2014 年第二季度手机病毒发展趋势报告

作者：包沉浮

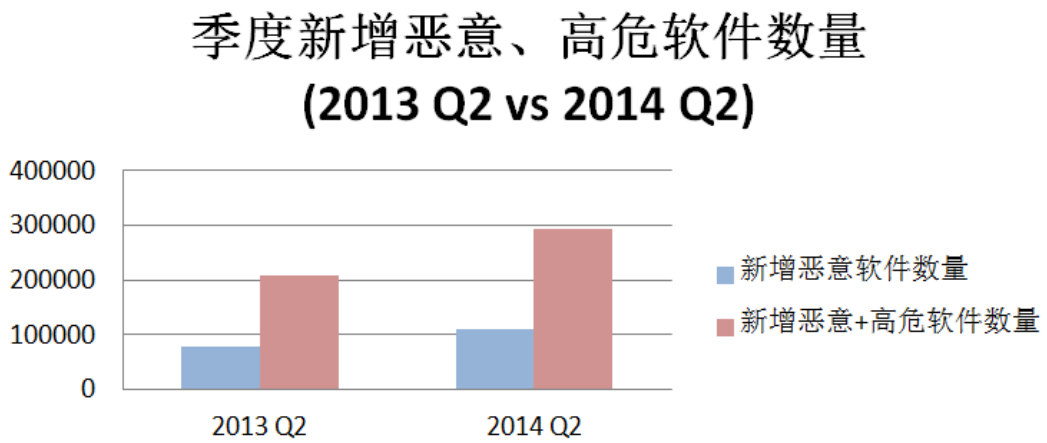
报告摘要

2014 年第二季度

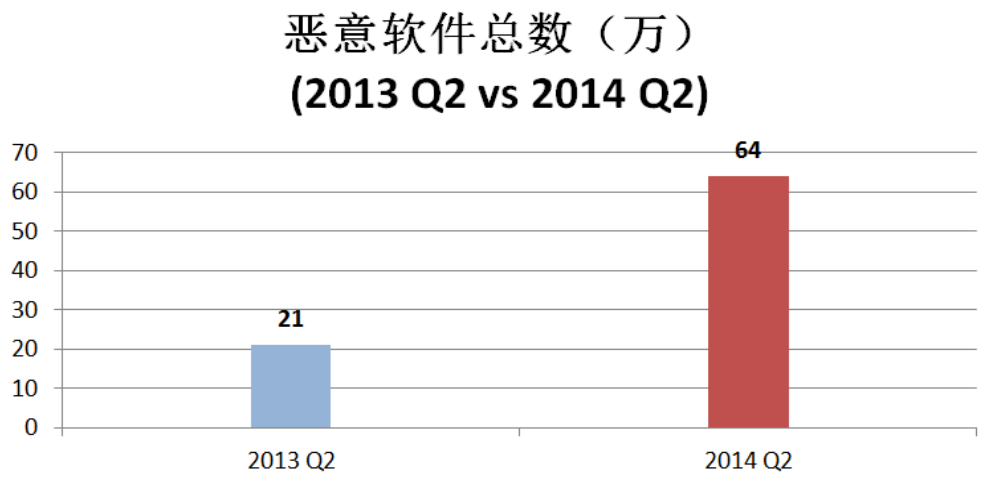
1. 恶意、高危软件增速持续
2. 隐私窃取类软件呈现爆发趋势
3. 新网银漏洞严重影响支付安全
4. Android 系统被曝拨打电话漏洞，影响面广泛

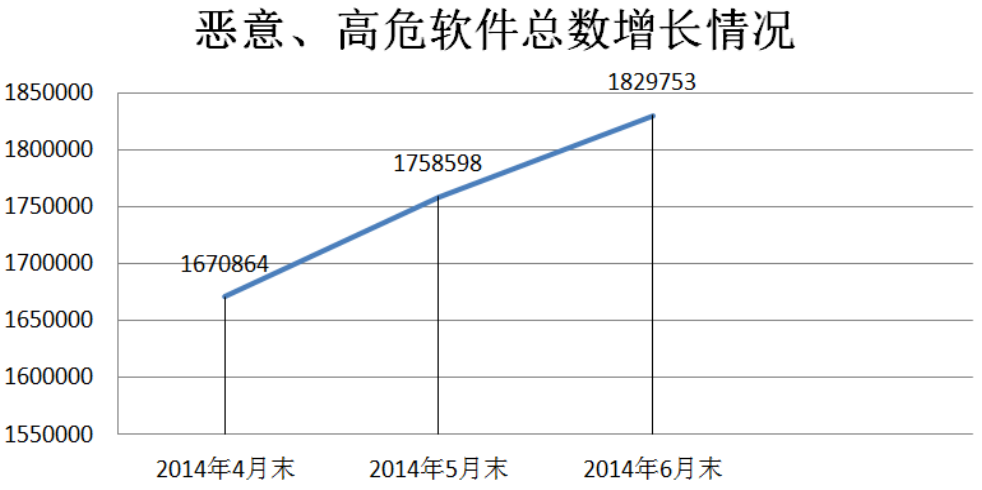
恶意、高危软件增速持续：恶意软件数量达去年同期三倍

根据百度安全实验室数据显示，本季度新增恶意软件 11 万款，高危软件 18 万款，继续保持很高的增速。恶意软件和高危软件的新增数量和去年第二季度相比，提高了 41%，其中恶意软件的新增数量提高了 43%。



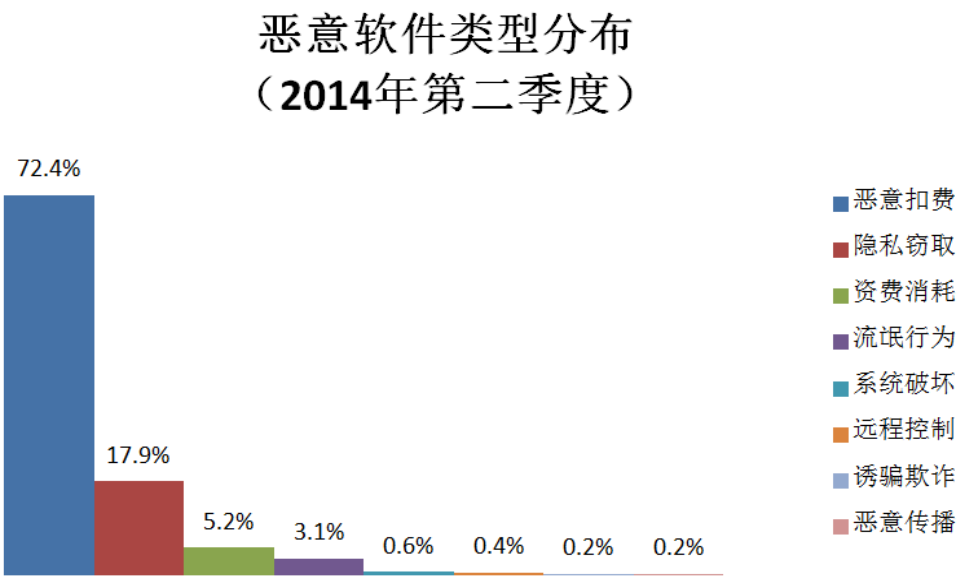
截至第二季度末，Android 平台上的恶意软件和高危软件累计已达 182 万款，其中恶意软件有 64 万款，恶意软件的数量是去年同期数量的三倍。





隐私窃取类软件呈现爆发趋势

百度安全实验室的统计数据显示，本季度，恶意扣费类软件仍然占据恶意软件的大多数，但是值得注意的是，隐私窃取类的恶意软件在本季度迎来了爆发。和上一季度相比，隐私窃取类恶意软件的比例上涨非常迅速，达到了 17.9%，上涨幅度达到了 57%。

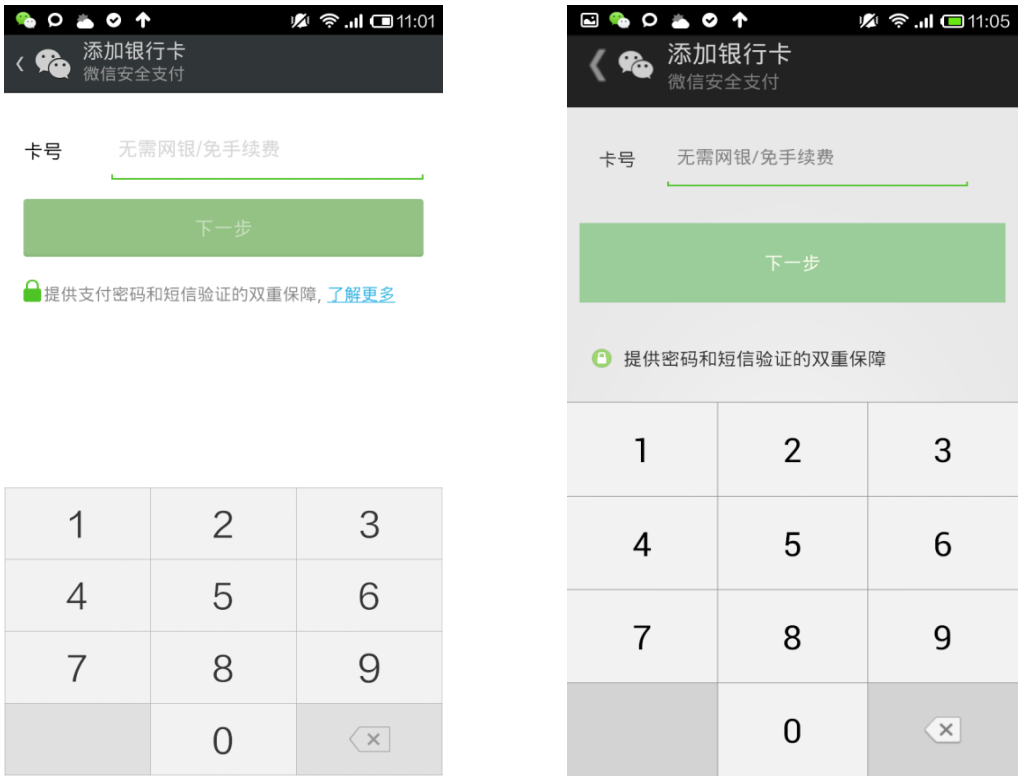


这是一个不容忽视的趋势，随着手机上的金融，购物，社交等功能逐渐成为人们生活中不可缺少的部分，人们的手机上也承载了越来越多的隐私信息。其中很多隐私信息与金钱利益直接或间接相关，因而很自然的成为了恶意软件开发者的目标。由于涉及用户隐私的应用种类繁多（比如手机银行就有数十家），对其中的某一种或者某几种隐私信息进行有针对性的窃取，相比于单纯窃取短信、联系人等行为隐蔽性更强，更难以被轻易检测到。

根据百度实验室的安全专家分析，隐私窃取类的恶意软件呈现出以下趋势：

1、大量以山寨应用方式呈现。

根据百度安全实验室的监测数据显示，针对网银、支付、购物应用和社交应用的山寨情况持续泛滥，光是各种网银应用的山寨版本就超过了 500 款。由于这类应用往往都需要用户输入账号密码等隐私信息，一旦用户使用山寨应用，这些隐私就会轻易被窃取。山寨应用的开发门槛极低，且欺骗性很强，已成为对用户隐私的最大威胁之一。近期安全实验室发现的“微信支付大盗”就属于一个典型的山寨软件，其界面足以以假乱真（左为正版，右为山寨版），普通用户根本无法分辨：



对此，建议普通用户尽量选择知名的应用商店，下载有“官方版”标识的应用，以避免下载到山寨应用。

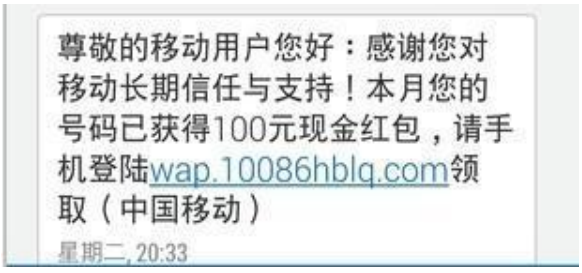
2、技术手段更加深入。

百度安全实验室近期发现的一款恶意软件甚至使用了进程注入的方式来窃取用户的 QQ 和微信的聊天内容，这也是 Android 平台上已知的首款通过进程注入方式进行隐私窃取的恶意软件。因为进程注入的方式一旦生效，会使得恶意程序有能力拿到被注入程序的所有运行时数据，甚至包括未加密之前的密码，所以威胁性极高。而这也对程序自身的安全机制提出了更高的要求，尤其是金融类，社交类软件，在技术上需要有更强的自我保护能力。由于 Android 沙盒机制的限制，此类手段大都需要恶意软件事先获取手机 root 权限，建议普通用户

要轻易 root 手机，或者授予不明来路的应用以 root 权限，以防被此类恶意软件植入系统中。

3、多种恶意手段的结合运用。

众所周知，银行、运营商等服务为了提供更高的安全性，通常使用手机验证码+密码的双重认证机制。为了突破这种认证机制，一些恶意软件中集成了网页钓鱼及监听手机短信等技术，一方面通过钓鱼网站或者页面窃取用户的密码信息，一方面通过监听用户短信来窃取手机验证码信息。此外，最近流行的“伪基站”技术也被恶意软件利用作为其分发渠道。百度安全实验室此前截获的一款伪中国移动客户端就使用了伪基站技术进行恶意分发，犯罪分子首先通过伪基站方式发送伪造 10086 的短信（如下图），



诱导用户点击钓鱼链接，并在钓鱼页面诱导用户输入网银账号和密码、下载安装伪中国移动客户端，该客户端可以后台运行，截获用户的手机短信验证码，以达到窃取网银资金的目的。普通用户为了避免这类威胁，要尽量做到不要在手机上安装来路不明的软件，不访问来路不明的网址。

网银漏洞：大量手机银行存在签名滥用行为

近期，百度安全实验室发现，有包括邮储银行，兴业银行，交通银行，广发银行，华夏银行，光大银行等在内的近 20 家手机银行软件都使用了或者曾经使用过同一款签名。而且经过实验室进一步分析发现，该签名甚至还用来签发了很多个人开发者的应用。调查得知，这些银行的手机客户端应用都是外包给一个名为“北京融易通信息技术有限公司”开发的。而且，有证据标明该公司并没有对该证书进行严格管理，导致其被用来签发了很多个人程序。

虽然目前安全实验室尚未发现此证书被利恶意利用，但是无疑该漏洞存在着巨大的安全风险。众所周知，Android 系统中证书是用来建立应用程序与其所有者之间的信任关系，是 Android 安全机制中的重要组成部分。各家银行作为独立的公司实体，且与用户财产密切相关，理应使用其独有的签名证书来标识其客户端的唯一性，并且严格管理此证书确保不会外泄。即使程序是由其他公司负责开发，证书也应该由银行自身来进行独立管理。否则基于 Android 系统中使用相同证书的应用可以利用的一些规则和权限，一旦证书被人用来制造恶意程序，就会给使用这些客户端应用的用户带来极大的安全威胁。

Android 系统新漏洞：CVE-2013-6272 漏洞细节被公开

近日，Curesec 团队公开了其之前发现的 Android 系统漏洞 CVE-2013-6272 的技术细节。该漏洞存在于 Android 系统的电话模块中，恶意程序可以利用该漏洞，在无需申请拨打电

话权限的情况下，在后台拨打任意电话（包括付费电话），给用户造成资费消耗；也可以挂断当前正在进行的通话，对用户造成严重的干扰。该漏洞的影响面很广，从 Android 4.1.1 版本开始就已经存在，直到 4.4.3 版本中才被修复。

目前百度安全实验室还没有发现利用此漏洞的恶意软件，但是因为其技术细节已经被公开，且目前受影响的这些系统版本（4.1.1-4.4.2）的使用非常广泛，可能会很快被恶意开发者利用。