易观智库&安全管家

--2012 年上半年手机安全行业联合专题

2012 年 7 月

目录

一、 专业术语

- 窃隐私：任何恶意软件都可能具有该恶意行为。读取用户的隐私信息，包括 imei 号码、手机号、短信息、联系人、通话记录等，然后用联网上传甚至发送短信的方式把这些信息发到指定的服务器或手机上。
- 暗扣费：私自发送短信订制 sp 服务，并且屏蔽回执短信，是暗扣费危害中比较典型的一种表现形式。
- 耗流量：私自联网下载软件是耗流量危害中比较严重的一种形式。

二、 上半年手机安全市场病毒状况

2012 年 1 月-6 月，安全管家通过移动云安全中心，共发现手机恶意软件 33930 款，其中安卓平台发现 26580 款手机恶意软件，塞班平台发现 7350 款。安卓平台相比去年同期增势猛劲，而塞班平台则出现下降趋势。具体如下：

塞班平台：

2012 上半年，塞班平台病毒危害特征与去年相比变化不大，主要集中在数据破坏、资费消耗、恶意扣费、恶意传播这四大大类。

数据破坏：大多数严重的流氓运行前就会关闭第三方安全类软件，在用户不知不觉中对用户造成损失。

资费消耗：频繁私自联网，消耗用户大量流量。

恶意扣费：私自发送定制业务短信，使用户在成不必要的损失。

恶意传播：捆绑安装其他流氓软件是一种比较常见的一种流氓传播方式。

安卓平台：

2012 年上半年，安全管家在安卓平台拦截查杀病毒数量相比去年同期有增长迅猛，尤其是 6 月份以来，安卓平台手机病毒种类与数量的高速增长尤为明显。

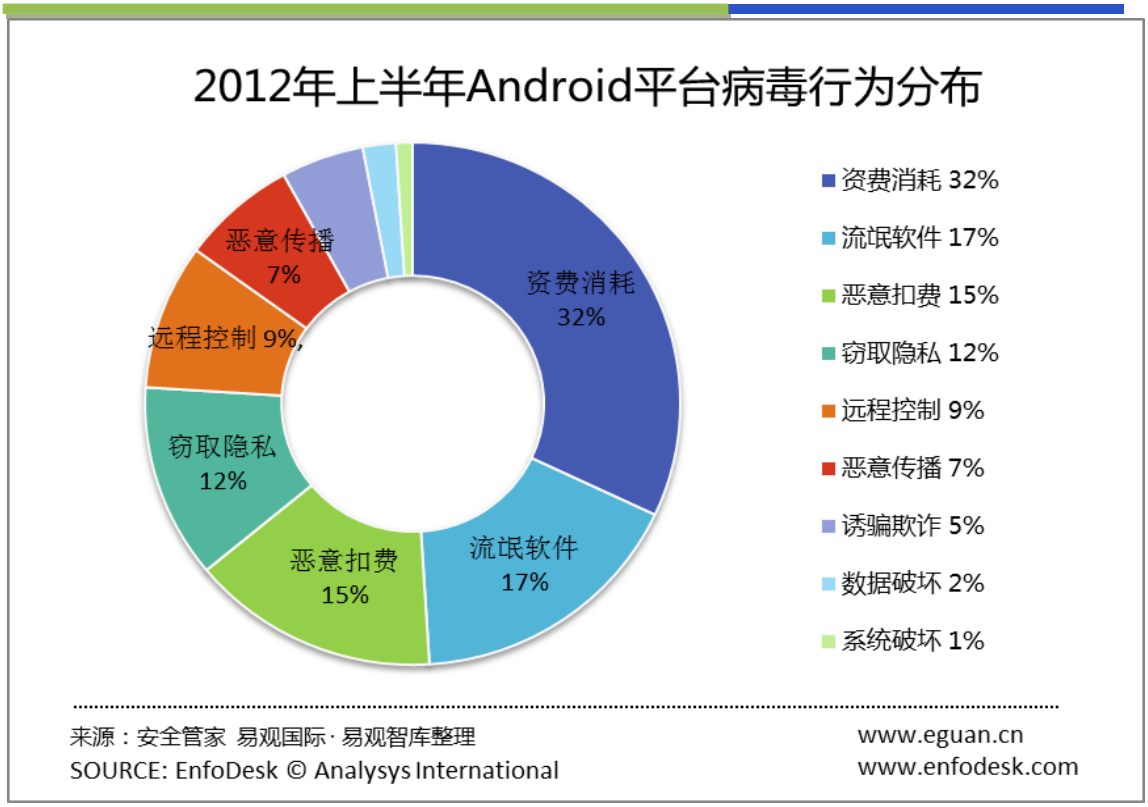
随着 Android 智能手机普及率的不断提高， Android 系统应用也如雨后春笋般蓬勃发展着，2011 年第四季度中 Android Market 更以每月 9.3%的应用增长速度首次超越苹果 App Store。

Android 系统应用爆发式的增长也令我们不得不面对应用整体质量下降、充斥垃圾应用以及病毒应用广泛传播，众多缺乏有效监管的第三方 Android 应用市场的涌现更是病毒应用滋生的沃土。对于私自下载流氓软件、发送恶意扣费短信、窃取用户隐私等病毒应用恶意行为，很多用户早已深恶痛绝。

此外，越来越多的传统互联网厂商进入到 Android 手机平台，通过直接推出互联网手机或者和其他厂商合作，预装各种应用软件，这在某种程度上加剧了手机病毒泛滥的趋势，也扩大了手机病毒投放的渠道。

6 月以来，Android 平台以恶意推广为主的病毒明显增多，感染热门游戏为主的手机病毒也呈连续递增趋势。破坏安全软件获取用户隐私的手机病毒的增长态势也让人忧虑。

2012 上半年病毒危害特征与全年相比变化并不大，由于 Android 平台的开源性以及 Android 平台的持续高速发展，窃隐私、暗扣费、耗流量等依然是 Android 平台占比较大的集中危害。



与传统的 Symbian 平台手机木马危害不同的是，15%的 Android 平台手机木马目标是悄悄吞噬用户的手机话费，另有 12%的安卓木马则瞄准了手机通讯录、照片、短信、设备信息等用户隐私， 6 月份安全管家解惑的隐私获取类病毒一个典型特征是，更多的不法分子受利益驱使开始通过破坏手机系统或者安全软件，影响用户对手机正常使用，继而在后台联网窃取手机用户的 IMEI 号或者 IMSI 等隐私或者通过病毒子包收集用户的联系人、短信信息发送到指定号码，造成隐私泄漏。

Enfodesk 易观智库研究发现，虽然 Android 病毒的危害总体还是以扣费、窃隐私、耗流量这三大项为主，但是具体形式更加多样，也更加令人防不胜防。

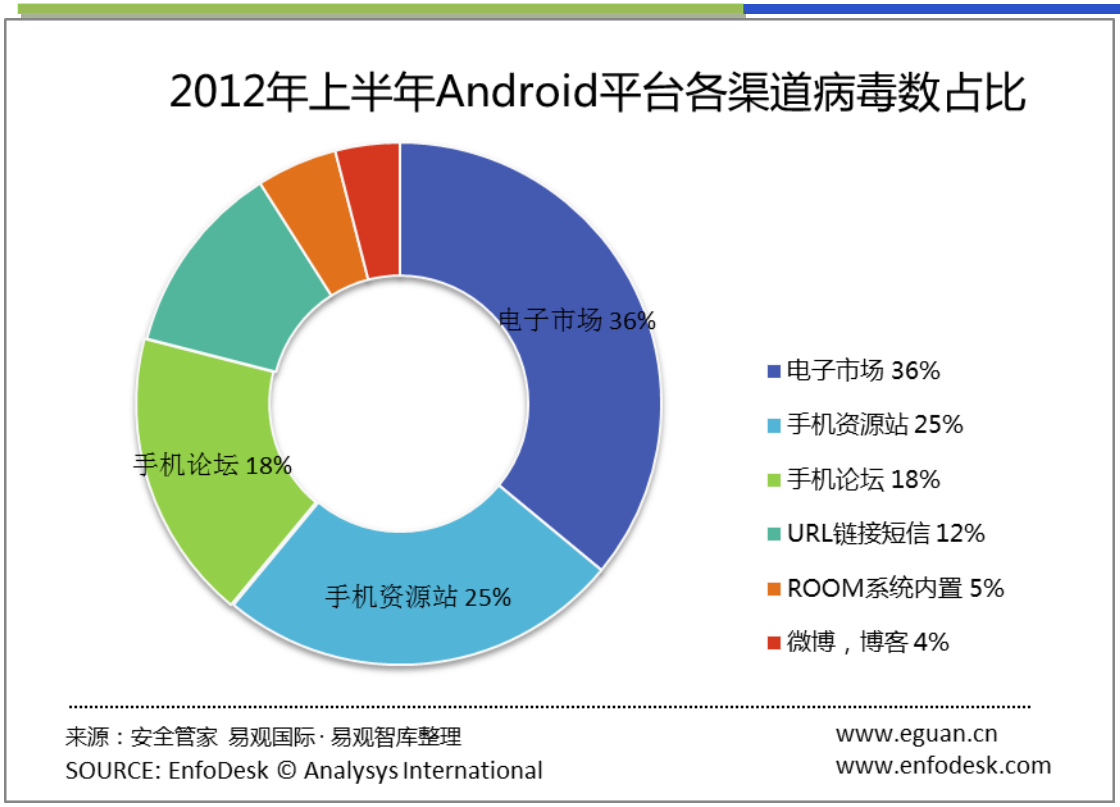
在上半年病毒数量大幅增长，特别是年初受节假日等消费高峰时段影响，扣费病毒在病毒数量中的占比较高。但是 Q2 开始，扣费病毒数量依然很多，并且依然呈上涨趋势但是由于病毒总数增长较快，扣费病毒在病毒数量中的占比下降，恶意广告推送类病毒开始流行。

手机病毒捆绑热门应用植入恶意推广广告，无提示私自下载推广软件或快捷方式，消耗

用户资费是 6 月份资费消耗类病毒一个最典型的特征。与此同时，一些常规的资费消耗类病毒会通过后台自动联网的方式，从服务端获取更多的指令，定制更多的 SP 收费业务；或者通过远程控制，私自发短信到制定号码到远程服务器造成资费消耗。另外，在系统破坏、隐私获取类、诱骗欺诈类病毒的行为特征之中，往往都伴随着着资费消耗，这也是资费消耗类病毒比例高居不下的原因。

上半年总体虽然 Android 病毒的危害总体还是以扣费、窃隐私、耗流量这三大项为主，但是具体形式更加多样，也更加令人防不胜防。面对日益严峻的手机安全形势，国家相关部门也加大了监管力度，6 月初工信部发布的《关于加强移动智能终端进网管理的通知》就明确规定了申请进网许可证的移动智能终端不得预装恶意软件，这对行货手机、平板来说是个不错的消息。

根据 2012 年上半年安全管家拦截病毒渠道的数据分析显示，电子市场、手机资源站和手机论坛是主要的病毒集中区域。其中电子市场占比高达 36%，主要原因很多审核宽松的第三方电子市场缺乏严格的软件安全检测机制，致使大量没有经过安全检测的软件在电子市场进行传播，目前电子市场已经成为了 Android 病毒传播的最重要渠道。



手机资源站，占比 25%。很多手机资源站同样具有审核不严的隐患，成为了病毒传播的另一个重要渠道。

手机论坛，占比 18%。由于手机论坛的审核机制很难阻止用户上传病毒附件或链接。

URL 链接短信，占比 12%。一些手机用户对 URL 链接短信已经有了防范意识，但是仍有很多相关常识薄弱的用户会下载到病毒。

ROOM 系统内置，占比 5%。水货手机市场的发达促进了手机刷机行业的繁荣，一些水货刷机商将病毒刷入手机 ROM 以获取更高的利益，这使得一般用户难以清除这些病毒。微博、博客占比 4%。微博作为近几年流行的社交方式，开始被利用以传播病毒，同样令人防不胜防，目前传播病毒，同样令人防不胜防，目前传播数量还比较少。

三、 下半年趋势预测

- 国家监管持续加强

2012 年 1 月开始执行《移动互联网恶意程序监测与处置机制》，6 月份工信部又发布了《关于加强移动智能终端进网管理的通知》，可以看出国家对移动互联网安全的重视，相信国家对移动互联网安全的监管力度会不断加强。

- 边缘病毒开始出现

随着国家的相关规定出台，打擦边球的病毒也会开始慢慢浮现，试图利用国家规定的漏洞或覆盖不到的范围而牟利或者进行其它损害用户利益的行为。这就需要第三方的手机安全软件以用户的利益和正常软件开发者的利益为保护对象，根据情况及时调整自己的查杀标准。

- 病毒类型更加多样、分散、复杂

扣费类病毒的占比会继续下降，病毒类型更加多样，原来数量较少的数据破坏、系统破坏类病毒会逐渐增长，一些较为复杂的病毒会慢慢浮出水面，在已 root 的手机环境下造成巨大的破坏和损失。一些病毒为了规避手机安全软件的查杀，潜伏期会更长，隐蔽性会更强。

四、 典型手机病毒

塞班平台：

s.payment.plbz:该类软件伪装成壁纸软件，私自发送定制业务短信，造成用户资费的大量消耗。

s. destroy.wlyx: 该类软件安装后会关闭第三方安全类软件 ,造成手机或软件无法正常使用。

s. unapproved.sdrj: 该类软件伪装成第三方杀毒软件，私自捆绑安装其他流氓软件。

安卓平台：

食人鱼：该类病毒私自发送短信定制 SP 服务，造成资费的消耗。

毒胶囊：该类病毒利用系统漏洞获取 ROOT 权限，无提示私自联网下载安装其他流氓软件，消耗用户高额的流量。

追踪大盗（gpssms）：该软件伪装成正常应用，判断地理位置来发送短信定制 SP 业务，并屏蔽运营商的回执消息，造成资费的大量消耗。

Picshow：利用系统漏洞获取 Root 权限，联网下载安装流氓软件，并卸载指定程序，造成手机或软件无法正常运行。

暗推（aseiei.apxxxx）：该软件被植入推广广告，私自联网下载推广软件，造成资费的消耗。

五、 易观建议

Enfodesk 易观智库分析认为，目前手机安全市场形势严峻，病毒错综复杂千变万化，各种新技术的结合运用更让病毒如同隐形。Enfodesk 易观智库建议手机用户在需要下载软件的时候，选择口碑不错、评价比较好或者是打分比较高的软件，对于一些知名软件尽可能到其官方网站进行下载，不要轻易下载安装来历不明的陌生软件。

此外，用户应该养成安全的手机使用习惯，对于手机论坛的破解版、汉化版等热门游戏的下载链接，应持有谨慎态度;应该选择经过手机安全软件认证或者病毒检测服务的电子市场下载软件;手机端应用市场与 PC 端相比，目前尚缺乏覆盖面广的有效病毒检测与防御机制，应该谨慎选择。

关于易观智库

易观智库是一款以订阅制方式为客户提供中国创新产业经济发展的商业信息服务平台。易观智库已成为国内外政府、企业、投资机构以及专业人士了解市场、提升判断力、创新力和决策力的首选信息工具。

易观智库拥有业内最丰富的内容资源与分析模型、最专业的信息分析与检索工具、最超值的分析师增值服务以及最便捷的定向推送服务。易观智库为客户提供可信、可靠、可用、成本有效的信息和数据，保障客户在市场持续发展和剧烈变化的过程中，把握商机、规避风险。

易观智库通过开放的平台，充分整合内外部资源，以数据、信息及工具等形式，构建成为一个富含丰富模块的商业信息服务平台 ,客户可以根据自身需求 ,选择并订阅所需的模块。

易观智库主要特色

- 帮助客户认知宏观经济环境的发展变化趋势；
- 帮助客户了解产业环境和市场发展趋势；
- 帮助客户洞悉现有或潜在的竞争对手与合作伙伴；
- 帮助客户掌握竞品的发展变化情况及创新产品动态；
- 帮助客户探求用户需求和行为变化.