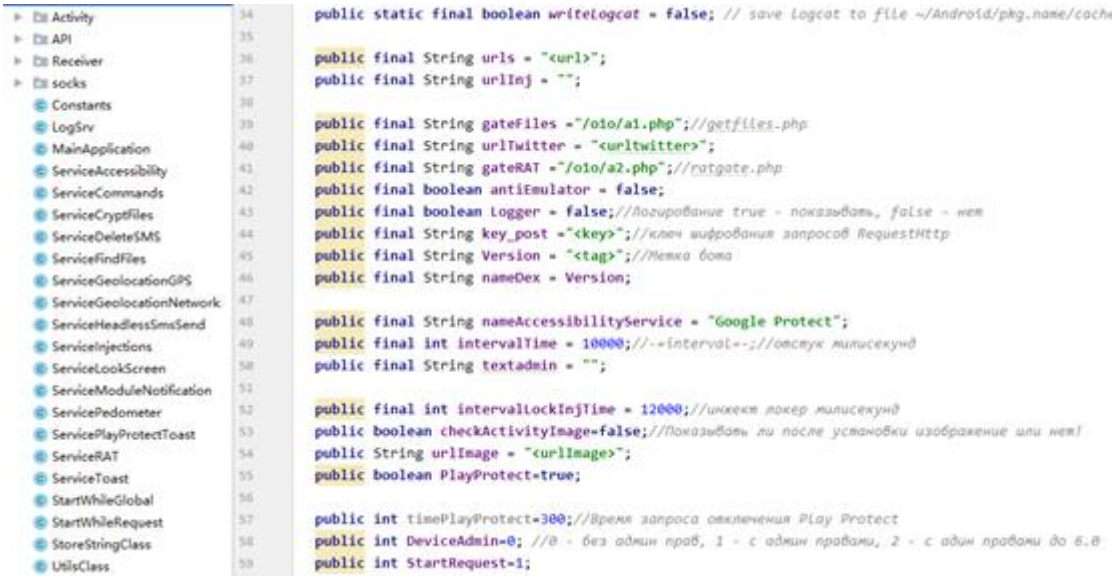


在分析两个网站制作 Anubis 银行木马的过程中，发现使用了两种不同的制作方法，其中一个网站使用 Anubis 反编译后的 smali 代码，另一个网站直接使用 Anubis 的源代码——这也说明 Anubis 应用程序源码早已泄露。



受控端源码

通过分析网站上的 Anubis 应用源码，我们发现其代码结构清晰，注释完整。下图为 Anubis 的配置相关代码，使用尖括号包含的字符串则为配置项，与网站提供的选项一致。



恶意功能

在功能方面，该代码主要功能如下：

- 将指定文本的短信发送到指定的号码；
- 执行 USSD 请求；
- 启动指定的应用程序；
- 更改 CC 的地址；
- 获取所有短信；
- 获取已安装的应用程序的信息；
- 获取所有申请的权限；
- 获取键盘记录；
- 显示指定内容对话框；
- 推送指定内容的通知；
- 通过 WebView 窗口阻止设备屏幕，该窗口将显示服务器指定的网页内容；

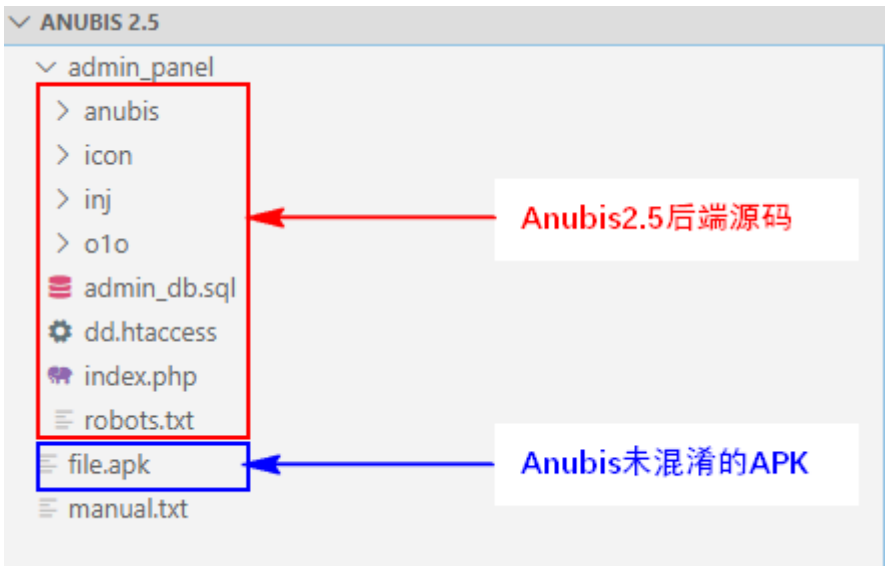
- 获取所有联系人号码；
- 向所有联系人发送短信；
- 请求访问数据的权限；
- 请求权限以确定设备的位置；
- 请求访问辅助功能；
- 请求访问其他权限；
- 将呼叫转移到攻击者指定的号码；
- 停止呼叫转移；
- 在浏览器中打开指定的链接；
- 在 WebView 中打开指向网页的链接；
- 加密存储在设备上的文件，并显示带有赎金请求的消息；
- 使用设备内置的麦克风开始录音；
- 反向连接代理；
- 数据擦除；
- 利用 Twitter/Telegram/Pastebin 作为跳板更新 CC。

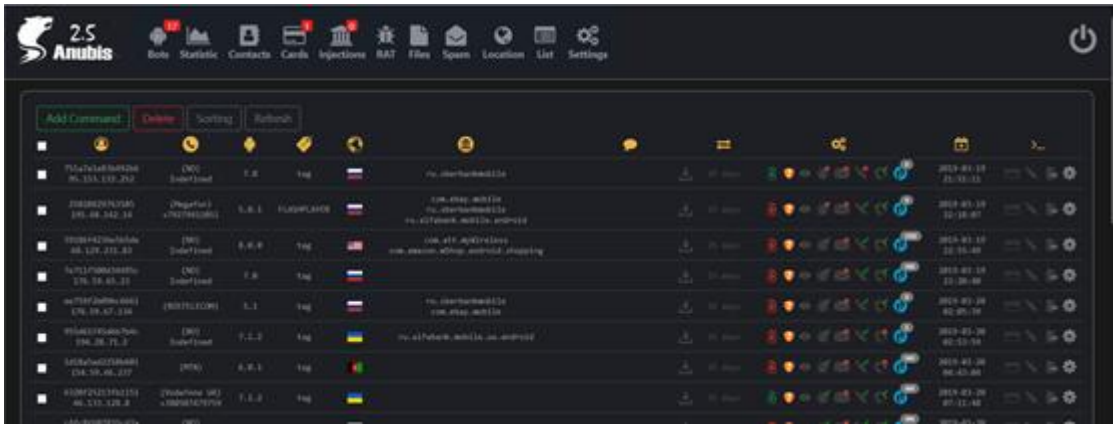
除了 Anubis 银行木马的功能代码外，在该网站上还发现了一份加固代码，该代码可以简单的保护 Anubis 银行木马，使其达到免杀的作用。

```
MainActivity
Protector
RC4
e Scripts

try {
    Class clsActThrd = Class.forName("android.app.ActivityThread");
    Class clsLoaded = Class.forName("android.app.LoadedApk");

    Method mtdCurActTrd = clsActThrd.getMethod( name: "currentActivityThread", new Class[]{});
    Object objCurActThrd = mtdCurActTrd.invoke( obj: null, new Object[]{});

    Field fidPkg = clsActThrd.getDeclaredField( name: "mPackages");
    fidPkg.setAccessible(true);
    Map map = (Map) fidPkg.get(objCurActThrd);
    String szPkg = mCtxBase.getPackageName();

    WeakReference wrefPkg = (WeakReference) map.get(szPkg);// mapPkg.get(szPkg);
    Field fidLoader = clsLoaded.getDeclaredField( name: "mClassLoader");
    fidLoader.setAccessible(true);
    ClassLoader ldrProtector = (ClassLoader) fidLoader.get(wrefPkg.get());
    DexClassLoader ldrSrcApk = new DexClassLoader(szPathSrcApk, szPathOptDex, szPathLibTree,
    fidLoader.set(wrefPkg.get(), ldrSrcApk);
```

控制端源码

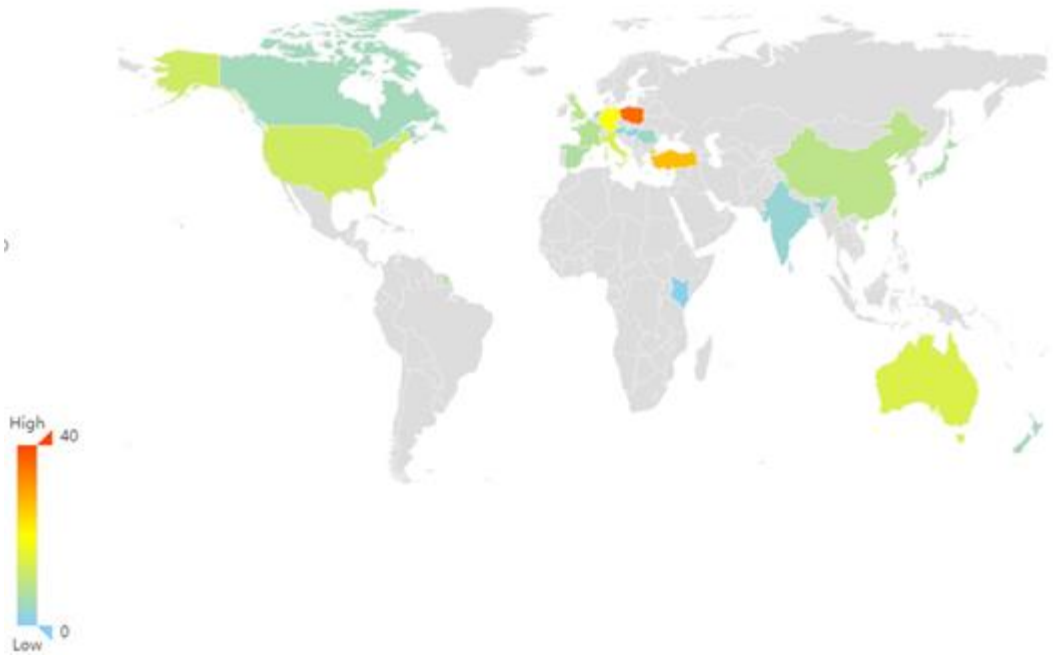
Anubis 银行木马的控制端源码主要提供了控制面板和钓鱼功能，其代码在 2019 年泄露，并且有详细的使用教程，任何人都可以利用该源码创建 Anubis 银行木马的后台系统，并且可以基于该代码添加其他钓鱼页面。

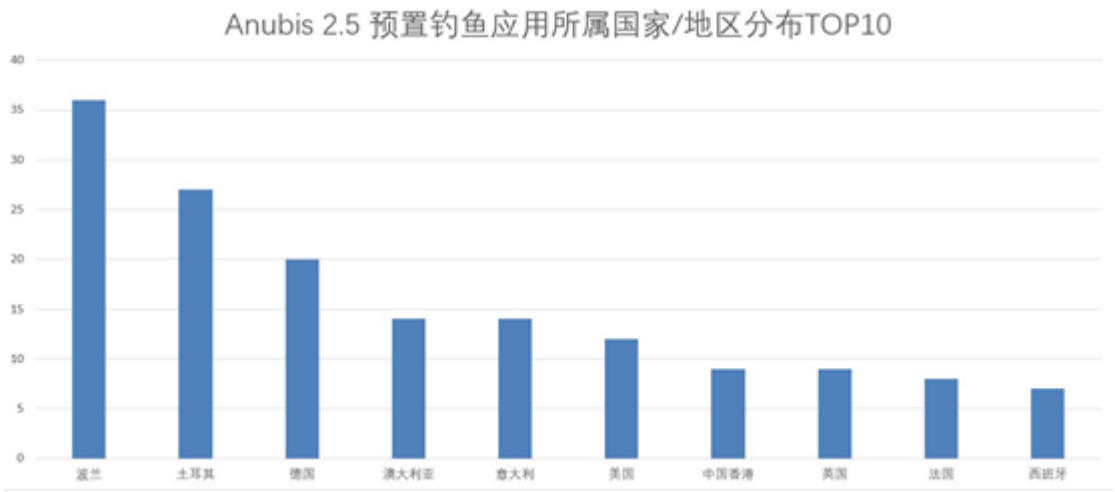




在 Anubis 控制端源码中，我们发现了大量的金融应用图标以及对应的钓鱼网站源码。涉及全球各地金融机构 300 多家，下图为部分金融机构的应用图标。

经分析，这些金融机构主要分布在欧洲，亚洲和北美的 20 多个国家/地区。下图显示了 Anubis 控制端代码中包含的钓鱼网站数量在不同地区的分布情况以及钓鱼网站最多的前 10 个国家/地区。

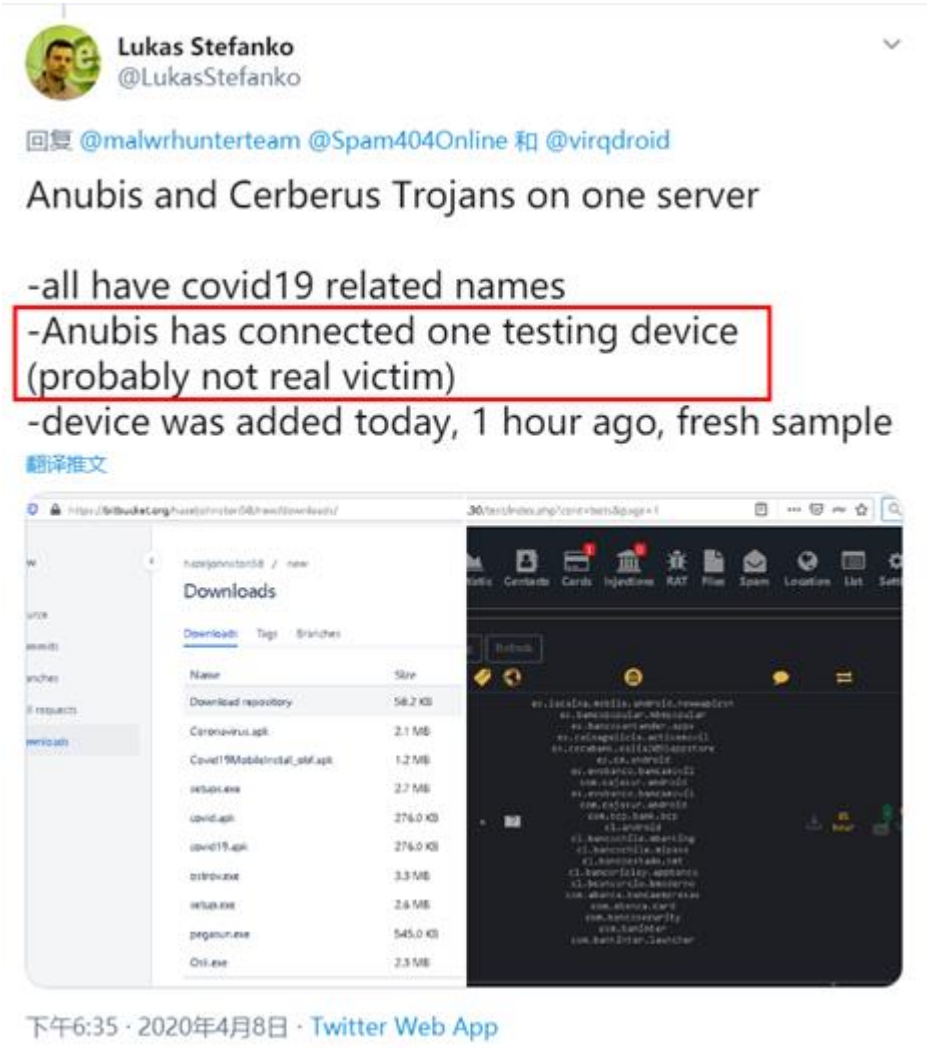




预警

2020 年 1 月至今，我们总共捕获到 6000 多个 Anubis 家族相关样本，根据伪装对象我们结合 Anubis 的宣传广告徽标制作了如下词云图，可以发现 FlashPlayer 出现的频率最高，为 Anubis 银行木马伪装最多的对象。

同时，我们也注意到随着今年新冠肺炎在全球的全面爆发，Anubis 银行木马运营者活动更加频繁，开始利用新冠肺炎事件进行传播。在已公开的情报中，我们就发现多起利用代码托管服务平台 Bitbucket 传播伪装成新冠肺炎相关应用的 Anubis 银行木马，且还在测试阶段，说明 Anubis 未来攻击的国家/地区可能是新冠肺炎爆发严重的区域。



总结

Anubis 作为一款最流行的银行木马，除了其功能强大之外，使用门槛也比较低，利用公开的银行木马制作网站和泄露的源代码，任何人都可以很简单的成为 Anubis 银行木马的运营者。虽然当前发现有部分伪装成中国香港金融行业相关应用的 Anubis 银行木马和钓鱼页面，但是随着 Anubis 应用程序源码的泄露，制作该家族木马的门槛进一步降低，未来可能把攻击目标进一步转移到国内的金融行业。360 烽火实

验室将持续关注 Anubis 银行木马相关动态，各金融相关的企业也需要做好自身 APP 防护，共同保障用户的财产安全。