瑞星 2014 年上半年中国信息安全报告

北京瑞星信息技术有限公司

2014 年 7 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 1 至 6 月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 1 至 6 月，瑞星“云安全”系统共截获新增病毒样本 3,032 万余个，病毒总体数量比去年同期增长 85.67%，呈现出一个爆发式的增长，其中主要以木马和蠕虫病毒为主。

- 2014 年 1 至 6 月，瑞星“云安全”系统截获挂马网站 341 万个（以网页个数统计），与去年同期相比上涨了 38.61%。由于今年 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，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。此外，在报告期内，瑞星“云安全”系统共截获钓鱼网站 352 万个，比去年同期降低了 11.78%，帮助用户拦截钓鱼网站攻击 1.19 亿余人次。

- 2014 年 1 至 6 月新增手机病毒样本 118 万余个，与去年同期相比增长了 4.62 倍，呈现爆发式增长态势，Android 操作系统新增 72 个漏洞，与去年同期相比下降了 12.19%。移动支付的迅速普及，使智能手机成为黑客的另一生财之道，监听隐私、盗刷网银带来的巨大利益让黑客制造出更多病毒，并通过广告弹窗、网站、论坛以及非正规的应用商店大量传播。

- 2014 年上半年，车联网开始进入人们视线。由移动互联网与智能车载系统结合带来的汽车远程遥控系统，成为大量车主关注的焦点。然而作为一项新兴技术，汽车远程遥控技术的应用还存在许多安全问题，遥控 APP 安全及服务系统后台安全，成为威胁车主生命安全的高危隐患。

- 2014 年上半年，WiFi 路由器安全是网民及媒体关注的重点问题。经瑞星调查，全国约有七成路由器缺乏安全防护，58%的用户曾遭遇过蹭网，31%的用户曾遭遇过 DNS 劫持，另有 5%的用户因路由器安全问题遭遇过盗刷网银。WiFi 弱口令、路由器无安全设置、DNS 劫持、公共场所 WiFi 监听、WiFi“黑网”、路由器漏洞、远程 Web 管理、DMZ 主机等问题成为主要安全隐患。

- 2014 年上半年，国际知名安全协议 OpenSSL 被曝出“心脏出血”漏洞，致使银行、电商的支付系统都不再安全。同时，由于云计算、虚拟化系统在国内迅速普及，其带来的安全问题也逐渐浮出水面，因此为虚拟化系统打造专属的信息安全解决方案是当务之急。此外，以 Windows 8 为代表的外国软件正逐渐被政府部门排除在外，中央网络安全和信息化小组的成立，标志着我国终于将信息安全提升至国家安全的重要地位，信息安全主权正逐步回到国家手中。

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）上半年病毒概述

1.病毒疫情总体概述

2014 年 1 至 6 月，瑞星“云安全”系统共截获新增病毒样本 3,032 万余个，病毒总体数量比去年同期增长 85.67%，呈现出一个爆发式的增长。这是由于病毒与杀软之间的技术对抗日益升级，病毒采用了更加复杂的加密、反查杀技术，因此出现了更多变种，而杀软则引进了人工智能技术及病毒基因检测技术，能够捕获更多病毒样本。

在报告期内，木马病毒占总体病毒的 69.29%，依然是第一大种类病毒。其中新增病毒样本还包括第二大种类病毒蠕虫病毒（Worm），占总体数量的 8.67%。另外黑客程序（Hack）占总体数量的 6.41%，后门病毒（Backdoor）占总体数量的 5.81%，位列第三和第四。其他类型、感染型（Win32）、病毒释放器（Dropper）和恶意广告（Adware）比例分别为 4.81%、3.88%、0.96%和 0.17%。

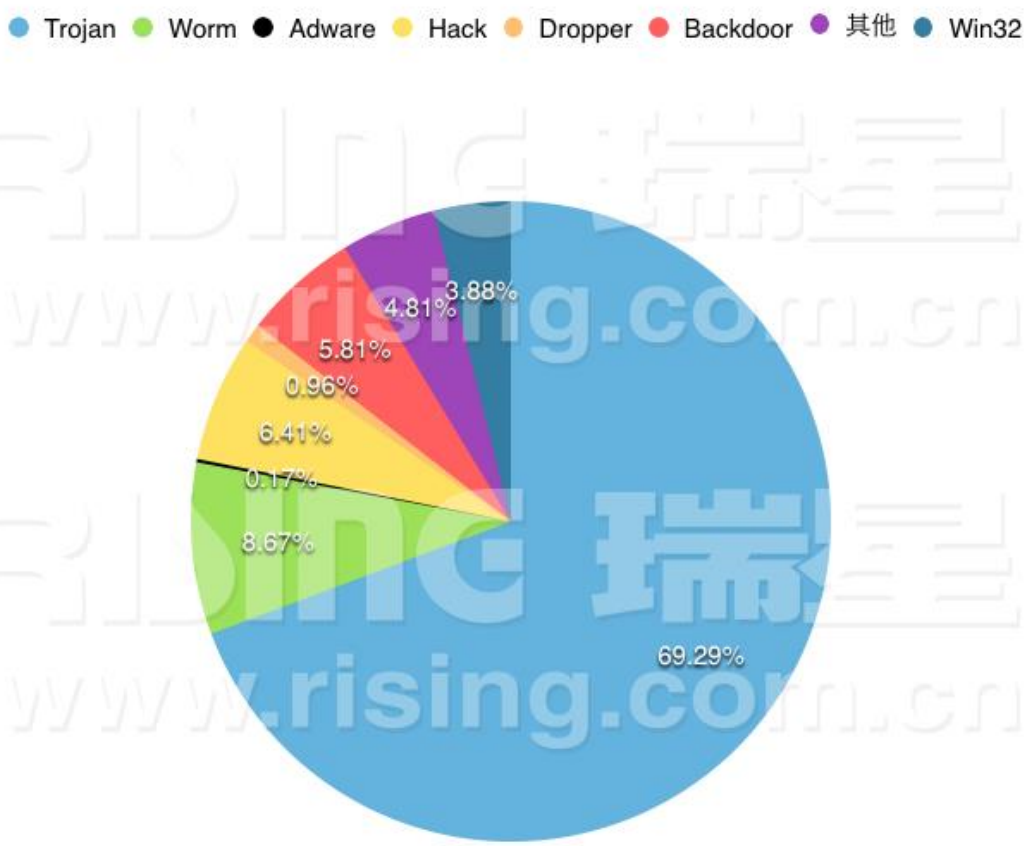

图 1：2014 年 1-6 月份病毒疫情总体统计

2014 年上半年共有 3.34 亿人次网民被病毒感染，有 1,491 万台电脑遭到病毒攻击，人均病毒感染次数为 22.4 次。木马病毒依然是主流病毒，黑客程序与 2013 年相比涨幅较大。

2. 病毒感染地域分析

在报告期内，广东省病毒感染为 4,002 万人次，依然位列全国第一，其次为山东省 2,225 万人次及江苏省 1,931 万人次。

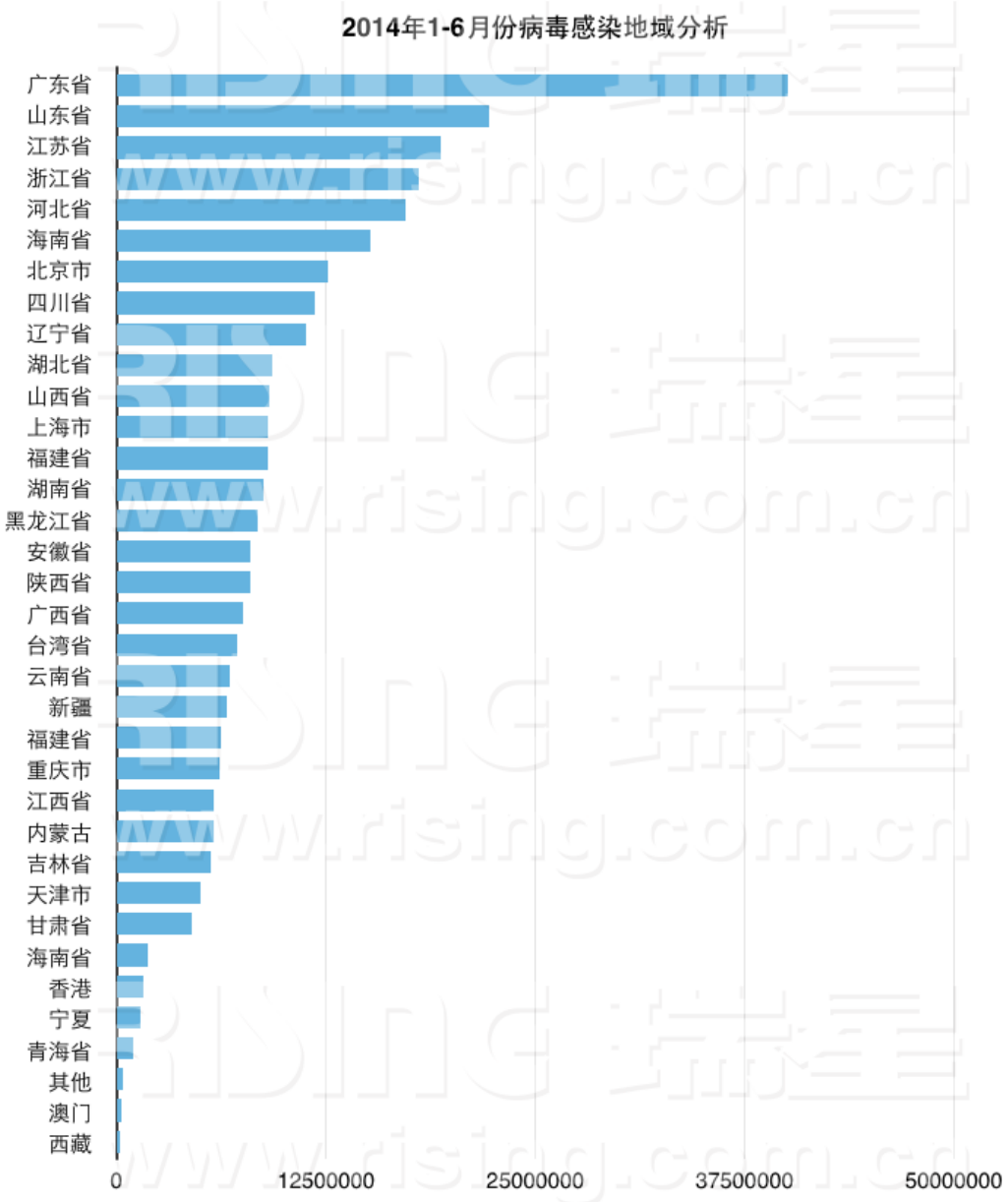

图 2：2014 年 1-6 月份病毒感染地域分析

（二）2014 年上半年病毒 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 上半年病毒 Top10:

2014年1-6月份病毒Top10

排名	病毒名称	病毒描述
1	Malware.FakeFolder@CV	蠕虫病毒，伪装成文件夹图标迷惑用户，中毒后打开后门，下载恶意程序并运行。
2	Trojan.Script.Lisp.ACAD	木马病毒，病毒会感染用户电脑中正常的lisp脚本，影响用户CAD操作，有较强的传播能力。
3	Backdoor.Overie	后门病毒，中毒后在系统中打开后门，使电脑沦为肉鸡。
4	Trojan.Kazy	木马病毒，中毒后在后台下载恶意程序并运行。
5	Trojan.DL.Script.JS.Agent.lok	木马病毒，用户访问挂马网站时会触发浏览器漏洞，造成电脑中毒，并下载其他恶意木马或后门病毒。
6	Trojan.PSW.Win32.Agent.exw	木马病毒，盗取网络游戏账号密码，并发送到指定网络地址。
7	Hack.Exploit.Script.JS.Bucode.i	黑客程序，利用浏览器漏洞挂马，用户在访问挂马网页后电脑会下载指定的病毒并运行。
8	Trojan.Script.VBS.Dole	宏病毒，感染用户office文档，影响用户使用，破坏数据。
9	Win32.Parite.b	感染型病毒，感染系统中的所有PE文件，运行后会下载指定的程序并运行。
10	Win32.KUKU.ky	感染型病毒，感染系统中的所有PE文件，运行后会下载指定的程序并运行。

图 3：2014 年 1-6 月份病毒 Top10

（三）2014 年上半年典型病毒分析

1. 《白日焰火》引发病毒潮

今年 2 月《白日焰火》在柏林电影节上摘得桂冠，一时之间，“白日焰火”、“廖凡”成为网上炙手可热的关键词。随后，瑞星“云安全”系统就拦截到了一款乔装为《白日焰火》视频文件的病毒，该病毒的文件名及图标都经过精心伪装，让普通网民难辨真假，一旦网民下载并打开，就会遭遇 QQ 账号被盗、隐私信息泄露等风险。

图 4：伪装成《白日焰火》视频文件的病毒文件

该病毒的图标显示为视频文件，文件名也经过“专业修饰”，采用了 unicode 字符误导网民，使网民误以为是正常的 mkv 视频文件。病毒运行后，就会自动检测电脑中是否正在运行 QQ 进程，并获取 QQ 的安装目录，进而修改 QQ 文件，劫持系统 DLL 文件，后台下载盗号工具。当中毒电脑再次启动 QQ 后，下载的盗号工具将被自动加载，截取网民输入的账号、密码和聊天内容等信息，并发送至黑客指定的服务器。同时，该病毒还会向用户加入的 QQ 群中上传带毒文件，实现进一步传播。

2.21 秒不雅视频藏病毒

今年 5 月，一个名为“李 21 秒”的某明星不雅视频悄然出现在网上，其后瑞星“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，让普通网民难辨真假。一旦网民下载并点击，在视频打开的同时将使电脑中毒，可能会导致网络账号密码被盗、隐私信息泄露、银行卡被盗刷等，同时电脑也将成为黑客“肉鸡”。

图 5：“李 21 秒”病毒视频截图

瑞星安全专家介绍，借用不雅照片、视频来传播病毒是黑客常用的小伎俩， “21 秒视频”后门病毒就是一个典型案例。黑客将视频文件和病毒一起打包成一个自解压包，当用户打开后，会释放出病毒和视频文件。殊不知，在视频播放时，电脑就已经中毒了，病毒会在

电脑中开后门，黑客可以直接对中毒电脑进行远程控制、拷贝文件、记录键盘操作、偷开摄像头录视频等危险行为。

3. Gamarue 蠕虫成 U 盘病毒新标准

上半年，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。而本次发现的 Gamarue 蠕虫可自动隐藏病毒程序，被感染后用户打开U盘后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

瑞星安全专家介绍，该类病毒的快捷方式往往带有迷惑性，使用户以为是某个自己的程序，并引诱用户双击打开，然而当用户进行该类操作时，病毒就会自动运行，届时电脑将出现网速缓慢，系统资源被大量占用等问题。

4. “超级电厂”席卷欧美

今年 6 月底，一种名为“超级电厂”的病毒正在席卷美国、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，并主要针对燃料供应系统及管道供应系统。该病毒收集 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，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。

瑞星安全专家介绍，目前“超级电厂”只进行了一些侦察监听活动，但未来可能会彻底控制这些电厂，并对国家的整个电力系统进行攻击。

二、恶意网站

（一）挂马网站

1. 挂马网站概述

2014 年 1 至 6 月，瑞星“云安全”系统截获挂马网站 341 万个（以网页个数统计），与去年同期相比上涨了 38.61%。这是由于今年 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，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。

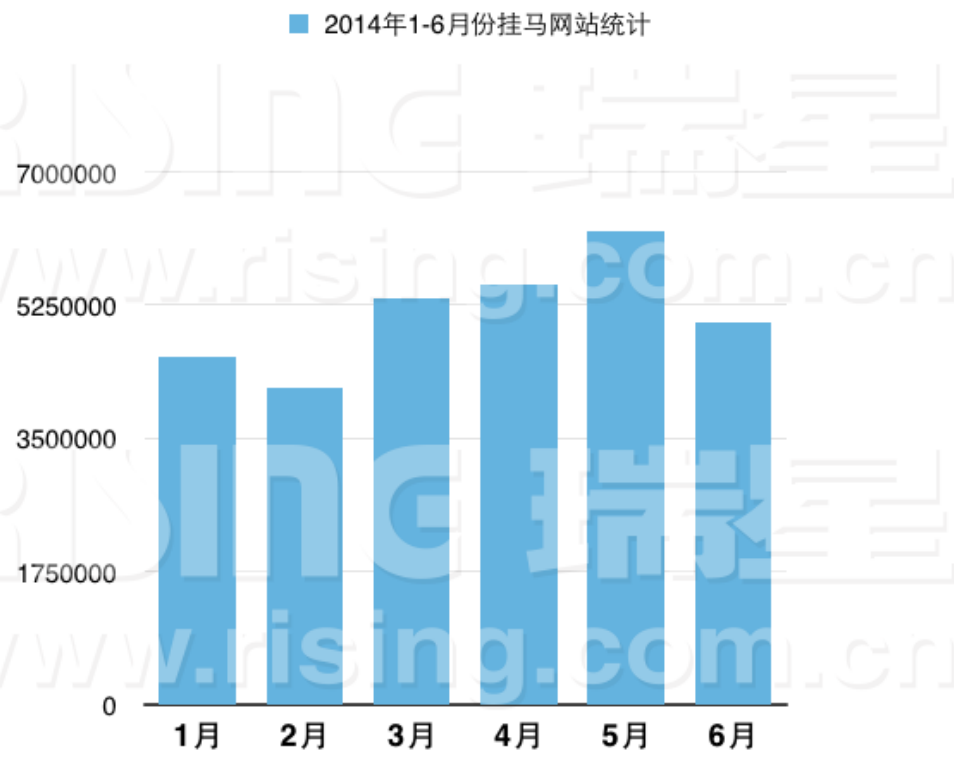

图 7：2014 年 1-6 月每月截获挂马网站统计

在报告期内，瑞星拦截挂马网站的攻击总计为 3,083 万余次，与去年同期相比上涨 77.59%。

2. 挂马网站趋势分析

从被挂马网站上分析，教育类网站和政府类网站是黑客攻击的主要目标，这是由于这两类网站安全性较低造成的。同时，在较多的游戏宣传页面和地方门户网站也会出现恶意挂马等现象。从网马植入的恶意代码来看，绝大部分木马是针对网络游戏账号密码进行盗取的恶意程序。从挂马手段和加密方式来说没有什么新的技术，从利用漏洞情况，与 2013 年相比，主要是出现了更多的利用 java、flash 漏洞的网马。

（二）钓鱼网站

1. 钓鱼网站概述

2014 年 1 至 6 月，瑞星“云安全”系统共截获钓鱼网站 352 万个，比去年同期降低了 11.78%，帮助用户拦截钓鱼网站攻击 1.19 亿余人次。

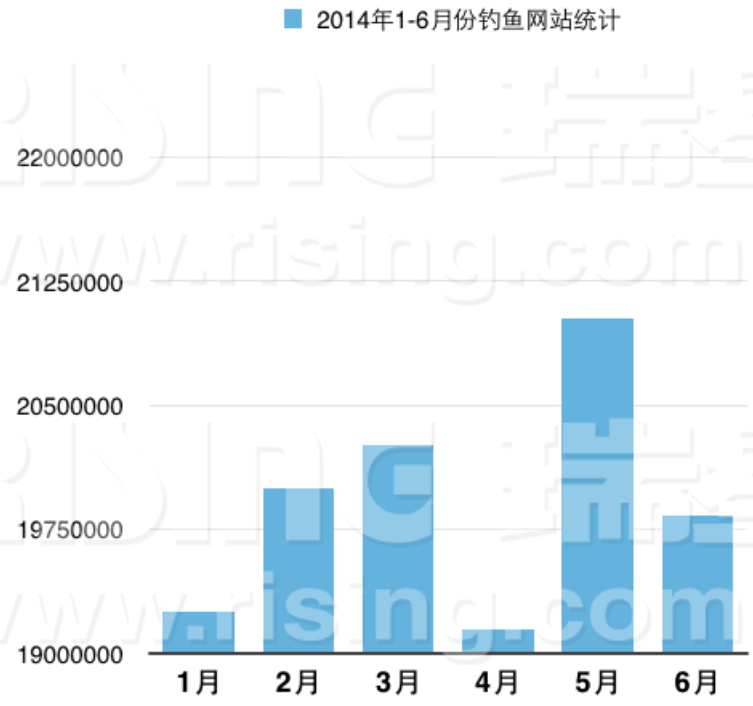

图 8：2014 年 1-6 月份钓鱼网站统计

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 27%，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 20%与 18%。

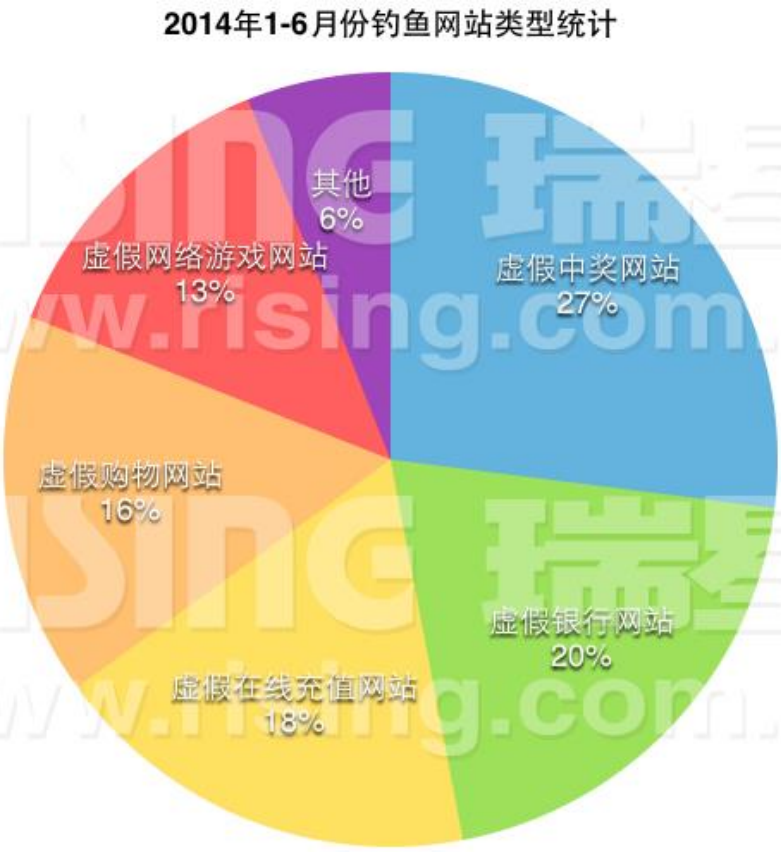

图 9：2014 年 1-6 月份钓鱼网站类型统计

3. 2014 年上半年重大钓鱼网站 Top10

2014年1-6月份重大钓鱼网站Top10

序号	网址	类型
1	wap.ixicbc.com	中国工商银行钓鱼网站
2	www.lolf2.com	QQ钓鱼网站
3	www.cicbxz.com	中国建设银行钓鱼网站
4	wangyin.ymzc.org	支付宝钓鱼网站
5	www.icpcxx.com	中国工商银行钓鱼网站
6	www.greatnflhereonlinesale.com	淘宝购物钓鱼网站
7	trgfhg.vdstetwfd.cf	淘宝购物钓鱼网站
8	www.tnd58.com	网络游戏钓鱼网站
9	www.hongfu5158pt.com	网络游戏钓鱼网站
10	www .wuifdsod.sfafefw.pw	在线充值钓鱼网站

图 10：2014 年 1-6 月份重大钓鱼网站 Top10

4. 2014 年上半年典型钓鱼网站分析

1) 世界杯赌球钓鱼网站盛行

今年 6 月四年一度的世界杯在巴西开战，与此同时瑞星“云安全”系统拦截到了大量世界杯赌球钓鱼网站，该类网站制作精良，“服务周到”，让网民放松警惕，进而向其指定账户打款。瑞星安全专家表示，赌球钓鱼类网站会以各种方式让玩家赔钱，网民一旦轻信就会血本无归，根本不存在“赢钱”的可能。

图 11：赌球类钓鱼网站以各种“奖励”诱惑网民充钱

该类钓鱼网站大都制作非常精良，页面更新速度极快，同时还有热情周到的“客服”指导网民如何参与“游戏”，赢取“奖励”。瑞星安全专家介绍，赌球看似是一种不受网站暗箱操作控制的赌博，但是网民往往不会注意到一旦自己在网站上充钱，这笔钱财就已经脱离自己的控制，成为他人的囊中之物。如果网民赢得了“奖励”想从网站取钱，网站就会以“系统维护”、“银行线路不好”等借口拖延网民取钱的时间，并让客服出马，劝说网民继续在其他“游戏”上投注，直到钱财全部输光为止。除此之外，一些更恶劣的钓鱼网站会直接制造假的网银支付页面，盗取网民银行卡账户密码，将卡内所有钱财瞬间全部转移。

2) 钓鱼网站盯上米粉节

今年上半年有网民在微博爆料，自己用手机购买红米 Note 时遭遇诈骗，损失近千元。据瑞星“云安全”系统监测显示，仅米粉节一周时间就拦截到大量假冒小米手机购物的钓鱼网站。该类钓鱼网站制作精良，仿真度极高，普通人很难分辨真伪。网民一旦被骗，轻则买到假货，并造成姓名、地址及电话等隐私信息泄露，重则银行卡被洗劫一空。

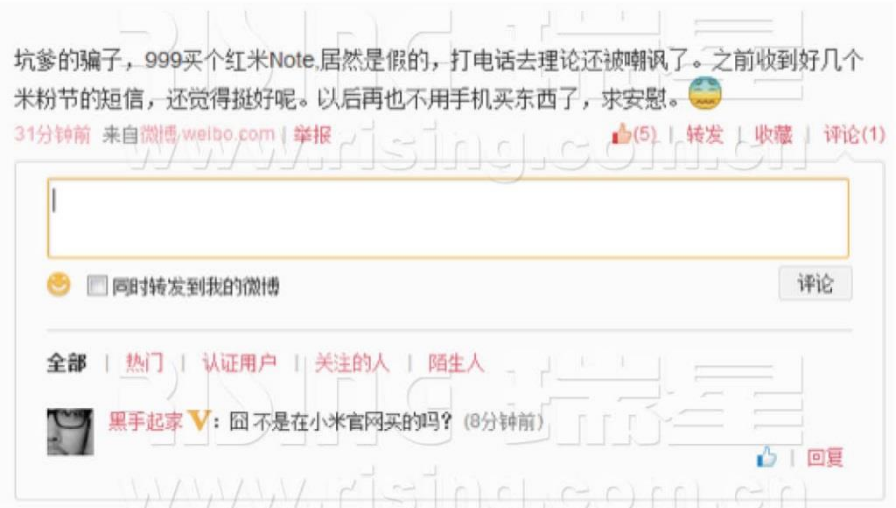

图 12：网民微博爆料手机购物买到山寨红米 Note

图 13：假冒小米手机购物钓鱼网站

瑞星安全专家指出，以往黑客经常利用电商“购物狂欢节”一类的集中打折促销时段，大量传播钓鱼网站，而目前这种钓鱼方式逐渐转移至移动互联网平台。恶意 APP 和假冒公共 WiFi 的黑网都能够对手机用户进行恶意弹窗，网民一旦不慎点击进入，就会打开黑客预先准备好的钓鱼网站，此类钓鱼网站不但售卖假冒伪劣产品，而且还会盗取用户隐私信息、盗刷用户网银。

5. 2014 年上半年新型钓鱼技术手段

2014 年上半年钓鱼网站的攻击方式较 2013 年之前又有了进一步的发展，主要表现在以下几方面：

1) 利用网上购物打折、返利等具有诱惑性的内容进行钓鱼，例如假冒淘宝网站骗取消费者浏览指定网站，进一步骗取用户执行指定操作，骗取用户的钱财。
2) 利用手机 web 端进行的钓鱼。随着便捷的移动网络使用率逐渐上升，很多钓鱼攻击者利用手机浏览器缺少安全防护进行钓鱼攻击。
3) 各种综艺节目火爆以后，网络中出现虚假中奖信息的钓鱼网站并结合电信手段进行钓鱼攻击。
4) 利用伪基站进行的钓鱼。随着终端网络的使用率逐渐上升，很多钓鱼攻击者利用网络传输缺少安全防护进行短信诈骗并与网站结合进行钓鱼攻击。

三、移动互联网

（一）智能手机安全

1. 手机病毒疫情总体概述

2014 年 1 至 6 月新增 Android 手机病毒样本 118 万余个，与去年同期相比增长了 4.62 倍，呈现爆发式增长态势，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。

在报告期内，Android 操作系统新增 72 个漏洞，与去年同期相比下降了 12.19%，其中 Android 系统漏洞 10 个，Android 应用漏洞 62 个，包括 Adobe 系列及以支付宝、财付通、京东商城、民生银行等知名 APP。

瑞星安全专家指出，近年来移动终端的普及极其迅速，尤其移动支付的应用，使智能手机成为黑客的另一生财之道，监听隐私、盗刷网银带来的巨大利益让黑客制造出更多病毒，并通过广告弹窗、网站、论坛以及非正规的应用商店大量传播。

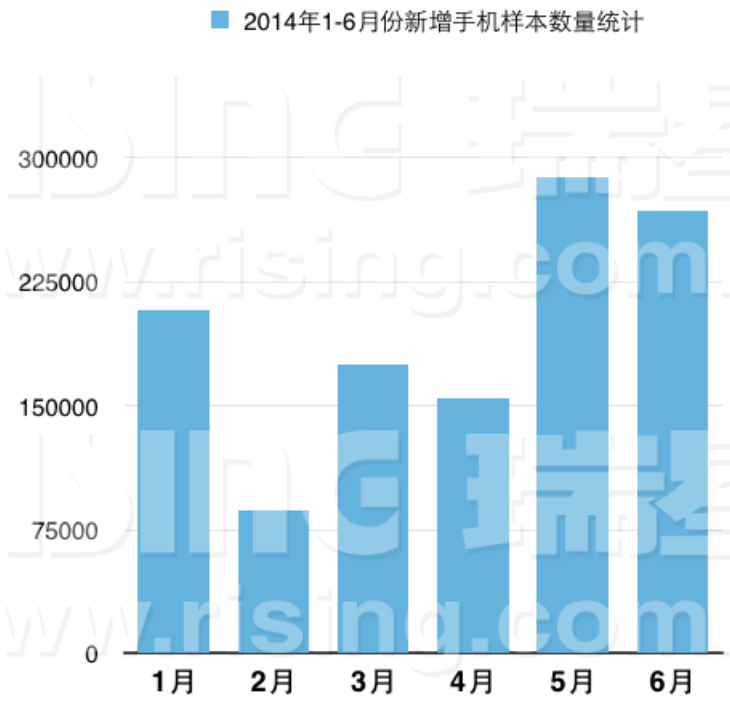

图 14：2014 年 1-6 月份新增手机病毒样本数量

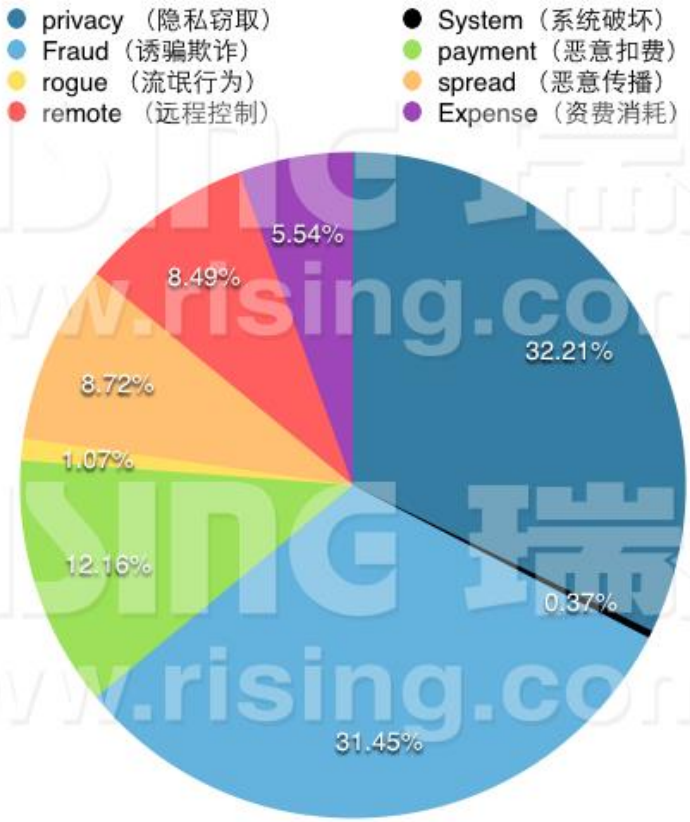

图 15：2014 年 1-6 月份手机病毒类型

2. 2014 年上半年典型手机病毒及趋势分析

1)“Android 窃听器”拨打电话即遭监听

今年 6 月，瑞星“云安全”系统拦截到一个名为“Android 窃听器”的高危手机病毒，手机中毒后只要拨打电话，就会被黑客监听。 “Android 窃听器”从图标和名称来看都是一款拨号应用，一旦被安装至手机，病毒就会在用户毫无察觉的情况下读取、拦截手机短信，获取手机通讯录联系人列表、历史通话记录、本机号码、手机 SIM 卡信息和手机位置信息等。除此之外，黑客还可通过病毒控制手机进行屏幕截图、通话录音、获取 QQ 和微信的好友列表及聊天信息，甚至还可悄无声息地自我删除。

图 16：伪装成拨号器的“Android 窃听器”病毒

2) Zcsoft.a 病毒可短信遥控手机

Zcsoft.a 是一款 Android 手机病毒，该病毒专门用于全方位监听、窃取隐私信息，手机一旦中毒，网民将面临隐私全面泄露的风险。病毒伪装成 Android 系统工具引诱用户下载安装，运行后将后台发送短信至黑客指定号码，黑客可通过短信遥控用户手机，拦截未读短信、读取手机定位信息、窃取通话记录、盗取通讯录，并实现来电录音。

图 17：Zcsoft.a 病毒伪装成系统工具入侵用户手机

3) 手机病毒由扣费向窃取隐私、远程遥控进化

与 2013 年相比，2014 年上半年的 Android 病毒抛弃以往简单的扣费、吸费模式，转而向更加复杂的隐私窃取、远程遥控进化。从上半年的多个重量级病毒来看，监听通话、窃取信息成为黑客的主要目的。瑞星安全专家指出，手机中存储的个人隐私信息往往要比电脑中更加全面真实，黑客可通过大量贩卖这种信息获得巨大利益。除此之外，在移动支付异常火爆的当下，验证码成为影响用户财产安全的关键信息，然而验证码服务严重依赖手机短信

业务，因此黑客只要拦截含有验证码的短信，就能盗取用户网银和支付平台的支付信息，并最终盗取用户的所有财产。

（二）“智能汽车”或成下一个黑客攻击目标

车联网是物联网延伸出的一个概念，它是由车辆位置、速度和路线等信息构成的巨大交互网络。目前，移动互联网及智能手机已经逐渐将车联网从抽象的概念变为现实。今年，包括特斯拉、宝马在内的多家汽车制造企业及第三方应用开发商都推出了自己的汽车远程遥控APP，用户只需在手机上进行操作，就可以遥控汽车点火、熄火、远程定位、锁定及开关空调。

汽车远程遥控应用的开发，大大方便了广大车主，然而却也存在不小的安全风险。首先，汽车远程遥控技术依赖于智能手机，如果手机遗失或被窃，汽车将同时面临被盗的危险。瑞星安全专家指出，与汽车钥匙被窃不同，安装远程遥控系统以后，手机内将会存有爱车的详细信息，其中包括品牌、型号、车牌号甚至地理位置，偷窃者只需根据这些信息即可找到汽车进行盗窃。

图 18：汽车远程遥控系统泄漏汽车信息

其次，当前的汽车远程遥控系统多是依靠验证码来实现远程点火、熄火等操作的，然而这种机制并不安全。今年 4 月，瑞星互联网攻防实验室对多款遥控应用进行了安全检测，发现大多数应用没有对验证码进行加密或采取其他保密措施，黑客可轻松拦截系统验证码，进而获取远程操控汽车的权限。

此外，汽车远程遥控技术本身基于一个服务性的网络平台，瑞星互联网攻防实验室通过大量调研发现该类平台普遍缺乏安全防护，很容易遭到入侵。恶意攻击者可以利用该类网络平台随意查看车辆信息，并直接发送指令，使正在行驶的车辆突然熄火，严重威胁车主的人身安全。

（三）十大 WiFi 路由器安全问题

1. 七成路由器缺乏安全防护

当前我国手机网民总数超过 5 亿，无线路由器、随身 WiFi 等设备普及极其迅速。但近年来随着路由器漏洞和黑客攻击事件不断增加，目前已知包括 D-Link、TP-Link、Cisco 等多家厂商的产品都存在不同数量的漏洞，尽管一些厂商已经在官网发布了修复补丁，但普通用户很难在第一时间获知漏洞及修复的详细信息，因此这些漏洞的影响仍在不断扩大。

瑞星通过在北上广等一线城市的抽样调查显示，七成路由器缺乏安全保护，有 73%的受访用户仍然使用 123456、000000 一类极易被猜中的 WiFi 密码，有 67%的用户使用易被破解的 WEP 模式加密 WiFi 密码，有 92%的用户没有修改过路由器设置页面的初始密码，甚至有 86%的用户在安装好路由器以后再也没有进入过设置页面。除此之外，有 58%的用户曾遭遇过蹭网，31%的用户曾遭遇过 DNS 劫持，而有 5%的用户因路由器安全问题遭遇过盗刷网银。瑞星安全专家指出，目前各种迹象均表明，路由器安全已成为威胁网络安全的重要因素，不但严重影响网民的日常生活，还危及网民的隐私信息与财产安全。

2. 简单 WiFi 密码形同虚设黑客可轻松“秒破”

虽然目前大多数网民都养成了给 WiFi 设密码的习惯，但通过调查发现，很多人仍在使用 WEP 这种极易遭到破解的加密方式。瑞星安全专家介绍，互联网上针对 WEP 加密的破解工具随处可见，即使用户频繁更改密码也无济于事。这种软件能够瞬间实现暴力破解，一旦成功破解，攻击者就可以进行蹭网，甚至窃取隐私信息。

3. 被用户忽视的路由器设置密码

无线路由器除 WiFi 密码之外，还存在一套进入路由器设置页面的用户名及密码，这是为保护无线路由器安全的第一道门槛。通常情况下用户都会对无线 WiFi 进行密码设置，然而很少有用户意识到路由设置页面的默认用户名及密码也是需要修改的。瑞星安全专家介绍，路由器的出厂默认密码可以说是一个“众人皆知的秘密”，它就相当于直接为黑客访问、控制路由器开通了一条“绿色通道”，只要利用一段 javascript 脚本代码，就能轻松进入设置页面，对路由器进行各种恶意操控。

图 19：利用 javascript 脚本代码篡改路由器设置

4. DNS 劫持致钓鱼网站泛滥

DNS 劫持是一种常见的路由器攻击手段，黑客通过篡改路由器的 DNS 设置，使网民访问正常网站时打开黑客指定的恶意网址。2013 年国内就发生过一起大规模 DNS 劫持事件，据不完全统计，当时每日遭遇攻击的网民数量在 800 万左右。瑞星安全专家表示，黑客在正常网站的页面嵌入恶意代码用于篡改路由器的 DNS 设置，届时网民即使在地址栏输入正确的网址，也只能打开黑客自制的钓鱼页面，网民稍不留神在该页面进行网购、网银转账等操作，就会泄露网银账号及密码。

图 20：遭遇 DNS 劫持后浏览器打开钓鱼网站

5. 公共场所 WiFi 藏黑客

瑞星互联网攻防实验室通过在北上广等地的多类公共场所进行实地调查后发现，绝大多数的公共 WiFi 环境缺少甚至毫无安全防护措施，这就导致了任何人（包括黑客）都可以加入。一旦攻击者进入该免费 WiFi 后，就会对网络中的其他用户进行嗅探，并截取网络中传输的数据。瑞星安全专家介绍，在这种情况下，用户在网络中传输的任何信息都完全暴露在黑客眼前，黑客通过专业软件可截获到各种用户名、密码、上网记录、设备信息、聊天记录及邮件内容等。

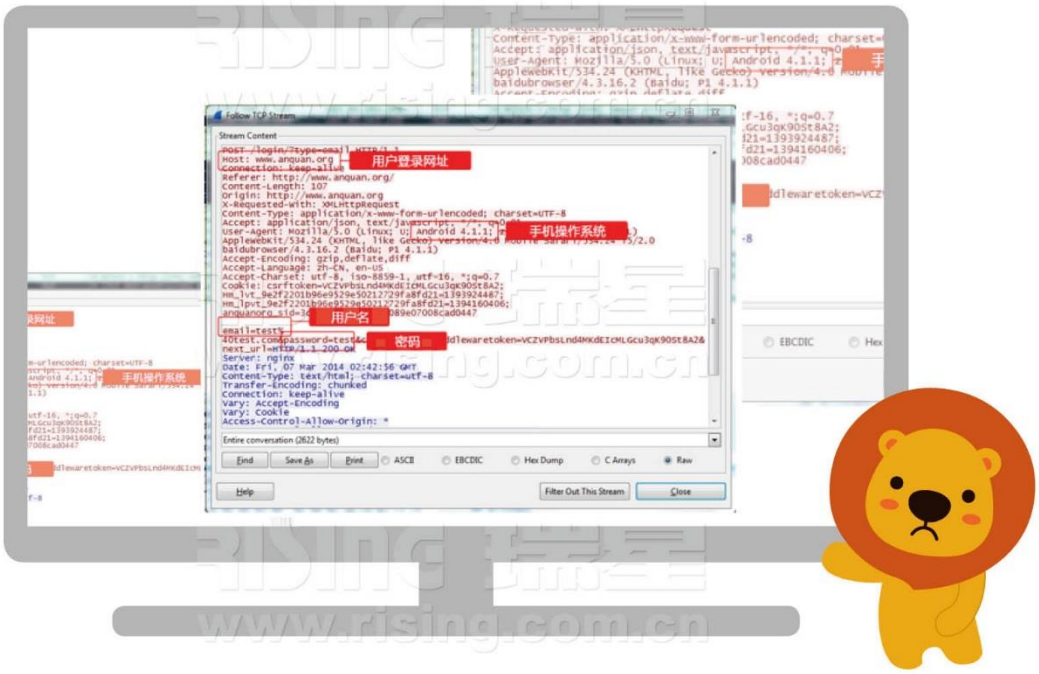

图 21：黑客使用监听软件抓取同一 WiFi 下用户发送的信息

6. 无密码 WiFi 多是“黑网”

“黑网”是黑客在人流集中的公共场所设置的无密码 WiFi。该类 WiFi 往往采用仿冒免费公共 WiFi 名称的方法引诱用户进入陷阱。一旦连接上“黑网”，用户发送的所有信息都将遭到监听。届时，不仅用户的隐私信息、网银账密将面临泄露，用户还有可能收到黑客推送的恶意推广信息。

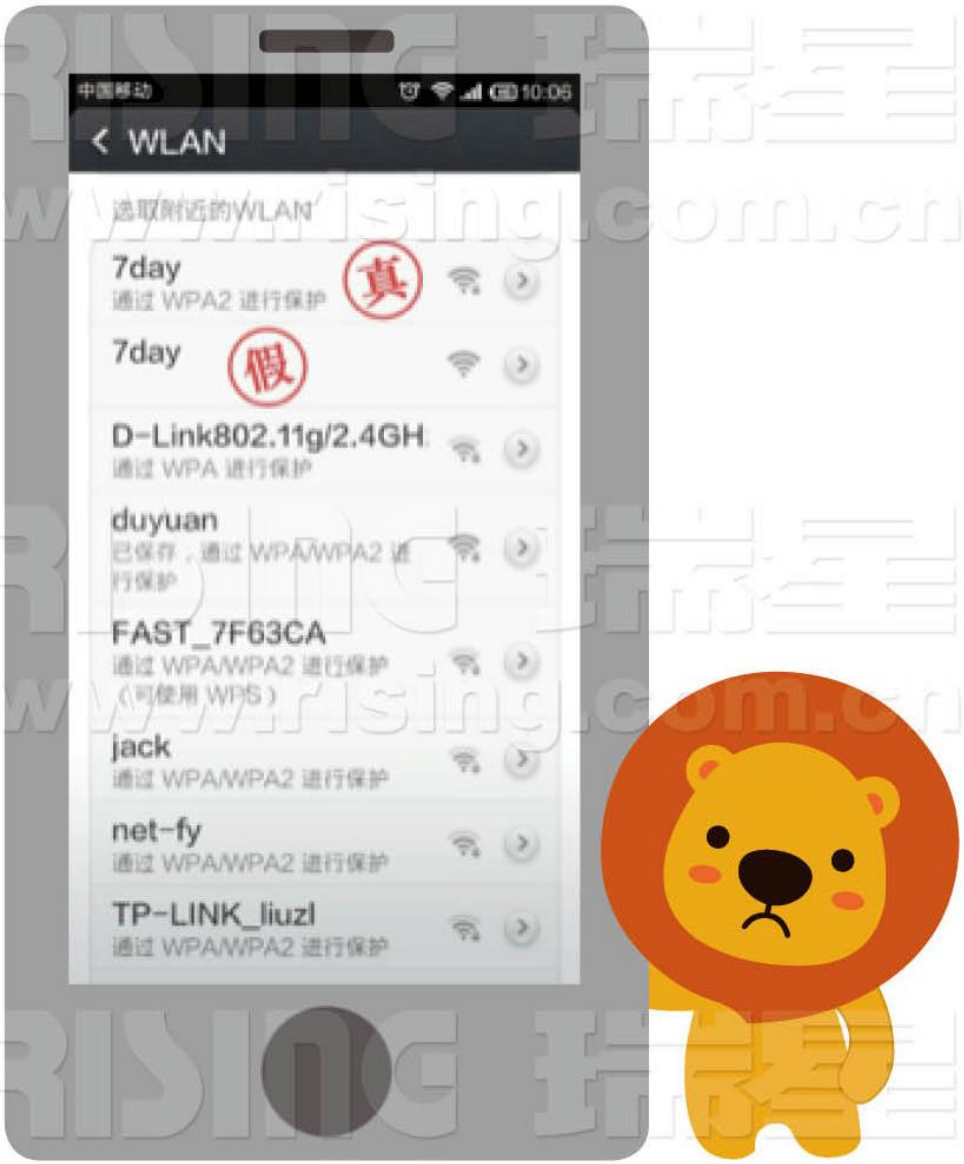

图 22：遭到仿冒的公共 WiFi

7. 路由器固件“后门”可泄露上网密码

瑞星工程师通过对大量路由器的调查发现，某些 TP-Link 系列的路由器存在“后门”。该类后门存在于 TP-Link 的某一固件版本内，在路由器的网络环境下，只要通过浏览器打开某一指定地址，就可以进入路由器的系统调试页面，该页面中存有网民的宽带用户名及密码，一旦该密码失窃，黑客可用其在网上进行恶意交易，造成网民的巨大经济损失。目前，已知

受到该漏洞影响的 TP-Link 路由器型号分别为：WR740N、WR740ND、 WR743ND、WR842ND、WA-901ND、WR941N、WR941ND、WR1043ND、WR2543ND、MR3220、MR3020 及 WR841N。

8. 路由器远程 Web 管理成黑客“帮凶”

目前大多数路由器都提供用户远程 Web 管理功能，使用户出门在外也可以远程登录路由器的 Web 管理页面。该功能虽然方便了用户管理路由器，然而却存在巨大的安全隐患。黑客可利用远程登录 Web 管理功能，并进一步配合其他漏洞，获取宽带密码，手动修改路由器 DNS 并传播钓鱼网站，甚至盗取机密信息。

9. DMZ 主机易导致黑客入侵

DMZ 主机是一种在内网和外网中间的缓冲区，许多企业将其用于电子邮件、FTP、论坛等 Web 服务。然而瑞星安全专家指出，这种设置不仅方便本地调试 Web 程序，搭建各种应用服务，同样也暴露了安全隐患。黑客可利用 DMZ 主机配合一些常见的远程溢出漏洞，获得相对应的系统权限，并入侵计算机及整个企业内网。

10. 普通网民难以做好路由器安全防护

无线路由器存在的巨大安全隐患与传统安全问题是完全不同的，并且绝大多数用户在无线路由器方面的安全意识几乎为零，这主要是由于路由器设置页面过于复杂造成的。瑞星安全专家指出，目前市面上绝大部分路由器的设置页面都充斥着复杂难懂的专业词汇，用户无法理解但是黑客却了如指掌，可以说这种设计本身就是存在缺陷的。

除此之外，许多路由器本身就存在漏洞，然而为路由器打补丁、更新固件却存在很大风险，该类操作稍有不慎会让路由器彻底瘫痪无法使用，瑞星在调研中发现，五成受访者都表示知道路由器缺乏防护，但不知道如何对其进行安全设置。另外也有一部分用户反映已经通过很多媒体得知路由器需要打补丁、更新固件，但却不知该如何操作。

瑞星安全专家表示，为了解决以上问题，瑞星已经推出了瑞星路由安全卫士，对路由器设置有困难的用户可以在瑞星官网免费下载使用。

四、企业信息安全

（一）2014 年上半年三大企业信息安全事件

1. 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。

根据漏洞平台出具的安全报告显示，OpenSSL 漏洞存在于 ssl/dl_both.c 文件中，是 Heartbleed 模块的一个 Bug 所致。漏洞可导致黑客远程读取网站服务器长达 64K 的数据，而这些数据中极有可能存储了用户的网银账号、订单信息、身份信息及支付密码等，黑客只需利用该漏洞反复进行内存记录读取，大量截获用户的敏感数据。

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。

据了解，OpenSSL 是为网络通信提供安全及数据完整性的一种安全协议，它囊括了主要的密码算法、常用密钥和证书封装管理功能以及 SSL 协议，并提供了丰富的应用程序供测试或其他目的使用。目前，占据全球三分之二市场份额的 Apache 和 Nginx 服务器都在使用 OpenSSL，此外，OpenSSL 还被大量应用于电子邮件客户端、聊天软件等互联网应用软件中。

2. Windows XP 停止更新不足一个月即曝漏洞

今年 4 月 8 日，Windows XP 正式停止更新服务，然而不足一个月的时间，XP 系统即曝出 0Day 漏洞（漏洞编号：CVE-2014-1776）。根据瑞星漏洞平台出具的报告显示，IE 浏览器的所有版本（IE6/IE7/IE8/IE9/IE10/IE11）均受到此漏洞影响。IE 中存在一个 use-after-free 漏洞，通过该漏洞，黑客可使用 Adobe Flash 来绕过 Windows 系统的 DEP 和 ASLR 两种漏洞防护机制，并以挂马的方式在用户电脑上远程执行代码，进而获取系统当前登录账号的所有权限。

瑞星安全专家表示，国内大量 XP 用户缺乏安全意识，日常都使用高权限的账号进行操作，因此一旦被黑客攻击，电脑将毫无防御能力，用户面临硬盘文件全面被盗、数据遭到篡改删除、网银账号密码及隐私信息泄露等风险。瑞星安全专家指出，由于微软停止了 XP 系统安全更新服务，因此给黑客可乘之机，今年很有可能爆发大规模的针对 XP 系统的恶意攻击。

3. 携程网站漏洞致信用卡信息泄露

今年 3 月，知名旅行网站携程惊现漏洞，攻击者可盗取存储于携程数据库中的用户姓名、身份证号、银行卡类别、卡号及 CVV 码等信息。次日，携程在媒体上公开发表声明，称网站漏洞已于两小时之内修复完毕，93 名潜在风险用户已被通知换卡。

瑞星安全专家指出，开户姓名、证件号码、卡号及 CVV 码都是信用卡的重要核心信息，一旦黑客获取到以上信息，就可以无需密码进行网上支付等行为。同时，卡号及 CVV 码都无法进行二次修改，一旦泄露就只能更换信用卡。因此，本次漏洞所带来的影响将远大于携程声明中所述。

无论是 Open SSL 的心脏出血漏洞还是携程信用卡信息泄露，都是震惊业界的重大信息安全事件。然而这些漏洞在公布于众之前，究竟存在了多长时间，又有多少用户在不知不觉间被盗刷过信用卡，都已无从考证。许多漏洞的第一个发现者很有可能不是信息安全人员而是黑客，他们往往会对自己持有的漏洞保持缄默，以便牟取暴利。此外，互联网服务供应商并非信息泄露事件的直接受害人，因此作为盈利机构，他们更多关注的是产品与用户体验，而安全防护很容易遭到忽视。当前，网银及信用卡的支付安全已成为全社会关注的热点问题，然而各大银行、电商、金融机构及网上交易平台的安全防护却依然存在大量疏漏，企业信息安全建设仍任重而道远。

（二）企业信息安全趋势展望

1. 虚拟化、云计算安全问题浮出水面

印象笔记（Evernote）是一款记事簿类软件，它能为用户提供云端笔记功能，并且可以在多种设备之间进行同步。今年 6 月，印象笔记社区的管理员 Geoff Barry 发布了一份关于数据泄露的声明，声明中指出印象笔记的社区被黑客入侵，并有可能已经获取到论坛成员的个人资料，大量的用户可能面临云端笔记被窃密的威胁。

近年来，虚拟化、云计算已越来越多的被应用于企事业机关单位的互联网服务平台。据相关机构数据显示，仅今年上半年，国内在建的大型虚拟化系统就有数十个之多，分布于通讯、能源、金融、教育、医疗、政府等行业。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。

瑞星安全专家介绍，虚拟化及云计算本身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，大面积数据泄露、客户端瘫痪，乃至办公系统整体瘫痪都不可避免。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。

目前，国内许多虚拟化系统的用户仍然使用传统的杀毒软件网络版进行安全防护。然而，虚拟化系统不同于传统的企业办公系统，资源高度集中使安全系统在扫描、运行时容易出现安全风暴，导致整个系统运行缓慢甚至出现崩溃的情况。除此之外，随着虚拟化技术的普及，针对虚拟化平台的病毒及 APT 攻击也逐渐进入人们视野，这也将是传统安全软件无法解决的难题。因此，建设专门针对虚拟化平台的整体信息安全系统将成为企业的必要工作。

2. 信息技术国产化是大势所趋

近期，全球知名信息安全厂商赛门铁克曝出后门丑闻。此次涉事产品为赛门铁克的数据防泄漏产品，有消息称，该软件存在“信息风险”，一些政府部门已在现有系统及未来采购中禁用该产品。瑞星安全专家介绍，这并不是第一次我国政府部门对国外 IT 产品发出禁用通知。早在今年 5 月，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。

随着中央网络安全和信息化小组的成立，标志着我国终于将信息安全提升至国家安全的重要地位。今年上半年，国产操作系统、国产办公软件以及国产信息安全软件成为政府关注的焦点。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，信息安全的自主知识产权至关重要，信息安全主权一定要掌握在自己国家手中，所以电子信息技术国产化将是今后的大势所趋。

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，我们建立了国内最专业、实力超强的研发队伍，二百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