【原创】秒抢红包锁屏样本手动查杀操作

zzzhhh / 2017-06-05 15:15:44 / 浏览数 4540

---

1 样本概况

1 样本概况

1.1 样本信息
病毒图标：
病毒名称： 秒抢红包病毒样本
所属家族： a.rogue.SimpleLocker.a
文件名称： com.h-1.apk
MD5值： 033ae1ba78676130e99acc8d9f853124
文件大小： 245.38KB
病毒行为：重置android系统密码，诱骗用户激活设备管理器，属于锁屏勒索类病毒。

1.2 测试环境及工具

AndroidKiller、夜神模拟器

1.3 分析目标

研究此病毒的恶意行为以及如何清除此病毒

2．具体行为分析

2.1 主要行为

2.1.1 恶意程序对用户造成的危害

主动修改用户系统密码给使用造成影响且勒索用户。
1、该样本安装后诱骗用户点击激活设备管理器，使自己无法被用户卸载

2、激活后屏幕界面锁屏，提供了序列号和勒索信息

2.1.2 恶意程序在Androidmanifest.xml中注册的恶意组件

(1)权限相关传递附加信息重置密码添加悬浮窗口激活ActivityForResult窗口信息添加View初始化Intent激活设备管理器
(2)服务/广播

2.2 恶意代码分析

2.2.1 恶意程序的代码分析片段

恶意代码修改系统密码相关函数。

自启动服务函数，调用com.h.s

密码生成函数分析

3．总结

3.1 提取病毒的特征，利用杀毒软件查杀

恶意代码特征：
（1） MD5：033ae1ba78676130e99acc8d9f853124
（2） 提取字符串：\u7528jj\u6233\u4E00\u4E0B\u4E5F\u80FD\u89E3\u9501\u54E6

3.2 手工查杀步骤或是工具查杀步骤或是查杀思路等。

1）提取样本
Android 中有两个目录是存放已经安装的 apk 目录
System/app 存放系统 apk
Data/app 存放用户安装的 apk
2）查找关键字

3）搜索字符串

4）使用自带的jd-gui查看密码加密的随机数与固定值，计算出密码

解密算法为：序号+8985 = 66645035 ）进入手机设置-安全-设备管理器，点击取消掉激活的勾

6 ）取消激活按钮点击时会遇到第二重密码，输入得到的密码固定值8985可解锁

7 ）最终我们会成功卸载掉这个恶意的APP的。

样本链接: https://pan.baidu.com/s/1kVC2G8B 密码: q5jw

压缩包密码：52pojie

点击收藏 | 0 关注 | 0

上一篇：【原创】一份通过IPC和lpkdl... 下一篇：【非原创】渗透测试标准

1. 1 条回复

如风 2017-09-14 07:10:41

其实这个锁屏木马很早据有了，发展至今网上有好几个演变版本，都是大同小异来着。

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