登录

“九头虫”病毒技术分析报告

阿里聚安全 / 2016-10-20 06:36:00 / 浏览数 13653 安全技术 技术讨论 顶(0) 踩(0)

一、背景介绍

近日，阿里移动安全收到多方用户反馈，手机中了一种难以清除的病毒。病毒一旦发作，设备将不断弹出广告，并自动下载、安装、启动恶意应用，最终设备衰竭而死，用户

我们分析发现，“九头虫”病毒利用多家知名root
sdk对设备提权，可轻松提权上万总机型，成功提权后获得设备最高权限，随后向系统分区植入多个恶意app，删除设备其他root授权程序、su文件，并替换系统启动脚本文

中毒设备将作为“九头虫”病毒的僵尸设备，每天推送上百万广告，其点击率大概15%（主要是病毒自身的模拟点击），也就是说每天广告点击上10万次，再加上静默安装与

二、“九头虫”传播途径与感染数据统计

2.1、传播途径
最早我们截获到伪装成“中国好声音”应用的“九头虫”病毒，通过排查历史样本，我们发现大量“九头虫”变种病毒，其传播方式包括：伪装成热门应用、重打包生活服务类、色
传播病毒图标

2.2、感染数据统计

1、全国地区感染分布
对2016年初到2016年10月的监测统计数据显示，“九头虫”病毒累计设备感染量高达33万。从感染地区分布图中可以看出四川、广东是感染重灾区。

2、每月设备感染趋势
从每月设备感染趋势图可以看出，“九头虫”病毒爆发周期是4～5个月，在随后的4～5个月每月感染数下降，这正好也是病毒变种的一个周期。最近在8月初达到峰值，随后几

三、深入分析
“九头虫”病毒分为注入rom病毒和恶意推广两个模块，注入rom病毒是“九头虫”家族的最新变种，执行流程图如下。

3.1、病毒母包
母包的MyApp组件是恶意代码入口点，完成libOgdfhhiaxn.so加载和assets目录下xhmf文件解密加载，随后“九头虫”病毒分别进行注入rom病毒和恶意推广。

3.2、“九头虫”注入rom病毒
“九头虫”释放多个家族恶意应用，潜伏在系统应用中，频繁弹出恶意广告，严重干扰手机正常使用。注入rom病毒过程如下。

执行提权
首先获取root工具包。libOgfhhixan.so动态加载由assets目录下的Zvtwk文件释放的oko.jar。oko.jar子包联网请求提权工具下载地址，随后下载并本地解密获得提权工具包
请求获取提前工具包下载地址图

提权工具包中文件以及功能如下表：

接下来加载执行root sdk既是data.jar文件，成功加载后“九头虫”会删除本地的cab.zip和data.jar文件。
动态加载执行data.jar图

从data.jar代码逻辑发现，“九头虫”病毒作者完全逆向重写了root精灵的rootsdk，根据设备型号等信息下载root-exp，其来源http://cdn.shuame.com/files/roots/xxx-id。
使用root精灵图

构建“免疫系统”
成功提权后，拿到设备至高权限，接下来构建自身“免疫系统”，执行如下操作。
（1）插入某杀软白名单
解密root工具包中的ql文件，获得将rom病毒写入某杀毒软件白名单的sql语句，通过工具包中的qlexec执行sql语句，下图将rom病毒插入杀软白名单来躲避监测。

（2）植入恶意app
将root工具包下的恶意app，以及libdataencrypt.so 植入系统目录，并使用chattr
+ia命令使得用户无法正常卸载，最后以服务启动恶意app。注意下图红色框中，将rom病毒lol.qv907a.Cqenthyrusxncy.apk备份到/system/etc/rom.dat，该病毒会在su和

（3）删除设备本身root相关文件
接续执行cl.sh脚本，删除设备本身root相关文件，保证设备上只有病毒拥有最高权限。

（4）禁用杀软
执行“pm disable”禁用多家知名杀毒软件。
pm disable com.qihoo360.mobilesafe
pm disable com.tencent.qqpimsecure
pm disable cn.opda.a.phonoalbumshoushou
（5）守护rom病毒
病毒通过替换系统服务，以致开机运行拷贝到/system/etc/目录下的守护模块，这里病毒替换了debuggerd和install-recovery.sh。这样深深植入rom的病毒，通过普通的恢
data都无法清除。

3.3、“九头虫”恶意推广
恶意推广包括应用推广和广告弹屏点击。推广APP应用是病毒的主要目的，既可以推广正规应用赚取安装费用，也可以推广其他病毒安装到手机；广告弹屏也是病毒牟利的一
静默安装

“九头虫”通过解析服务端返回的数据，对包含“silencePackageUrl”字段的应用进行静默安装。恶意推广数据来自http://in[.]stidreamtrip.com/ni.do，每次请求上传设备信息

下图解析“silencePackageUrl”字段信息进行静默安装。

根据silencePackageUrl里的url字段，将apk
下载存放在/sdcard/android/data目录。在静默安装之前会从http://cdn.stidreamtrip[.]com/accurate/loveApp/xiaoaisup下载xiaoaisup文件，xiaoaosup是一个本地库

xiaoaisup释放的各文件功能及作用如下表格：

realroot用来解密释放root-exp，并执行提权。对释放出root-exp分析发现，“九头虫”病毒竟然使用root大师的某一方案。

设备成功root后，使用自身释放的ppm对应用进行静默安装。

恶意弹屏广告
“九头虫”病毒集成“广点通”和“bdssp”，默认以CPC（点击计费）计费模式，也就是只要广告被点击，广告主就要支付费用。广告弹屏形势包括全屏、横幅、banner、插屏、

四、“九头虫”C&C端分析
hxxp://115[.]159.20.127:9009/gamesdk/doroot.jsp
hxxp://rt-10019850[.]file.myqcloud.com/83330905/nocard0908/qv907apwedmmc001.zip
hxxp://cdn[.]shuame.com/files/roots/xxx-id
hxxp://in[.]stidreamtrip.com
hxxp://yxapi[.]youxiaoad.com

前两条来自国内某云，用来存放加密的提权工具包，第三条是病毒破解某知名root接口后，直接从root精灵下载root方案，这里我们主要分析最后两条域名。stidreamtrip.c
hxxp://cdn[.]stidreamtrip.com/accurate/loveApp/xiaoaisup [xiaoaisup提权工具包]
hxxp://cdn[.]stidreamtrip.com//accurate/niicon/a52e15d0-0353-43a4-a684-d1199f682271.png
hxxp://cdn[.]stidreamtrip.com//accurate/niadimg//2e528c28-9d09-4f5c-ad2e-0616f63a5c01.png
hxxp://cdn[.]stidreamtrip.com/accurate/apk/44915bcf98724663851faa75ab73dff9.apk
hxxp://cdn[.]stidreamtrip.com/accurate/apk/f823e088d9ff4481914c9cbd21700e49.apk
hxxp://cdn[.]stidreamtrip.com/accurate/apk/6f24ea54ad1642189545e0aeee0d202e.apk
hxxp://cdn[.]stidreamtrip.com/accurate/apk/9de7f70625e5416b8a7739db6f64baaf.apk
hxxp://cdn[.]stidreamtrip.com/accurate/apk/25205b91d6484fde961e5a9487346981.apk
hxxp://cdn[.]stidreamtrip.com/accurate/apk/89f7b2f7-6bd5-49e9-a236-49f4ddc9ab0e.apk

通过域名备案查询发现，stidreamtrip.com是重庆一家广告投放公司，目前该站点首页已不能访问，但存放的恶意文件任可下载。

根据网站备案编号关联到4个网站，其负责人都是同一个。目前cn-dream.com站点未使用，zpmob.com站点是“重庆xx网络科技有限公司”主站，stidreamtrip.com站点是主

我们继续通过域名whois历史中涉及的qq邮箱追踪，下图伪装成广告主与公司负责人聊天。

在该公司的广告平台上找到一公司客服，下图与该公司客服对话。“那个已经不外放了”，也证实了从9月“九头虫”病毒设备感染下降趋势。

五、安全建议
“九头虫”病毒直接非法利用知名厂商root sdk，以致轻松入侵上万种机型，对于root厂商，应严格校验root
请求方，对如此危险的提权代码应得到严密保护，对于用户，尽量使用大厂商设备，及时做设备系统升级；日常使用手机过程中，谨慎软件内推送的广告；来源不明的手机软

作者：阿里移动安全，更多安全类技术文章，请访问阿里聚安全博客（http://jaq.alibaba.com/community/index.htm）

上一篇：《中国互联网地下产业链分析白皮书》 下一篇：正儿八经的测试
1. 2 条回复

水滴石穿 2017-05-25 13:48:22

感谢分享

0 回复Ta

mozi 2018-08-28 16:51:40

为什么四川中病毒的那么多呢？

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板