瑞星 2014 年中国信息安全报告

北京瑞星信息技术有限公司

2015 年 1 月

地址：北京市中关村大街 22 号中科大厦 1305 室
邮编：100190　总机：(010)82678866　传真：(010)62564934

免责声明

本报告综合瑞星“云安全”系统、瑞星客户服务中心、瑞星互联网攻防实验室、瑞星漏洞平台等部门的统计、研究数据和分析资料，仅针对中国 2014 年网络安全现状与趋势进行统计、研究和分析。本报告提供给媒体、公众和相关政府及行业机构作为互联网信息安全状况的介绍和研究资料，请相关单位酌情使用。如若本报告阐述之状况、数据与其他机构研究结果有差异，请使用方自行辨别，瑞星公司不承担与此相关的一切法律责任。

地址：北京市中关村大街 22 号中科大厦 1305 室
邮编：100190　总机：(010)82678866　传真：(010)62564934

目录

报告摘要

- 2014 年，瑞星“云安全”系统共截获新增病毒样本 5,145 万余个，病毒总体数量比 2013 年同期增长 55.44%，病毒疫情持续处于高危状态。此外，感染型病毒已超过蠕虫病毒，成为年度第二大种类病毒。

- 2014 年，瑞星“云安全”系统截获挂马网站 466 万个（以网页个数统计），与 2013 年同期相比下降了 16.93%。4 月份微软对 Windows XP 操作系统停止更新，一些针对 XP 系统的漏洞逐渐曝光，因此导致网站挂马数量在 4 月份后出现近年来罕见的高峰。瑞星安全专家指出，然而挂马网站的攻击手法单一，未来如无新型攻击出现，挂马网站仍将逐年递减。此外，在报告期内，瑞星“云安全”系统共截获钓鱼网站 559 万个，比 2013 年同期下降了 11.97%，帮助用户拦截钓鱼网站攻击 2.42 亿人次。

- 2014 年新增手机病毒样本 183 万个，与 2013 年相比上涨了 128.75%，其中以隐私窃取、诱骗欺诈、恶意扣费、恶意传播、资费消耗等几大类为主。随着移动支付的广泛应用，网银、淘宝等手机支付应用成为病毒攻击的重灾区。

- 2014 年，据瑞星“云安全”系统监测，有 1300 万台路由器遭遇过 DNS 篡改，2510 万台路由器未修改过出厂设置，1700 万台路由器管理账号存在弱密码问题，2500 万台路由器 WiFi 账号存在弱密码问题。同时，在报告期内，国内知名路由器厂商 TP-Link、腾达、中兴先后被曝出重大产品漏洞。

- 2014 年，NFC 支付开始得到广泛关注，隔空盗刷、恶意篡改卡片、NFC 病毒、VISA 卡闪付漏洞成为 NFC 支付的四大安全问题。瑞星安全专家警告，由于全面涉及到财产安全、企业安全及金融安全，NFC 支付在全面普及前应做好安全防护工作。

- 超级电厂病毒、Windows OLE 漏洞、OpenSSL 心脏出血漏洞、SSLv3 POODLE 漏洞及 12306 用户信息泄露成为 2014 年度五大信息安全事件。此外，随着信息技术的迅猛发展，物联网、虚拟化及云计算已越来越多地被应用到日常生产生活当中，然而由于网络环境复杂、跨地域、数据与资源集中等问题，该类技术面临着严峻的安全考验。

- 受不断升温的国际信息安全对抗事件影响，国产 Linux 操作系统普及在即，未来在 2015 年，Linux 病毒或将大面积爆发。在过去的一年中，Windows 操作系统的漏洞已大幅减少，为节约成本提高收益，黑客将形成规模组织并更多地攻击企业及政府。此外，许多古老而缺乏维护的开源系统越来越受到黑客的关注，预计未来针对该类系统的攻击可能将愈加频繁。

地址：北京市中关村大街 22 号中科大厦 1305 室
邮编：100190　总机：(010)82678866　传真：(010)62564934

一、病毒和木马

（一）2014 年病毒概述

1. 病毒疫情总体概述：全年人均感染病毒 23.6 次

2014 年，瑞星“云安全”系统共截获新增病毒样本 5,145 万余个，病毒总体数量比 2013 年同期增长 55.44%。报告期内，共有 5.46 亿人次网民被病毒感染，有 2,317 万台电脑遭到病毒攻击，人均病毒感染次数为 23.6 次。木马病毒依然是主流病毒，感染型病毒与 2013 年相比涨幅较大。

在报告期内，新增木马病毒占总体病毒的 80.13%，依然是第一大种类病毒。感染型病毒超过了蠕虫病毒，成为第二大种类病毒，占总体新增病毒样本的 8.6%，第三大种类病毒为蠕虫病毒，占总体比例的 6.81%。另外，后门病毒（Backdoor）占总体数量的 1.86%，恶意广告（Adware）占总体数量的 1.2%，分别位列第四和第五。其他类型、病毒释放器（Dropper）比例分别为 1.14%和 0.26%。

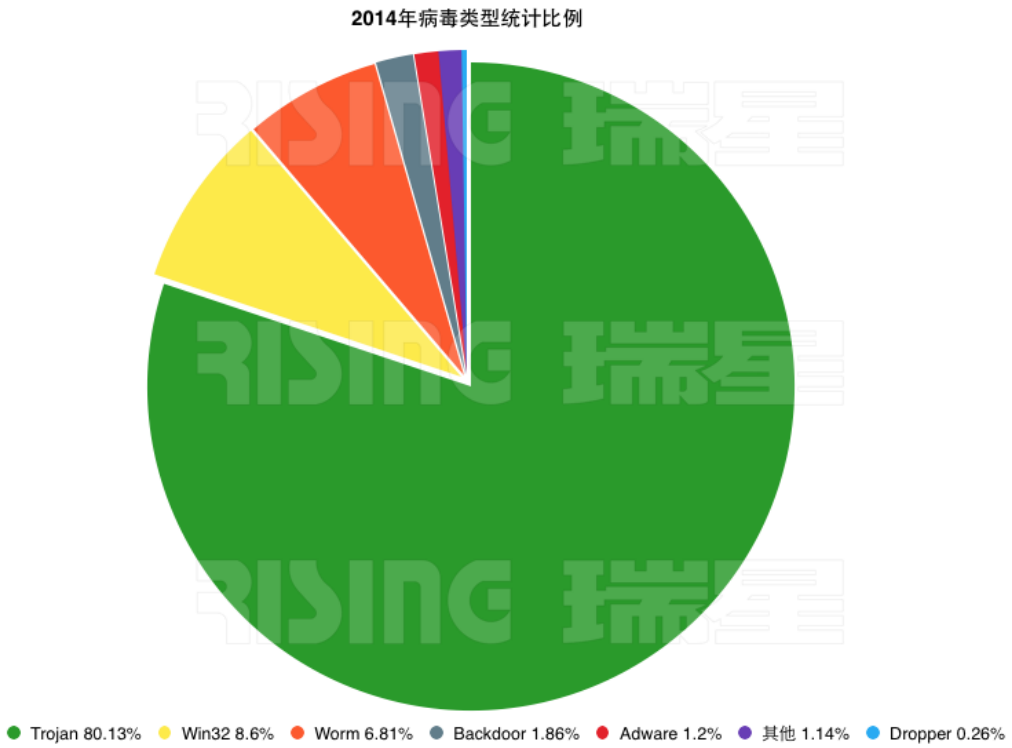

图 1：2014 年病毒类型统计

2. 病毒感染地域分析

在报告期内，广东省病毒感染为 6,767 万人次，依然位列全国第一，其次为山东省 3,665 万人次及江苏省 3,306 万人次。

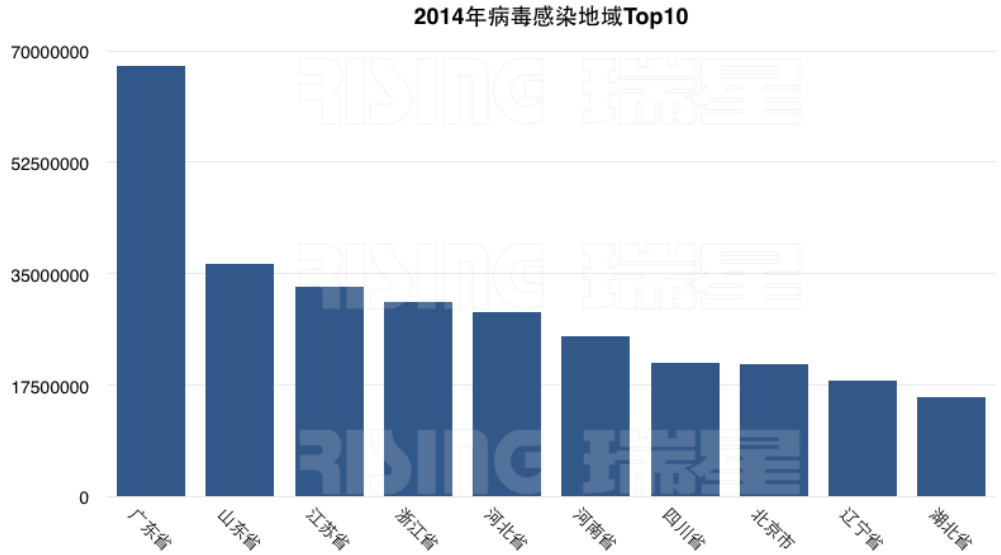

图 2：2014 年病毒感染地域 Top10

（二）2014 年病毒 Top10

根据病毒感染人数、变种数量和代表性进行综合评估，瑞星评选出了 2014 年病毒 Top10：

2014年病毒Top10

排名	病毒名称	病毒描述
1	Malware.FakeFolder@CV!1.6AA9	蠕虫病毒，伪装成文件夹图标迷惑用户，运行后在电脑中开启后门，下载恶意程序并运行。
2	Trojan.Script.Lisp.ACAD	脚本木马病毒，具有很强的传播能力，病毒会感染正常lisp脚本，影响CAD操作，偷取CAD工程文件。
3	PUF.GMUnpackerInstaller!1.9C4F	木马病毒，病毒运行后在后台偷偷安装推广程序。
4	Dropper.Script.VBS.Fednu.a	脚本病毒，运行后在电脑中开启后门。
5	Trojan.Kazy	木马病毒，运行后在后台下载恶意程序并运行。
6	Trojan.PSW.Win32.Agent.exw	木马病毒，盗取网络游戏账号密码，并发送到指定的网络地址。
7	Win32.Ramnit	感染型病毒，全盘感染exe文件。病毒运行后会释放后门，使用户电脑沦为"肉鸡"。
8	Trojan.Win32.Imehost.a	木马病毒，运行后窃取用户隐私信息。
9	Trojan.DL.Script.JS.Agent.lok	木马病毒，利用挂马网站触发浏览器漏洞，电脑中毒后下载恶意木马或后门病毒。
10	Worm.Script.VBS.Autorun.bt	蠕虫病毒，创建恶意的快捷方式指向病毒，病毒运行后会占用电脑资源使系统运行缓慢，并下载恶意程序。

图 3：2014 年病毒 Top10

（三）2014 年典型病毒分析

1. “120 名艺人涉毒名单”病毒现身

2014 年 8 月，一些娱乐圈明星被曝吸毒，一条“警方早已掌握两岸三地 120 名艺人涉毒名单”的消息在网上被疯狂转发。随即，瑞星“云安全”系统截获到一例名为“120mingdan.doc.exe”的后门病毒，该病毒通过隐藏文件扩展名将自身伪装成一个 word 文档，病毒运行后会收集电脑中记录的隐私信息、网银账密，同时开启后门，让电脑变成黑客的“肉鸡”。

图 4：病毒隐藏文件扩展名并将自身伪装成 Word 文档

2. 不雅视频藏病毒

2014 年 5 月，瑞星“云安全”系统拦截到了一个乔装为“21 秒”视频文件的后门病毒。该病毒的大小、文件名、文件格式及图标都经过精心伪装，一旦网民下载并点击，在视频打开的同时将使电脑中毒，网民会面临网络账号密码被盗、隐私信息泄露、银行卡被盗刷等风险，同时电脑也将成为黑客“肉鸡”。

图 5：“李 21 秒”病毒视频截图

3. Gamarue 蠕虫成 U 盘病毒新标准

2014 年，一类名为 Gamarue 的蠕虫病毒利用 U 盘大量传播。以往病毒使用 U 盘传播时都是依靠在 U 盘中生成自动播放文件进而运行病毒。目前，这种方法已能被大多数杀软查杀，因此威胁性大大降低。本次发现的 Gamarue 蠕虫可自动隐藏病毒程序，被感染后，用户打开 U 盘只能看到一个快捷方式，所有病毒相关文件都被移动到一个隐藏文件夹中。

图 6：Gamarue 伪装成用户图标引诱用户点击

二、恶意网站

（一）挂马网站

1. 挂马网站概述：挂马将成非主流

2014 年，瑞星“云安全”系统截获挂马网站 466 万个（以网页个数统计），与 2013 年同期相比下降了 16.93%。在报告期内，瑞星“云安全”系统拦截挂马网站的攻击总计为 4,263 万余次，与 2013 年同期相比下降了 23.38%。

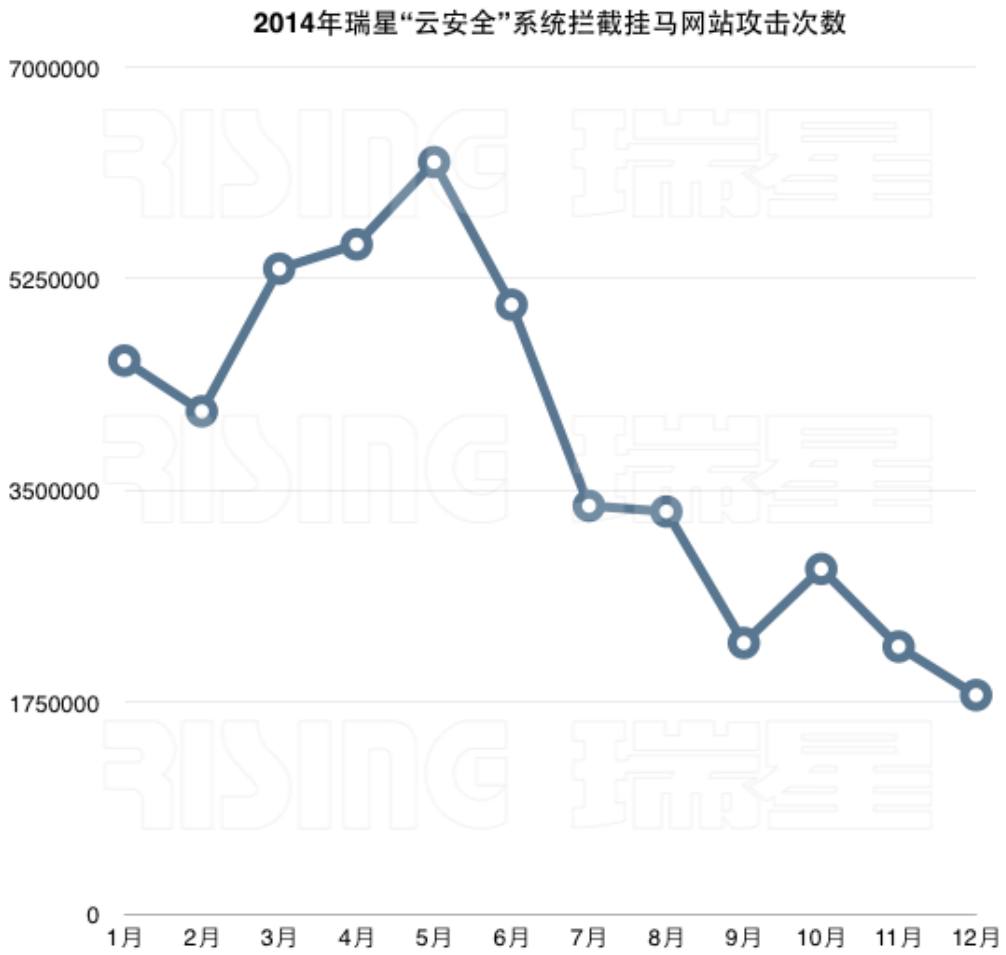

图 7：2014 年瑞星“云安全”系统拦截挂马网站攻击次数

2. 挂马网站趋势分析

由于 2014 年漏洞爆发频率较低，挂马网站仍然在使用 2013 年的一些漏洞，因此挂马攻击成功率不高。4 月，微软对 Windows XP 操作系统停止更新后，一些针对 XP 系统的漏洞逐渐曝光，网站挂马数量在 4 月份后出现近年来罕见的高峰，然而由于挂马网站的攻击手法单一，反挂马技术已非常成熟，因此大部分来自挂马网站的攻击都能被拦截。瑞星安全专家指出，如无新型攻击手法出现，挂马网站将逐年递减。

3. 2014 年十大挂马漏洞

2014年十大挂马漏洞

序号	漏洞CVE编号	类型
1	CVE -2013-3912	IE漏洞
2	CVE-2013-3203	IE漏洞
3	CVE-2013-1378	Flash漏洞
4	CVE-2012-0155	IE漏洞
5	CVE-2013-5330	Flash漏洞
6	CVE-2013-2440	Java漏洞
7	CVE-2014-0282	IE漏洞
8	CVE-2013-5456	Java漏洞
9	CVE-2013-3127	Windows Media Player漏洞
10	CVE-2014-6332	IE漏洞

图 8：2014 年十大挂马漏洞

（二）钓鱼网站

1. 钓鱼网站概述：全年人均访问 1.5 次

2014 年，瑞星“云安全”系统共截获钓鱼网站 559 万个，比 2013 年同期下降了 11.97%，帮助用户拦截钓鱼网站攻击 2.42 亿余人次，平均每人每年访问 1.5 次钓鱼网站。

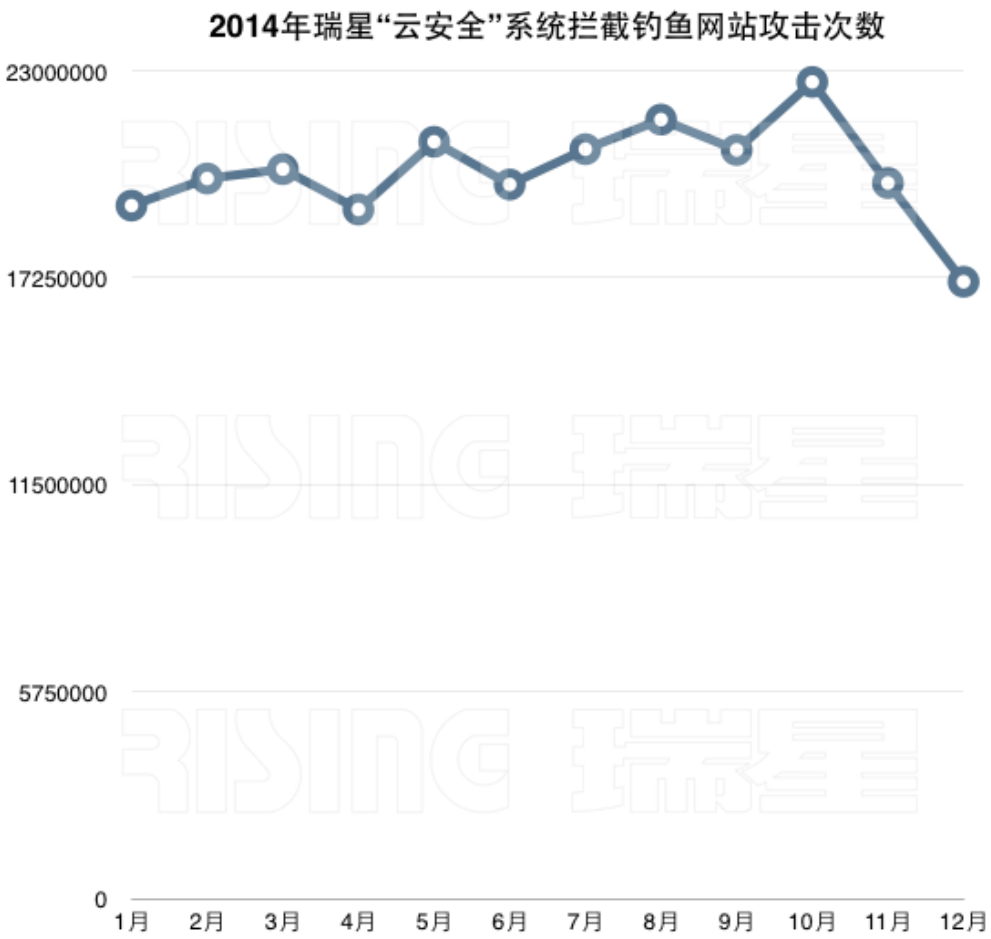

图 9：2014 年瑞星“云安全”系统拦截钓鱼网站攻击次数

2. 钓鱼网站类型统计

在报告期内，虚假中奖类钓鱼网站占全部钓鱼网站的 35%，位列第一，其次为虚假银行类钓鱼网站与虚假充值类钓鱼网站，分别占全部钓鱼网站的 26%与 15%。

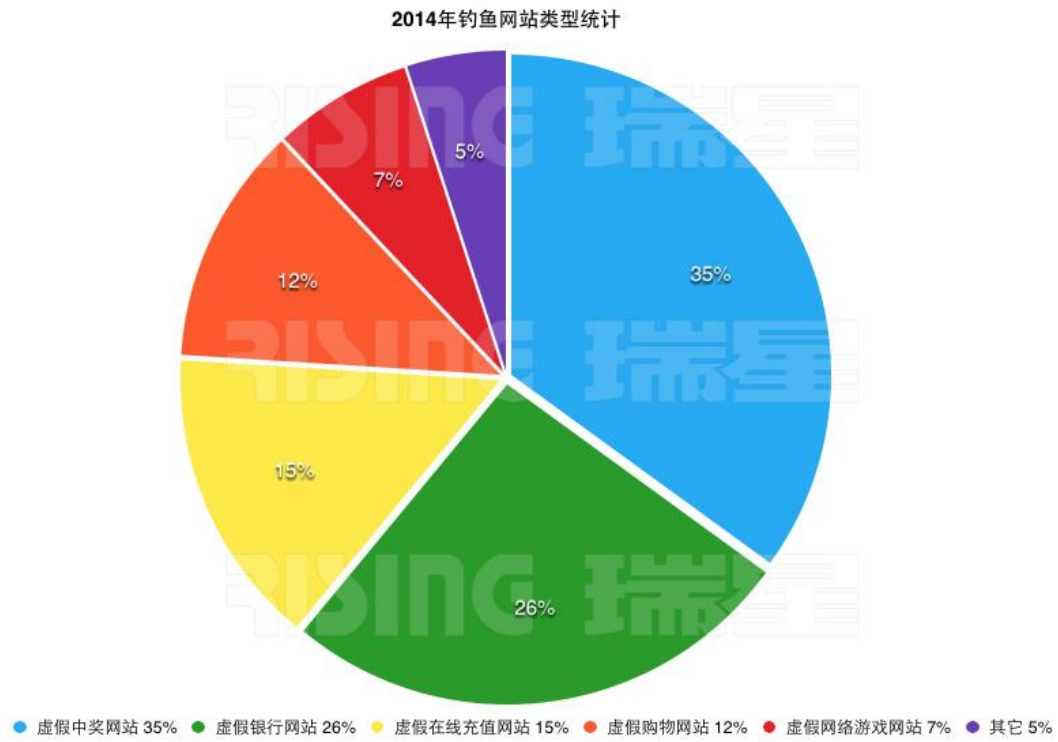

图 10：2014 年钓鱼网站类型统计

3. 2014 年重大钓鱼网站 Top10

2014年重大钓鱼网站Top10

网址	类型
http://70.39.88.18	工商银行钓鱼网站
http://irnrhm.com/b1.asp	支付宝钓鱼网站
http://vervoortbvba.be/dtrade	邮箱类钓鱼网站
http://tbao.fgsst.info/	淘宝钓鱼网站
http://59.188.69.169/com/icbcmybank.htm	中国工商银行钓鱼网站
http://www.huaxiang666pt.com/ccccbb.asp	建行钓鱼网站
http://mi1.yaanbx.com	购物钓鱼网站
http://www.cfyxgl.com/	网络游戏钓鱼网站
http://www.zjwstv.com	综艺节目网站
http://pp57.jianke.com	医药类钓鱼网站

图 11：2014 年重大钓鱼网站 Top10

4. 2014 年新型钓鱼技术手段

2014 年钓鱼网站攻击较 2013 年在数量上有所增加，主要通过以下手段进行钓鱼：

- 利用网上购物打折、返利进行钓鱼。例如假冒淘宝网站，骗取消费者浏览指定网站，遥控消费者执行指定操作，进而骗取钱财。
- 利用邮件进行钓鱼。例如假冒网购打折邮件或假冒他人发送的邮件，并在邮件中发送钓鱼网址。
- 利用微博宣传并发布钓鱼短链接。随着智能手机、平板电脑等移动终端的使用率逐渐上升，很多钓鱼攻击者利用移动终端缺少安全防护的缺陷进行钓鱼攻击。
- 《爸爸去哪儿》、《奔跑吧兄弟》等综艺节目火爆以后，网络中出现假冒该类节目官网并结合电信手段进行攻击的钓鱼网站，与以往的《中国好声音》钓鱼网站手法很相似。

三、移动互联网安全

（一）手机病毒

1. 手机病毒概述

2014 年新增手机病毒样本 183 万个，与 2013 年相比上涨了 128.75%，其中以隐私窃取（privacy）、诱骗欺诈（fraud）、恶意扣费（payment）、恶意传播（spread）、资费消耗（expense）等几大类为主。

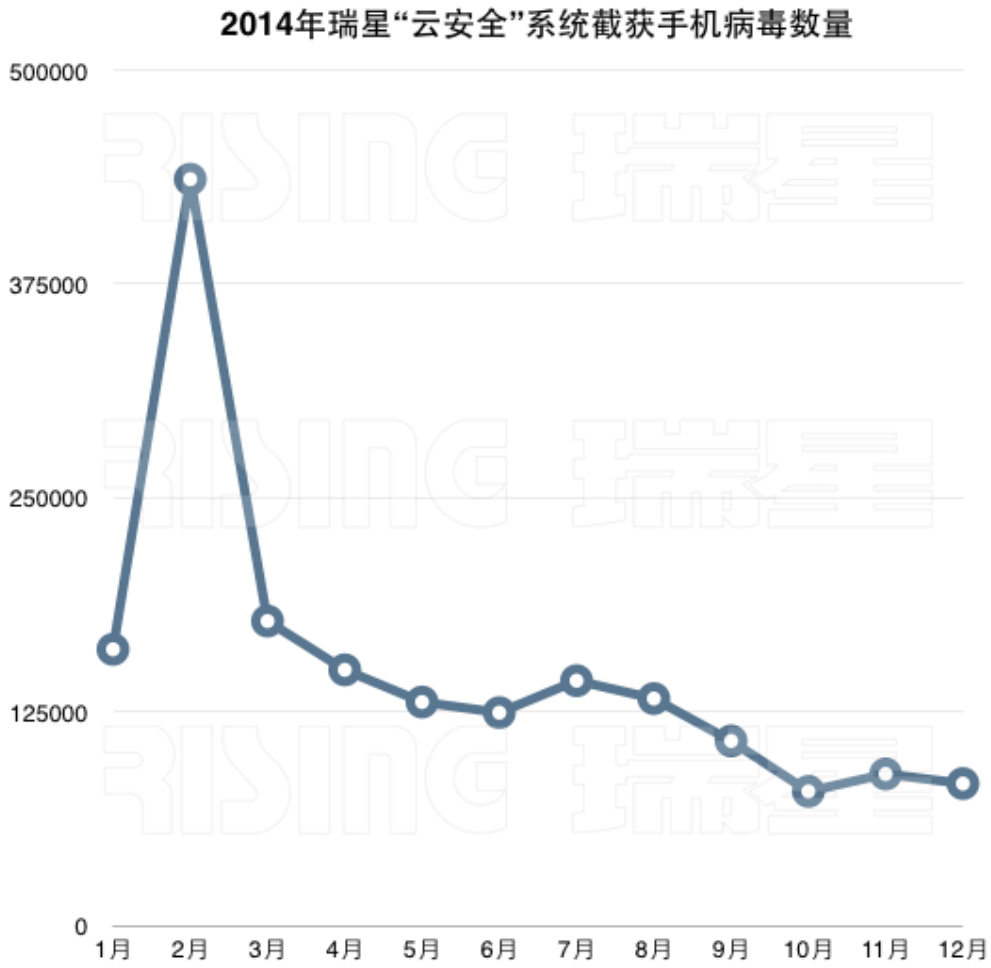

图 12：2014 年瑞星“云安全”系统截获手机病毒数量

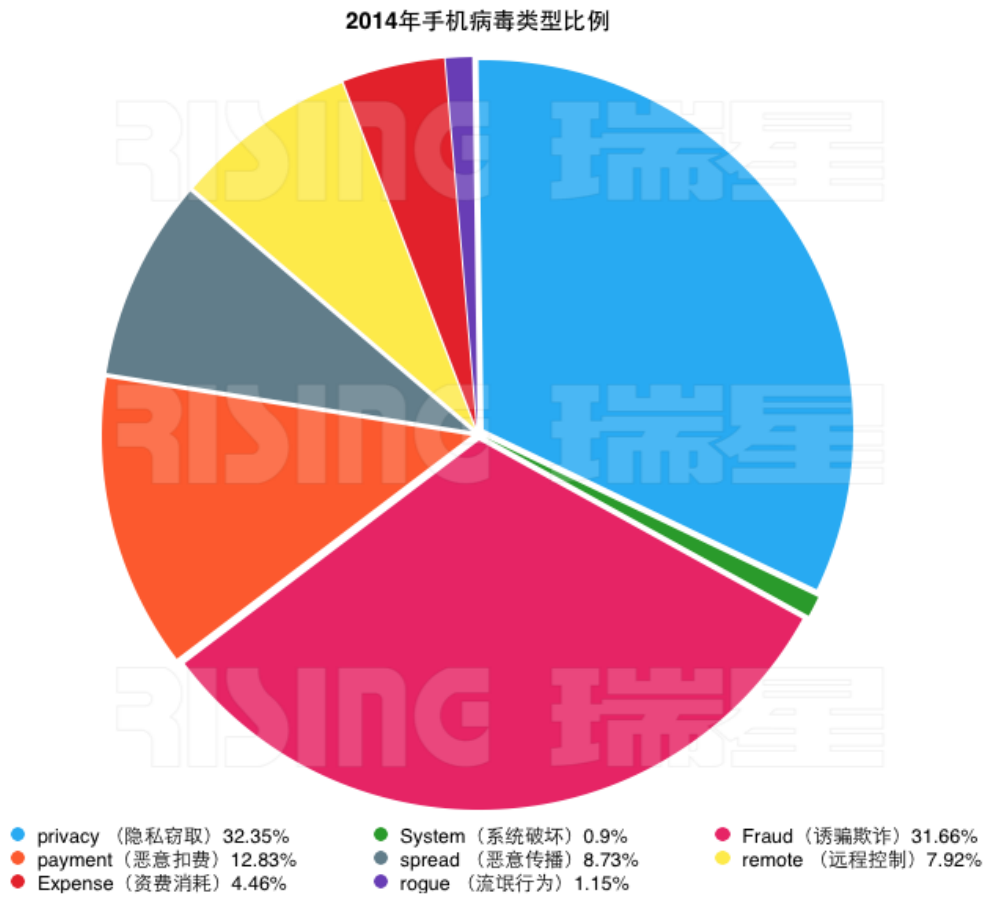

图 13：2014 年瑞星“云安全”系统截获手机病毒类型比例

2. 2014 年手机病毒 Top10

1) 不死木马：重启后满血复活

2014 年出现的不死木马成为年度威胁性最高、感染最为广泛的手机病毒，该病毒下载海量恶意程序，并大量消耗手机资费，即使用户进行杀毒，该病毒也会在手机重启时再次复活。最新的不死木马二代隐蔽性更强，甚至实现了“无进程”、“有进程无文件”等高级特性。

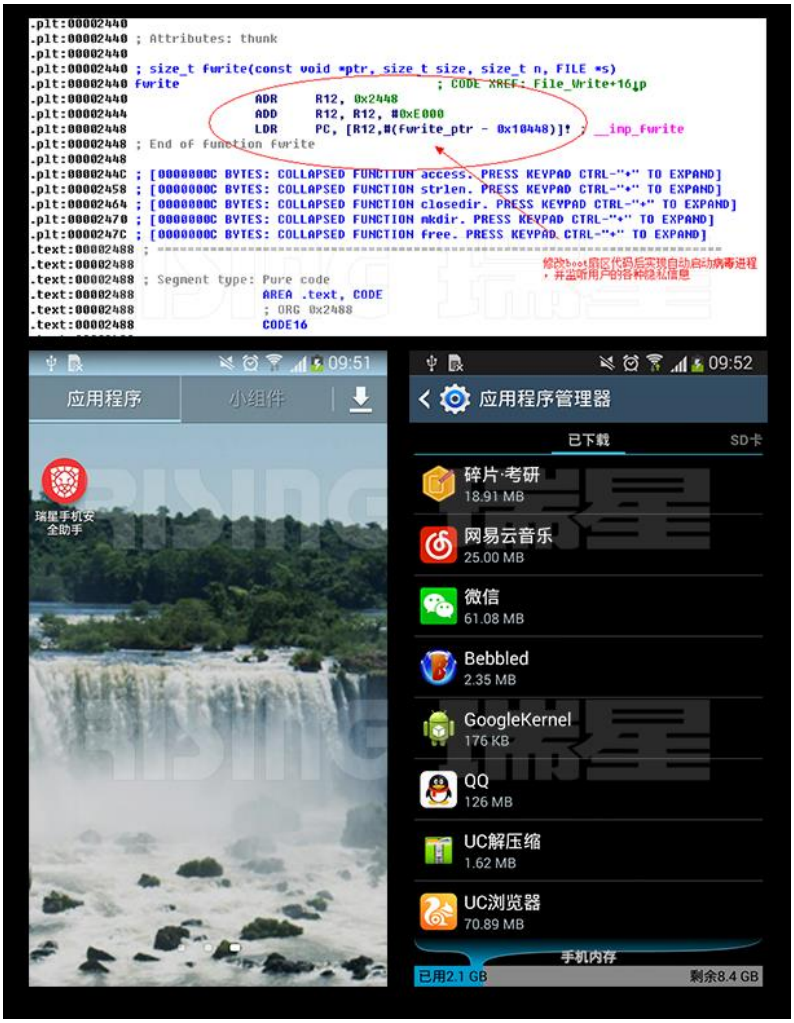

图 14：不死木马病毒截屏及恶意行为代码

出于便宜、性价比高等考量，许多国内用户热衷于购买水货手机。瑞星安全专家指出，正是水货的盛行催生了刷机产业，而不死木马正是通过刷机来进行传播的。目前，不死木马病毒虽已能够被查杀，但是难保更多的刷机程序中存在还未曾被发现的病毒。

2) WireLurker 病毒：攻破苹果安全神话

2014 年 11 月，苹果 IOS 系统曝出被 WireLurker 病毒攻破的新闻。该病毒利用苹果“企业部署”技术（Enterprise Provisioning，一种让企业为员工统一安装内部软件的技术）向苹果手机安装恶意软件，目前已使得数十万 IOS 用户被感染。WireLurker 会收集用户的各种信息，还能向黑客发送升级请求。苹果安全神话被破，虽然目前该病毒只是在中国大陆地区传播，但毫无疑问，苹果 IOS 系统正面临着越来越严峻的安全考验。

3) XX 神器：病毒借短信泛滥

2014 年 8 月，一个名为 XX 神器的安卓病毒在国内大面积爆发。该病毒利用了短信传播，并且在短信内容中加上了收件人的姓名称谓等（存储在发件手机上的联系人名称），降低了收件人的警惕性。瑞星安全专家表示，XX 神器病毒本身并没有多少技术含量，它的大规模爆发主要由于网民缺乏安全意识，对于联系人列表上的“熟人”过于信任造成。

图 15：XX 神器病毒截图及恶意行为代码

4) NFC 病毒浮出水面

2014 年，瑞星“云安全”系统截获了一款针对 NFC 功能的手机病毒。该病毒能够在手机与 IC 卡通讯的过程中改写 IC 卡中的某些数据，从而破坏或者修改 IC 卡。近期，NFC 已成为黑客重点关注对象，未来必然还会出现更多具有高威胁性的 NFC 手机病毒。

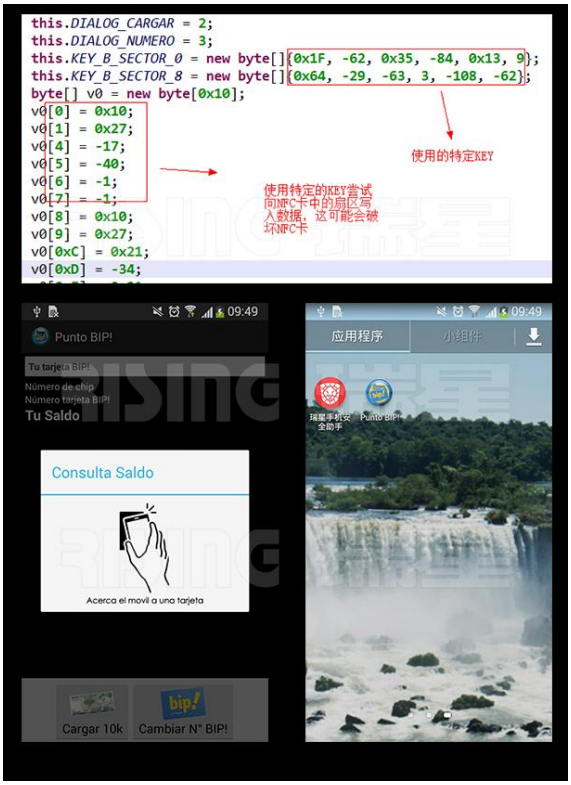

图 16：NFC 病毒截屏及恶意行为代码

5) 聊天大盗：监控聊天

QQ、微信、陌陌等应用已经成为国内用户主要的聊天软件，而针对该类应用的手机病毒也是层出不穷。聊天大盗就是一款监听聊天内容的病毒，该病毒通过 ptrace 进程注入的方式实现对手机 QQ、微信、陌陌聊天内容的实时监控。手机一旦中毒，用户就将遭到有针对性的监听，严重者甚至有可能面临人身威胁。

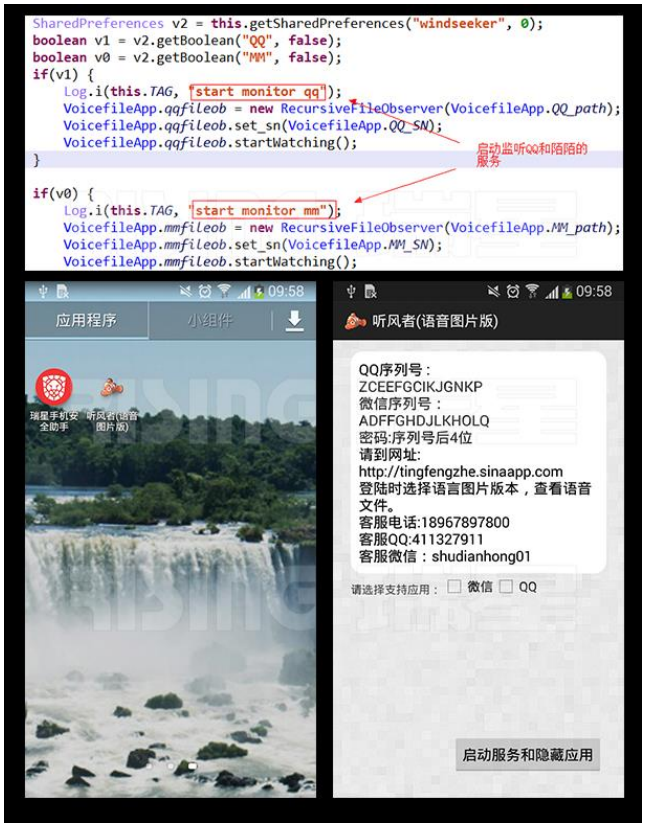

图 17：聊天大盗病毒截屏及恶意行为代码

6) 中国移动吸费病毒：自动后台购买应用

以往的恶意扣费病毒多是通过发送 SP 短信、拨打付费电话等方式消耗手机资费，而 2014 年一款名为 MMarketPay.A 的新型恶意扣费软件则能通过私下购买软件、视频等付费资源的方式来窃取用户资费。该病毒利用网点为 CMWAP 的用户接入 M-Market（http://mm.10086.cn，中国移动官方应用市场平台）无需登录的特性，修改用户的接入网点，后台购买黑客指定的应用，拦截验证码信息，完成付费流程。因此，手机一旦中毒，用户将面临大额资费消耗。

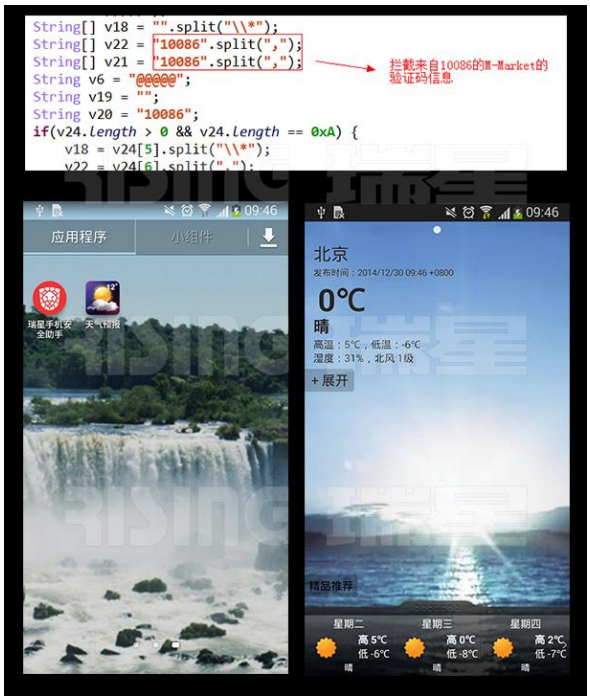

图 18：中国移动吸费病毒截屏及恶意行为代码

7) 银联间谍：专盗卡号密码

银联间谍是一款典型的支付类钓鱼欺诈病毒，该病毒通过伪装正常的银行应用来诱骗用户安装，以盗取用户的银行卡卡号、密码、信用卡有效期、CVV2 号等信息，还会诱导用户激活设备管理器以阻止用户将其删除。此外，银联间谍还伪造了一个名为“卸载程序”的应用来欺骗用户，当用户点击这个假冒的卸载程序后，病毒会自动隐藏，并继续在后台运行。

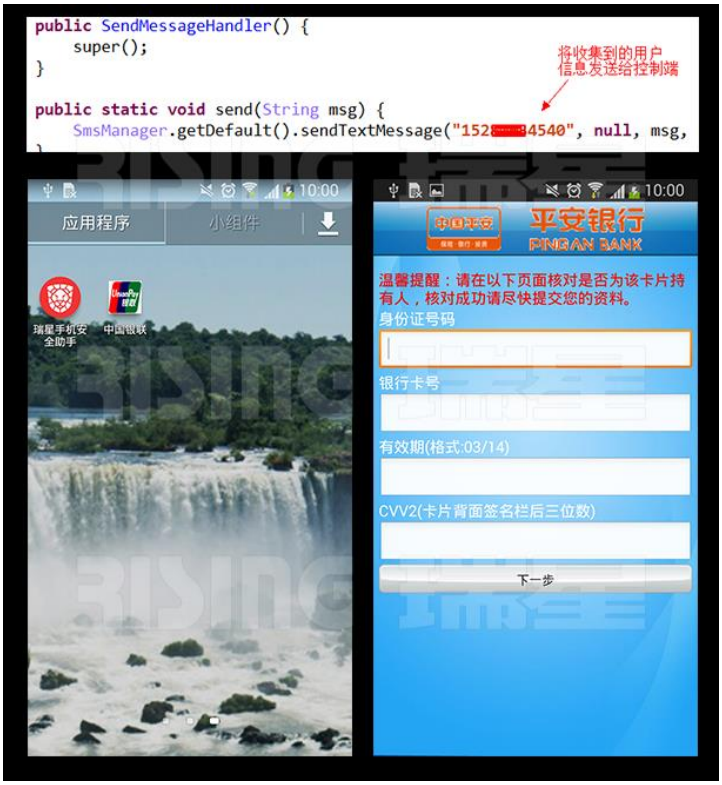

图 19：银联间谍病毒截屏及恶意行为代码

8) 短信蠕虫：推送海量广告

短信蠕虫是一款恶意广告病毒，该病毒嵌入 AdMob 广告插件，向通知栏推送广告，修改浏览器主页，私自向桌面发送不同网址的快捷方式，同时读取手机中的联系人信息，并根据后台木马控制端的指示向联系人私发短信传播病毒。手机一旦中毒，用户将收到海量垃圾信息及恶意推广信息，此外，该病毒还将造成大量资费消耗。

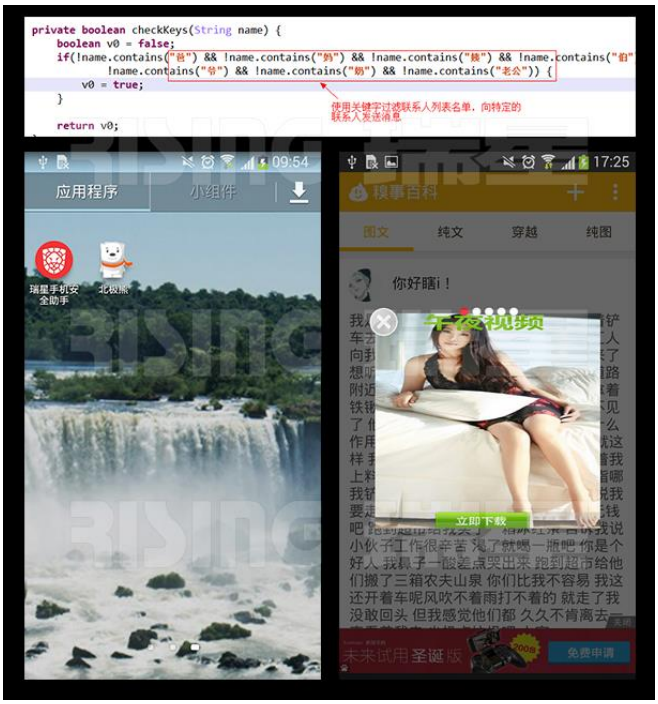

图 20：短信蠕虫病毒截屏及恶意行为代码

9) 隐私猎手：私自开启摄像头偷拍隐私

隐私猎手是一款隐私窃取类病毒，它是同类病毒中最具威胁性的一种，除盗取用户的地理位置、本机号码、本机 IMEI、联系人信息、短信收发件箱、通话记录外，它还能在远程控制手机开启摄像头拍摄照片，后台拨打电话给指定号码以监听用户声音，并将所有隐私信息上传至指定邮箱，堪称“隐形间谍”，对用户的人身安全造成极大危害。

图 21：隐私猎手病毒截屏及恶意行为代码

10) FakeTaobao 家族：专门洗劫支付账号

这是一类专门针对淘宝等手机交易应用的病毒。该类病毒功能简单、伪装方式多变、样本数量大、感染区域广。通常伪装成手机系统服务、手机营业厅、淘宝客户端以及各种照片，手机一旦中毒，病毒将窃取用户的银行账密信息，使用户财产受到严重威胁。

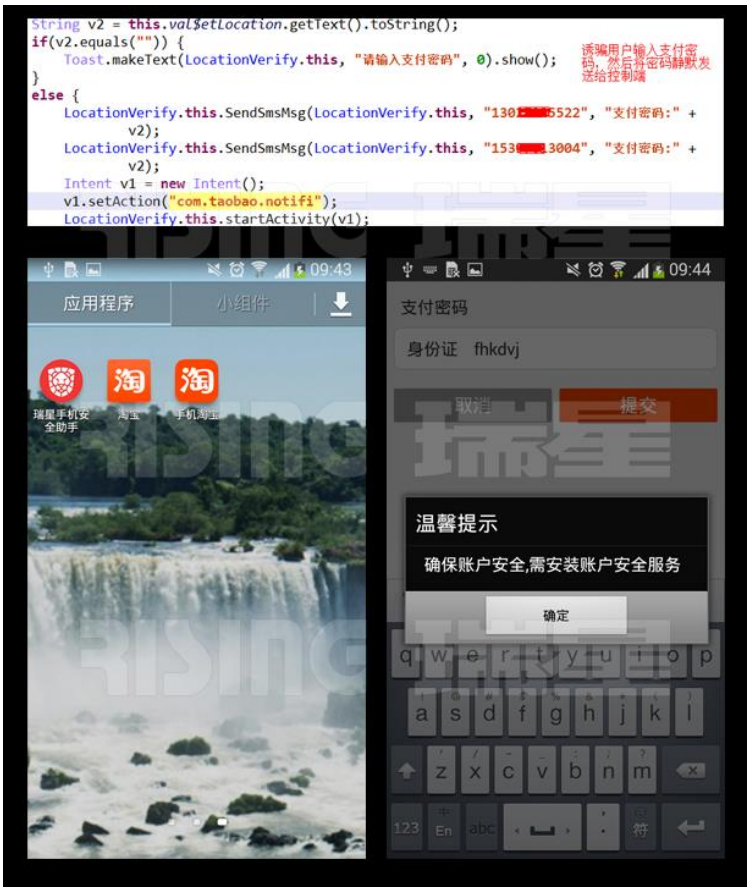

图 22：FakeTaobao 家族截屏及恶意行为代码

瑞星安全专家指出，FakeTaobao 家族的传播更具有社会工程学特点，并不依靠第三方软件市场等传统渠道，而以二维码、网盘链接、短信链接等方式发送，利用人们轻信的心理进行点对点传播。

3. 手机病毒趋势分析：技术手段向两极化发展

2014 年手机病毒的发展趋势可以从恶意行为、技术手段以及传播方式这三个方面来分析。行为上看，2014 年手机病毒并没有太大改变，依旧是以恶意扣费、隐私窃取类病毒为主。随着移动支付的广泛应用，网银、淘宝等手机支付端成为重灾区。

从技术手段来看，有两个极端发展的趋势。其一是病毒制作的门槛降低，网络上充斥着各类教程和能够直接使用的病毒源码，使得病毒制作更为简便。8 月爆发的 XX 神器，其制作者声称“只用了几周时间看书找教程就写出来了”。近期出现的一种名为“易安卓（E4A）”的中文编程语言，大大降低了病毒制作门槛。目前，利用该语言编写的病毒已在市面上流行。

另一方面，许多病毒在技术上又呈现了复杂化的特点。年初出现的不死木马是技术复杂化的典型案例，其使用的 Bootkit 技术显示手机病毒有向 PC 病毒学习的趋势。同时，进程注入、激活设备管理器以防止卸载等技术在手机病毒中的应用越来越广泛。此外，手机病毒

还显示出将恶意代码向.so 文件转移的倾向，加大了杀软查杀和逆向分析的难度。需要特别注意是，2014 年新增的手机病毒中有很大部分采用了加壳和混淆技术，说明该类技术已经开始成熟。

从传播方式来看，2014 年手机病毒依旧是主要依靠第三方软件市场，大量病毒伪装成正常软件欺骗用户下载。利用二维码传播的病毒也开始出现，应当引起警惕。

（二）路由器安全

1. 路由器安全概述

据瑞星“云安全”系统检测，2014 年，有 1300 万台路由器遭遇过 DNS 篡改，2510 万台路由器未修改过出厂设置，1700 万台路由器管理账号存在弱密码问题，2500 万台路由器 WiFi 账号存在弱密码问题。在报告期内，路由器漏洞主要由任意命令执行、未授权访问、任意文件下载、后门等四大类组成。

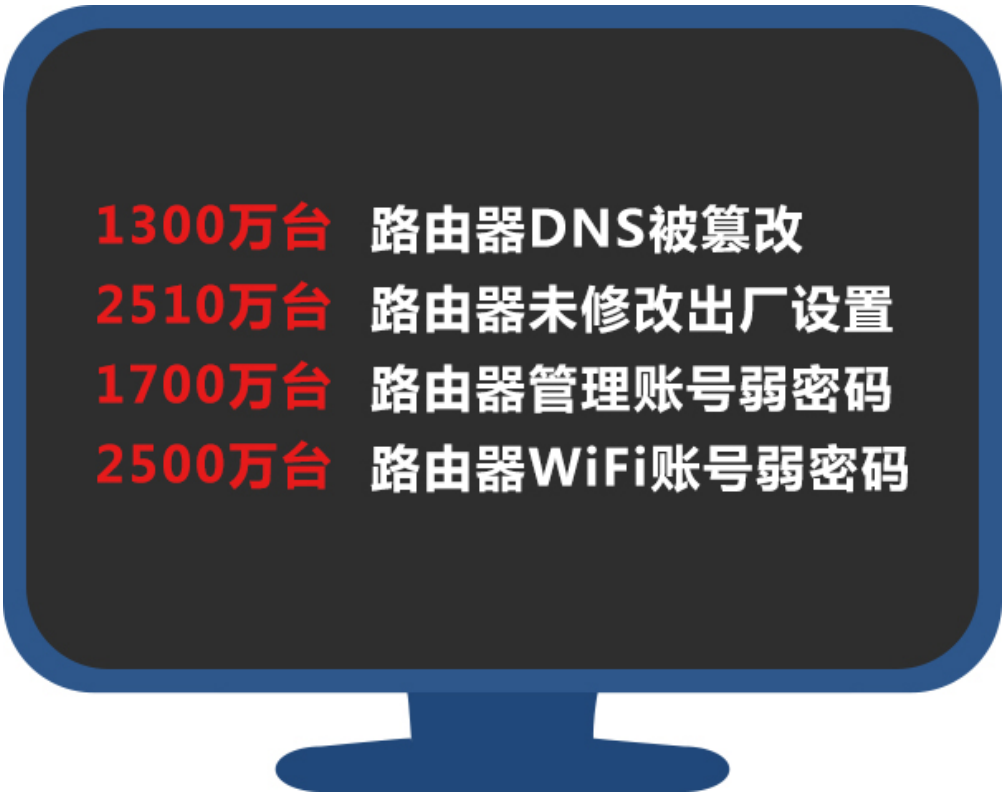

图 23：2014 年路由器四大安全问题

2. 2014 年路由器漏洞 Top10

根据受攻击人数、威胁性及代表性进行评估，瑞星评选出了 2014 年路由器漏洞 Top10：

2014年路由器漏洞Top10

1	任意命令执行
2	任意文件下载
3	未授权访问
4	XSS跨站脚本
5	设计逻辑错误
6	配置不当
7	弱口令
8	系统后门
9	权限绕过
10	拒绝服务

图 24：2014 年路由器漏洞 Top10

3. 路由器重大漏洞及实例分析

1) 腾达路由器存 XSS 漏洞

2014 年 9 月，腾达路由器 4G301 型号被发现存在存储型 XSS 跨站脚本漏洞（漏洞编号 RSV-2014-001）。黑客可通过该漏洞，精心构造一段攻击代码，使路由器的 URL 过滤、客户端过滤等功能失效。届时，黑客可入侵整个网络，随意蹭网、盗取隐私信息、推送诈骗网站、盗取各类网络账号或向移动设备植入病毒，用户很难察觉。此外，该漏洞攻击代码可以在路由器管理页面进行保存，在这种情况下，用户只能通过重置路由器恢复出厂设置，才能摆脱恶意代码的困扰。由于腾达路由器拥有大量用户，因此，一旦漏洞被黑客利用，将严重威胁企业和网民的隐私安全。

图 25：瑞星路由安全卫士检测出腾达 4G301 路由器存在漏洞

2) 中兴路由器曝 0DAY 漏洞

2014 年 10 月，中兴 E5502 型路由器被曝存在漏洞（漏洞编号 RSV-2014-002），可导致管理员密码泄露。该漏洞存在于路由器管理页面的密码修改功能中，黑客无需在该页面填写任何内容，只要点击确认按钮，即可获取路由器密码。届时，黑客将获取路由器的最高管理权限，开启远端 Web 管理功能，随时随地监听用户在互联网上发送和接收的所有消息，并通过篡改 DNS 向用户强制推送钓鱼网站和恶意广告弹窗。用户的路由器一旦遭到攻击，将面临隐私信息泄露、各种网络账号被盗、银行账密信息泄露等风险，同时还有可能遭遇钓鱼诈骗，损失大笔财产。

3) TP-Link 存在任意文件读取漏洞

2014 年 12 月，瑞星“云安全”系统监测到 TP-Link WR2041+型路由器存在任意文件读取漏洞。该漏洞可导致路由器内的任意文件被黑客读取，从而泄露管理员账号密码，使黑客能够进一步控制路由器，篡改 DNS 设置，向用户发送钓鱼网站及恶意广告弹窗。此外，黑客还可利用该漏洞获取用户宽带账户，并使用宽带账户在网上商城消费。路由器一旦遭到攻击，用户将面临网络钓鱼诈骗、隐私信息泄露、宽带账号被盗等风险。

4) 路由不安全易导致网店信息泄露

2014 年 8 月，一位周小姐在网上购买了一千余元的商品，第二天就接到诈骗电话，幸而周小姐非常谨慎，识破骗局，避免了大笔的钱财损失。然而，在该案件发生后，店家和提供交易服务的网站都进行了自查，却未发现任何订单信息泄露事件。

瑞星安全专家指出，该类情况有可能是网店本身缺乏路由安全防护，遭到了黑客攻击导致的。黑客只需对路由器或 WiFi 网络进行攻击，即可入侵网店的内部网络，届时网店的所有在线交易信息都会遭到监听，造成大量订单信息在不知不觉间被泄露。

4. 2014 年路由器安全现状分析

随着智能手机、平板电脑等设备的发展，路由器已在家用领域大规模普及。然而，作为互联网的入口，路由器，尤其是家用路由器在安全防护方面暴露出了巨大的隐患。从 2014 年路由器四大安全问题来看，有三项是由用户安全意识不足引起的。由于路由器具有一次设置后可自动连接的特性，多数用户对路由器操作没有任何概念，甚至干脆忽视路由器的存在，这就为黑客带来可乘之机。

与此同时，蹭网是最普遍的一类通过路由器盗用他人网络资源的现象，然而许多网民对蹭网行为表现出出乎意料的宽容。在瑞星路由器安全抽样调查中，超过五成的用户认为，只要不影响自己的网速，陌生人蹭网是无所谓的事情。瑞星安全专家警告，WiFi 是内网的重要组成部分之一，对于没有经过系统安全建设的家庭网络而言，黑客很可能通过 WiFi 接入家庭网络，进而进行监听，截获各类网络账密、银行卡账户及用户的隐私信息。同时，黑客进入 WiFi 后，还可轻易获取路由器的控制权限，随意篡改路由器设置，甚至获取用户的宽带账户，并利用宽带账户在网上商城消费。

此外，随着电子商务的迅速发展，网购已经成为许多人生活中不可或缺的一部分，然而受到成本限制，国内中小规模的网店和 B2C 电商的路由器普遍缺乏专业维护，存在致命的隐患。黑客只要入侵网店的内部网络，就可以获取店家的订单信息，并向店家发送钓鱼页面，套取店家的银行账户、网络交易平台账号等信息，甚至将店家的资产洗劫一空。

（三）NFC 支付安全

1. 隔空盗刷成 NFC 防护难题

随着 2015 年 IC 芯片银行卡全面取代普通磁条银行卡，NFC 支付成为全社会关注的焦点。然而由于 NFC*技术一直未被大面积应用，因此作为备受瞩目的下一代支付方式，NFC 支付存在很多安全防护漏洞，这些漏洞如不能得到妥善处理，将埋下巨大的安全隐患。

图 26：隔空盗刷成 NFC 防护难题

NFC 技术可让用户进行转账、支付或自动读取身份信息等操作，完成该类操作时，卡片无需与手机直接接触，只要在一定距离内，手机就可隔空甚至隔着衣袋、皮包读取卡内信息。因此在公交、地铁、商场等人流密集的公共场所，只需一个擦身而过的瞬间，用户就可能丢失大笔财产，泄漏重要的身份信息。此外，市面上已经出现一些专业黑客设备，可利用 NFC 功能直接盗取 IC 芯片卡内的钱款和个人身份信息。

注：NFC 即 Near Field Communication，近距离无线通信技术。*

2. 恶意篡改可致大额金融犯罪

NFC 技术发明有十余年之久，目前已应用于门禁卡、食堂饭卡、身份证、公交卡等领域。针对该类卡片的篡改技术，早已有许多版本的攻略在网上流传。2012 年，美国两个安全研究人员就曾利用地铁系统的漏洞，对 NFC 公交卡进行篡改，最终实现了“免费”乘坐地铁的目的。2014 年 11 月，国内某知名安全网站也公布了一个篡改食堂饭卡的攻略。瑞星安全专家指出，黑客只需要花几十元购买一台专业设备即可对卡片余额或其他信息进行篡改、复制。因此未来在 IC 银行卡普及以后，不排除出现利用篡改技术进行大额金融犯罪的可能。

图 27：恶意篡改可致大额金融犯罪

3. 针对 NFC 的病毒已经出现

前文已介绍过，瑞星“云安全”系统曾截获一例 NFC 病毒，可在手机与 IC 卡通讯的过程中改写 IC 卡中的数据，以达到篡改或破坏 IC 卡的目的。目前，该病毒技术尚不成熟，行为也较为单一，然而 NFC 支付的发展空间巨大，一旦有更多利益可图，黑客将加大对 NFC 病毒的挖掘，届时，利用病毒盗取银行账户内的钱款，或盗取用户的隐私信息，将很快被实现。

图 28：针对 NFC 的病毒已经出现

4. “闪付”功能存在漏洞

绝大部分 IC 芯片银行卡都带有“闪付”的功能，无需密码就可在 POS 机上完成小额支付转账。然而这种“闪付”功能并不完善，目前已发现“闪付”在某些 VISA 卡中存在外币支付的漏洞，可使得小额支付的限额失效，最高可利用“闪付”无密码刷取近百万美元的巨额钱款。

图 29：“闪付”功能存在漏洞

5. NFC 安全需从两个维度实现

NFC 技术是一种信息交换技术，因此，想要保护 NFC 支付的安全，必须从两个维度来实现。首先，对于广大消费者及用户来说，无论使用 IC 银行卡，还是公交卡、身份证、门禁卡、食堂饭卡，都应做好防护工作。卡片应存放在足够安全的地方，最好使用专业的 NFC 卡保护套。其次，对于银行、地铁、食堂等提供 NFC 服务的企业，应为 NFC 服务系统建立一套有效的防护机制，并实时更新最新的安全补丁，以避免可能发生的安全事件。

四、企业信息安全

（一）2014 年重大企业级漏洞及趋势分析

2014 年漏洞形式可谓是五花八门，传统的 SQL 注入虽然处于高危行列，但由于专业的防注入技术越来越成熟，因此该类攻击已显得愈发困难，黑客开始转而关注拒绝服务、任意文件上传、任意文件下载等其他漏洞。

根据 2014 年瑞星“云安全”系统的监测，以下为 2014 年重大企业漏洞数据统计：

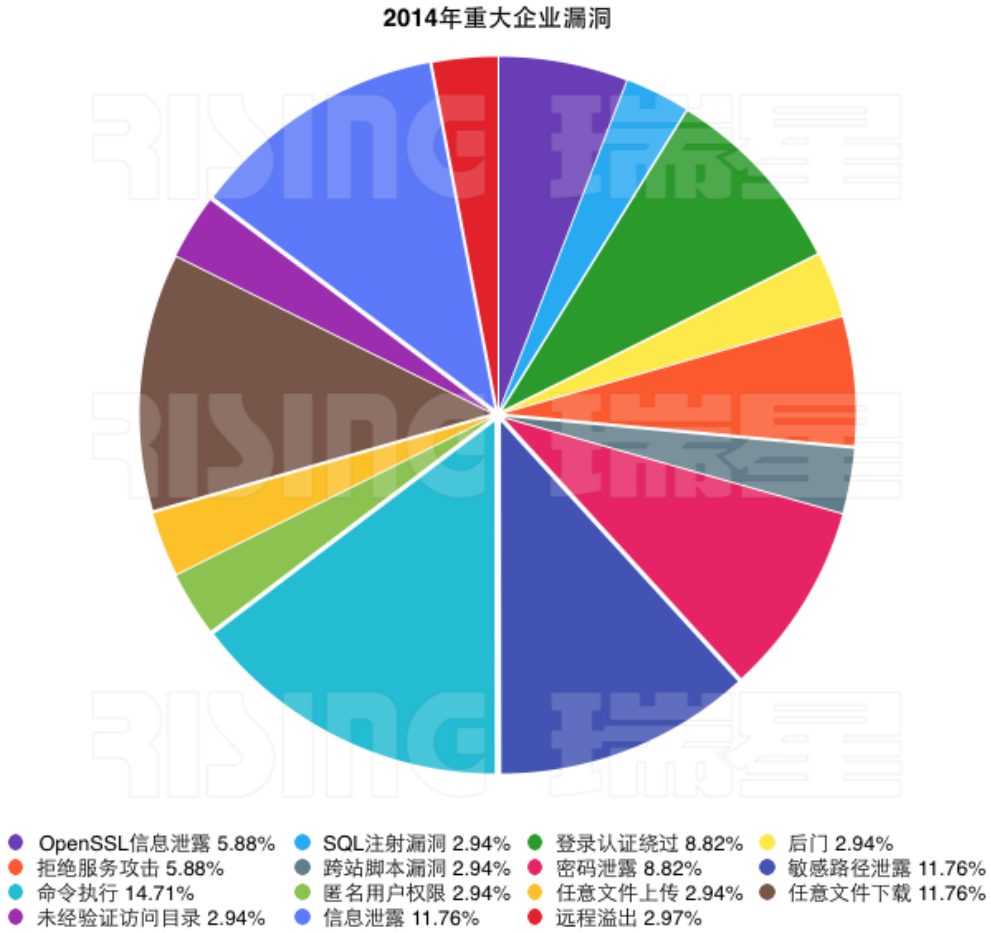

图 30：2014 年重大企业漏洞

目前，国内系统运维人员安全意识相对薄弱，多数网络入侵都是由于网络管理人员的运维不当导致密码及敏感信息泄露所造成。此外，2014 年上半年 OpenSSL“心脏出血”漏洞爆发，由于部分网站没有及时对漏洞进行修复和防护，加大了被入侵的可能性。从 2014 年被入侵的网站及部分漏洞可以看出，2015 年的漏洞发展形势并不乐观，需加强网站密码及敏感信息的管理避免信息泄露。

（二）2014 年五大信息安全事件

1. 超级电厂席卷欧美

2014 年 7 月，一种名为超级电厂的病毒席卷了美国、西班牙、法国、意大利、德国、土耳其以及波兰等多个发达国家的 1018 个发电站。据媒体报道，超级电厂的作者是一个名为“蜻蜓”（Dragonfly）的黑客组织，该组织企图通过病毒远程访问并控制电站的燃料供应系统及管道供应系统。用户电脑一旦遭到感染，病毒就会收集 VPN 配置文件及重要机密文件，并上传至黑客指定地址。除此之外，该病毒还会收集密码并进行屏幕截图，对整个系统进行严密监控。根据瑞星“云安全”系统监测到的数据来看，超级电厂只进行了一些侦察监听活动，但不排除未来“蜻蜓”可能会利用该病毒彻底控制被入侵的电厂，并对国家的整个电力系统进行攻击。

2. 俄黑客组织“沙虫”利用 OLE 0Day 漏洞制造病毒

2014 年 10 月，俄罗斯一个名为“沙虫”的黑客组织利用 Windows 的 OLE 0Day 漏洞制作出病毒，并向他国政府和科研机构发动攻击。病毒伪装成正常的 Office 文档，当用户打开染毒文档时，恶意代码将被触发，病毒会在后台连接黑客指定服务器，下载其他恶意程序和木马病毒至用户电脑。届时，用户硬盘中存储的隐私信息、机密文件以及用户的各类网络账号和银行账号都将面临被盗的风险。

图 31：瑞星杀毒软件 V16+查杀 OLE 0Day 漏洞病毒

瑞星安全专家介绍，OLE 0Day 漏洞影响极广，不但波及 Windows Vista SP2 至 Windows 8.1 的所有操作系统，作为服务器系统的 Windows Server 2008 和 2012 也不能幸免，因此遭遇病毒袭击的用户将比以往更多。

3. OpenSSL 心脏出血漏洞致银行电商大规模泄密

4 月 7 日，国际知名安全协议 OpenSSL 被曝出存在漏洞，其官方网站发布安全公告称 OpenSSL1.0.1f 版本中存在一个严重漏洞（CVE-2014-0160），可导致网站服务器被黑客监听，用户的敏感信息被泄露。据媒体报道，国内约有 3 万余个网站受此漏洞影响，其中包括银行、电商、金融及社交等涉及用户关键信息的网站。

瑞星安全专家介绍，该漏洞被业内称为“心脏出血”漏洞，黑客可利用该漏洞获得大量的用户真实姓名、年龄、性别、手机号码、常用地址、身份证号码等，甚至连网银账密、购物网站支付密码等信息也可窃取。一旦网站因 OpenSSL 漏洞遭受黑客攻击，网民将在毫不知情的情况下面临隐私信息泄露及财产被盗的风险。

4. SSLv3 曝“POODLE”0Day 漏洞

2014 年 10 月，知名加密协议 SSLv3 曝出名为“POODLE”的高危漏洞（漏洞编号 CVE-2014-3566），可导致网络中传输的数据被黑客监听，使用户的敏感信息、网络账号和银行账户被盗。该漏洞影响所有 Windows 版本，其中 IE、Firefox、Chrome 等浏览器用户在使用免费 WiFi 以及安全级别较低的路由器时极易遭到攻击。黑客可利用“POODLE”漏洞劫持用户与网站之间传输的数据，窃取用户名、密码等敏感信息。此外，攻击者还可随意篡改用户接收到的信息，甚至向传输数据中植入恶意代码，进而对用户进行钓鱼、挂马等一系列攻击。届时，用户的网络账密、银行账号、机密文件以及隐私信息都将面临泄露的风险。

5. 12306 用户信息泄密 旗下 6 分站曝重大漏洞

2014 年 12 月 25 日，一个 14M 的文本文件在互联网上疯传，内含 13 万条 12306 网站（中国铁路客户服务中心）的用户数据，包括用户邮箱、密码、姓名、身份证、手机等关键隐私信息。瑞星互联网攻防实验室对该事件进行了调查，发现 12306 网站主域名下共 6 个分站存在 Strust2 框架的远程执行漏洞，黑客可使用专业工具直接对网站进行攻击，遥控网站服务器下载恶意文件，获取最高控制权限，进行跳板攻击，进而对 12306 整个网站进行入侵，获取所有数据库中的信息。

瑞星安全专家表示，本次信息泄露事件危害极高影响恶劣。13 万条用户信息虽然对 12306 网站的数据库来说只是冰山一角，然而，由于信息真实性高，且都是涉及身份信息的关键性资料，因此不排除部分黑客看到了里面蕴含的巨大经济利益，进而对 12306 进行后续攻击。

（三）物联网、虚拟化及云计算安全

1. 智能设备与大数据带来安全威胁

近年来，智能设备、可穿戴设备已经逐渐得到全社会的广泛关注，智能手机、智能手表、云摄像头、智能眼镜等产品正在逐渐走入人们的生活，智慧家庭、智慧地球等字眼越来越高地被科技媒体提及。瑞星安全专家介绍，智慧家庭使许多设备串联在一起，组成了小规模的物联网，在网络中，每个设备都不是孤立的，它们之间相互协作来完成用户的指令，而协作联动又依靠数据交换。通常情况下，智能设备的数据交换依靠提供云服务的大数据托管商来完成，这就带来了安全隐患，一旦数据托管商的服务器遭遇攻击，用户就将面临大规模的真实信息泄露，届时，从汽车牌号、家庭住址，乃至居室的布局、卧室的家具摆放，都有可能遭到恶意监控。

2. 物联网存巨大安全隐患

相对于更高级的企业应用，智慧家庭其实只是物联网的一个很小的组成部分。目前，在通讯、医疗、教育、金融等行业，物联网已经肩负起至关重要的作用。银行的 ATM 设备是最常见最典型的应用案例，用户通过联网的 ATM，可对自己的银行账户进行存取款操作，而无需通过银行的柜台窗口。然而近两年，ATM 遭到攻击的事故却频频出现在世界各地的新闻中。

此外，由于医疗器械大量接入医院内网，医疗网络也成为黑客关注的对象。瑞星安全专家指出，病患的身份信息和健康信息仅是黑客关注的一小部分。此前，黑帽安全大会中曾有人公布过一个利用发射天线远程操控医疗设备对病患进行攻击的模拟实验。未来，对医疗设备的攻击，甚至有可能演变成为恐怖袭击。

3. 云计算及虚拟化安全至关重要

瑞星安全专家指出，无论是大数据存储还是高级物联网应用，实际上都是基于虚拟化系统来完成的。近年来，虚拟化、云计算已越来越多的被应用于个人信息存储、通讯、医疗、教育、金融、航空航天等领域，据相关机构数据显示，仅 2014 年上半年，国内在建的大型虚拟化系统就有数十个之多。然而相对急速扩张的虚拟化市场，配套的信息安全建设却并没有跟上。

从互联网攻防的角度来看，虚拟化及云计算系统需要建立严格的防护制度，不但要对病毒入侵、恶意攻击能够准确识别并快速拦截，同时还应建立严格的内网准入制度，对联网的终端进行有效识别，拒绝陌生设备的接入。

从存储和资源整合的角度来看，虚拟化及云计算以高度集中为主要特性，其理念在于将基础设施、资源以及服务整合成为资源池，并按需分配给每一个用户。这大大提高了资源利用率和管理效率，但同时也为安全埋下隐患。一旦承载虚拟化系统的主机出现问题，存储在云端的数据将大面积泄露，同时整个网络还将面临客户端瘫痪，乃至系统整体瘫痪。因此，没有安全防护措施的虚拟化系统，将是极度脆弱与危险的。

五、2015 年安全趋势展望

（一） 国产操作系统逐步取代国外产品

2014 年 8 月，《人民日报》在其英文 Twitter 账号上发布消息称，政府采购部门已经将赛门铁克与卡巴斯基从安全软件供应商名单中排除出去。此前，早在 5 月份，中央国家机关政府采购中心就宣布，政府部门采购的计算机不得安装 Windows 8 操作系统。此外，在 2014 年中央国家机关政府采购协议供货商名单中，Deepin（深度）、SPGnux、中标麒麟（NeoKylin）、中科方德、优麒麟、阿里云、龙鑫等多款国产操作系统进入名单。

瑞星安全专家表示，经过棱镜门事件，国家间的信息对抗已由暗转明。斯诺登多次爆料使欧美国家的科技巨头对中国及其他国家的长期技术渗透全面暴露。为保证国家安全，以本土产品替换外国科技产品，将国外产品从银行、军事、国企和重要政府部门中“清除”，是大势所趋。

（二）Linux 病毒或将大面积爆发

1) Linux 病毒由来已久

2014 年，受科技产品国产化的影响，国产操作系统开始受到政府及大型企事业机关单位的高度重视。许多人认为，以 Linux 系统为基础的国产操作系统最符合国家、政府和企业信息安全需求，它不但拥有无后门、无插件等天然优势，同时还没有漏洞，不会遭遇病毒入侵。然而，瑞星安全专家指出，这种认知不完全正确。

Linux 无病毒的说法有一部分来自于对 Linux 系统一知半解的网民。因为 Linux 的运行方式、计算方法和底层代码都与 Windows 有着本质区别，所以一部分人认定，Linux 系统没有病毒。事实上，早在 1996 年，破解组织 VLAD 就发布了世界上第一个 Linux 病毒 Staog。在其后的 18 年中，脚本病毒、蠕虫病毒、黑客后门病毒、可执行文件病毒等各式各样的 Linux 病毒层出不穷，几乎囊括了所有已知种类，时至今日，任何在 Windows 中出现的病毒类型，都曾在 Linux 系统中被发现过。

国家漏洞库的数据显示，从 2005 年至今，Linux 系统曝出的漏洞就有 3300 余个，Linux 病毒也正是来源于此。由于源代码完全公开，黑客只要对 Linux 系统足够熟悉，就可轻松利用漏洞制造病毒。目前，瑞星的病毒库中，已有 6 万余条样本记录属于 Linux 病毒。由此可见，从 Staog 诞生之日起，Linux 从未摆脱过病毒的阴影。

2) Linux 病毒的制作成本更加低廉 原理与 Windows 病毒无二致

虽然 Linux 系统与 Windows 系统有着本质的区别，然而在病毒制作的原理方面却并无二致。瑞星安全专家指出，与 Windows 雷同，Linux 病毒也大都利用漏洞获取系统权限，进而入侵电脑。从病毒行为来看，无论是 Windows 还是 Linux，甚至还包括 Mac、Android、IOS 等系统，病毒进入电脑后只有三件事可做：破坏系统、收集设备中的数据信息（盗取隐

私信息、银行账户或机密文件等）和获取设备的控制权（为黑客开启“后门”）。

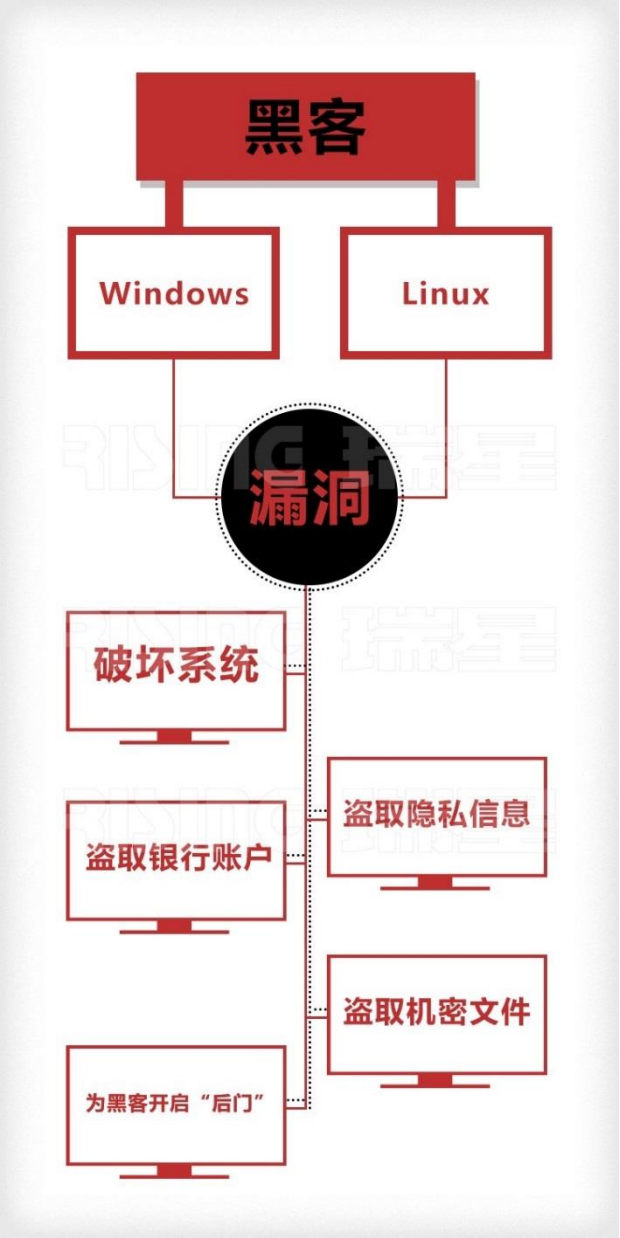

图 32：Linux 病毒原理和目标与 Windows 病毒并无二致

瑞星安全专家强调，Linux 病毒的制作成本实际上比 Windows 病毒更加低廉。与 Windows 系统不同，Linux 系统是一个完全开放的系统，任何人都可以获得其完整的源代码。因此，黑客在制作病毒的过程中，省去了破解系统源代码的工作，而这一环节恰恰是最复杂、成本最为高昂的环节。

3) 用户总量决定病毒数量 Android 系统是前车之鉴

既然 Linux 病毒与 Windows 病毒并没有本质区别，甚至 Linux 病毒的制作成本要比 Windows 更加低廉，那为什么没有出现过 Linux 病毒大面积暴发的事件呢？瑞星安全专家指出，根据瑞星 20 余年的反病毒经验，用户总量才是决定病毒数量的关键因素。Linux 病

毒之所以不像 Windows 病毒那样普遍，完全是因为 Linux 用户稀少的缘故。据媒体数据显示，截至 2013 年，Linux 系统在 PC 市场的占有率只有 1.52%，而 Windows 则有 91.19%。这种量级上的悬殊差距意味着即使需要花费更多的精力，制作 Windows 病毒的投入产出比仍远远高于 Linux 病毒。因此，Linux 系统并不受到黑客们的重视，而且 Linux 病毒也变得非常罕见。

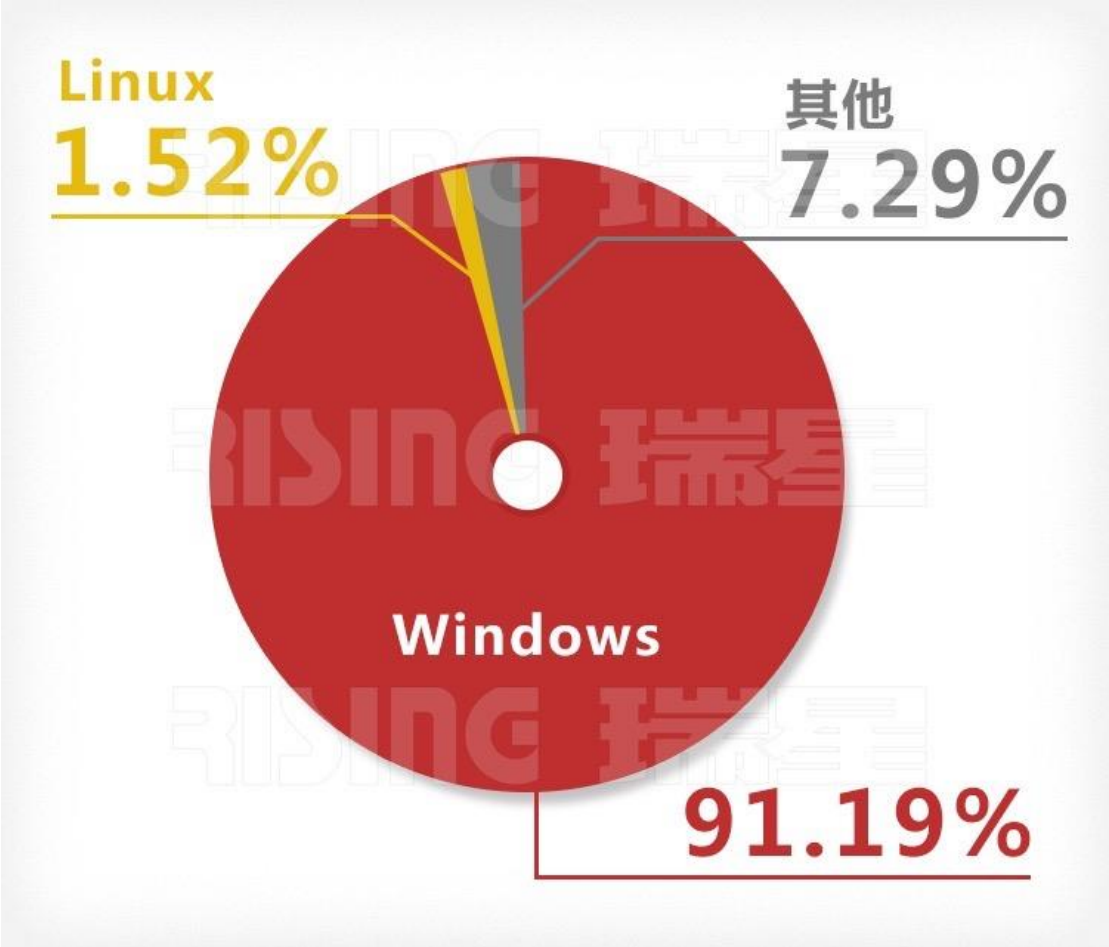

图 33：稀少的市场份额使 Linux 病毒具有局限性

到此为止，许多人可能仍然有一个疑问，Linux 尚未普及，那怎么能断定普及后会出现大量病毒呢？其实关于这个问题，已经有了一个前车之鉴，那就是 Android 系统。Android 作为一个开源系统，被广泛用于智能手机、平板电脑、智能电视以及众多智能设备中。它是全世界市场占有率最高的移动设备操作系统，这个系统使用的正是 Linux 的内核程序。根据瑞星云安全系统监测，仅 2014 年，瑞星“云安全”系统就拦截到 183 万余个 Android 病毒样本，这个数字与 2013 年同期相比增长了 128.75%。显而易见，随着 Android 系统的大量普及，专门针对该系统的病毒也出现了大面积爆发的情况。因此可以预见，Linux 一旦普及，针对该系统的病毒也会全面爆发。

（三）开源系统将继续引发安全问题

2014 年曝出了三个重量级开源系统漏洞——OpenSSL 心脏出血漏洞、SSLv3“POODLE”漏洞以及 Shellshock 漏洞。这些漏洞所涉及到的开源系统都拥有十数年甚至更长时间的历史，由于缺乏经费，其核心代码已有很长时间没有进行过维护审计。然而不幸的是，这些开源系统恰恰是现代互联网的基石，至今仍有许多先进的大型网络平台依赖该类开源系统。因此可以预见，在 2015 年，大量的黑客及安全研究人员将投入到开源系统的研究中，更多开源系统的漏洞将被曝出，同时对开源系统的安全维护也必将得到全世界的关注。

（四）Windows 漏洞逐渐减少 黑客攻击由个人转向企业

相较于 2013 年，2014 年 Windows 操作系统的 0Day 漏洞有较大数量的下降，预计 2015 年以后会更大幅度的减少。从 Windows7 版本开始，Windows 系列操作系统的安全性正在不断提高。然而随着系统安全性的提高，漏洞挖掘变得更为困难，使得挖掘成本大幅提升，黑客将逐渐形成组织化及团队化规模，以降低成本并获取更大利益。瑞星安全专家预测，受此影响未来，针对个人的漏洞攻击会大幅减少，以经济或政治利益为目的黑客袭击事件将更加频繁。

（五）大数据、云计算及虚拟化问题将进一步凸显

随着智慧家庭、高级企业物联网应用的大面积普及，一场悄无声息的攻防战也将围绕着大数据、云计算及虚拟化拉开帷幕。从 2014 年的安全形势来看，黑客拖库的数据可以达到数十亿规模，这说明云服务供应商及各类虚拟化平台的安全防护仍有所欠缺。此外，一些证据表明，黑客已经具备大数据的分析和监控能力，可通过云端对海量目标进行 24 小时不间断的监控，只要监控目标中出现安全防护薄弱的行为，黑客就能立刻发现，并进行实时攻击。

瑞星安全专家指出，得大数据者得天下，商家有了大数据可以随时获取商机，而黑客拥有了这些数据不但有可能危害个人的人身安全，更有可能针对企业、政府乃至整个国家进行各类攻击。因此，大数据、云计算及虚拟化安全，将是 2015 年最受瞩目的核心焦点。

=====END=====

关于瑞星：

瑞星公司成立于 1991 年，作为亚洲最大的信息安全厂商之一，瑞星一直专注于信息安全领域，致力于帮助个人、企业和政府机构有效应对各种信息安全威胁，保护用户的系统安全和网络安全。

在瑞星不断发展与壮大的过程中，我们建立了国内规模最大、实力最强的研发团队，二百余名国内顶尖的反病毒专家和软件工程师，开发了瑞星品牌的全系列安全产品。从面向个人的安全软件，到适用于大型企业网络的软件、硬件和专业服务，瑞星公司为各种用户提供了信息安全的整体解决方案。

欲查询公司详情，请访问我们的网址：http://www.rising.com.cn/
免费服务专线：400-660-8866