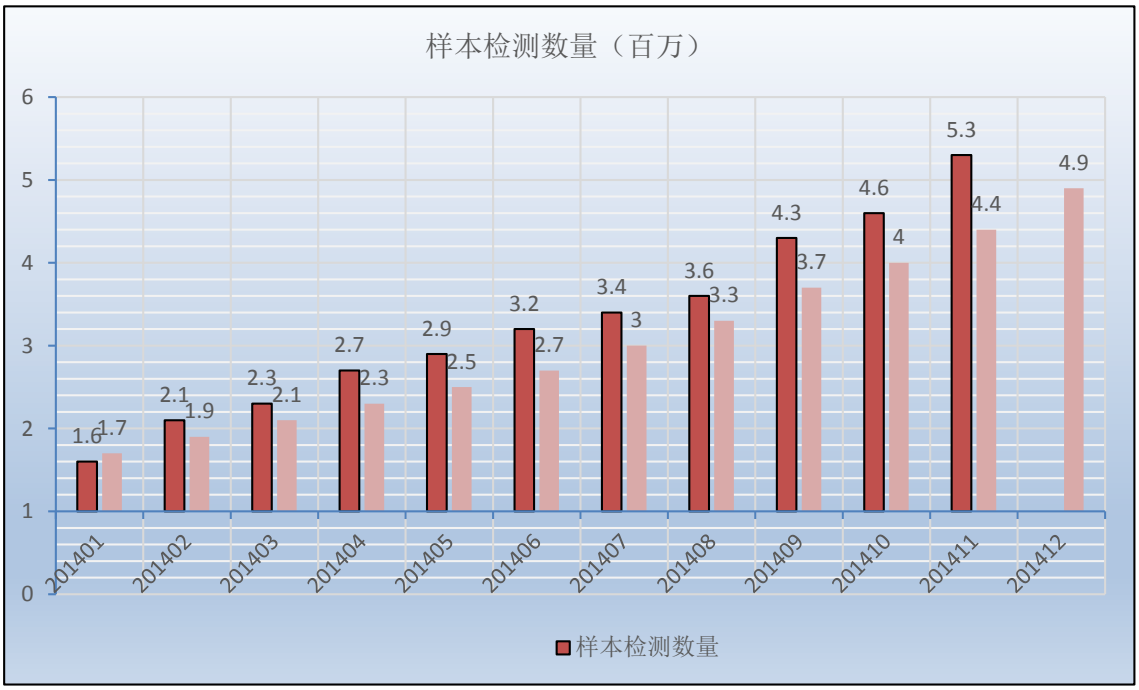
趋势科技移动客户端病毒报告

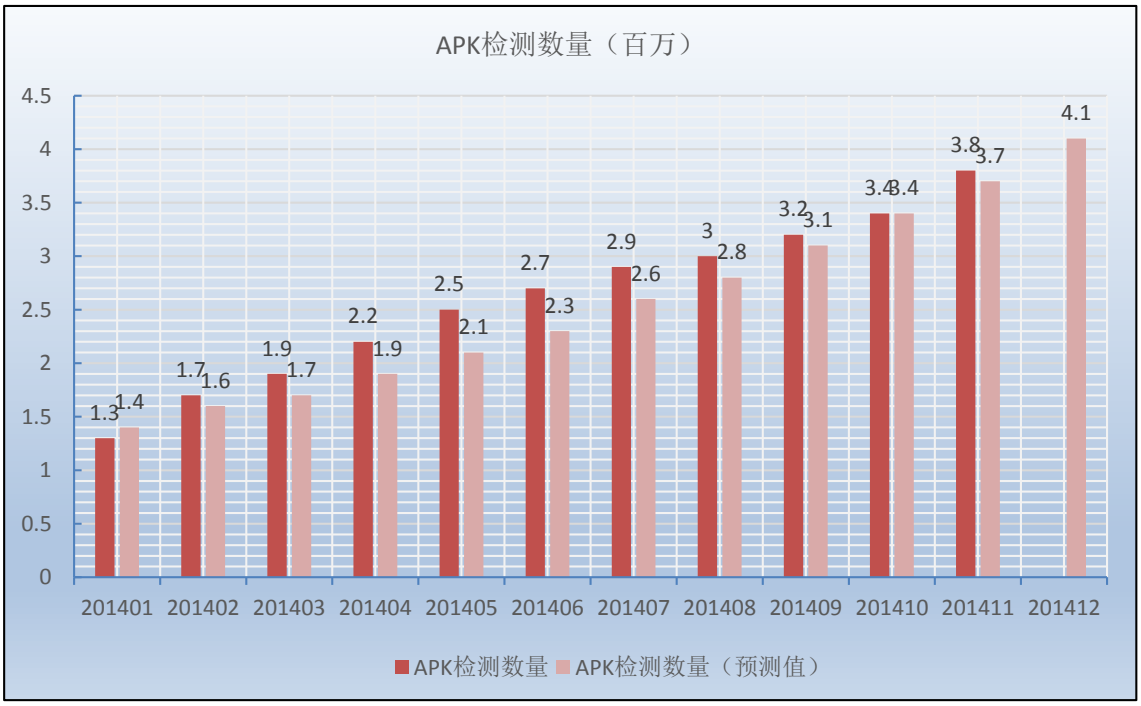
2014年11月移动客户端安全威胁概况

本月，截至 2014.11.30 日，发布中国区移动客户端病毒码 1.787.00，大小 33,723,295 字节。

样本检测数量



APK检测数量


APK检测数量（百万）
4.5
4
3.5
3
2.5
2
1.5
1
0.5
0
1.3
1.4
1.7
1.6
1.9
1.7
2.2
1.9
2.5
2.1
2.7
2.3
2.9
2.6
3
2.8
3.2
3.1
3.4
3.4
3.8
3.7
4.1
201401
201402
201403
201404
201405
201406
201407
201408
201409
201410
201411
201412
APK检测数量
APK检测数量（预测值）

黑客开始利用 Android APP 破解 RFID 支付卡

我们最近监控到一款来自智利的高危 Android 恶意程序，检测名为 ANDROIDOS_STIP.A。该程序在论坛和博客上传播，可以用来入侵用户的 RFID 卡片来达到非法充值的目的。这款恶意程序的机制是什么？RFID 支付卡带来的安全隐患又是什么呢？

RFID 卡支付的方式越来越流行，越来越多的设备也加入了对 NFC 的支持。银行，商业和一些其他的公共服务也开始向他们的客户提供带有预存费用的 RFID 卡。

注：以下讨论的恶意软件样本不是由官方 Google Play Store 下载的。

RFID 卡的安全问题

因为应用广泛，RFID 卡成为被攻击的目标这一点都不奇怪。例如最近发生在智利的 Tarjeta bip!卡被破解的事件。该卡是基于 MIFARE 的智能卡；MIFARE 是一类广泛用于非接触式近距离感应智能卡中的芯片。

Process of writing MIFARE cards

```
if(v3.authenticateSectorWithKeyB(v9_1, this.KEY_B_SECTOR_8)) {
    v3.writeBlock(33, this.DATA_CARGA_B21);
    v3.writeBlock(34, this.DATA_CARGA_B22);
}
```

图 1.MIFARE 设备

从上图中的代码我们可以看出，如果代码运行在有 NFC 的设备上时，它能够进行卡的读写。该恶意程序向卡写入预定义数据，将用户的账户余额提高到 10000 智利比索（约合 15 美元）。这种方法只适用于这种票卡，因为此方法依赖于卡的格式。这个工具的作者是如何在没有认证秘钥的情况下重写卡上的数据的呢？这是因为这些卡基于旧版本的 MIFARE，而旧版本的 MIFARE 有许多安全漏洞。攻击者能够在 10 秒内克隆或修改 MIFARE Classic 卡。而这种攻击所需的相关设备（如 Proxmark3）在网上也有售卖。

图 2.Proxmark3

攻击者可以利用市面上这些工具破解卡的认证秘钥，并通过移动端的应用程序使用获得的秘钥轻易地克隆目标卡。

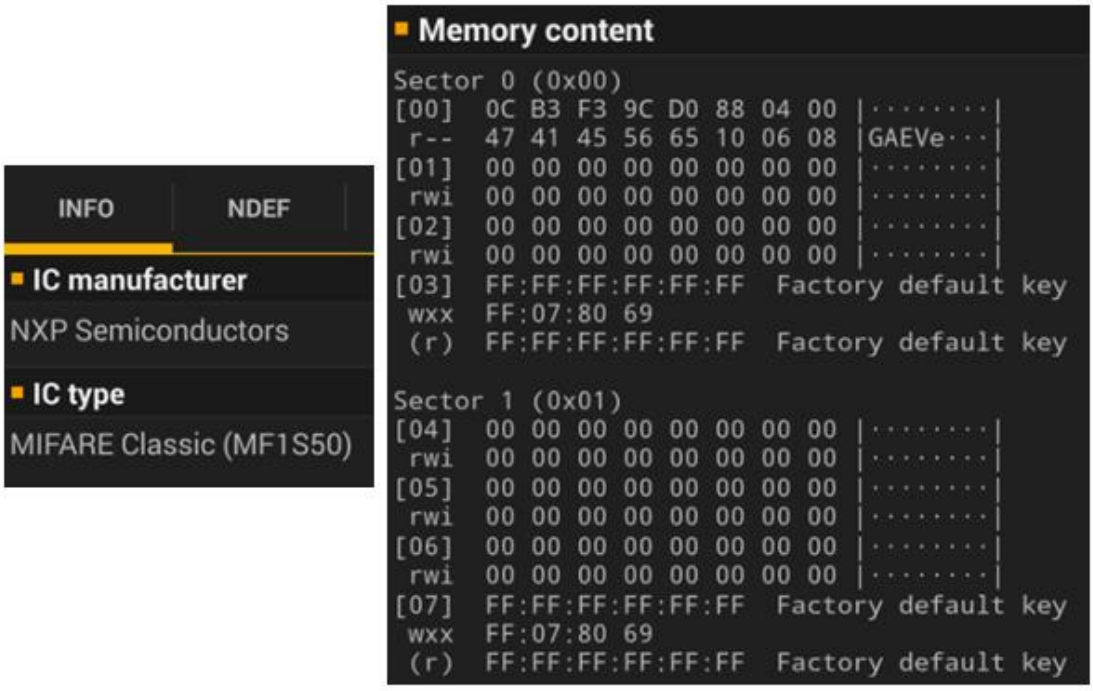


图 3.MIFARE Classic 卡的内存信息

同时，我们还监测到针对另外一种 MIFARE 卡（MIFARE DESFire 卡和 MIFARE Ultralight 卡）的攻击。至少有三种已知的卡片存在漏洞，包括带有银行账户的社会保障卡，用于交通和购物的支付卡，以及就餐卡。这种存在漏洞的社保卡至少有 700 万的用户数量。

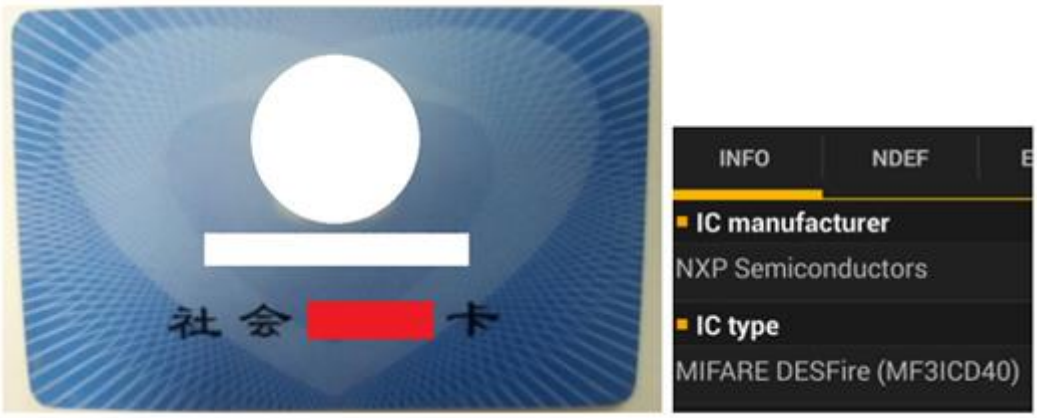


图 4.基于 MIFARE DESFire 的社保卡

上面提到的基于 MIFARE Classic 的就餐卡，以及我们的研究都能够证明卡片上的信息是可以被操纵和修改的。其他两种是基于 MIFARE DESFire 的，存在漏洞，可被边信道攻击利用。如果监控耗电情况，这些卡片的加密系统会泄露出相关信息，攻击者可以在七小时内还原出秘钥。如果秘钥不是随机生成的，那么这些卡片可以像 MIFARE Classic 卡那样被复制，甚至可能被带有 NFC 模块的设备直接操控。

总结

以上这些 MIFARE 格式都已经不再开发，并被新型的、更安全的模型取代。然而，许多卡片发行者会因为预算的考虑选择旧的方案，这等于将用户的安全置于危险的境地。我们建议用户提高安全意识，保护 RFID 卡的安全。经常查看卡片中的余额。如果可能的话，还应该关注自己使用的卡片是否存在安全漏洞并将这些情况反馈给卡片的发行者。针对 RFID/NFC 的攻击已经受到了广泛关注，终端用户以及企业用户可以参阅我们之前发布的相关安全提示，保障信息的安全。

http://blog.trendmicro.com/trendlabs-security-intelligence/good-nfc-habits

http://blog.trendmicro.com/trendlabs-security-intelligence/safe-nfc-for-businesses

关于趋势科技（Trend Micro）

趋势科技是全球虚拟化及云计算安全的领导厂商，致力于保障企业及消费者交换数字信息环境的安全。趋势科技始终秉持技术革新的理念，基于业内领先的云计算安全技术(Smart Protection Network)核心技术架构，为全世界各地用户提供领先的整合式信息安全威胁管理技术能防御恶意软件、垃圾邮件、数据外泄以及最新的 Web 信息安全，保障信息与财产的安全。同时，遍布全球各地的 1,500 余名趋势科技安全专家可为各国家和地区的企业级个人用户提供 7×24 的全天候响应及技术支持服务。更多关于趋势科技公司及最新产品信息，请访问：www.trendmicro.com.cn。请访问 Trend Watch：www.trendmicro.com/go/trendwatch 查询最新的信息安全威胁的详细资讯。