中国地区 2014 年度
网络安全威胁回顾及预测

2015/3

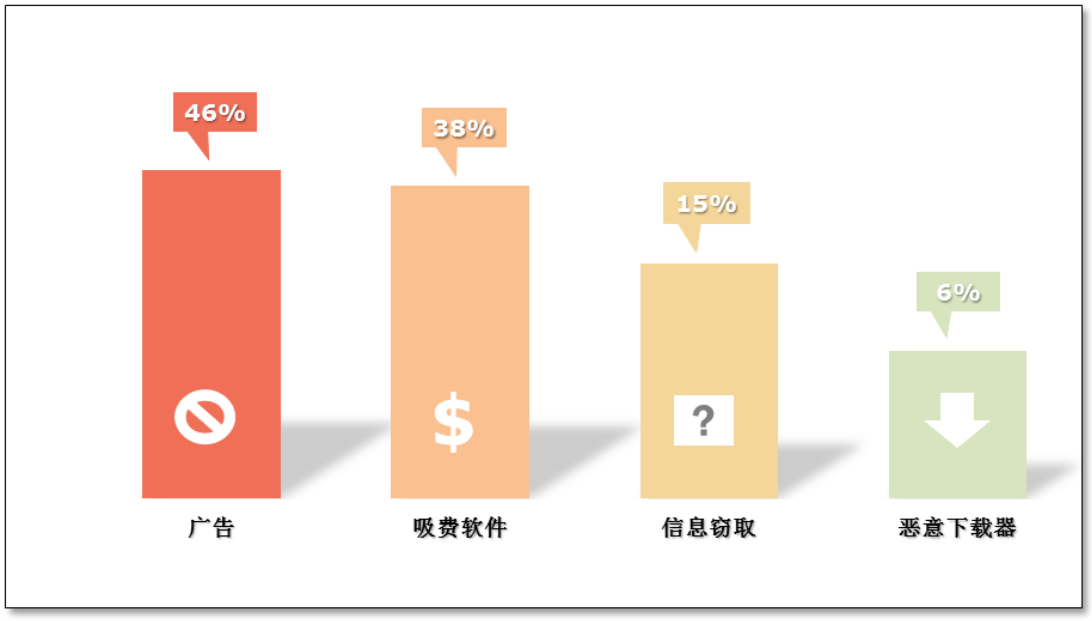
CHINA RTL

目录

趋势科技 2014 年度安全威胁回顾

1. 移动设备恶意软件数量增长迅速

移动设备安全问题日趋重要，从历史数据来看，安卓平台的恶意软件数量呈直线上升趋势。截止至 2014 年年底，趋势科技对 APK 文件的检测数量累计达到近 400 万个。其中以广告、吸费软件、信息窃取和恶意下载器这几种类型的恶意软件所占比重最多。恶意软件通常利用用户希望免费下载到收费应用或免费享用附加功能的心理来骗取下载量并进行传播。而在日常应用中，的确有许多用户会为此而 root 或是越狱自己的设备，这种行为会使用户设备更容易被恶意利用。值得注意的是，安卓平台用户并不是唯一受到威胁的移动设备用户群体，苹果 iOS 系统威胁在 2014 年逐渐浮出水面。诸如在 2014 年里披露的针对该系统的 WireLurker 家族病毒和 Masque 家族病毒，它们甚至可以感染未越狱的设备。

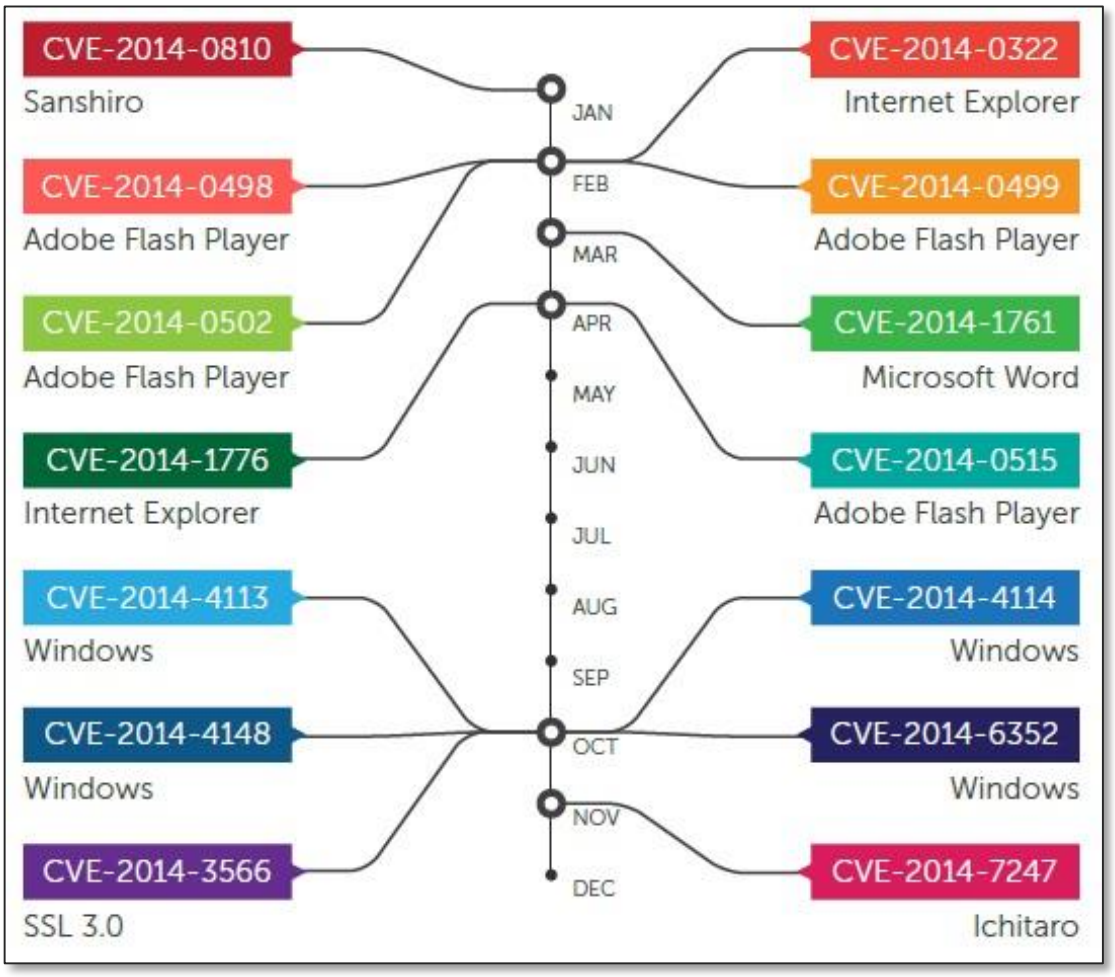


安卓系统主要恶意程序类型分布

2. 漏洞发现数大幅增加，第三方应用程序漏洞最多

据来自美国国家漏洞库(NVD)公布的统计数据：在 2014 年整年中 NVD 新加入漏洞共计 7,038 个，平均每日增加 19 个漏洞。与 2013 年的数据相比，2014 年漏洞数大幅增加，连续 3 年处于急速上升趋势。据统计，虽然在 2014 年中被标注为“严重”的漏洞比例较上年有所下降，但其总数高于 2013 年“严重”级别的漏洞数量，共计 1,704 个。在所有漏洞中有 83%的漏洞属于第三方应用程序上的漏洞，其次是操作系统漏洞占 13%，硬件漏洞占 4%。其

中浏览器中发现的漏洞数量最多：IE、Chrome 和 Firefox 这些流行浏览器漏洞数分别位列前三；Flash 和 Java 位列第四和第五。OpenSSL 心脏出血(Heartbleed)漏洞和 Unix 系统上的破壳(Shellshock)漏洞，这两个漏洞于 2014 年期间发现，影响范围十分巨大的漏洞，它们的发现警示人们没有一个应用程序或是操作系统是永不可摧的。

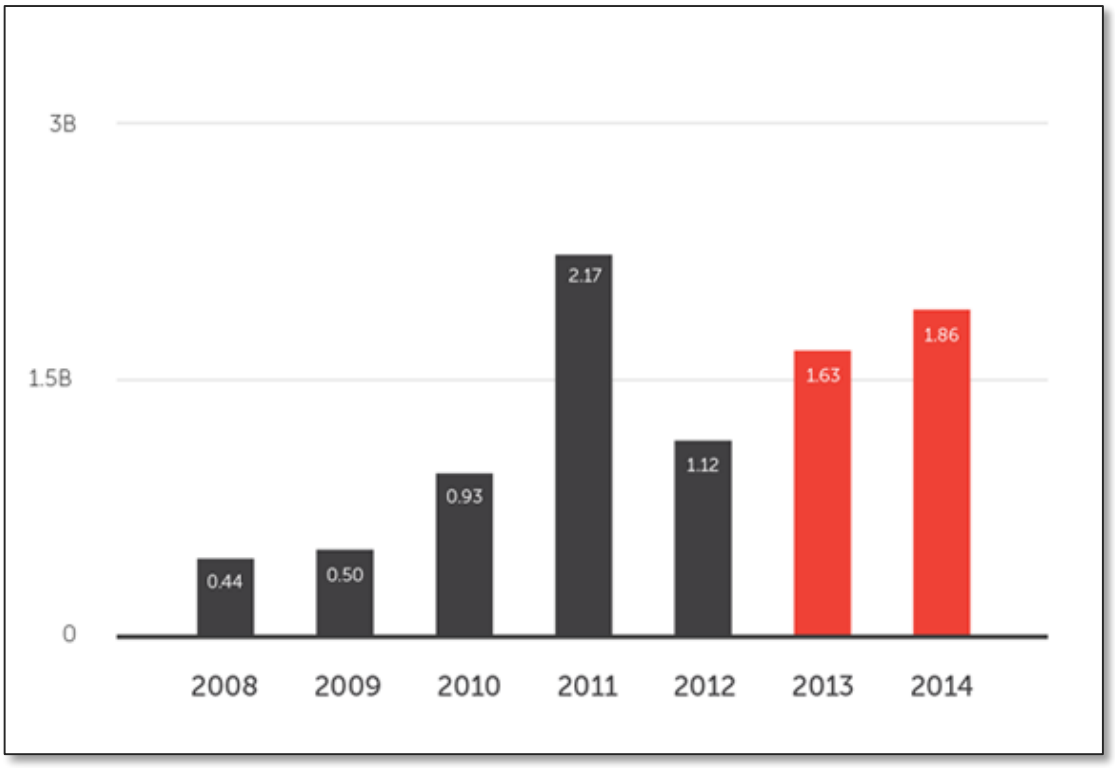


2014 年发现的主要零日漏洞时间表

3. 垃圾邮件数量略有上升，UPATRE 家族病毒附件传播最多

从我们的蜜罐数据得到的结果中，在 2014 年共捕获 19 亿封垃圾邮件，较 2013 年的 16 亿有所上升。虽然该数据不能代表所有垃圾邮件的总体状态，但也可从中探得垃圾邮件数量的整体趋势。从蜜罐数据中还反映出 UPATRE 家族病毒作为垃圾邮件传播的情况非常突出。UPATRE 家族通过一个名为 Cutwail 的僵尸网络进行传播，这个僵尸网络早在 2007 年就已出现，并在 2009 年被认定为是最大的垃圾邮件僵尸网络。

本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。



垃圾邮件增长趋势图 来源：蜜罐数据

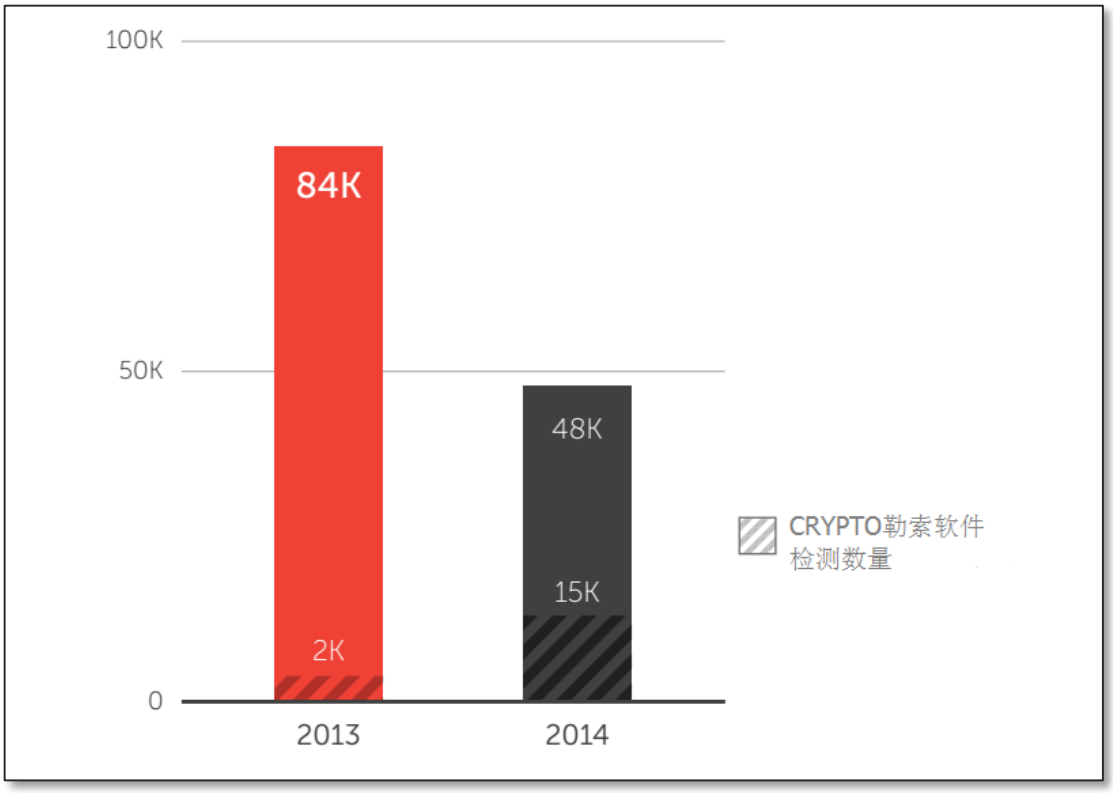
4. 木马、后门、间谍软件类型增幅最大

对 2014 年新增病毒种类按类型统计的数据可知，木马类型病毒增幅远高于其它类型恶意软件。2014 年趋势科技在中国地区监控到新增木马病毒特征共计 1,383,604 个，后门类型与间谍软件紧随其后，在一整年中分别新增 301,404 与 276,135 个。与蠕虫、感染型病毒不同的是这些类型的病毒并不以大范围破坏文件、拥堵网络为目的，而是瞄准受害者的资金账户，它们通常以窃取攻击目标的账户密码为目的，从而获得经济利益。在中国地区，这三种类型的病毒一直高居榜首。

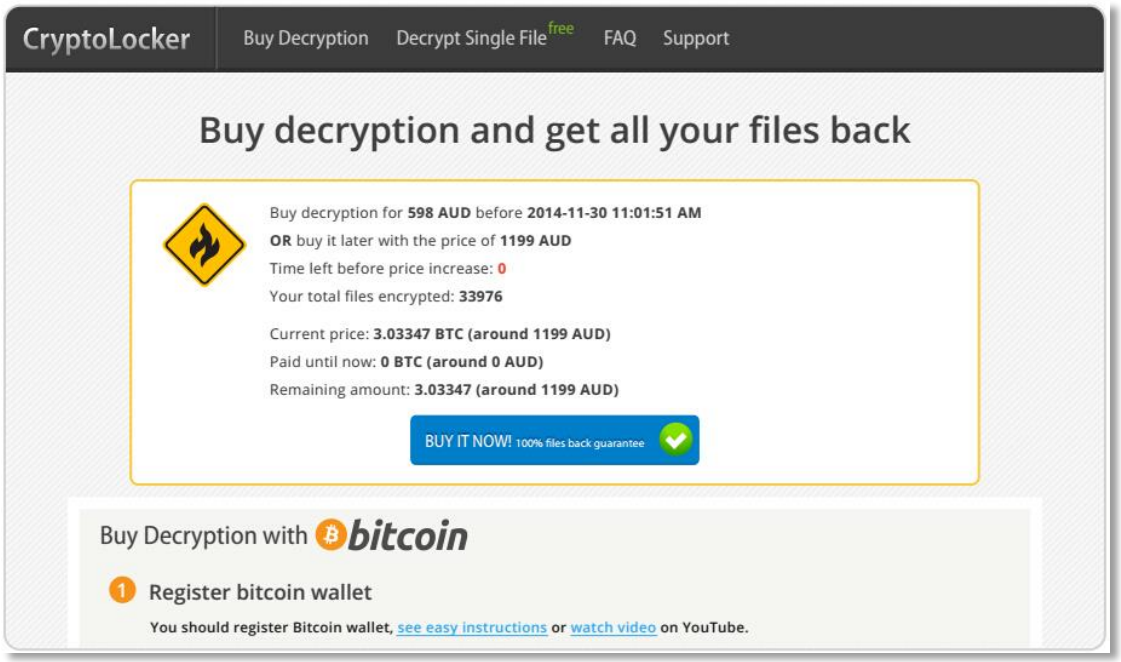
5. 勒索软件传播地区扩大并日趋复杂

勒索软件在过去一年中逐渐变化，其散播地区正逐渐扩大。新的变种不再只是发出空洞的威胁信息，取而代之的是它们会付诸实际行动，其手段通常是将用户的个人文档进行加密，继而对受害者进行勒索。虽然 2014 年的勒索软件的检测量比 2014 年有所下降，但是在 2013 年占据大部分比重的传统勒索软件(如 REVETON 家族和 RANSOM 家族)在 2014 年大幅减少，新型 CRYPTO 家族勒索软件在 2014 年所占比例上升了 27.35%。

本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。



2013 VS 2014 检测到勒索软件的计算机数量

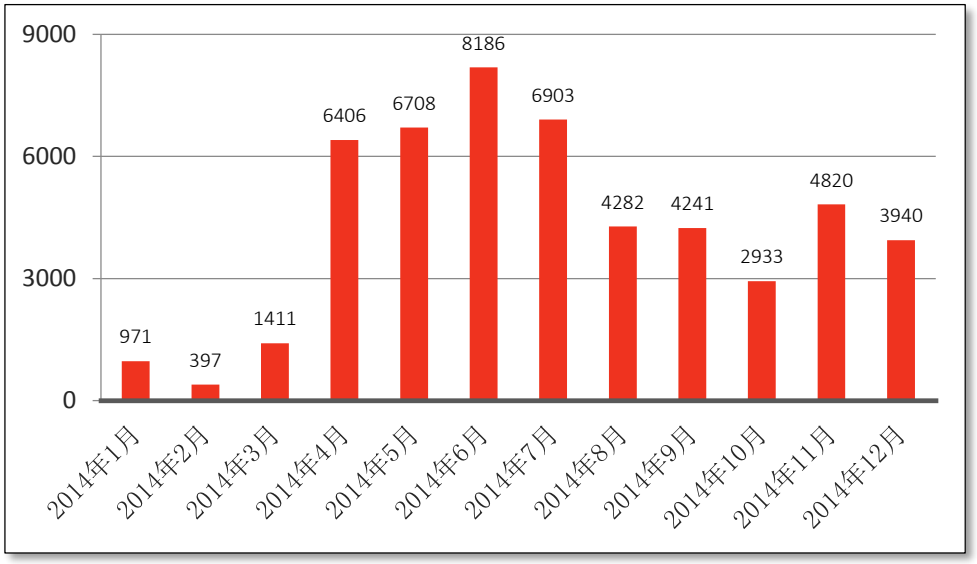


CryptoLocker 勒索信息

本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。

6. 钓鱼网站紧跟热点话题进行欺诈

从中国反钓鱼联盟得到的数据，2014 年 1 月至 2014 年 12 月共计 12 个月中，处理钓鱼网站共计 47,258 个。截至 2014 年 12 月底，联盟累计认定并处理钓鱼网站 220,033 个。对中国地区钓鱼网站历史数据监控可以发现，钓鱼网站的仿冒对象往往会追随媒体热点话题的变化而转移。通常在法定小长假期间，针对“旅行社类”、“航空公司类”、“酒店类”等相关假日消费行业的钓鱼网站数量会出现小高峰。此外，诸如电子产品新品发布、重大新闻事件等热点都会被钓鱼网站制作者借题发挥，制造恶意钓鱼地址诱骗用户点击进而窃取访问者的个人敏感数据。



2014 年中国地区钓鱼网站数量

本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。

趋势科技 2015 年及未来安全八大预测

1. 更多网络犯罪集团将利用黑暗网络和地下论坛贩卖犯罪软件

除了恶意软件，黑暗网络中还包含手枪、大麻商品，甚至是“买凶杀人”的服务

美剧《纸牌屋》中提及的深层网络(DeepWeb)、黑暗网络(Darknet)是真实存在的。在这些搜索引擎无法找到的，或是需要加密客户端才能访问的站点上，网络攻击服务以及犯罪软件的价格正在逐年下滑，出现这一现象的原因在于恶意软件在地下市场供应量的增加。

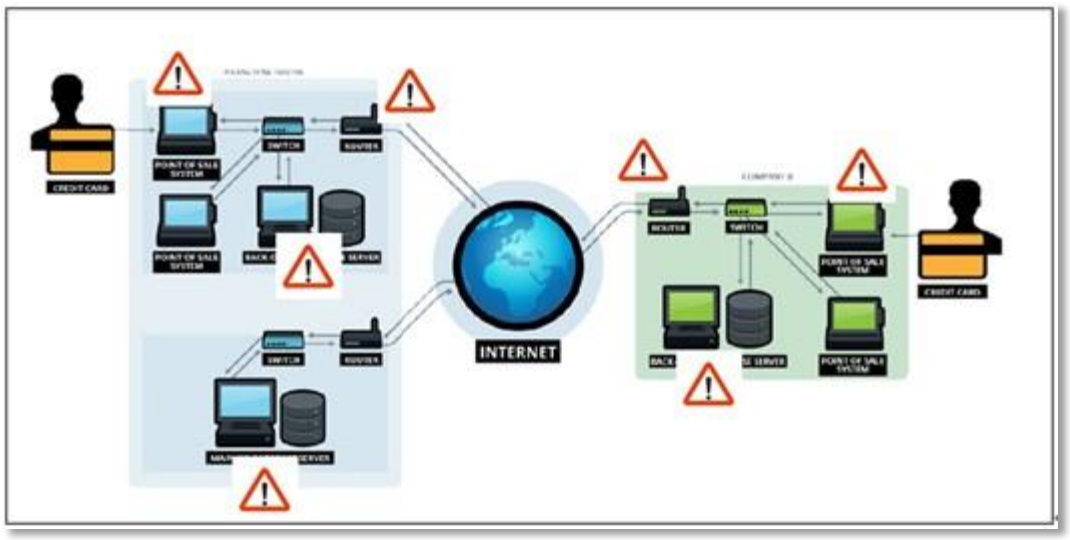
不仅美国失窃信用卡资料、Facebook 和 Gmail 账号密码的价格大幅下跌，中国地下网络市场上的犯罪工具和服务也非常“琳琅满目”，而且采用了“明码标价”、“打包优惠”等促销模式。

本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。

2. 网络犯罪活动加剧将催生更多黑客工具及攻击手法

截至 2014 年 10 月大型数据泄露事件的统计数字

2014 年的网络犯罪攻击愈演愈烈，美国 Target 超市 7000 万笔客户资料、美国 Home Depot 家饰建材连锁卖场的 6000 万笔客户资料、eBay 遭到神秘黑客的攻击、iCloud 泄露出大量好莱坞影星私密照片。



入侵 POS 系统,网络及数据库等重要主机

通过攻击频率数据的发展态势判断，趋势科技预计未来每个月都将见到两起或更多起大

本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。

型资料外泄事件，而这些事件背后，正是那些神秘而强大的黑客工具。例如：发展迅速的 POS 病毒家族，犯罪集团所采用的恶意软件可以轻松入侵那些安装了 POS 软件的商家计算机，从而截获每笔付款的信息。这种恶意软件被用来取代以前在“ATM 上安装摄像头”等物理方式来进行的数据窃取。

3. 移动设备漏洞逐渐成为重要的感染途径，漏洞利用工具将锁定安卓平台

新型数据窃取恶意软件将会出现，网上银行恶意软件将继续发展，这让移动恶意软件和高风险应用程序的数量持续增长。趋势科技预计 2015 年安卓威胁累积数量将达到目前的二倍，800 万将是人们不愿正视的数字。

安卓威胁累积数量将达到 800 万

另外，移动设备、平台及应用程序的漏洞数量将会增加，这将带来更严重的网络风险。未来，攻击移动设备的黑客将使用类似黑洞(Blackhole)漏洞利用工具，向安卓设备传播越来越多的网银病毒及勒索病毒。趋势科技还发现，不但第一个针对移动设备的勒索程序 REVETON 已经现身，名为埃曼塔行动(Operation Emmental)的全新网络犯罪行动背后的网络犯罪集团，他们不仅诱骗欧洲银行的客户安装恶意的安卓应用来骗取其账号密码，其威胁也已经蔓延到亚洲。

4. 针对性攻击将变得与普通网络犯罪一样普遍

尽管 2014 年很多政府机构和全球化企业在安全控管上都投入了巨大的人力和物力，但是针对性攻击仍然渗透进这些组织，黑客将锁定高度机密的政府数据、金融信息、数字资产、工业设计资料等等。今年，网络犯罪集团成功利用针对性攻击，在美国和加拿大制造多起大

本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。

型数据外泄事件。趋势科技威胁防御专家预测，在 2015 年，越南、英国和印度等国黑客也将跟进，更多针对性来源和目标国家的名字，将会出现在 2015 年的盘点列表上。

另外，电子邮件成为了黑客最易取得针对性成效的入口。在某些案例中，攻击者会利用受害者的电子邮件账号来增加他们鱼叉式网络钓鱼攻击邮件的可信度。而经过足够多的研究分析后，网络犯罪份子可以制造出社会工程诱饵，骗取足够多的员工点击网络链接或者打开邮件附件。

5. 新的移动交易支付方法将带来全新威胁

预计 2017 年全球移动支付市场规模将高达 900 亿美元，移动支付服务这种新的支付形态很可能成为黑客攻击的新目标！当下，国外移动支付将因 Apple Pay、Google Wallet 催化而逐渐迈入主流，而国内“双十一”支付宝移动支付交易数达到 1.97 亿笔，同比增长 336%。那么，移动支付的新风险又在哪里呢？

趋势科技认为，随着如心脏出血漏洞、破壳漏洞等更多漏洞的发现，未来将可预见专门针对移动支付平台的威胁。例如安卓平台的 FakeID 漏洞可能引发的风险，这可以让恶意应用程序冒用合法程序、存取设备上的敏感数据、访问 NFC 安全芯片上的内容。

所以，用户需要在未来重点观察和防止利用近场通信(NFC)科技的犯罪行为，不要执行破解程序、在不使用 NFC 功能时将其关闭、定期检查软件是否有更新，开启屏幕密码锁并为移动设备安装防护软件。而在国内，用户更应减少苹果设备越狱，提高安卓系统第三方应用商店的安全管理，因为这里都为移动支付威胁提供了滋生的沃土。

6. 将会出现更多针对利用开源应用程序漏洞的攻击

由于微软 Windows 和其他知名操作系统在安全方面的改进，将使得漏洞逐渐减少。所以，黑客将被迫转移目标到开源系统平台及应用程序的漏洞。一些存在多年的开源代码程序漏洞，今年都遭到了大量的攻击并造成了严重的灾情。

未来几年之内，黑客仍将继续挖掘一些像心脏出血漏洞和破壳这类潜藏已久的漏洞，它们可能会比 25 年前就存在的漏洞更加古老，而对安卓等其他终端系统造成更大的风险。这些漏洞可以入侵 Linux 桌面终端和服务器，控制安卓系统及应用连接的内容，盗取数据或利用这些移动设备发动分布式拒绝服务(DDoS)等攻击。

7. 物联网设备上数据将会成为黑客的新目标

IoE、IoT 是近年最盛行的科技流行语，不仅手机、电脑、电视机等传统信息设备将连入网络，日常生活物品都将实现数字化、网络化、智能化。任何新科技产品在设计时都会考虑到网络的连接性，这可能包括：汽车、智能型烤面包机、计步器、婴儿监视器和电器设备。

设备的网络连接和运算能力，让它们变的“更聪明”，但也会带来安全风险。IoE、IoT 设

本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。

备对黑客来说，充满了无限的可能性，黑客会想尽办法找到可攻击的目标。借助设备中的处理能力与储存的数据，他们可以执行更复杂、更严重的破坏性任务，例如非法控制电灯、门窗等设备，甚至破坏一个国家的基础民生设施，威胁人身安全。

8. 未来将出现更严重的网上银行及其它金融相关威胁

网上银行恶意软件数量在 2014 上半年持续稳定增加，趋势科技监测结果显示，截至到第三季度，这些恶意程序的数量已经达到了 13.7 万个。如埃曼塔行动这样的复杂攻击手法，证明了即使是银行的双重认证机制也可能出现漏洞，而未来几年之内，跨平台的网银攻击会更加频繁。

网络是一个自由的空间，它给每个人自由选择的权利，但现在这个环境越来越难恶劣。对此，安全专家表示：“如果隐藏的威胁已经浮上台面，仅仅做到关注是不够的，在这场黑与白的较量中获胜，需要主动的行动和全球用户的合力。当众多厂商在市场竞争压力下，不断推出更多缺乏安全机制的设备以满足日渐扩大的市场需求时，黑客也将发现更多可利用的漏洞，智能型设备制造商必须考虑如何协助用户保护这些设备当中的数据，而非仅保护设备本身。”

本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。

关于趋势科技

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。

TREND MICRO 趋势科技 [全程护航 迈向云端]

关于中国区网络安全监测实验室

趋势科技“中国区网络安全监测实验室”是国际杀毒厂商中第一家针对“中国特色病毒”提供解决方案的监测机构。通过 MOC 监控中心和 SPN 数据分析中国区用户的网络安全状况，主动收集中国地区的病毒样本，对病毒样本进行快速分析，发布专门针对中国地区的病毒码(China Pattern)和解决方案，大幅提高对中国区病毒的查杀率。为中国地区用户提供更广泛、及时、有效的反病毒支持。趋势科技“中国区网络安全监测实验室”利用趋势科技的全球资源优势以及自身的高技术人员资源，真正帮助中国区用户解决病毒危机，营造安全的网络环境。倾力服务中国用户。

ChinaRTL

中国区网络安全监测实验室