INCLUDEPICTURE "http://www.venustech.com.cn/vc/img/banner0726.jpg" * MERGEFORMATINET

首款集勒索、间谍、银行木马于一体的新型综合型Android病毒深度分析

发布时间 2018-09-21

一、简述

启明星辰ADLab近期发现一款集勒索加密病毒、间谍软件、银行木马于一体的新型Android恶意代码,其实现了如加密勒索（Ransomware）、键盘记录（keylogger）、远程访问木马（RAT）、短信拦截、呼叫转移和锁定屏幕等多种功能。

详细分析该恶意代码后发现，该恶意代码新变种可劫持几乎涵盖全世界各大金融机构的手机APP，总数有300多个，涉及中国、美国、英国、日本、中国香港、法国等40多个国家和地区。该恶意代码还具有勒索软件的功能，会使用256位对称密钥对受害用户的手机文件进行加密处理，并且以“.AnubisCrypt”作为加密文件的扩展名，同时还伪造了FBI警告界面通知受害用户以比特币的方式支付罚金方可对文件进行解密。另外，它还能够被用于进行网络间谍活动，例如：监视受感染设备主窗口活动、进行屏幕截图并发送给攻击者、使用内置麦克风监听受感染设备周围环境中的声音等等。

二、恶意代码发现

2018年8月底，启明星辰ADLab监测到一个当月新注册的异常Twitter账户，该账户在Twitter上发布了一些类似用base64编码的推文。其2018年8月27日发布了两条似乎完全相同的推文，并且在我们发现当天，又连续发布两条不同的推文（见图1）。

INCLUDEPICTURE "https://www.venustech.com.cn/uploads/2018/09/211424302632.png" * MERGEFORMATINET

图1 可疑Twitter账户推文

我们通过base64解码这些推文后，仍然看不到任何有意义的数据。因此，我们通过该Twitter链接“https://twitter.com/sHybzhzZWJgdbdj”来做关联分析，并且发现了一些可疑的apk文件，通过分析确认该apk文件为Android平台下一款危害性极大的恶意APP，并且目前还处于活跃状态。通过深入分析我们发现，该恶意APP会连接该Twitter链接“https://twitter.com/sHybzhzZWJgdbdj”获取推文，并将其解密成为C&C地址，其解密算法模拟了base64的效果，但并非为base64算法，以此迷惑发现异常推文的分析人员。解密后的字符串如表1所示：

INCLUDEPICTURE "https://www.venustech.com.cn/uploads/2018/09/211425031643.png" * MERGEFORMATINET

表1 推文的解密

一直到9月2日，黑客删除了其中的3条推文，只留下最近的一条推文（见图2）。说明利用该恶意代码进行的网络攻击活动正在进行。

INCLUDEPICTURE "https://www.venustech.com.cn/uploads/2018/09/211426051682.png" * MERGEFORMATINET

图2 攻击者的推文只剩下一条C&C

我们注意到，该Twitter账户使用了被称为“全世界最大的骗子”的俄罗斯金融诈骗犯Sergei Mavrodi的照片作为图像，推测攻击者很可能是Sergei Mavrodi的粉丝。Sergei Mavrodi（1955年

8月11日- 2018年3月26日）生于莫斯科，1989年成立了MMM公司，MMM宣称以摧毁世界不公正的金融体系为目标，实际上是玩了一个“大众集资”的庞氏骗局游戏。国内的e租宝、钱宝网等也都被认定是庞氏骗局。在Sergei Mavrodi和其MMM公司将俄罗斯几乎能骗的人都骗完了之后，2015年Sergei Mavrodi将他的游戏带入了中国，并且为了躲避监管，Sergei Mavrodi团队“创新地”将比特币支付引入了其支付系统，鼓励投资者使用比特币进行转账交易，并为此特意制作了比特币扫盲视频，见图3。

INCLUDEPICTURE "https://www.venustech.com.cn/uploads/2018/09/211426347707.png" * MERGEFORMATINET

图3 Sergei Mavrodi团队制作的比特币扫盲视频

三、样本演化

根据样本关联分析，我们发现该恶意代码样本为Anubis的一个新变种。

2017年1月，安全公司Dr.Web曾发出警告，银行木马BankBot的源代码被公开发布在了一个论坛上。随后，有网络犯罪分子利用该源码创建了安卓银行木马Android.BankBot.149.origin，彼时的BankBot还仅是一个典型的银行木马，能够利用网络钓鱼对话框窃取感染用户手机银行的敏感信息，如银行详细信息和信用卡数据。

2018年3月5日，PhishLabs发现了银行木马BankBot的一个新变种，并第一次将其命名为Anubis，Anubis同样基于BankBot源码开发，并整合了众多不同类型恶意软件的功能于一身。

2018年7月，IBM X-Force的移动恶意软件研究人员观察到了大量的Android恶意软件下载器被上传到了Google Play。这些恶意软件下载器会在受感染设备上安装Anubis。这表明一个特定的恶意软件分销商已经从使用Marcher转向了分发Anubis。

四、功能介绍

Anubis新变种整合了多种类型恶意软件功能于一身，图4是其功能示意图，该变种包含勒索软件功能、键盘记录功能、RAT功能、短信拦截功能和呼叫转移功能等。同时，Anubis还可以窃取受害用户的通讯录、短信等敏感信息。此外，攻击者还可以远程控制受感染设备，利用受感染设备向攻击者指定的目标发送特定短信。不难想象，攻击者完全可以对受害者的社交网络进行全方位渗透和欺诈。

INCLUDEPICTURE "https://www.venustech.com.cn/uploads/2018/09/211428051650.png" * MERGEFORMATINET

图4 Anubis功能示意图

图5是我们抓取到的该恶意代码变种和C&C服务器通信的数据包，从图中可以看出，该变种使用http协议和C&C服务器进行通信，通信数据被加密处理后进行传输。我们利用分析出的解密算法对图中加密数据进行解密，分别得到“aa5193bdfeb39625:(CHINA MOBILE):4.4.4:cn::AOSP on HammerHead (aosp_hammerhead):V::0:0:”和“|OK|”，很显然是一个木马上线包。

INCLUDEPICTURE "https://www.venustech.com.cn/uploads/2018/09/211428296185.png" * MERGEFORMATINET

图5 C&C上线包

C&C命令和其附加数据采用同样的加密方案传输，我们将该恶意代码变种包含的主要C&C命令及其含义归纳到了表2：

INCLUDEPICTURE "https://www.venustech.com.cn/uploads/2018/09/211428569828.png" * MERGEFORMATINET

表2 主要的C&C命令和功能

五、典型行为分析

5.1、窃取受害者银行账户凭证

Anubis监视目标应用程序启动，然后使用对应的钓鱼屏幕覆盖掉合法的应用程序以窃取受害者的账户凭证（见图6和图7），同时会利用短信拦截功能来拦截银行发送给受害者的所有短信（见图8），这样攻击者就绕过了银行的双层身份认证，成功对受害者的财产进行洗劫。

INCLUDEPICTURE "https://www.venustech.com.cn/uploads/2018/09/211429525727.png" * MERGEFORMATINET

图6 加载钓鱼页面的代码

Anubis伪造的钓鱼页面：

INCLUDEPICTURE "https://www.venustech.com.cn/uploads/2018/09/211430251343.png" * MERGEFORMATINET

图7 伪造的钓鱼页面

恶意代码将自身设置成默认短信应用，拦截用户短信：

INCLUDEPICTURE "https://www.venustech.com.cn/uploads/2018/09/211430539716.png" * MERGEFORMATINET

图8 拦截用户短信

攻击者的劫持目标几乎涵盖全世界各大金融机构的手机APP，总数达到了300多个，涉及中国、美国、英国、日本、中国香港、法国等40多个国家和地区，部分目标金融APP的包名见表3：

INCLUDEPICTURE "https://www.venustech.com.cn/uploads/2018/09/211431217625.png" * MERGEFORMATINET

表3 部分目标金融APP

5.2、加密受感染设备文件，对受害者进行勒索

不同于常见的只是简单禁止受害者访问手机界面的锁定屏幕的勒索软件，Anubis对受害用户的文件进行了加密，加密的目录包括“/mnt”、“/mount”、“/sdcard”、“/storage”以及用户的内在存储卡目录，见图9。

INCLUDEPICTURE "https://www.venustech.com.cn/uploads/2018/09/211431589818.png" * MERGEFORMATINET

图9 加密的文件目录

Anubis的模块使用256位对称密钥对文件进行加密处理，并以“.AnubisCrypt”作为加密文件的扩展名，见图10。

INCLUDEPICTURE "https://www.venustech.com.cn/uploads/2018/09/211432355842.png" * MERGEFORMATINET

图10 加密操作

在完成文件加密后，Anubis会加载其锁定页面（图11），提示受害用户的手机已经被锁定并且文件被加密，需要受害用户支付比特币方可对文件进行解密。

INCLUDEPICTURE "https://www.venustech.com.cn/uploads/2018/09/211433096772.png" * MERGEFORMATINET

图11 加载锁定页面

锁定页面htmllocker是从远程服务器动态获取到的并保存在其配置文件set.xml中，如图12，我们可以看到FBI WARNING的勒索信息：告知受害用户的手机被锁定，并且所有的文件被加密，用户的数据将会被传送到FBI，除非受害用户支付罚金方可解密。

INCLUDEPICTURE "https://www.venustech.com.cn/uploads/2018/09/211433334552.png" * MERGEFORMATINET

图12 配置文件中的锁定页面代码

图13是htmllocker代码加载后的页面，该页面做的相当逼真，在“FBI WARNING”文字上方是“FBI”的LOGO，下方即是图12配置文件中的那一段勒索信息。

INCLUDEPICTURE "https://www.venustech.com.cn/uploads/2018/09/211433541318.png" * MERGEFORMATINET

图13 锁定页面

5.3、利用设备拨号应用执行USSD命令

USSD为GSM系统所使用的一种通讯协议，用户可以通过手机拨号程序输入特定的指令取得系统服务商提供的服务，比如查询预付卡余额等，也可以用于查询手机内部信息，如“*#06#”可以查询手机的IMEI码。也有部分手机厂商使用自定义的USSD指令对手机做特殊的设定或操作，例如将手机恢复为出厂设置，开启手机的工程模式等。

该变种利用受感染设备的拨号程序来执行远程服务器传来的指令，从图14中我们可以看到，攻击者首先打开拨号程序，然后输入从C&C获取到的恶意指令，不同的指令对应不同的功能。不排除攻击者对受感染设备恢复出厂模式或者恶意格式化受感染设备存储卡等可能性。

INCLUDEPICTURE "https://www.venustech.com.cn/uploads/2018/09/211434198499.png" * MERGEFORMATINET

图14 利用设备拨号应用执行USSD命令

5.4、设置呼叫转接

设置受感染设备的呼叫转接号码为攻击者远程指定的手机号码（见图15）。攻击者首先打开受感染设备的拨号程序，然后通过输入“*21*手机号码#”对受感染设备设置呼叫转接。这样，攻击者就可以成功拦截受害用户的手机来电，并且可以利用此功能对受害用户进行欺诈。

INCLUDEPICTURE "https://www.venustech.com.cn/uploads/2018/09/211434416536.png" * MERGEFORMATINET

图15 设置呼叫转接

六、建议

建议用户不要轻易点击短信中的不明链接，不要安装不明来源的APP。对申请可疑权限尤其是短信读写、打电话以及需要激活设备管理器的APP要特别留意，涉及到金钱的操作要格外谨慎。遇到操作异常，应当及时使用杀毒软件查杀或找专人处理。目前互联网上也充斥着形形色色的第三方APP下载站点，很多甚至成了恶意应用的批发集散地。用户应特别留意不应轻易的在一些下载站点下载APP，尽量从官网下载所需APP应用，在不得不从第三方下载站点下载软件时，要高度保持警惕，认真甄别，防止误下恶意应用，给自己造成不必要的麻烦和损失。

参考链接：

HYPERLINK "https://securityintelligence.com/anubis-strikes-again-mobile-malware-continues-to-plague-users-in-official-app-stores/" \t "_blank" https://securityintelligence.com/anubis-strikes-again-mobile-malware-continues-to-plague-users-in-official-app-stores/

HYPERLINK "https://blogs.quickheal.com/android-malware-combines-banking-trojan-keylogger-ransomware-one-package/" \t "_blank" https://blogs.quickheal.com/android-malware-combines-banking-trojan-keylogger-ransomware-one-package/

PAGE