编者按 近日，一款名为Android.Kmin.e的新型Android手机病毒传播于用户手机中，该病毒一旦发作，可以每隔1秒就发送1次扣费短信，给中毒用户造成巨额话费损失。事实上，随着移动互联网发展，特别是移动应用的丰富，作为承载了个人和公司各种核心信息的移动智能终端将面临巨大的安全挑战。本期，《通信世界周刊》特邀多位安全专家，共同探讨移动终端安全威胁以及2012年发展趋势，呼吁运营商、安全企业等各方携手合作，共同进行移动终端安全防护系统建设。

2011年安卓手机木马激增 六大安全厂商共话移动终端安全趋势

本刊记者 | 黄海峰

石晓虹 360安全专家
Android木马量一年增加400倍

2011年，Android（安卓）木马呈现爆发式增长，相较2010年全年共发现12个木马样本相比，今年1月~12月，360手机云安全中心捕获新增Android木马样本4722个，被感染人数超过498万人次。从今年8月起，Android平台每月新增木马连续4个月超过Symbian（塞班）平台，在新增安全威胁的增速与增量上全面居首，成为新的移动互联网安全攻防主战场。

虽然Symbian平台恶意软件及木马数量有增无减，全年新增3992个，但由于诺基亚的市场占有率的持续下降，再加上Symbian平台本身严格的应用审核机制的限制， 2011年下半年该平台被感染人数为1049万人次，比上半年的1206万人次下降13%。

在传播途径上，Symbian平台新增恶意软件及木马较为传统，最主要传播途径为Wap/Web下载。但Android木马在传播途径上发生了变革，由传统的Wap/Web下载转向水货存储卡/Rom预装、应用商店/市场、手机下载站及手机论坛，传播途径趋于多样化和复杂化。

除恶意扣费外，窃取用户隐私已经上升为手机木马的主要危害之一。例如震惊全球的“CIQ内核间谍软件”。

360安全中心统计数据显示，360手机卫士2011年全年为国内7000万用户拦截的垃圾短信超过100亿条。其中，根据用户举报上传的垃圾短信内容统计分析，打折促销类垃圾短信占比近四成，高居各单类别榜首，而冒充亲友欺诈、中奖钓鱼诈骗、虚假慈善捐款等恶意欺诈类短信比例也达到了24%。

唐威 瑞星安全专家
手机面临三大安全威胁

我们认为目前手机存在的安全威胁主要包括三个方面，一是电话骚扰和垃圾短信增多的威胁，二是个人手机信息和手机存储数据的安全泄露威胁，三是手机病毒影响手机用户的正常使用，有些恶意软件还会带来手机吸费的威胁。

去年移动互联网进入爆发期，安全需求也逐渐显现。所以，去年我们开始了对手机安全软件的大量投入。去年9月15日，我们正式发布了安卓版瑞星手机安全软件，去年底发布了基于iOS的瑞星手机安全助手。目前我们的安卓手机安全软件已经有超过500万次的安装。

个人手机安全市场像互联网应用一样，呈现免费态势，但是一些创新的模式依然可以让安全企业获得收益。企业级手机安全市场要求安全企业的专业性，为保证业务的安全，生产企业也愿意为高性能的安全防护系统付费。这将是我们的重点发展市场。

王志海 明朝万达总裁
移动安全市场处于发展初期

移动智能终端安全防护目前还处于发展初期，大部分厂商主要集中在病毒木马防护领域，而明朝万达可以提供整体的移动智能终端安全防护方案。

运营商与移动智能终端有着天然的联系，运营商在移动终端安全防护领域预计将扮演关键的综合安全保障服务者角色，一方面运营商有义务为其网络中的移动智能终端提供可靠安全防护服务，另一方面运营商也有优势选择能够提供优质产品和服务的安全厂商为其个人用户和企业用户的移动智能终端提供安全服务。目前，运营商应该积极宣传移动终端安全防护意识，并应该建立一整套可信、可靠和可证明的评估标准，选择出优秀的移动终端安全防护产品推荐给用户。

明朝万达自2006年即开始研发移动安全产品，并针对公安、电信等特定行业提供服务。明朝万达的方案特点有两个方面，一是聚焦于数据的安全管理，针对企业级移动用户的数据安全生命周期各个环节进行研究和防护；二是整体性，提供了涵括用户身份、通信、加密和设备等多个方面的安全管理和防护。目前，明朝万达与国内三大运营商在多个层面都建立了合作，为运营商的政企客户提供整体的移动安全解决方案，同时也为运营商自身的移动安全应用提供安全保障。

王南 卡巴斯基亚太区技术副总裁
移动终端防护是庞大的系统工程

移动互联网时代是以用户为中心的，运营商应该扮演积极参与者的角色，与内容提供商、服务提供商、移动终端厂商、安全厂商等一起投入，努力为用户打造安全的环境，在网关增强保护与过滤措施，强化监管职责，针对不良信息与软件的传播在上游对其进行有效遏制。

我们认为，移动终端防护不是简单做一款杀毒软件就可以达到的，而是一个庞大的系统工程，应该针对不同行业、合作伙伴与终端用户的具体需求，提供不同的安全服务，配合产业链上的其他环节，创建绿色环境。

针对移动终端安全需求，卡巴斯基实验室不仅推出了为个人用户设计的产品，同时也为有移动办公应该的企业用户提供了安全解决方案。卡巴斯基安全产品适用于运行Android、Symbian等使用不同操作系统的移动终端，保护不局限于基础的反病毒防火墙等安全服务，而且加强了隐私保护、反盗窃、垃圾短信骚扰电话过滤等高端智能管理需求，不仅能应用在各平台的智能手机上，还专门为基于Android的平板电脑开发了有针对性的方案。

在企业解决方案中，卡巴斯基实验室将移动终端安全保护整合到了整体企业解决方案中，管理员使用同一管理平台就能轻松管理企业中各种客户端。目前卡巴斯基和电信运营商的合作主要是在OEM合作，将已应用于卡巴斯基PC版上的KSN云扫描（卡巴斯基安全网络）整合到移动产品中。

邹仕洪 网秦手机安全专家
个人与企业移动安全需求不同

在移动安全市场方面，有人认为免费的个人市场不如企业市场潜力巨大。对此，我们认为个人与企业移动的需求并不太一样，个人移动手机安全市场比较注重对费用及隐私的防护，而企业则对保密性的防护，如机密文件等，侧重点不一样。

从个人安全市场来看，我们看到了部分应用企


瑞星安全专家 鹿旗


明朝万达总裁 王志海


网秦手机安全专家 邹仕洪


金山网络安全工程师 李铁军

业采用的是免费的服务模式，但我们仍然看到了大量的用户在希望享受免费基础服务的同时，在有选择地通过合理付费订购一些差异化服务，而伴随用户碎片化需求的增加，个人安全市场以及付费产品服务的潜力仍然巨大。

在企业安全市场，更多企业的信息管理人员已意识到，安全已成为了企业信息化面临的最大阻碍，当企业信息化从导入期进入到成熟期之时，企业多会增大对安全的投资，而其潜在的市场容量和服务前景也非常广阔。

对于免费、付费的商业模式，实际并没有优劣之分，无论是哪种模式都可以做出优秀的产品以及优秀的公司，比如微软和Google，两者一个是付费一个免费的商业模式，但这并不影响他们提供优秀的产品以及成为优秀的公司。

相比目前市场上的其它安全产品，网秦公司推出的产品具备三大特点，一是我们安全信息积累的厚度更高，如网秦目前具备全球最大的恶意软件样本库；二是产品最早就提出的一站式立体防御的概念，阻止来自不同层面的安全威胁；三是我们的产品、服务均具备跨平台、跨终端的服务能力，如通过手机中的“网秦安全”备份数据，可以通过PC和手机登陆查看，这是目前国内厂商基本不具备的。

李铁军 金山网络安全工程师
应用层威胁超过操作系统层

就目前来看，大部分手机上的安全威胁都并非操作系统层面，而是来自于应用层面。为了保证应用的丰富，操作系统不得不提供权限。对于一般用户来说，目前的安全威胁不完全在操作系统上。需要注意的是各家推出自主操作系统的同时也会推出应用商店，对开发者上传应用的审核能力也影响着用户安全。

同时操作系统应该自我反思的是其是否提供了应有的基础安全能力，权限管理机制是否完备，是否提供了足够的安全引导及启动链的保护，包括防止因手机丢失发生数据泄露的数据加密功能。

操作系统层面的防护需要集中通用机制、如TPM(TCM)的可信引导；DEP、ASLR等漏洞防范；应用商店安全审核则需专业安全厂商参与。同时上层应用传输时数据及应用数据安全则应用本身也需考虑，不完全是操作系统保护范畴。

目前金山手机卫士在手机终端通过检测病毒的具体行为进行判定，从而帮助监测更加细致。终端只是我们作为样本及其特征捕获的方式之一，除此之外，我们在云端也进行了大量的工作，最终形成一套将终端特征检出、清除、阻断技术手段与云端对应的特征库结合处理的解决方案。

手机病毒呈高增长态势 江苏移动规模试用“一体化”防护技术

中国移动江苏公司 | 来晓阳

2011年，随着移动互联网和智能手机市场的持续发展，手机病毒继续保持着从2010年初开始高增长态势。据手机杀毒厂商统计，2011年新发现手机病毒及恶意软件种类超过历史总和，2011年底达到5000个以上。Symbian系统下的病毒数量和感染用户数量占到了全部数量的70%以上，Android系统病毒从2010年底开始持续增长，目前占全部用户数量20%，估计2013年以后，Android系统的病毒将成为手机病毒的主题。

手机安全威胁日趋严重

根据江苏移动对手机病毒监测分析，手机病毒和恶意软件充分利用了计算机病毒多年发展积累的技术，已经具备比较固定的传播和牟利模式，形成了一条黑色产业链。部分不法SP与部分山寨机合作，内置后门，强制用户订购业务或者盗取用户信息，垃圾广告商与手机恶意软件编写者相勾结，利用被控终端传播广告，而手机恶意软件编写者又为不法SP、部分山寨机提供软件工具。手机病毒防治工作非常艰巨。

目前在应用软件中捆绑恶意软件成为手机病毒和恶意软件传播的主流方式，占到手机病毒和恶意软件感染总量的70%左右，通过诱骗短彩信传播方式也占整个感染量的20%左右。

对广大用户而言，手机病毒危害主要表现在话费损失、个人信息泄密、受垃圾信息侵扰、部分应用无法正常是用、待机时间缩短等几个方面。对运营商而言，手机病毒会导致网络资源浪费，网络质量下降，同时还将严重的伤害运营商的企业社会形象。

“江苏模式”取得成功

江苏移动从2010年开始，开始探索手机病毒的治理工作，逐步建立了手机病毒防护体系。该体系依托组建专业的病毒防护团队，利用国际领先的网络侧手机病毒监测防护系统、根据手机病毒处置工作流程，开展病毒检测、病毒研判、病毒预警、病毒控制、应急响应等各项专业化的手机病毒处置工作，实现了控制手机病毒在移动网络内的传播，保护了客户权益、提升了网络质量。

经过近2年来的积累，目前江苏移动网络侧手机病毒监测系统可监测拦截近800个系列数千种手机病毒，目前南京地区手机病毒感染用户从2011年年初的25万下降到不足6万。降幅近80%，病毒产生的垃圾流量降低95%。相关技术和管理成果荣获通信学会安全应用奖二等奖及通信行业管理创新成果。

根据测算，到2012年底，手机恶意软件总数将达到10000种，新的传播和威胁形式还将不断出现，病毒编写者将会尝试各种手段试图逃避技术手段的检测和拦截。因此手机病毒防治工作将会是长期的持续不断地过程。

目前终端侧和网络侧手机病毒防护技术已经初步成熟，但是由于这两种技术手段目前没有充分结合，因此手机病毒处置窗口期仍然比较长，部分地区和部分机型上手机病毒感染情况非常严重，仍然有着很大的提升空间。

江苏移动未来将逐步融合终端-管道-云端，为用户提供一体化的手机病毒防护服务。相对与互联网厂家提供的手机病毒防护手段，电信运营有着掌握管道的天然优势。该防护体系推出后，将会极大提高手机病毒治理效能。

2011年安卓手机木马激增六大安全厂商共话移动终端安全趋势

作者：黄海峰
作者单位：
刊名：通信世界
英文刊名：Communications World Weekly
年，卷(期)：2012(9)