2014 年第一季度手机病毒发展趋势报告

作者：包沉浮

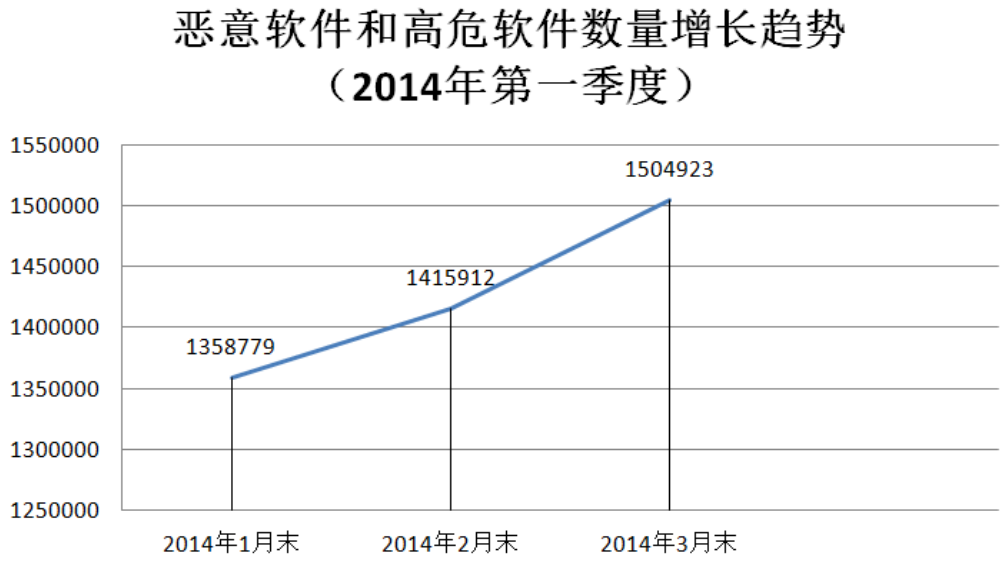
报告摘要

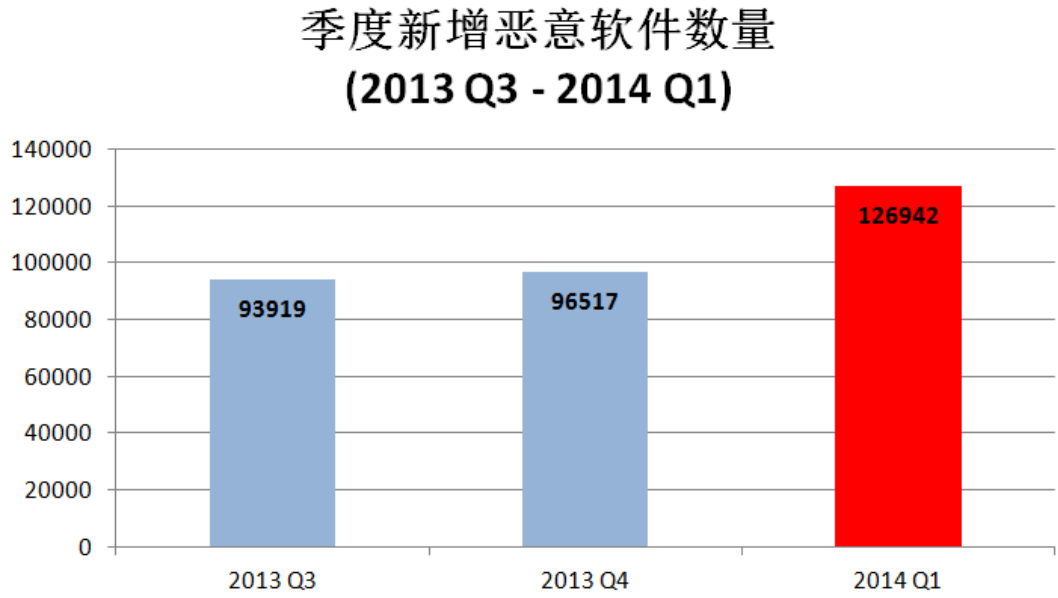
2014 年第一季度

1. 恶意/高危软件持续高增长，首次突破 150 万大关
2. 针对手机支付的钓鱼行为逐渐兴起
3. 病毒开始更多的利用“应用加固”技术

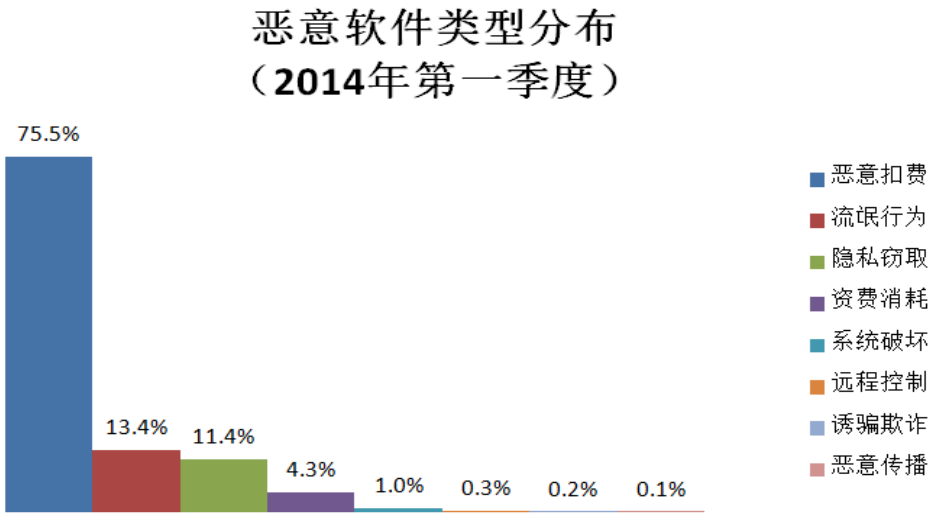
恶意/高危软件综述：突破 150

截至 2014 年 3 月 ,Android 平台上的恶意软件和高危软件总数首次突破了 150 万款大关，其中恶意软件共 53 万款，高危软件共 97 万款。恶意软件的增长速度在这一季度出现了大幅提升的态势，这一季度新增的恶意软件就超过了 12 万款，比上一季度高出了 3 万。

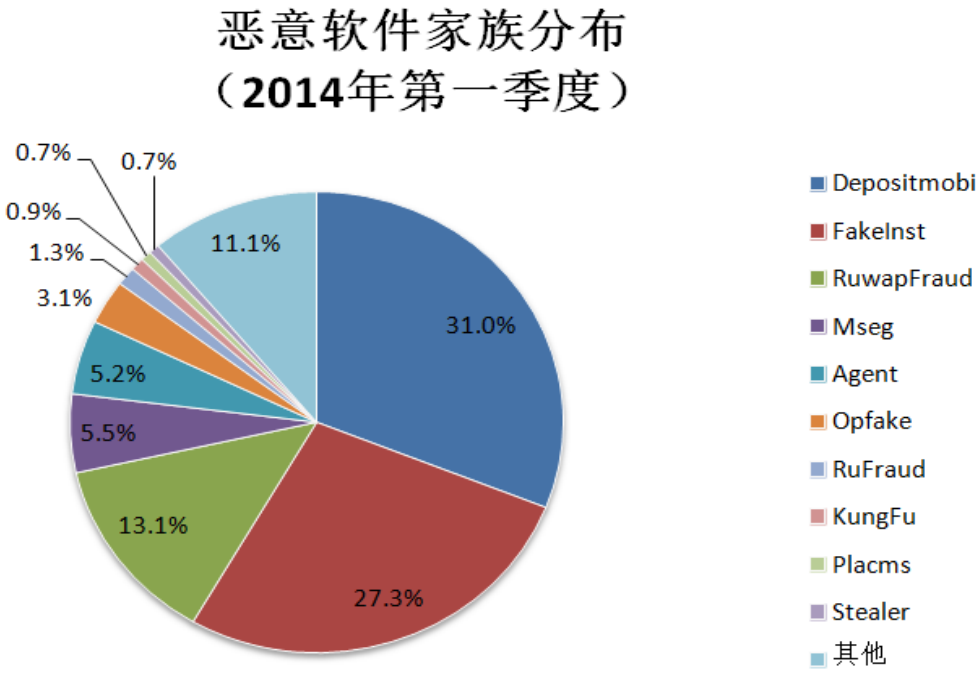




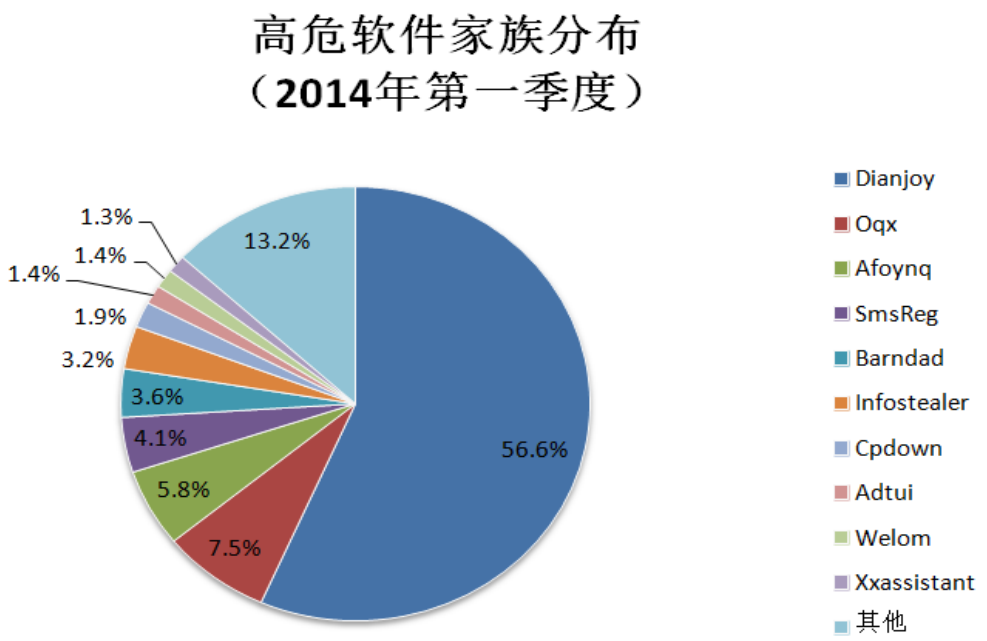
恶意扣费类软件仍然是 Android 平台上最大的安全威胁，这一类软件在 2014 年第一季度的恶意软件总数中占到了 75.5%，其次是占比 13.4%的隐私窃取类软件。



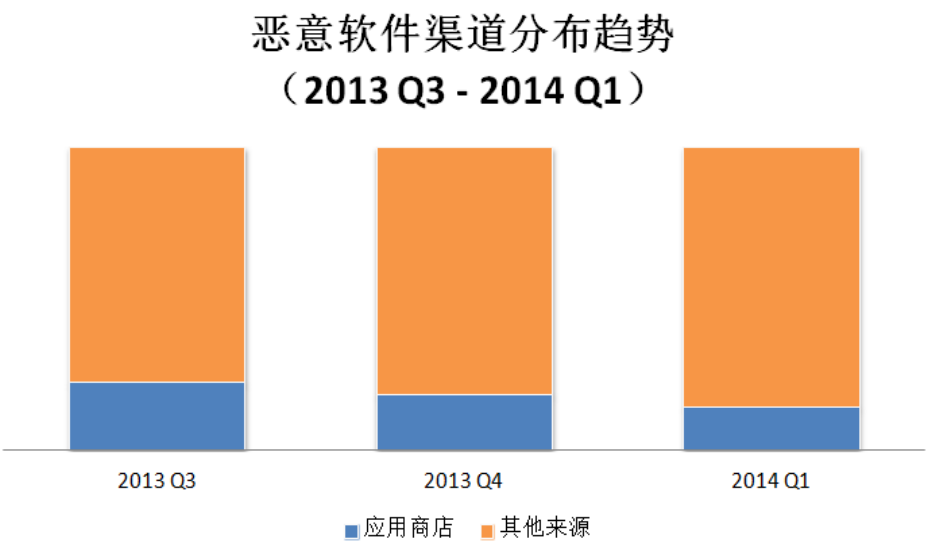
在恶意软件方面，Depositmobi，FakeInst，RuwapFraud 三个家族占到了全部恶意软件总数的 71.4% ,这几个很长时间以前就已经存在的恶意扣费软件到目前为止仍然非常活跃。



包含 Dianjoy 广告平台的软件占据了近期高危软件的半数 ,该广告平台会向用户推送应用，可能会给用户带来不必要的流量损失。



这一季度，来自于应用市场的恶意软件比例相比于上一季度有较大幅度的下降。随着应用商店审核机制的逐渐严格，这一比例已经连续三个季度有所下降，恶意软件开发者已经将目标逐渐转移到了其他的分发渠道。不过百度安全实验室仍然在超过 40 家应用商店中发现了恶意软件的存在，应用商店的安全性依旧不容忽视。



针对手机支付的钓鱼软件兴起

2014 年第一季度共新增恶意软件和高危软件类型 200 种，其中有 63 款属于全新的恶意软件和高危软件家族。这一数字比起上一季度略有下降，但是一些趋势仍非常值得关注。

在这一季度新发现的威胁中，出现了大量针对手机支付和网购客户端的“钓鱼”类软件。

为了盗取用户的银行账号和密码等隐私信息，这类“钓鱼”软件通常会在用户打开手机银行等软件的时候，将正常的软件页面关闭，取而代之的是弹出一个足以以假乱真的钓鱼界面。和在 PC 上常见的钓鱼网站相比，由于钓鱼客户端不依赖于浏览器，因此呈现出来的界面中并不包含任何网址等标识信息，普通用户几乎完全没有能力鉴别其真伪，因此对于用户来说危险性极高。此外，由于用户手机的短信收发过程也可以被恶意软件完全控制，短信验证码这

一通常的安全手段也有可能被轻易绕过。恶意软件通过这种方式，可以在不知不觉中窃取用户的信息，给用户的账户安全带来了极大的安全威胁。

“银行悍匪”软件伪造的工商银行客户端界面

加密手段增强：“应用加固”被恶意软件利用

为了对抗安全分析，很多恶意软件都会在代码中使用各种各样的加密和反调试手段。此前，Android 平台上的大部分恶意软件使用的都是代码混淆，字符串加密等简单的保护方式。而现在，更多的恶意程序开始利用一些公开的“应用加固”服务为其提供代码加密、反调试等保护，以达到更强的保护能力。

根据实验室的数据，本季度发现的恶意软件中，有超过 400 款使用了公开的应用加固服务，这一数字远远高出之前的比例。

这些应用加固厂商提供服务的初衷本是好的，可以在一定程度上保护软件开发者的知识产权。但是它很显然也是一把双刃剑，因为一旦审核过程出现问题，导致恶意软件被加固并发布，将会增大安全分析人员检测和分析其恶意代码的难度，从而不知不觉中成了恶意软件的“帮凶”。对此，加固服务提供商通常都会在加固之前使用第三方扫描引擎对应用进行一些安全扫描，但是对于之前并没有出现过的恶意软件，这种扫描几乎是没有作用的。