勒索拦截马 Trick 分析报告

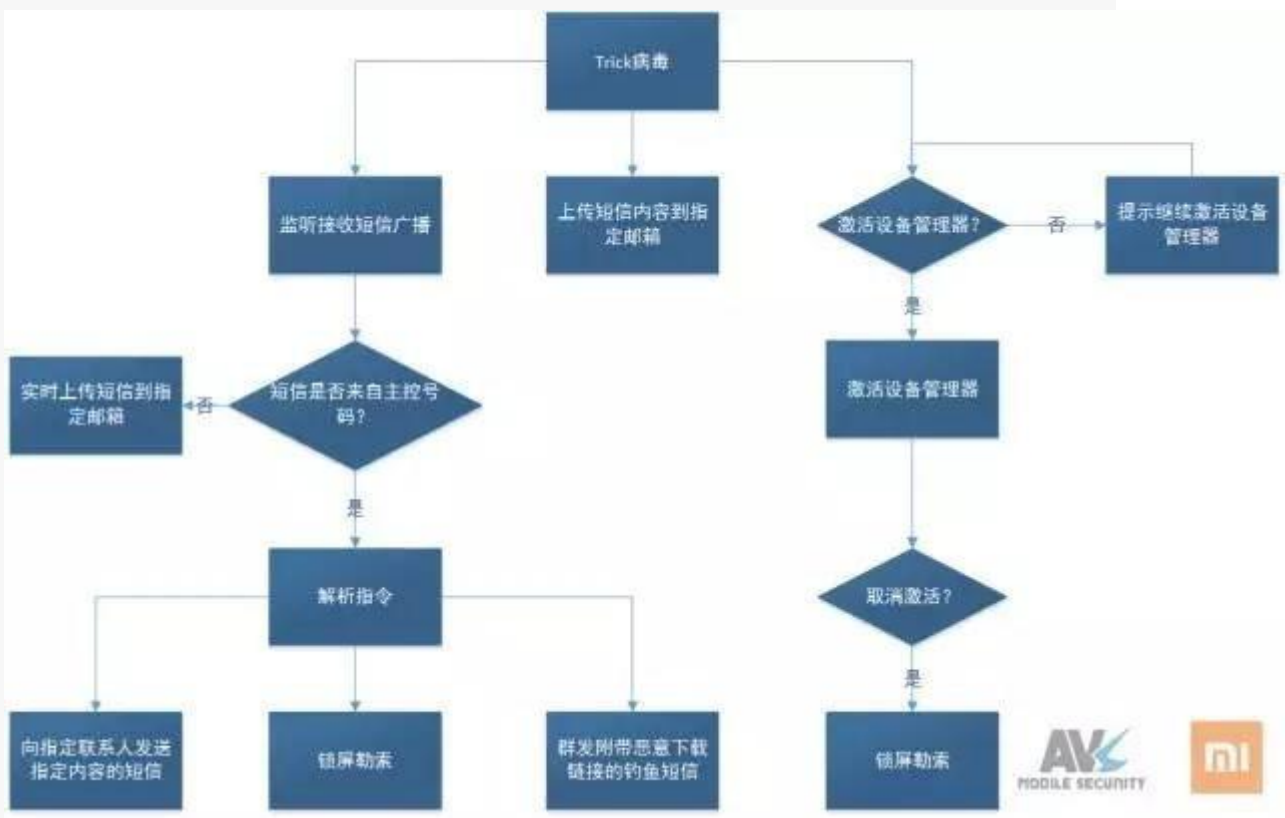
安天 AVL 移动分析团队

近期，安天 AVL 移动安全团队和小米 MIUI 安全中心发现一款携带勒索功能的拦截马 Trick，经过样本溯源发现，该病毒竟出自国内一名高中生之手。该病毒伪装成中国移动，以免费获取话费的短信诱惑用户下载安装。

该病毒运行后会执行以下恶意行为：

- 窃取用户短信并上传到指定邮箱；
- 根据短信指令锁定手机进行勒索；
- 根据远程短信指令遍历联系人，并向所有联系人群发附带恶意下载链接的钓鱼短信进行恶意传播；
- 一旦发现用户执行卸载此恶意软件的操作，该病毒会直接锁定用户手机，并对用户进行勒索。

病毒运行流程图如下：



病毒行为详细分析

1.窃取用户短信信息

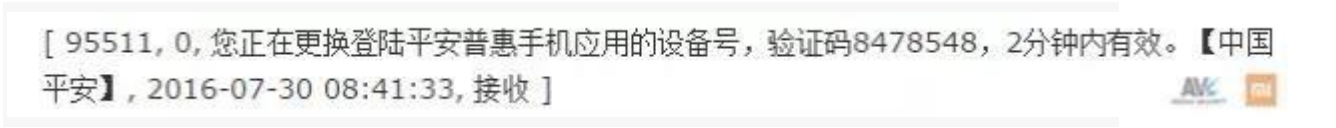
Trick 病毒程序运行后，首先获取用户手机中的所有短信，以邮件正文的形式上传至指定邮箱，同时还会将短信内容写入 txt 文件中，通过邮箱上传，邮件标题为“短信”。

通过对 Trick 病毒样本的溯源，我们发现了该恶意开发者的邮箱信息，在邮箱中发现大量感染用户的隐私信息，其中以各类短信验证码最为常见。

虽然该病毒样本本身并没有窃取用户账户信息的功能，但是考虑到目前大量的隐私信息被泄露，恶意开发者极有可能通过其他渠道获取到感染手机 QQ、微信、银行卡账户等信息，后续通过短信拦截马执行解绑、改密、转账等操作。

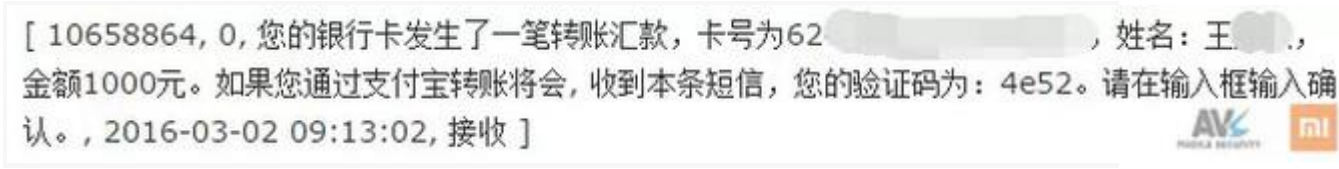
- 更换微信绑定关系：

- 更换平安普惠设备验证码：

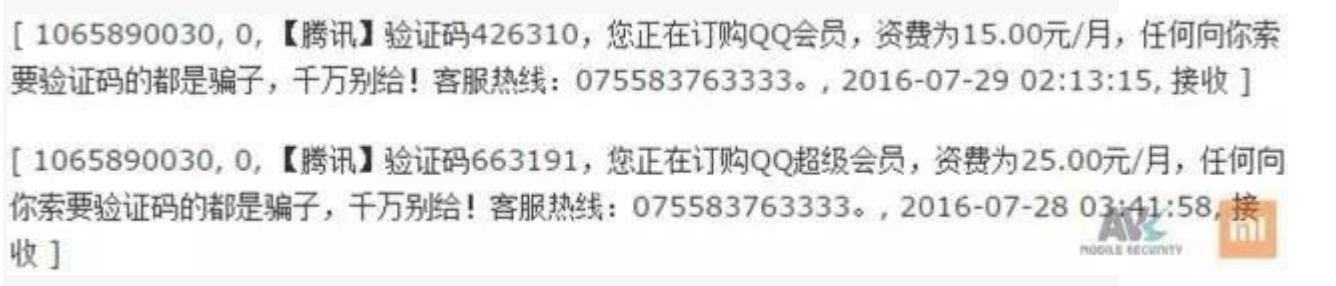


- 更换 QQ 号绑定手机：

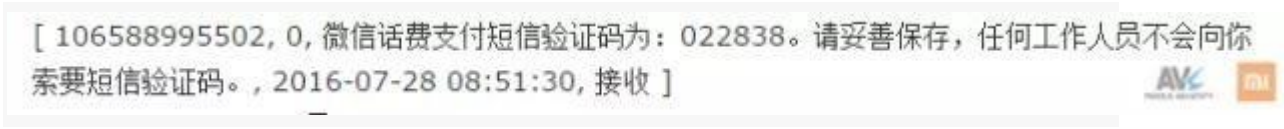
- 银行转账验证码：



- 订购腾讯业务：

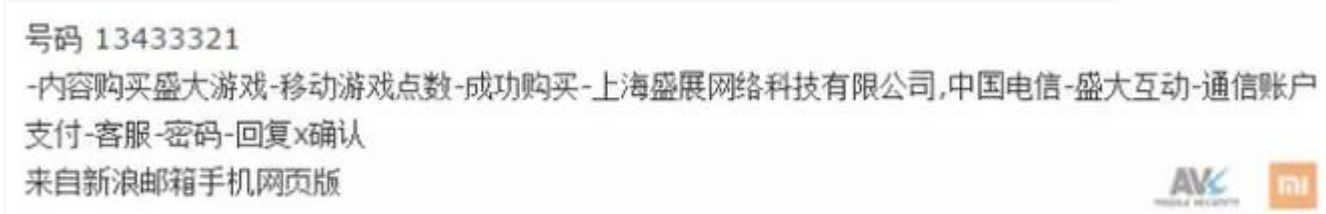


- 微信支付验证码：



- 更改银行预留电话验证码，开通手机银行：

- SP 订阅：



2.激活设备管理器

运行后，Trick 病毒会诱导用户激活设备管理器，若用户成功激活设备管理器，

则会提示用户重启软件：

```
@Override public void onEnabled(Context arg8, Intent arg9) {
    System.out.println("激活使用");
    super.onEnabled(arg8, arg9);
    Toast.makeText(arg8, "软件已成功运行 请重启软件 ", 3000).show();
}
```

3.隐藏图标

激活设备管理器后，Trick 病毒会弹出虚假对话框，提示虚假信息“程序异常已自动卸载”，并隐藏启动图标。

```
@Override public void run() {
    MainActivity.this.getPackageManager().setComponentEnabledSetting(MainActivity.this.getComponentName(),
            2, 1);
    Toast.makeText(MainActivity.this, "软件出现异常 已自动卸载成功", 3000).show();
}
```

4.接收短信指令进行远控行为

Trick 病毒隐藏图标后继续在后台运行监听系统接收短信的广播。接收到主控手机 187********发来的短信，解析此短信内容发现它会执行以下操作：

指令 1：锁机

锁机指令即是对用户手机进行锁定，全屏置顶一个勒索的界面，要求用户联系 QQ2038******有偿解锁。

指令 2：短信

短信指令即通过解析主控手机发送的短信，获取要发送的内容和号码，并控制用户手机在后台发送。

指令 3：群发

群发指令即遍历用户手机中所有联系人进行短信群发，短信内容为“http://pre.im/ZxI2 下载登录进去填我邀请码 156941 可以领话费我已经领了30”。该网址下载的就是其自身应用，当前该链接已失效。

该应用的图标为中国移动，配合钓鱼短信内容，恶意诱导性极强。

5.实时上传短信

Trick 病毒通过监听系统接收短信的广告，将非主控手机发送的短信通过邮件实时上传，邮件标题为“小伟拦截马”。

6.卸载程序锁机

Trick 病毒运行后会启动设备管理器，用户卸载应用之前必须先取消激活设备管理器。一旦监测到用户执行取消激活设备管理器的操作时，该病毒会直接将用户手机锁屏并勒索，勒索界面与以上锁机界面相同：

7.第三方推送服务

Trick 病毒还实现了 Bmob 的第三方推送服务功能，在当前的程序中并没有对推送消息进行处理，可以推测在后续的版本中可能会实现执行更多的指令控制或其他功能。

恶意开发者追溯

1.追溯恶意开发者主控手机号码以及地域信息

我们从代码静态分析中得到恶意开发者发送指令的主控手机,通过对主控手机归属地的查询，可以看到该号码号码归属地为四川德阳市：

您查询的手机号码段	18 测吉凶(新)
卡号归属地	四川 德阳市
卡 类 型	移动187卡
区 号	0838
邮 编	618000 更详细的

2.追溯恶意开发者 SNS 账号信息及姓名

我们从代码静态分析中得到恶意开发者邮箱信息,在邮箱中有蒲公英应用分发平台上的账号，从中可以得知作者的名字和 QQ：

通过分析我们还发现该恶意作者存在对外兜售拦截马的行为：

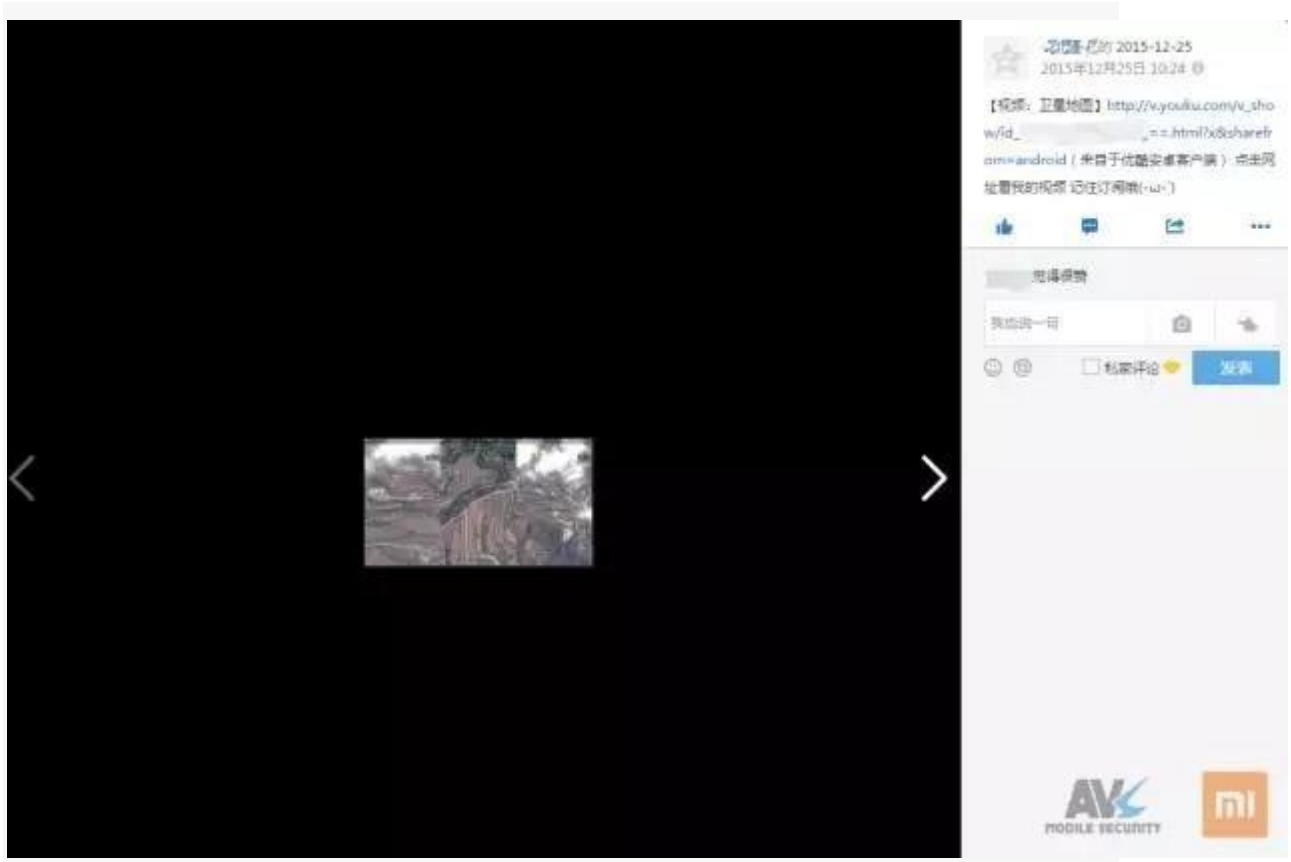
3.进一步判断恶意开发者身份

a)通过上一追溯环节的结论，我们得到了恶意开发者的 qq 账号，以下是其 qq 账号个人资料信息。从下图可以看到，该开发者的年龄为 18 岁（但该信息不一定可靠），初步推断其为高中生的可能性。

b)通过访问该 qq 对应的 qq 空间，我们看到其空间中展示了某渠道拦截到的受害者短信信息，为该 qq 与实际攻击者进行了一次强关联，也进一步保证了我们通过该 qq 收集的攻击者信息的可靠性。

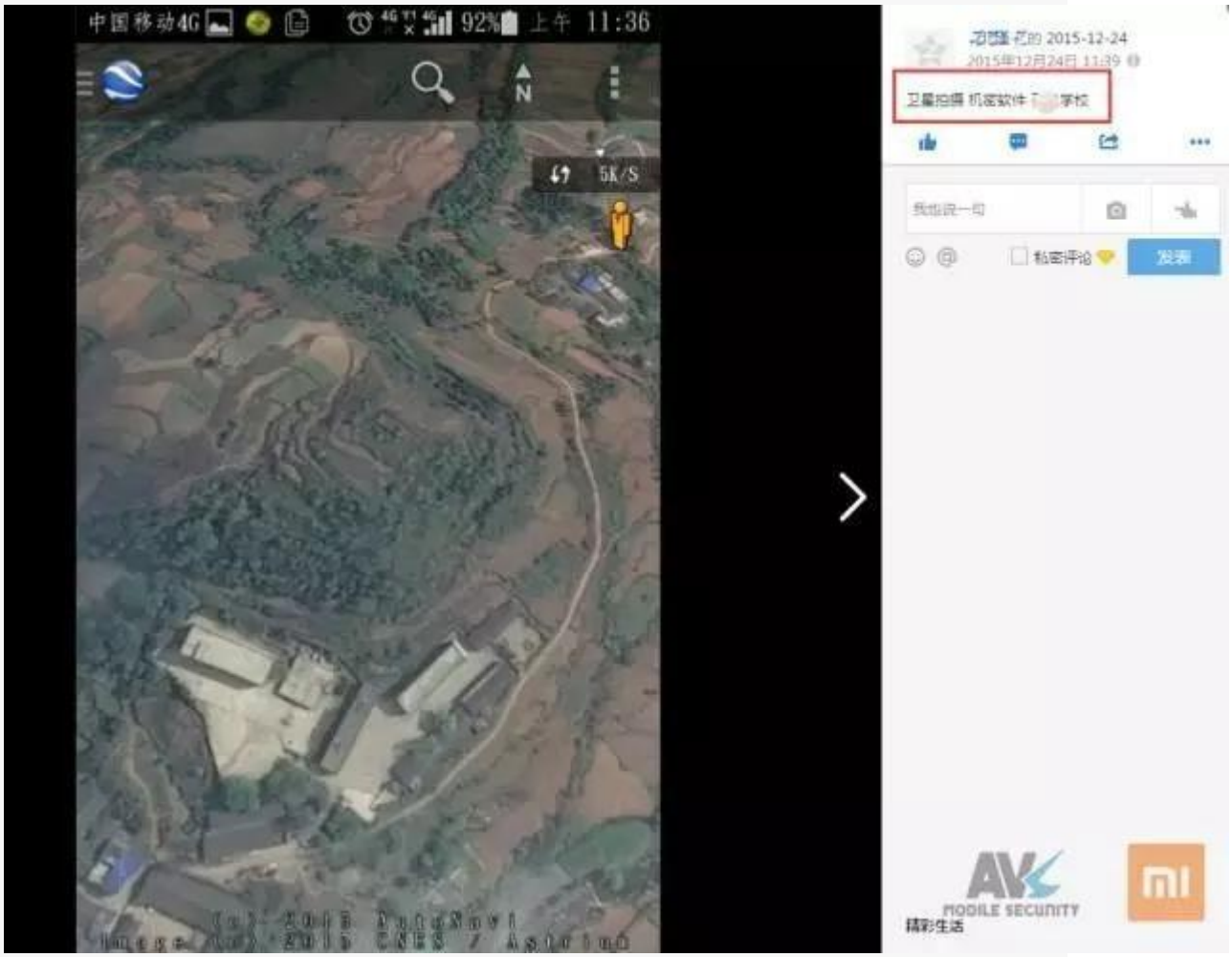
c)该空间中上传了一些学校运动会的照片，可以推断出该攻击者为一名学生。

d)我们在其空间中看到了攻击者发布的学校位置的卫星图以及对应的卫星拍摄视频地址。通过查看该卫星拍摄视频，视频结尾呈现了视频制作者姓名，而该姓名与前面追溯环节所得到的攻击者姓名信息完全一致。




[拍客]卫星地图
19
优酷
乐秀
2015.12.24
03:24 / 03:25

e)更为关键的是，该卫星拍摄地图以及空间中的说说信息中，披露了一所高中的校名以及地理位置。其指向的是四川省德阳市下某县的某所高中，进一步印证了攻击者为高中生的推测。



综上，我们可以推断出该恶意开发者极有可能是来自四川省德阳市下某高中的一名高中生。

总结

Trick 病毒伪装成中国移动，以免费获取话费的钓鱼短信诱导用户下载并安装病毒。该病毒运行后窃取用户的短信内容并上传至指定邮箱，同时向联系人群发

钓鱼短信进行恶意传播。此外，该病毒通过短信指令远控执行恶意行为，后续可能进一步形成僵尸网络。

Trick 病毒虽然没有窃取用户账户密码的恶意功能，但从恶意开发者邮箱内的短信内容可以合理推断出该恶意开发者极有可能通过其他渠道获取用户的 QQ、微信、甚至银行账户等隐私信息，后续通过解绑、改密的方式登录用户账户，对用户财产造成极大的安全风险。

一个出自高中生之手的病毒技术如此高明，让我们深感如今高中生信息技术水平之高的同时，也警醒我们应该加强对网络安全感兴趣的年轻人的正向引导，将他们的技术天赋应用在对抗网络攻击上，而不是开发病毒窃取别人的隐私、财产，否则黑客最终将会受到法律制裁。

安全建议

针对 Trick 拦截马病毒，集成 AVL 反病毒引擎的 MIUI 安全中心已经实现全面查杀。安天 AVL 移动安全团队和 MIUI 安全中心提醒您：

- 请从正规的应用市场下载应用，不要在不知名网站、论坛、应用市场下载应用
- 谨慎点击短信中附带的链接
- 不要在任何场合随意泄露自身隐私信息，注重自身隐私保护
- 建议在手机中至少安装一款杀毒软件，同时保持定期扫描的习惯

本文原标题《Trick 蠕虫病毒来袭！幕后主使竟是一名高中生“黑客”!》,作者：安天 AVL&小米安全中心，转载自安天 AVL 移动安全团队公众号，雷锋网(公众号：雷锋网)已获授权转载。

http://www.leiphone.com/news/201611/AEqK6KSmCokhMRrT.html

追踪 |“中国移动”App 竟然是锁机病毒，幕后主使是一名高中生“黑客”

本文作者：史中　　2016-11-04 11:44　　安天移动勒索木马电脑被锁机小米安全