瑞星 2015 年中国信息安全报告

北京瑞星信息技术股份有限公司

2016 年 1 月

免责声明

本报告综合瑞星“云安全”系统、瑞星客户服务中心、瑞星安全研究院、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 2015 年 1 至 12 月的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。

目录

报告摘要

- **新增病毒样本 3,715 万个 木马病毒最多**

  2015 年，瑞星“云安全”系统共截获新增病毒样本 3,715 万个，病毒总体数量比 2014 年下降了 27.79%,共有 4.75 亿人次网民被病毒感染,有 1,332 万台电脑遭到病毒攻击，人均病毒感染次数为 35.65 次，比 2014 年人均染毒次数增加 12.05 次。其中木马病毒样本数量最多，流氓软件感染最为频繁。广东省连续三年成为染毒最多的省份。

- **挂马网址死灰复燃 增长 11.37%**

  2015 年，瑞星“云安全”系统截获挂马网址 519 万个（以网页个数统计），与 2014 年相比上升了 11.37%。在报告期内，瑞星“云安全”系统拦截挂马网址的攻击总计为 4,709 万次，与 2014 年相比上升了 10.46%。

- **钓鱼网站上升 31.84% 每人平均访问钓鱼网站 1.74 次**

  2015 年，瑞星“云安全”系统共截获钓鱼网站 737 万个，比 2014 年上升了 31.84%。在报告期内，瑞星“云安全”系统拦截钓鱼网站攻击 3.17 亿人次，平均每人访问钓鱼网站 1.74 次，比 2014 年人均上升 0.25 次。其中，虚假中奖类钓鱼网站最为猖獗，支付类钓鱼网站威胁性最高，假冒综艺节目中奖成为钓鱼网站最为常用的手段。

- **色情诈骗威胁人身安全 受骗网民有苦难言**

  2015 年内，网络色情业发展迅速，并伴随钓鱼诈骗、敲诈勒索等犯罪行为出现。网络色情交易主要利用伪基站、社交 APP 及伴游网站进行信息交流，并利用视频、会员俱乐部、KTV 等线上线下平台进行色情交易。该类行为较高比例会发生危及网民人身安全的情况，然而由于牵扯到道德及法律问题，受害人大都有苦难言。

- **Android 手机新增病毒样本数量翻番 每月人均收 10 条垃圾短信、17 个骚扰电话**

  2015 年，新增手机病毒样本 261 万个，与 2014 年相比增长了 203.9%。在报告期内，瑞星“云安全”系统监测到全国垃圾短信总量为 246 亿条，每月人均接收垃圾短信 10 条。骚扰电话出现总量为 412 亿次，每月人均接收骚扰电话 17 次，广告骚扰电话最多，占比 92.3%。

- **“苹果不安全”影响 10 亿用户**

  2015 年是苹果走下安全神坛的一年，在移动安全领域先后曝出 Safari 跨域漏洞和 Airdrop 漏洞，此外，XcodeGhost 也让更多用户对苹果系统的安全失去信心。相较于苹果爆发式的漏洞增长速度，Android 系统作为安全性屡遭质疑的智能设备系统，其漏洞增长趋于平稳。

- **约 5000 万台路由器存在安全隐患 “admin”成为“最弱”路由器密码**

  2015 年，有 2,040 万台路由器遭遇过 DNS 篡改，4,860 万台路由器未修改过出厂设置。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。此外，“admin”成为“最弱”路由器密码。

- **企业终端安全已成为全球性安全威胁 “筛王”Flash 仍是黑客最爱**

瑞星“云安全”系统统计，报告期内有 117.7 万新增病毒在企业内网进行传播，主要类型为感染型病毒和宏病毒。近年来，黑客攻击不断变化翻新，许多病毒开始结合钓鱼邮件、社会工程学等手段在企业中流传，著名的“密锁”系列敲诈病毒就是以包含感染宏病毒的恶意邮件作为攻击手段。报告期内，重大企业终端漏洞中 Flash 漏洞占据总体数量的 3/7。该软件在安全业内素有“筛王”之称，每年均以漏洞多、威胁性高、影响广泛成为黑客最为关注的多媒体应用程序。此外，除常规的 Windows 漏洞外，2015 年出现了威胁性较高的 Ubuntu（一款 Linux 操作系统）漏洞。由此可见，随着 Linux 系统的广泛使用——尤其是国产化操作系统普及后 Linux 的大面积应用，相关漏洞可能会在未来大量曝出。

- **DDoS 攻击全球增加近两倍 政府、教育类网站遭 APT 居民数据泄密超 1 亿**

  2015 年，全球信息安全事件成爆发式增长，信息泄漏已难以遏制。DDoS 攻击全球增加近两倍，家用路由器和 Linux 服务器在新型攻击下大量被黑客控制，组成僵尸网络。政府、教育类网站由于漏洞多、防护脆弱，成为黑客重点攻击的目标，居民数据泄密超 1 亿，影响范围极广。

- **一年两个重大漏洞 虚拟化安全环境日趋严峻**

  虚拟化转型遇安全之痛，2015 年，虚拟化系统曝出两个漏洞，分别为“毒液”和 QEMU 网卡设备漏洞。相较于 2014 年及之前的几年，2015 年虚拟化漏洞的曝光有显著增加，由此可见，无论是黑客还是安全人员，都已将大量的精力投入到虚拟化安全的漏洞挖掘与修补当中。

- **全球安全局势恶化 黑客攻击事件将继续影响 2016**

  2015 年上半年发生了 Hacking Team“网络核武”泄漏事件，下半年挂马网址及黑客攻击事件频繁密集发生，同时，APT、DDoS 攻击在数量和频率上都有了进一步发展，量级超过 100 Gbps 的 DDoS 攻击峰值达到 12 次/季度。目前，网络上公开流传着海量的黑客工具，该类工具已完成从复杂操作到“傻瓜式”操作的进化。受此影响，越来越多的不法分子开始具备黑客能力，带有经济目的或政治目的 DDoS 和 APT 攻击已成常态，并将在 2016 年愈演愈烈。

- **“互联网+”将进一步促进虚拟化安全技术发展**

  2015 年年初，国家总理在政府工作报告中提出了“互联网+”计划，该计划是要推动互联网和传统行业的融合。这不仅意味着我国今后将快速向互联网化发展，也意味着云计算、大数据将成为未来支撑企业日常办公、运营的重要组成部分。然而就 2015 年曝出的重大漏洞来看，未来会有大批黑客重点关注云计算、大数据、虚拟化方面的漏洞挖掘。

一、个人互联网安全

（一）病毒和木马

1. 人均染毒增加 12.05 次 流氓软件感染最为频繁

（1）新增病毒样本 3,715 万个 木马病毒最多

2015 年 1 至 12 月，瑞星“云安全”系统共截获新增病毒样本 3,715 万个，病毒总体数量比 2014 年下降了 27.79%。报告期内，共有 4.75 亿人次网民被病毒感染，有 1,332 万台电脑遭到病毒攻击，人均病毒感染次数为 35.65 次，比 2014 年人均染毒次数增加 12.05 次。

在报告期内，新增木马病毒（Trojan）占总体病毒的 61.79%，依然是第一大种类病毒。蠕虫病毒（Worm）是第二大种类病毒，占总体新增病毒的 11.22%，第三大种类病毒为恶意广告（Adware），占总体数量的 8.09%。感染型病毒（Win32）占总体数量的 7.43%，后门病毒（Backdoor）占总体数量的 1.47%，病毒释放器（Dropper）占总体数量的 1.26%，分别位列第四、第五和第六，此外，其他类型病毒占总体数量的 8.74%。

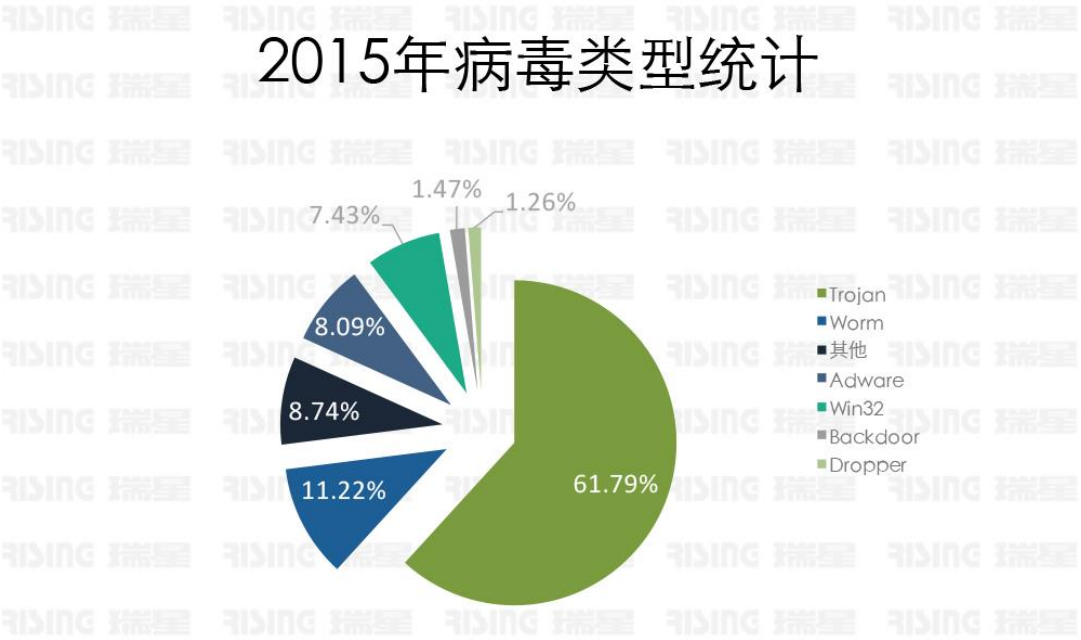

图 1：2015 年病毒类型统计

（2）广东省连续三年染毒人次最多

在报告期内，广东省病毒感染为 3,212 万人次，位列全国第一。其次为江苏省 1,570 万人次及山东省 1,427 万人次。从 2013 年起，广东省连续三年成为病毒感染最多的省份，江苏省的染毒数量则稳步上升，由第 9 名跃至第 3 名后，于 2015 年上升为第 2 名。河南、上海作为曾经的“亚军”和“季军”，在近两年中已退出前三甲。

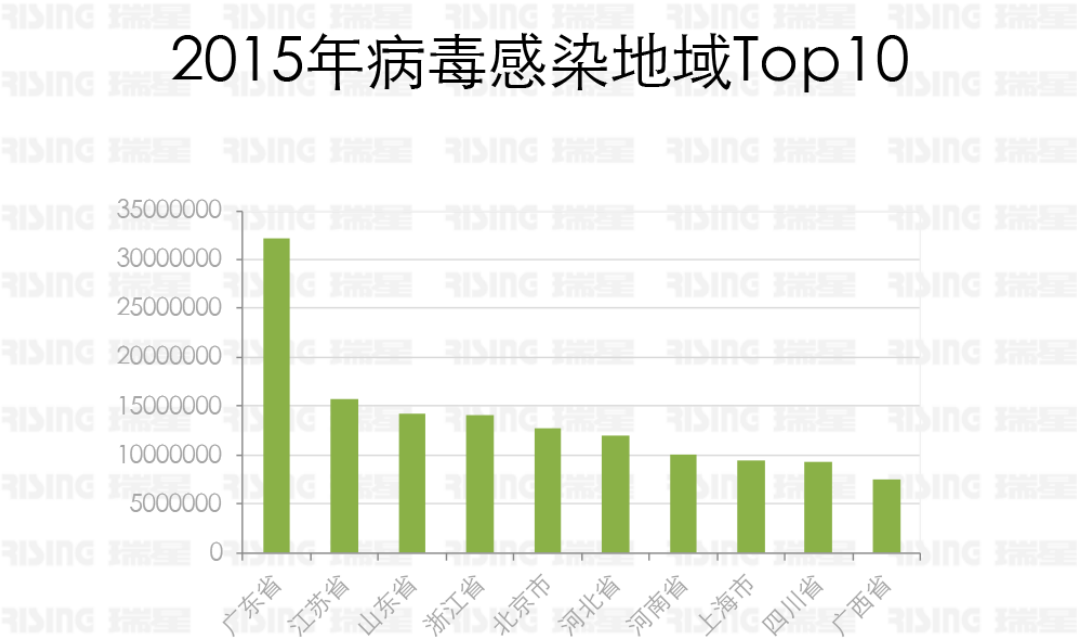

图 2：2015 年病毒感染地域 Top10

三年内染毒最多的省份Top3

排名	2015	2014	2013
1	广东	广东	广东
2	江苏	山东	河南
3	山东	江苏	上海

图 3：三年内染毒最多的省份 Top3

2. 2015 年病毒 Top10 海量流氓软件为黑客敛财

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 2015 年病毒 Top10，

其中，恶意广告、恶意软件类占据 Top10 中 3 个名额，应引起网民的特别警惕，感染型病毒则成为在企业中传播最为广泛的一类病毒，在 Top10 中占据 2 个名额。

2015年病毒Top10

排名	病毒名称	病毒描述
1	Adware.BrowseFoxl1.A1B7	恶意广告，劫持用户浏览器，安装广告插件显示商业广告，下载其他恶意软件。
2	Worm.Win32.Mira.b	蠕虫病毒，运行后大量自我复制，造成系统资源耗尽。
3	Dropper.Script.VBS.Ramnit.a	脚本病毒，感染exe、dll、html文件，开启后门，收集用户隐私信息。
4	Backdoor.Overiel1.64BD	后门病毒，规避反病毒软件的查杀，在电脑中开启后门。
5	Malware.Techsnabl6.2585	恶意程序，强制播放广告，下载其他恶意软件。
6	Trojan.Win32.Reveton.a	木马病毒，在系统目录下大量自我复制，造成系统资源耗尽或网络严重拥堵。
7	Worm.Win32.Allaple.a	蠕虫病毒，衍生大量病毒文件，并窃取用户重要信息。
8	Win32.KUKU.ky	感染型病毒，感染系统内的exe和scr文件，后台下载其他病毒。
9	Virus.Virutl1.A08B	感染型病毒，感染系统内的exe和scr文件，开启后门，并下载其他恶意程序。
10	Adware.SwiftBrowsel6.1BA9	恶意广告，强制弹出广告，为黑客指定网站刷流量，收集用户信息，下载其他恶意程序。

图 4：2015 年病毒 Top10

（二）挂马网址

挂马网址死灰复燃 增长 11.37%

2015 年 1 至 12 月，瑞星“云安全”系统截获挂马网址 519 万个（以网页个数统计），与 2014 年相比上升了 11.37%。在报告期内，瑞星“云安全”系统拦截挂马网址的攻击总计为 4,709 万次，与 2014 年相比上升了 10.46%。

2015 年上半年未出现较为严重的漏洞，因此挂马攻击仍持续使用 2014 年的老旧技术，安全软件可对其进行有效拦截。Hacking Team“网络核武”泄漏事件爆发以后，大量高危漏洞被曝光，导致下半年挂马攻击在部分地区呈上升趋势。

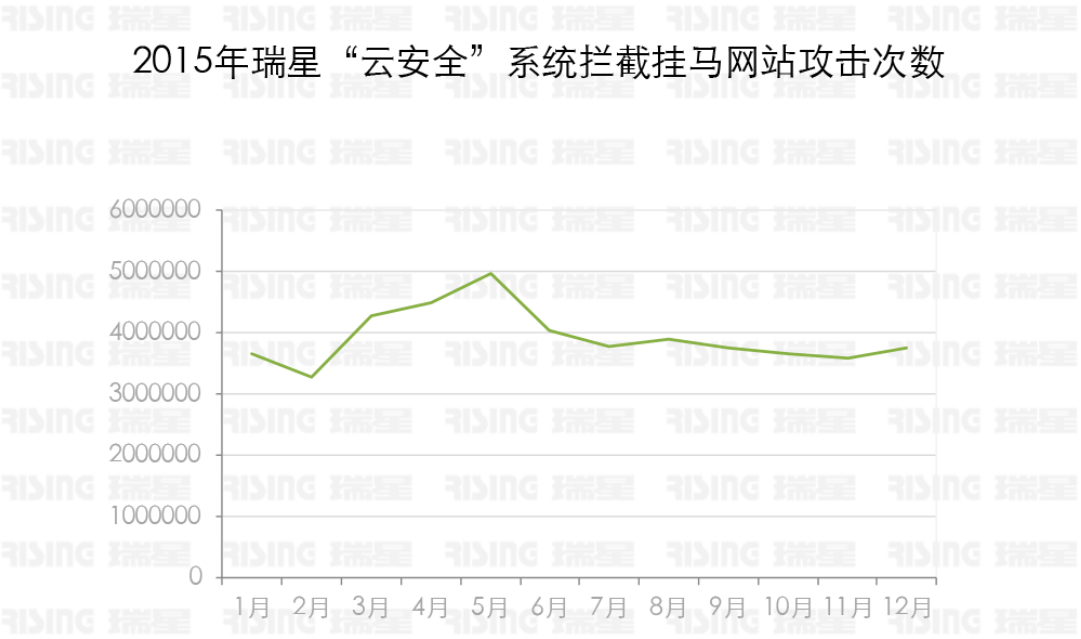

图 5：2015 年瑞星“云安全”系统拦截挂马网址攻击次数

（三）钓鱼网站

1. 钓鱼网站上升 31.84% 每人平均访问钓鱼网站 1.74 次

2015 年，瑞星“云安全”系统共截获钓鱼网站 737 万个，比 2014 年上升了 31.84%。在报告期内，瑞星“云安全”系统拦截钓鱼网站攻击 3.17 亿人次，平均每人访问钓鱼网站 1.74 次，比 2014 年人均上升 0.25 次。

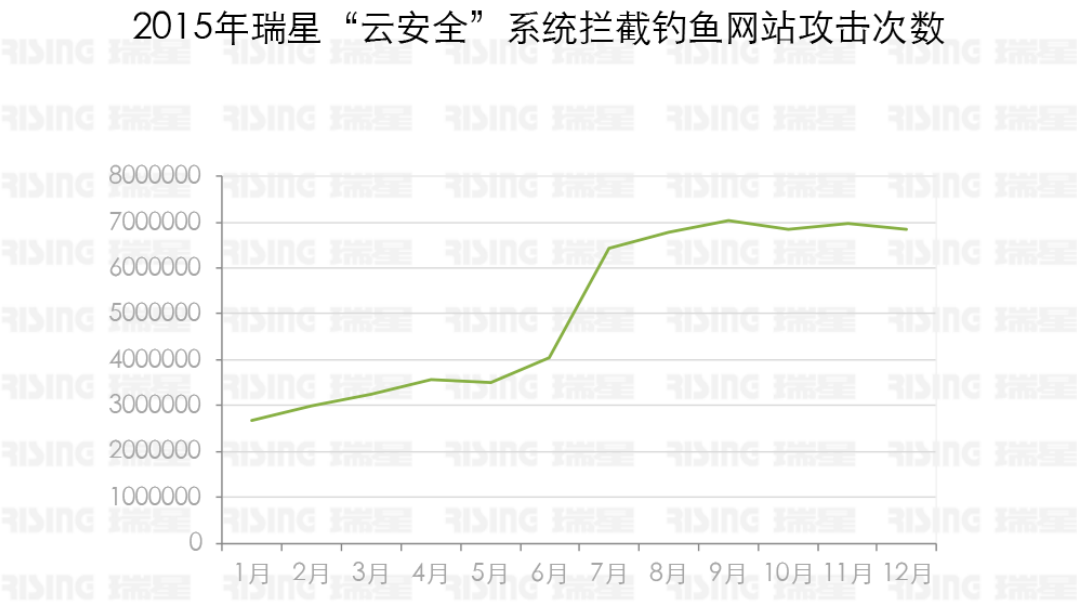

图 6：2015 年瑞星“云安全”系统拦截钓鱼网站攻击次数

2. 虚假中奖类钓鱼网站最为猖獗

在报告期内，虚假中奖类钓鱼网站占全部钓鱼网站的 56%，位列第一，其次为虚假银行类钓鱼网站与虚假在线充值类钓鱼网站，分别占全部钓鱼网站的 15%与 10%。

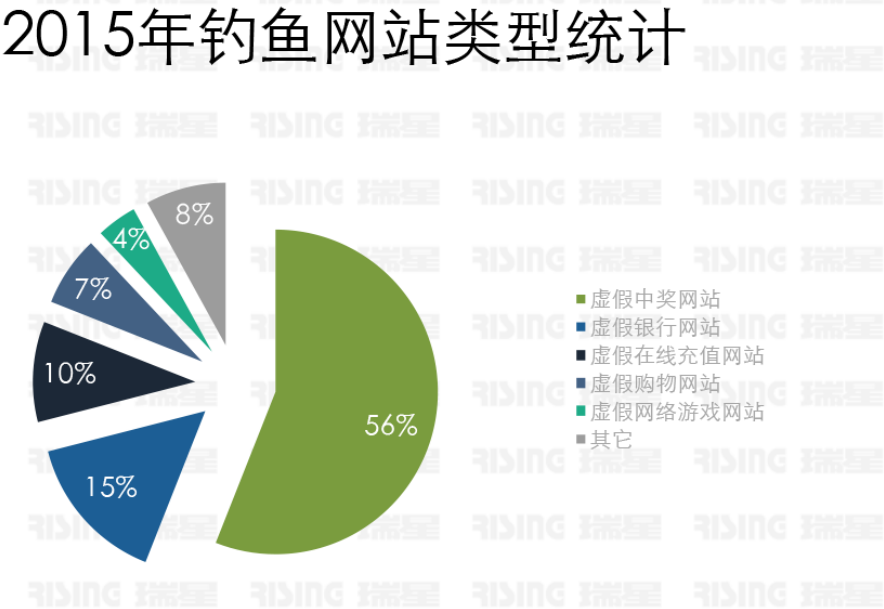

图 7：2015 年钓鱼网站类型统计（饼图）

3. 2015 年重大钓鱼网站 Top10 支付类钓鱼网站威胁最高

2015年重大钓鱼网站Top10

序号	网址	类型
1	http://wap.icbcopy.com/login.asp	工商银行钓鱼网站
2	http://aky.k7w.org/apay/	支付宝钓鱼网站
3	http://anindyavoice.com/includes/dpbx/	邮箱类钓鱼网站
4	http://www.shly-art.com/	金融类钓鱼网站
5	http://www-icbcv.com/login.asp	工商银行钓鱼网站
6	http://www.jsduihuanjifen.com/	建设银行钓鱼网站
7	http://h1n6.com/	购物钓鱼网站
8	http://www.cf004.com/	网络游戏钓鱼网站
9	http://www.hsyih.com/	综艺节目网站
10	http://www.hujiayiweiqing.com/	医药类钓鱼网站

图 8：2015 年重大钓鱼网站 Top10（图表）

4. 钓鱼网站趋势

报告期内，钓鱼网站有较为明显的上升趋势，尤其下半年钓鱼网站数量急速增加，并主要通过以下手段进行钓鱼攻击：

- 利用双 11、双 12、黑 5 等购物节及购物返利活动进行钓鱼。黑客伪造淘宝、京东等网站，诱骗消费者打开指定链接，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。

- 利用垃圾短信、伪基站推送恶意网址给用户，诱骗用户打开钓鱼网站。

- 利用手机 APP 进行钓鱼。随着智能手机的广泛普及，越来越多的钓鱼攻击者将钓鱼链接植入手机 APP，伪装成正规 APP 诱骗用户下载并推送钓鱼网址。

- 《奔跑吧兄弟》、《我是歌手》、《跟着贝尔去冒险》等综艺性节目火爆以后，网络中出现大量假冒该类节目官网，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》手法极为相似。

（四）色情诈骗威胁人身安全 受骗网民有苦难言

1. 伪基站海量传播“学生妹招嫖”短信

近年来，随着伪基站的泛滥成灾，各种垃圾短信、钓鱼短信始终困扰着广大网民。12月，瑞星客服中心大量接到用户举报，称收到“学生妹招嫖”短信。经相关部门调查，该类短信实为伪基站发送的色情诈骗信息，拥有一套通用模板，不法分子只需将模板中的联系方式替换为自己的联系方式，即可使用伪基站定点在人群密集的地方海量发送。网民只要联系短信中留下的电话，骗子会以见面、购买服务等名目，要求用户先行向其打款，网民一旦轻信，就会遭受钱财损失，打款后不会有任何服务提供，更不可能与“学生妹”见面。

图 9：不法分子利用伪基站发送“学生妹招嫖”短信

2. 社交 APP 暗藏黄色陷阱

当前，微博、微信、陌陌等社交 APP 都带有定位功能，可搜索附近的用户，帮助网民实现本地交友。据瑞星“云安全”系统监测，自 2015 年上半年以来，社交 APP 涉黄情况日趋严重，有不法犯罪团伙在社交 APP 上打着性交易的旗号，对网民进行诈骗、勒索。

该类诈骗通常以固定的 KTV 为据点，有专门的“枪手”通过社交 APP 发布招嫖信息，随后安排“小姐”进行接待，但不会提供任何服务，一旦网民察觉事情有异要求离开，埋伏在附近的打手会立刻出现，索要高额嫖资、包间费、酒水费、介绍费等。

除 KTV 勒索以外，不法分子还会乔装美女主播，在微博、微信上留下各类露骨的照片，静等网民上钩。网民一旦与其联系，“美女主播”会以购买视频服务、会员服务等方式，引诱网民向其打款，一旦网民轻信付款，“美女主播”将在第一时间消失无踪。

3. 以旅游陪玩为名 伴游网站成色情交易平台

2015 年，央视曝光了一系列以美女旅游向导、旅游陪玩为名目，暗地进行色情交易的伴游网站。该类网站以“美女向导”、“白领”、“女大学生”等噱头招徕网民，并抛出真人秀、视频认证等诱饵，在网民注册以后进一步进行色情交易劝说，并引导网民成为 VIP 会员向网站付款。据瑞星“云安全”系统监测，该类伴游网站虽然在曝光之初曾暂时关闭，但目前已更换域名重新开放。

图 10：伴游网站以“美女导游”为名进行色情交易

瑞星安全专家指出，异地雇佣没有正规执照的导游本身就存在严重安全隐患，极易在旅游时碰到诈骗、勒索甚至抢劫等问题。同时由于涉及色情交易，本身属于违法行为，进一步讲，在社会上该类行为也是违反社会道德的，网民一旦因此遭遇人身威胁，很有可能无法报案，只能有苦难言。

（五）海淘钓鱼网站野蛮增长 境外购物无安全保障

随着网络购物的普及，海外直购成为网民追捧的新型购物方式，便宜、足不出户、跨国购物、快递到家是海淘为人津津乐道的优势，但是，这种方便快捷的优势却存在致命的安全隐患。2015 年，瑞星“云安全”系统截获大量境外网购、支付类钓鱼网站，其中仿冒亚马逊、仿冒 PayPal 及仿冒苹果网站的钓鱼网址数量最多。黑客通常会制作一批高仿页面迷惑用户，并通过文字链和短链接，在国内论坛、QQ 群、微信群等渠道扩散，许多网民并不熟悉国外购物网站的正确地址，一看见钓鱼页面的超低折扣容易被冲昏头脑，从而落入黑客设下的陷阱。网民一旦中招，轻则面临货款两失的风险，重则可能遭遇第三方支付账号被盗或信用卡被刷爆的损失。

图 11：仿冒亚马逊、信用卡及苹果网站等境外钓鱼网站

此外，瑞星安全专家表示，国外购物的税费计算方式与国内存在很大区别，多数网民不会计算，许多看似低价的折扣，在实际完成购买、运输流程以后并不比国内便宜，甚至有些还贵得惊人。同时，一些海淘商品也存在不合海关规定的现象，在清关过程中还可能面临被海关扣押、销毁等问题。

二、移动互联网安全

（一）手机安全

1.Android 手机新增病毒样本数量翻番

2015 年新增 Android 手机病毒样本 261 万个，与 2014 年相比增长了 203.9%，其中以恶意传播（spread）、资费消耗（expense）、隐私窃取（privacy）、诱骗欺诈（fraud）、恶意扣费（payment）等几大类为主。

2015年瑞星“云安全”系统截获手机病毒类型比例

病毒样本类型	比例
系统破坏（system）	0.06%
黑客工具（hacktool）	0.10%
隐私窃取（privacy）	0.53%
恶意传播（spread）	0.01%
资费消耗（expense）	3.79%
恶意广告（adware）	21.55%
诱骗欺诈（fraud）	0.01%
流氓行为（rogue）	6.00%
恶意扣费（payment）	1.16%
远程控制（remote）	0.08%
木马病毒（trojan）	39.27%
恶意程序（malware）	0.55%
其他	26.89%

图 12：2015 年瑞星“云安全”系统截获手机病毒类型比例

2. 全国每月人均接收 10 条垃圾短信、17 个骚扰电话

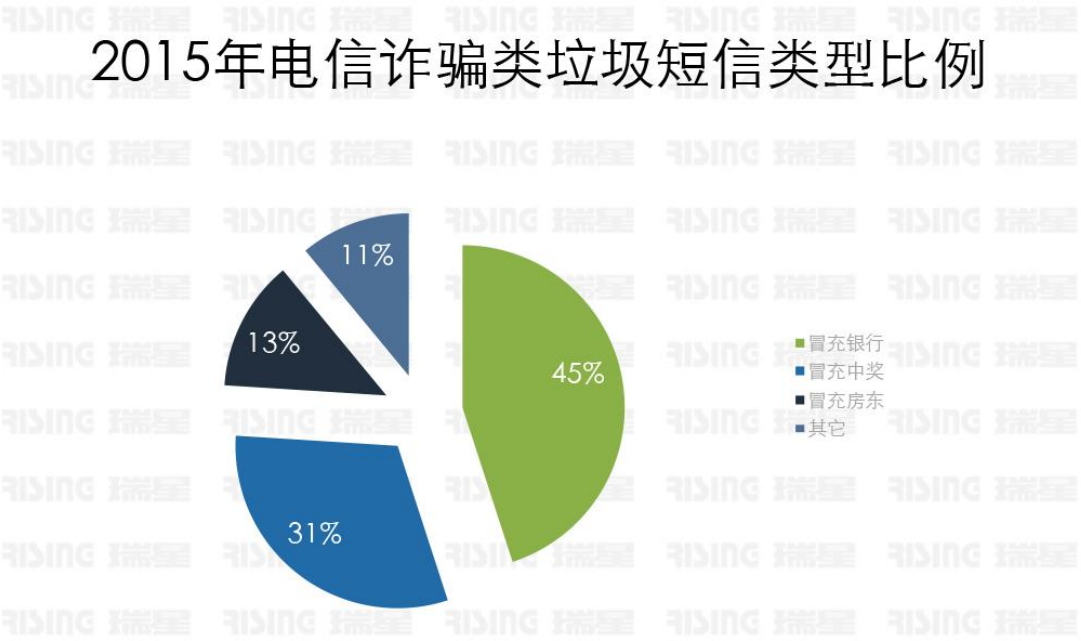

图 13：2015 年电信诈骗类垃圾短信类型比例

在报告期内，瑞星“云安全”系统监测到全国垃圾短信总量为 246 亿条，每月人均接收垃圾短信 10 条。

电信诈骗类短信最为猖獗，其中 45%的短信为冒充银行类诈骗短信，31%为冒充中奖类诈骗短信，13%为冒充房东类诈骗短信，11%为其它类诈骗短息。

此外，在广告类垃圾短信中，化妆品、服饰类分别以 25%、18%的数量占比位居前两位，数量要高于房屋出租等垃圾短信。其他垃圾短信中，代开发票占比较高，其次为赌博、色情服务。

在报告期内，骚扰电话出现总量为 412 亿次，每月人均接收骚扰电话 17 次，广告骚扰电话最多，占比 92.3%。据瑞星“云安全”系统监测，骚扰电话主要集中在每日 9 时至 18 时的工作时间，其中 10 时和 16 时为骚扰电话的高峰期。

3. Android 盗版 APP 团购类相对数量最多 与正版数量持平

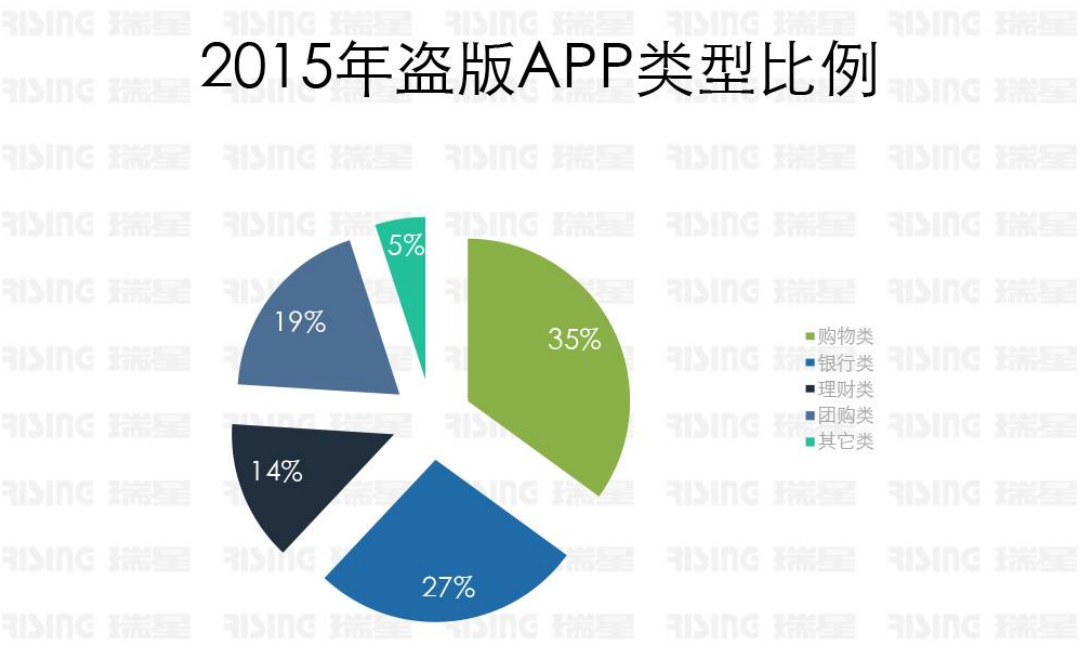

图 14：2015 年盗版 APP 类型比例

由于 Android 系统底层技术平台是开放的，盗版应用便如雨后春笋般的冒出。目前，在所有 APP 品类中，金融支付类的盗版情况最为严重，其中购物类应用占 35%，银行类应用占 27%，理财类应用占 14%，团购类应用占 19%，其它类应用占 5%。此外，按数量比例计算，团购类 APP 盗版最多，正版与盗版的比例接近 1:1。

瑞星安全专家指出，正版的 APP 通过公开、正当的手段获取收益，而盗版、二次打包的 APP 则通过非法植入广告、吸费等方式获取收益，严重损害用户的利益。此外，一些恶意仿冒、恶意篡改、病毒木马植入的假冒 APP，还经常盗取用户的隐私信息及银行账户内的钱款，使用户蒙受巨大的经济损失。

针对上述状况，瑞星已拥有成熟的 APP 加固方案，可从 APP 自我保护、数据安全、本地组件、业务及接口、第三方 SDK 等五个维度检测 APP 的安全性，并针对 APP 现存的安全问题进行修复和加固，最终达到防止盗版、恶意篡改、二次打包、插入广告、病毒木马植入、泄露核心业务逻辑及数据等目的。

4. Android 病毒 资费消耗为黑客牟取暴利

根据病毒感染人数和代表性进行综合评估，瑞星评选出了 2015 年 Android 手机病毒 Top10。从下图中可以看出，资费消耗仍是传播范围最广、影响最为恶劣的一类病毒。

2015年Android手机病毒Top10

序号	病毒名称	病毒类型	病毒行为
1	a.Rogue.MMVideo/Android	流氓行为	具有弹出广告窗口、下载推广软件、让用户无法正常卸载、删除或退出软件进程等行为。
2	a.Privacy.Fakesysui/Android!148C	隐私窃取	具有获取用户个人信息、通讯录信息、短信收件箱、手机号以及系统软硬件信息等行为。
3	a.Expense.SMSAgent.t/Android!1726	资费消耗	具有通过自动拨打电话、发送短信、彩信、邮件、频繁连接网络等行为。
4	a.Payment.SexyV/Android!1762	恶意扣费	具有通过隐蔽执行、欺骗点击等手段订购各类收费业务或使用移动终端支付等行为。
5	a.Rogue.Gray/Android!148A	流氓行为	具有弹出广告窗口、下载推广软件、让用户无法正常卸载、删除或退出软件进程等行为。
6	a.Expense.SmsPay/Android	资费消耗	具有通过自动拨打电话、发送短信、彩信、邮件、频繁连接网络等行为。
7	a.Privacy.PornVideo.b/Android!126E	隐私窃取	具有获取用户个人信息、通讯录信息、短信收件箱、手机号以及系统软硬件信息等行为。
8	a.Fraud.Yongrungirl/Android!1762	诱骗欺诈	具有通过伪造、篡改、劫持短信、彩信、邮件、通讯录、通话记录、收藏夹、桌面等方式，诱导用户触发点击等行为。
9	a.Adware.Appsgeyeser.a/Android!1631	恶意广告	具有通过在Android系统第三方知名应用的指定页面上强行显示推广广告信息、通知栏插入广告、主屏幕弹窗广告等行为。
10	a.Expense.SMSReg/Android!165C	资费消耗	具有通过自动拨打电话、发送短信、彩信、邮件、频繁连接网络等行为。

图 15：2015 年 Android 病毒 Top10

5. Android 病毒实例分析

（1）病毒仿冒移动运营商 拦截网银验证码

9 月，瑞星“云安全”系统截获一个名为“中国移动伪装者”的手机病毒，该病毒在 Android 手机上传播，并伪装成中国移动掌上营业厅的程序引诱用户下载安装，点击运行后诱导用户给予程序 Root 权限。病毒获取权限后，将提醒用户 APP 版本过低，并立刻跳转到假的中国移动界面（http://www.10086m***/）下载“更新”程序，该“更新”一旦被安装，将获取系统敏感权限，诱骗用户激活设备管理器，拦截并转发用户未接短信。由于该病毒诱导用户操作获取大量系统敏感权限，有可能造成用户隐私信息泄漏、手机被定向监听、第三方支付及网银验证码被拦截进而账户被洗劫一空等风险。

图 16：“中国移动伪装者”诱导用户获取敏感权限

（2）正版未至病毒先行 Google Play 遭遇李鬼

2015 年 Google 重回中国市场的消息成为媒体关注的焦点，2010 年 Google 宣布退出中国，受此影响 Google 作为原生 Android 系统的开发商，其官方的 APP 商店 Google Play 一直未能登陆中国市场。然而，就在 Google Play 尚处于捕风捉影的时候，瑞星“云安全”系统已经拦截到伪装成 Google Play 的病毒。

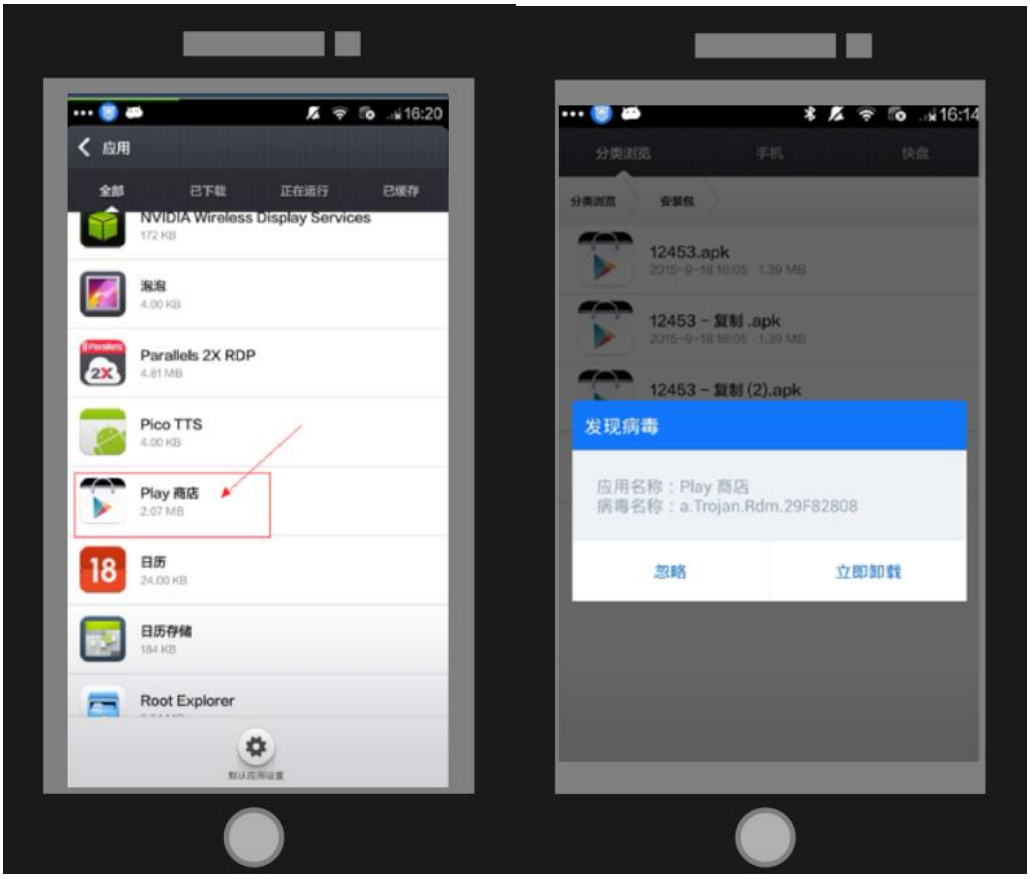

图 17：“Google Play”病毒

“Google Play”病毒预装在不规范的安卓手机系统中，依靠用户或经销商对手机进行刷机操作传播。病毒伪装成 Android 原生系统的官方 APP 商店，运行后并不会在手机桌面上显示，如果打开系统设置中的应用程序管理，可看见一个与 Google Play 图标一样的 Play 商店。病毒运行后，首先会向系统申请发短信及静默安装等高危敏感权限，随后隐藏在 Android 系统目录下。该病毒会收集手机中存储的隐私信息，同时后台连接黑客指定地址，私自下载并安装其他恶意程序。手机一旦中毒，用户将面临隐私信息泄漏、手机被强制安装流氓软件等风险。

（3）XcodeGhost 爆发 中国 APP 开发商遭遇最严重水坑攻击

9 月 18 日，苹果 iOS 被曝出安全漏洞，黑客利用经过篡改的开发工具 Xcode 向 300 余款千万量级的热门 APP 注入了木马病毒，致使上亿用户的手机配置信息被第三方提取，并随时存在用户隐私信息泄漏、Apple ID 账密泄漏、网银及第三方支付账户被盗等风险。

XcodeGhost 是篡改了 Xcode 编译环境的 LD 配置文件（Xcode.app/Contents/PlugIns/Xcode3Core.ideplugin/Contents/SharedSupport/Developer/Library/Xcode/Plug-ins/CoreBuildTasks.xcplugin/Contents/Resources/Ld.xcspec）的 DefaultValue 字段。该字段定义了执行 ld 时的默认参数，XcodeGhost 在此值的末尾追加了-force_load $(PLATFORM_DEVELOPER_SDK_DIR)/Library/Frameworks/CoreServices.framework

/CoreServices，使 Xcode 在进行 ld 时，强制 link 了包含恶意代码的 CoreServices。在 APP 启动时，CoreFoundations.m 中的 UIWindow::didFinishLaunchingWithOptions 函数得到执行，恶意代码被激活。

类似 XcodeGhost 的攻击手段，是一种面向编译器的攻击，该类攻击并非其第一次被使用。2009 年就出现过一个被称为“Delphi 梦魇” （Win32.Indcu.a）的病毒，它向人们展示了面向编译器攻击的威力。与 XcodeGhost 不同的是，它具有自我传播的能力，却没有疑似“间谍/后门”软件的功能，应该说，Win32.Indcu.a 更像是纯粹的实验性的“游戏”， 而 XcodeGhost 更像是为了“未来某个时刻的收割”而进行的一次有预谋的恶意代码散播。

瑞星安全专家指出，本次攻击事件的发生绝非偶然，这是一次蓄谋已久的针对 APP 开发者的“水坑攻击”*，其危害之大、范围之广，史无前例，也很大程度上挑战了 iOS 以及苹果 APP 生态链的安全性。

**水坑攻击指是黑客在受害者必经之路上设置一个“水坑(陷阱)”。最常见的做法是,黑客分析攻击目标的上网活动规律,寻找攻击目标经常访问的网站的弱点,先将此网站“攻破”并植入攻击代码,一旦攻击目标访问该网站就会“中招”。*

（4）Android 幽灵推感染 3,658 个品牌、14,847 种型号设备

8 月，一个名为幽灵推（GhostPush）的 Android 病毒被曝光，该病毒自带 Root 功能，首先会对手机进行 Root 操作，并获取系统最高权限。用户很难用杀毒软件对其彻底清除。该病毒在被曝光时已感染了 3,658 个品牌、14,847 种型号的手机、Pad 等智能设备，感染高峰期每日有 70 万台设备中毒。据相关机构统计，目前为止有上万种机型受到了幽灵推的影响，感染用户遍布东欧、俄罗斯、印度、墨西哥、委内瑞拉、中东、东南亚、以及中国南部等地区。

6. 2015 年移动安全漏洞 “苹果不安全”影响 10 亿用户

2015 年是苹果走下安全神坛的一年，在移动安全领域先后曝出 Safari 跨域漏洞和 Airdrop 漏洞，此外，XcodeGhost 也让更多用户对苹果系统的安全失去信心。此外，相较于苹果爆发式的漏洞增长速度，Android 系统作为安全性屡遭质疑的智能设备系统，其漏洞增长趋于平稳。

2015年重大移动安全漏洞

时间	漏洞名称	描述
4月	“WiFi杀手”Android漏洞	利用该漏洞，黑客可对开启了WiFi的Android手机进行远程攻击，窃取用户手机内的照片、通讯录等重要信息。
4月	Safari严重跨域漏洞	该漏洞影响Safari浏览器的手机端、MAC端和Windows端。黑客可利用该漏洞绕过Safari的同源策略，盗取其他域下的用户cookie，篡改页面内容。据统计，大约10亿设备受到该漏洞的影响。
7月	Stagefright漏洞	黑客可通过该漏洞执行恶意代码进而获取Android设备的控制权。
9月	Airdrop漏洞	Airdrop漏洞影响iOS/OSX设备，黑客可利用该漏洞重写目标设备上的任意文件，并在未经用户允许的情况下向设备安装恶意应用。
10月	Wormhole“虫洞”漏洞	该漏洞存在于国内多款热门Android系统APP中，黑客利用该漏洞实现远程静默安装应用、远程启动任意应用、远程获取用户的GPS地理位置信息、获取MEI信息等操作。
11月	Android系统远程重置密码漏洞	该漏洞存在于Android系统5.0以下（含5.0）的版本中，Android系统的开发商Google可利用该漏洞重置上述系统的设备密码。

图 18：2015 年重大移动安全漏洞

（二）路由器安全

1. 约 5000 万台路由器存在安全隐患

据瑞星“云安全”系统监测，2015 年，有 2,040 万台路由器遭遇过 DNS 篡改，4,860 万台路由器未修改过出厂设置。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。

2. 2015 年路由器漏洞 Top10

2015年路由器漏洞Top10

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

图 19：2015 年路由器漏洞 Top10

3. “admin”成为“最弱”路由器密码

由于智能路由诞生，弱密码问题已经得到缓解，然而路由器管理账号的用户名仍是用户忽视的盲区。瑞星信息安全研究院对北、上、广等一线城市进行抽样调查，在获得用户许可的情况下，统计出 2015 年常用路由器管理账号用户名及弱口令密码。

2015年路由器常用用户名Top10

排名	用户名
1	admin
2	user
3	admim
4	tmardlkt93319
5	root
6	support
7	dxdsl
8	adsl
9	guest
10	zxdsl

图 20：2015 年路由器常用用户名 Top10

2015年路由器弱口令密码Top10

排名	弱口令密码
1	admin
2	user
3	gvt12345
4	dlkt93319
5	password
6	root
7	dlkt20090202
8	support
9	senha123
10	admim

图 21：2015 年路由器弱口令密码 Top10

4. 2015 年路由器安全趋势分析

随着路由器安全普及的发展，WiFi 密码强度有所增加，根据 12 月瑞星在北、上、广的抽样调查可以看出，WiFi 的验证方式从以往的 wep 模式逐步换成 wpa/wpa2 模式，这种变化

降低了定向爆破的成功率。但随着 WiFi 共享类 APP 的广泛应用，用户仍面临 WiFi 分享功能带来的潜在风险，由该功能导致的非法“蹭网”行为有所增加。

2014 年前后出现了批量扫描攻击的软件，采用路由器默认远程登录账户和端口执行命令。利用该种方法，黑客开发了针对路由器的病毒，并以染毒路由器组建僵尸网络。此外，由于路由器是一种更新换代周期较长的设备，较为老型号的路由器仍处于漏洞爆发期中。部分用户知道路由器存在安全漏洞，但由于缺乏专业知识因此只能放弃升级，导致在 2015 年出现大面积以老型号路由器进行 DDoS 攻击的僵尸网络。

5. CSRF 攻击致百万 TP-Link 设备成为攻击目标

CSRF（Cross-site request forgery 跨站请求伪造）是一种近年来开始流行的攻击方式，2015 年，CSRF 被用于攻击家用路由器，目前国内有百万 TP-Link 设备或将受其影响，成为黑客攻击的目标。

该类 CSRF 攻击主要利用带有恶意代码的网页攻击路由器，利用 TP-Link 默认的出厂用户名密码尝试登录路由器的管理账号，并执行任意文件读取命令。路由器一旦遭受攻击，用户将面临 DNS 篡改、路由器管理账号密码遭篡改、路由器重启、路由器变成黑客肉鸡等风险。此外，黑客一旦入侵路由器，还可能通过路由器获取用户内网的共享文件，并截获用户的各类网络账号密码，导致隐私信息泄漏、网银被盗等情况发生。

三、企业信息安全

（一）企业终端安全

1. 企业终端安全已成为全球性安全威胁

根据瑞星“云安全”系统统计，报告期内有 117.7 万新增病毒在企业内网进行传播，主要类型为感染型病毒和宏病毒。其中，感染型病毒 Win32.KUKU.a 是拦截数量最多的一种病毒，该病毒最早在 2008 年就已经在全球流行，然而由于互联网时代所有企业都不是独立存在的，只要存在业务往来企业就有不断染毒的可能性。因此，虽然杀毒软件已经可以对进行彻底清除，该病毒仍然还在企业内网中极为活跃。

宏病毒是一种寄存在文档或模板的宏中的电脑病毒，主要寄生于 Office 文档中，用户在不知情的前提下打开染毒文档，其中的恶意代码就会自动运行，并感染电脑上所有自动保存的文档。该类病毒曾于 2005 年在国内广泛传播，然而由于回报低、技术手段落后等原因，宏病毒在当时并没有得到进一步发展。近年来，黑客攻击不断变化翻新，该类病毒开始结合钓鱼邮件、社会工程学等手段在企业中间流传，著名的“密锁”系列敲诈病毒就是以包含感染宏病毒的恶意邮件作为攻击手段。

此外，瑞星安全专家强调，企业终端安全已成为全球性安全威胁，主要表现为感染型病毒和宏病毒正逐渐向 APT 攻击转型，企业内网一旦染毒，极有可能遭受有预谋的、带有明确目的性的攻击，并有可能遭受以下两类致命性打击：

- 企业重要业务中断。企业业务的连续性和持续性是企业生存和发展的保障，如果因 APT 攻击使业务不能稳定，那么企业不但会蒙受交易损失，还将面临信誉危机。

- 企业资金及核心机密被盗。一些病毒及 APT 攻击以企业资金与核心机密为目标，一旦企业现金流出现问题，资金链断裂，企业就将面临倒闭的风险。此外，核心机密是企业最主要的商业财富，机密泄露也就意味着企业将面对对手发动的恶性竞争。

2. 2015 年企业重点病毒 Top5

2015年企业重点病毒Top5

序号	病毒名称	病毒行为及危害
1	CTB-Locker	“密锁二代”病毒，通过邮件附件的形式传播，运行后下载病毒主体，加密文件，勒索用户。
2	Rombertik病毒	一种可记录击键并盗窃数据的新型间谍软件，如果发现自己被分析和检测，就会改写硬盘主引导记录或破坏所有的文件。
3	方程式(Equation)病毒	硬盘固件木马病毒，这些受到感染的硬盘使得攻击者可以持续的对受害者的计算机进行控制和数据窃取。
4	Duqu2病毒	利用漏洞攻击，进而窃取机密信息。
5	CTB-Locker变种	“密锁二代”病毒升级版，邮件发送js脚本传播，加密用户文件，迫使用户向其打款。

图 22：2015 年企业重点病毒 Top5

3. 2015 年重大终端漏洞 “筛王”Flash 仍是黑客最爱

从下表中可以看出，报告期内重大企业终端漏洞 Flash 占据总体数量的 3/7。该软件在安全业内素有“筛王”之称，是名副其实的漏洞之王，每年要曝出数十个漏洞，其中至少 2 到 5 个威胁性极高。目前，从瑞星“云安全”系统及瑞星安全研究院的监测来看，黑客已经开始对 FLV 文件格外关注，尤其在 Hacking Team 被公布的 400G 文件中，含有重量级的 Fash FLV 漏洞。未来，黑客可能会花费更多的精力挖掘关于 FLV 的 Flash 漏洞。

此外，除常规的 Windows 漏洞外，2015 年出现了威胁性较高的 Ubuntu（一款 Linux 操作系统）漏洞。由此可见，随着 Linux 系统的广泛使用——尤其是国产化操作系统普及后 Linux 的大面积应用，相关漏洞可能会在未来大量曝出。

2015年重大终端漏洞

序号	漏洞编号	漏洞归属	漏洞描述
1	CVE-2015-0313	Flash	这个漏洞是Flash长期存在的未公开漏洞，允许攻击者远程获取PC控制权,分析发现这是一个UAF类型的漏洞。这种情况下，domainMemory引用的内存会被释放掉，攻击者能够读写内存甚至执行任意代码。
2	CVE-2015-3113	Flash	黑客可利用该漏洞制作恶意的Adobe Flash player SWF文件和FLV文件，电脑一旦中毒就会向黑客开启后门。该漏洞影响Windows7及更低版本中的IE，以及Windows XP上运行的Firefox。
3	CVE-2015-1328	Ubuntu	漏洞存在于Ubuntu 12.04、14.04、14.10、15.04版本中，本地攻击者能够利用该漏洞获取目标电脑的最高权限。
4	CVE-2015-1635	IIS	该漏洞存在于安装了IIS6.0以上的Windows操作系统中，黑客可利用该漏洞远程执行任意代码。
5	CVE-2015-0359	Flash	Adobe Flash Player中存在双重释放漏洞。攻击者可利用该漏洞执行任意代码，控制受影响系统。
6	CVE-2015-6172	Outlook	黑客利用该漏洞，以“特定打包的微软Office文件”作为附件，由Outlook发送后，可允许远程代码执行。
7	CVE-2015-2426	Windows	该漏洞影响所有主流Windows系统，黑客可借助特制的OpenType字体利用该漏洞执行任意代码。

图 23：2015 年重大终端漏洞

（二）企业网络安全

1. 2015 企业网络安全事件 Top10 全球信息泄漏已难以遏制

2015年全球企业网络安全事件Top10

序号	病毒名称	病毒行为及危害
1	Hacking Team泄露400G“网络核武”	全球知名入侵及监控技术公司Hacking Team遭入侵，400G核心数据、0Day漏洞及超级入侵工具被公布在互联网上，或将在未来造成针对企业、政府及重要组织的大规模攻击。
2	Xcode Ghost挂马事件	苹果应用的开发工具Xcode遭到篡改，致使包括微信、12306、高德地图、滴滴打车在内的数千款热门APP染毒，此次事件保守估计影响用户超过1亿。
3	网易邮箱数据泄露事件	10月，网易邮箱被曝上亿条用户信息泄漏，此次信息泄露事件可能是国内信息泄露最严重的一次也是涉及用户量最大的一次。此外，还发现一些苹果用户的iCloud账号被盗，后经鉴定是注册网易邮箱导致的。
4	世界上最大成人交友网站AdultFriendFinder数据库泄露，近400万会员性生活曝光	一位匿名黑客在暗网公开了世界上最大的交友网站之一AdultFriendFinder的数据库，泄漏的数据库信息中包括400万用户的电子邮件、IP、出生日期、性取向等。
5	美8000万医疗用户数据泄露	美国第二大的医疗保险服务商Anthem公司遭遇黑客攻击，超过8000万用户的姓名、生日、医保ID号、社会保险号、住宅地址、电子邮箱、雇佣情况，以及收入数据遭到泄漏。
6	美国OPM入侵事件	6月，黑客攻击入侵了美国人事管理局（OPM），该部门专门负责收集联邦雇员的人事信息，导致400万现任及前任雇员信息遭泄漏。
7	卡巴斯基遭APT攻击	全球知名网络安全公司卡巴斯基实验室遭遇APT攻击长达数月未察觉,实施攻击的病毒Duqu2.0是现今为止最为复杂的蠕虫病毒，被广泛应用于各种APT攻击事件中。
8	国际黑客组织匿名者（Anonymous）发动代号为OpChina的对华网络攻击	国际黑客组织匿名者（Anonymous）于2015年5月30日发动对华网络攻击，行动代号”OpChina”。日本、菲律宾、越南的黑客响应了本次行动，后由于事件升级，黑客大战于29日悄悄提前开始了，国内部分政府网站、公共事业网站及非营利组织网站遭遇了攻击。
9	Vtech（伟易达）数据泄露事件	Vtech伟易达公司是全球最大的婴幼儿及学前电子学习产品制造商，2015年发生数据泄漏事件，涉及范围覆盖480万家长和超过20万儿童。
10	德国联邦议院内网再遭黑客入侵	5月22日，媒体消息称德国联邦议院公开承认其机构IT系统遭到了黑客的入侵，联邦议院的IT职员发现有不明身份的黑客试图渗透进德国国会的内部网络，一些高度敏感信息有可能遭到泄露。

图 24：2015 年全球企业网络安全事件 Top10

2. DDoS 攻击全球增加近两倍 国内路由器成为重灾区

（1）DDoS 成为互联网企业的最大威胁之一

DDoS 即分布式拒绝服务攻击，该类攻击通常是由海量电脑肉鸡联合起来组成僵尸网络，通过大量合法的请求占用网络资源，造成目标服务器网络瘫痪。瑞星安全专家指出，DDoS 是目前互联网企业面临的最大也是最普遍的信息安全威胁。针对企业的 DDoS 攻击一旦发生，企业将面临网络堵塞、业务中断、系统宕机等风险。因此，DDoS 一旦发生，企业的经营活动及核心数据都面临着崩溃损毁的威胁。

（2）连续两年翻倍增长 DDoS 转型后全球大面积爆发

根据相关机构的调研报告显示，2014 年全球 DDoS 攻击数量增加了 200%，2015 年该类攻击增加到 2014 年的 180%。

瑞星安全专家介绍，DDoS 的兴盛是从 PC 接入互联网开始的，木马病毒的流行使黑客能够迅速捕获大量肉鸡，组建僵尸网络。然而随着 WiFi2.0 时代的到来，传统 PC 终端已经不再直接接入互联网，大量家庭开始使用路由设备，因此，传统的“扫肉鸡”工具已经开始无法适应当前的互联网环境,越来越多的“牧马人”将市场定位到 Linux 服务器和路由设备上。

根据瑞星“云安全”系统监测，2014 年到 2015 年的两年之中，仅国内就有 2,000 多万台路由器存在安全漏洞。由于多数路由器没有自动更新功能，因此上述路由器将极易遭受攻击，并成为黑客发起 DDoS 攻击的肉鸡。

（3）新型僵尸获取手段：种类多、效率更高、更廉价

根据瑞星安全研究院的报告显示，2015 年僵尸网络中的肉鸡主要依靠路由器漏洞、服务器应用漏洞、弱口令爆破、网络挂马四种方式获取，呈现终端系统类型种类多、攻击效率高、攻击成本低等特点。

路由器漏洞：由于传统路由器向智能路由器更替需要一个时间周期，在这个周期内，比较老旧的路由器没有进行漏洞修复,容易成为黑客重点攻击的对象。从 2014 到 2015 年的两年间，路由器漏洞爆发频繁，造成了大量路由器成为僵尸网络的一部分。

服务器应用漏洞：2015 年 Redis 未授权漏洞导致大量 Redis 服务器遭到暴力扫描。此外，JBoss、weblogic 等 Web 中间件 java 反序列化漏洞造成了批量扫描入侵的事件，影响极为恶劣。目前，从漏洞发布到大规模扫描利用的时间周期越来越短，然而网络运维工作的反应相对较慢，黑客利用时间差可制造大量网络攻击。

弱口令爆破：2015 年的弱口令爆破攻击已经从传统的针对 Windows 服务器转向 Linux 服务器，由于 Linux 没有 Windows 图形界面进行管理，管理者无法定位出恶意木马，因此也无法根除，进而海量 Linux 服务器也成为僵尸网络中的一员。

网络挂马：2015 年 Hacking Team 公司遭到黑客入侵，其中泄漏的 0Day 漏洞利用工具堪称“网络核武”。在 2015 年挂马事件中，该类工具包遭到大量挂马利用，没有进行及时升级的 PC 主机及路由器将沦为肉鸡。

（4）DDoS 趋势与防护方案

目前，DDoS 的利用工具从网上公开的情况来看已经进行过三次更新换代，从最初的简单上传写入 webshell、执行 cmd 命令，到支持对 JBoss，weblogic，websphere 三款中间件利用，功能越来越强大，攻击效果越来越显著。此外，在一些地下网站，一款新型的 DDoS 工具也在测试阶段。瑞星安全研究院通过分析发现该工具为一个单独 JSP 文件调用，由国外某知名渗透测试工具生成而来，支持 Linux，Windows 系统环境，利用已经公开的 payload 进行代码组装实现了半自动僵尸肉鸡获取。瑞星安全专家表示，该工具可能是前期测试版本，其正式版可能已经被大量应用。

针对目前 DDoS 攻击的情况，瑞星安全专家建议广大运维管理人员加强以下五个方面的工作：

- 注意服务器的自身安全配置，避免资源耗尽型的 DDOS 攻击。
- 监控入网流量，发现无效数据及时拦截。
- 对 Web 和其他资源使用负载均衡的同时，也要有效保护 DNS。
- 针对流量消耗型攻击，可采用提升自身宽带流量的办法。
- 购买第三方清洗流量设备或服务进行流量清洗。

3.政府、教育类网站遭 APT 居民数据泄密超 1 亿

（1）政府、教育类网站 APT 事件频繁、漏洞多

据瑞星“云安全”系统监测，2015 年政府网站和教育网站遭遇的 APT 攻击事件，分别占国内 APT 攻击事件的 2.16%和 0.96%。瑞星安全研究院针对上述两类网站进行安全检测，大部分网站具备以下三个特征：

- 网站以 JSP 脚本的站居多，且大多数站点都引用了 Struts2 框架，所以 Struts2

漏洞是政府站中出现率较高的安全漏洞之一。

- 政府站多使用 JEECMS 及 ewebditor 编辑器，因此这两种 CMS 的漏洞在政府网站安全问题中也占有较高比例。

- SQL 注入漏洞同样在政府网站占有极大的比例。

与此同时，根据众多的报告显示，政府站点大部分被架设在 Windows 系统中，且将网站存放在 D 盘中的居多，这样的架站基本成为政府网站的一个通用模式。根据上述特点，黑客可遵循固定模式对网站进行攻击，大大降低攻击成本，并能提高攻击效率。

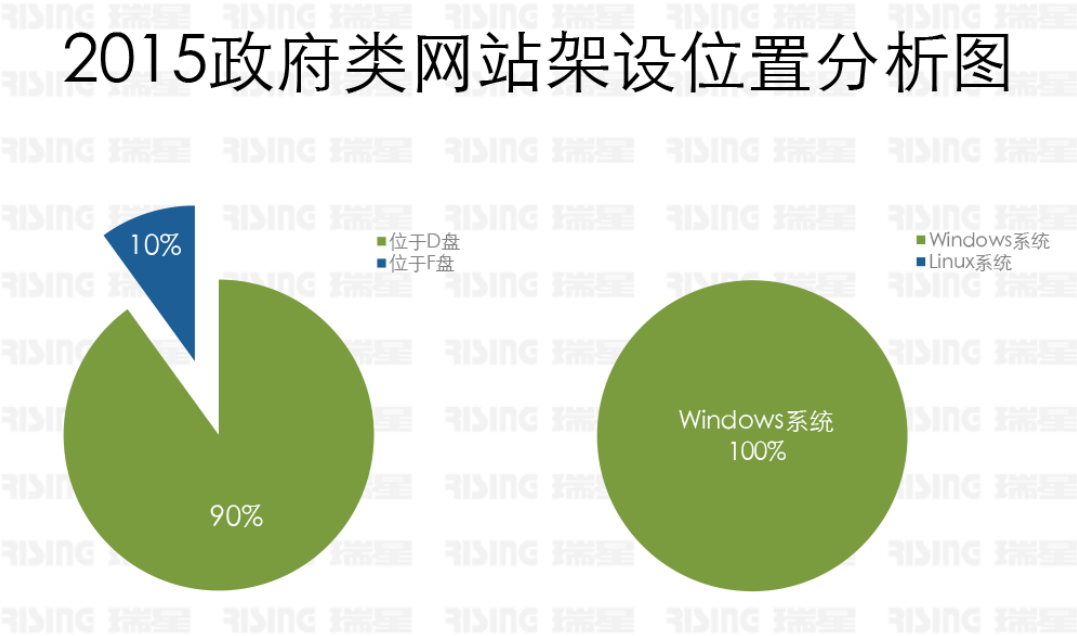

图 25：2015 政府类网站架设位置分析图

（3）政府及教育类网站信息泄漏事故规模大、影响范围广

2015年政府及教育类网站信息泄漏大事记

时间	事件
2月	疑似某交通管理部门数据库弱口令致使新某省70万机动车信息泄露
3月	某学校网站管理系统数据库下载导致用户密码泄露
4月	东北师范大学学生数据泄露/服务器可内网漫游
4月	19省社保系统信息泄露涉及5200万居民
10月	国家旅游局漏洞致6套系统沦陷，涉及全国6000万客户
12月	国内30个学校存在网站备份下载导致源码数据泄漏

图 26：2015 年政府及教育类网站信息泄漏大事记

从政府及教育类网站信息泄漏大事记中可看出，仅 2015 年政府及教育网站信息泄漏的数据总量已经过亿。由于政府、教育类网站的数据库通常都存储了大量学生、居民的个人身份信息，包括姓名、地址、身份证号、手机号、照片甚至身份证扫描件，因此，该类网站的数据一旦遭到泄漏将为整个社会带来巨大的经济损失。

图 27：2015 年政府及教育类网站信息遭大量泄漏

（3）政府类网站漏洞实例分析

实例一：某区政府网站可上传任意文件导致 Getshell

图 28：某政府网站安全分析

漏洞详情

存在问题 URL 地址:http://www.**.gov.cn/manager/editor/admin/default.php

该地址存在编辑器上传漏洞，网站使用的编辑器默认的管理员用户名及口令均为 admin，经测试，管理员并没有修改默认口令。攻击者可使用默认账密成功登录编辑器后台管理系统，进而获取 Web 控制权限，可删除、修改、下载、上传任意文件。

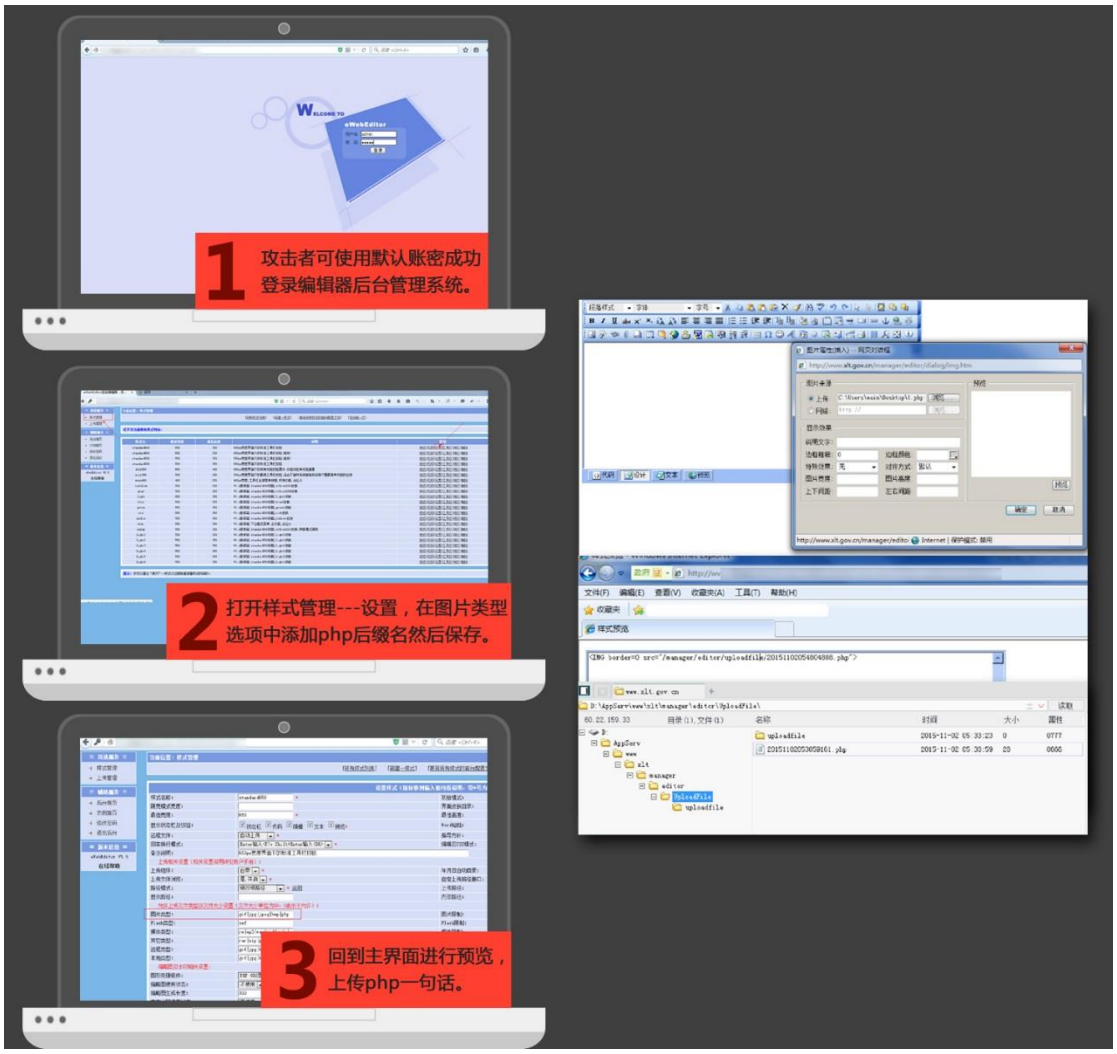

图 29：某政府网站存编辑器上传漏洞

漏洞危害

- 可利用 Web 权限进行挂马传播病毒。
- 可获取数据库重要信息，如个人账号密码、身份资料、信息资料等。

修复方法与建议

- 更改默认的用户名及密码。
- 对上传格式进行严格过滤，禁止上传一些可执行代码文件。
- 编辑器路径修改较为复杂的目录。

实例二：某市人民政府网后台存在 SQL 注入

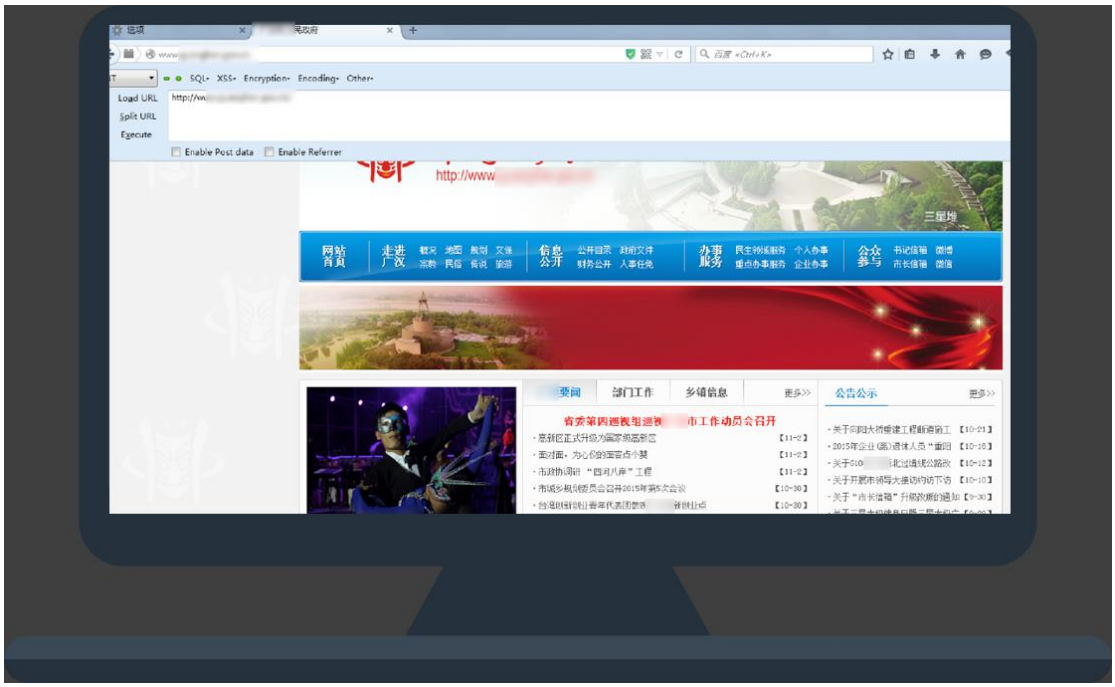

图 30：某政府网站安全分析

漏洞详情

URL 地址:http://www.**.gov.cn/admin_manage/为后台管理系统的网址，用户名处存在 SQL 注入漏洞，导致黑客可利用特殊语法构造进入后台，进而获取后台操作权限。

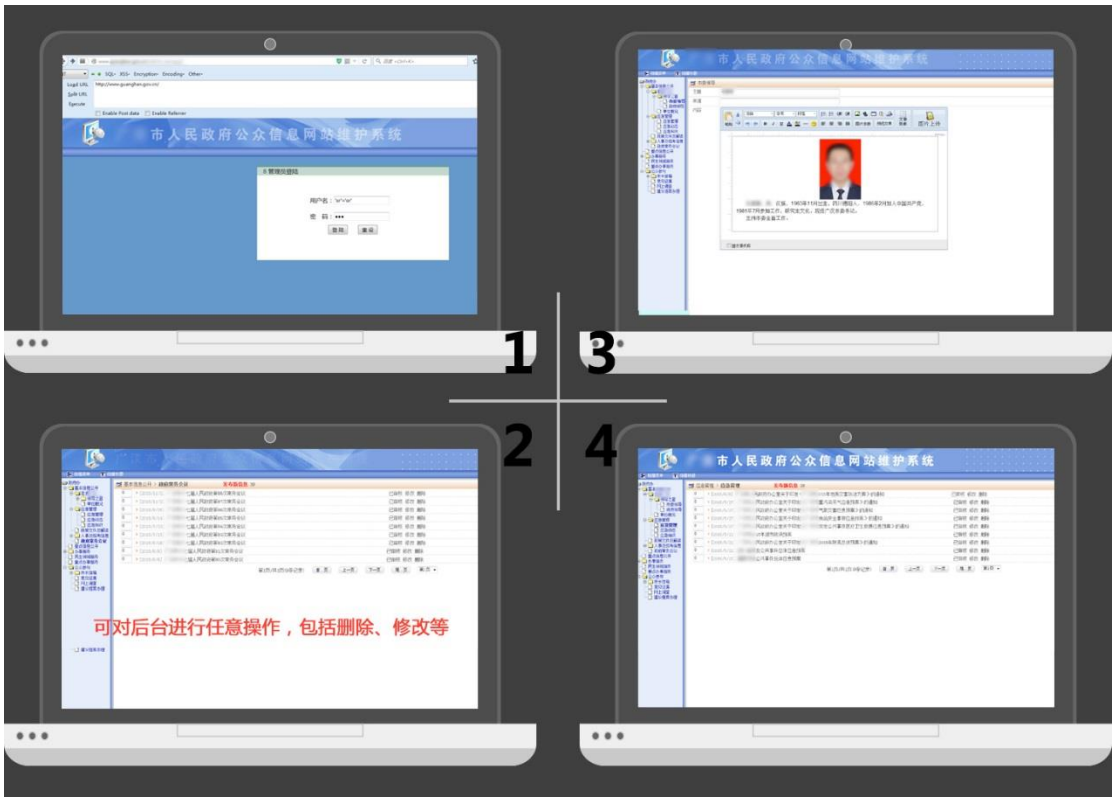

图 31：某政府网站存 SQL 注入漏洞

漏洞危害

黑客可利用 SQL 注入漏洞可获取数据库中敏感信息，如个人账号密码、身份资料、信息资料等。数据库重要数据信息可遭篡改，黑客可拿下数据库后利用数据进行非法获利，将造成严重的信息泄漏事故。

修复方法与建议

- 对相关参数进行过滤。
- 后台目录应相对复杂。
- 过滤一些常见的查询字符语句，如：select,updata,and,order,from 等语句。
- 采取数据库系统账号与应用账号分离，即创建应用程序需要访问的账号。
- 采取收缩权限并设置指定 IP 地址可以远程访问数据库。
- 对用户密码进行加密保存。
- 对整站程序进行排查，检查存在问题并修复。

（三）虚拟化、云计算、大数据安全

1. 大数据安全决定“互联网+”成败

近年来，互联网、云计算和大数据发展迅速，2015 年初“互联网+”计划的提出，更加速了传统行业与互联网融合的进程。然而，随着商务、政务乃至制造业向数据化信息化极速迈进，各类网站服务器宕机、网站瘫痪的安全事故层出不穷，大数据安全和企业业务安全问题逐渐显露。

2015年全国信息安全事故

时间	事件
5月	网易新闻客户端瘫痪
5月	携程宕机
6月	淘宝网瘫痪
9月	苹果官网瘫痪
9月	新浪微博网页版瘫痪
9月	成自泸高速缴费系统瘫痪
10月	滴滴打车系统宕机
10月	知乎出现瘫痪
11月	支付宝支付系统被挤瘫痪
11月	山西证券交易系统瘫痪

图 32：2015 年全国信息安全事故

从全国信息安全事故 Top10 中可以看出，仅 2015 年，由黑客攻击、系统宕机、意外灾害引起的重大信息安全事故不下 10 起。瑞星安全专家指出，在“互联网+”下任何的数据损毁和业务中断，都有可能为企业带来致命性打击，因为数据时时刻刻都在交换、流通，没有数据企业业务就无法实现，企业的所有经营活动都将成为一纸空谈。因此，大数据就是企业最重要的核心资产之一，搭建一套一体化的大数据备份恢复系统是企业迫在眉睫必须做的事情。

2. 海量云存储安全建设仍存技术壁垒

随着硬件及虚拟化技术的不断进步，拥有海量云存储的特大型数据库开始越来越多的应用于媒体、科研及许多大型高科技行业。瑞星安全专家表示，大量数据的集中也意味着云存储系统面临着更高的病毒威胁，一个病毒文件的流入，很有可能影响的是整个业务平台的运行，甚至可能造成海量的病毒感染和病毒传播。

然而，由于文件数量多、单个文件数据量大、文件读写频繁等原因，传统的病毒查杀系统在专业的海量云存储数据库面前显得捉襟见肘。设备成本高昂、查杀效率低、资源占用率高等问题不断困扰着该类平台的运维人员。

瑞星安全专家指出，传统的病毒查杀方法已经不能满足云存储的病毒防护需求，一些安全厂商试图依靠大型的硬件设备来解决查杀效率和资源占用的问题。但随之而来的，不仅是安全建设成本高居不下，同时，大型的硬件设备也并不能解决根本问题，仍会严重影响用户对云存储系统的正常使用。

针对上述情况，瑞星安全研究院根据多年的项目经验积累以及独家的虚拟化安全技术，

开发了一套专门用于海量云存储的解决方案。该方案采取软件部署的形式，查杀效率高、稳定性强、性价比高，可在不影响正常使用的情况下有效保护云存储系统的数据安全。

3. 一年两个重大漏洞 虚拟化安全环境日趋严峻

2015 年，虚拟化系统曝出两个漏洞，分别是“毒液”和 QEMU 网卡设备漏洞。

毒液漏洞（漏洞编号：CVE-2015-3456）是一个存在于虚拟软盘驱动器（FDC）代码中的安全漏洞，该代码存在于许多计算机虚拟化平台之中。该漏洞可允许攻击者从受感染虚拟机中摆脱访客身份限制，并很有可能获取主机的代码执行权限。此外，攻击者还可利用它访问主机系统以及主机上运行的所有虚拟机，且能够提升重要的访问权限，攻击者能够获得目标计算机以及其上运行的所有虚拟机的控制权。

QEMU 网卡设备漏洞（漏洞编号：CVE-2015-6815），是 QEMU 软件的虚拟网卡设备存在的一处逻辑漏洞，攻击者可利用该漏洞对虚拟机进行拒绝服务攻击，使目标服务器长时间保持高 CPU 占用率，进而影响同一台物理设备上的其他虚拟机。

目前，涉及上述两个漏洞的虚拟化平台都已经发布了修复补丁。然而，相较于 2014 年及之前的几年，2015 年中虚拟化漏洞的曝光有显著增加，由此可见，无论是黑客还是安全人员，都已将大量的精力投入到虚拟化安全的漏洞挖掘与修补当中。

四、趋势展望

（一）全球安全局势恶化 黑客攻击事件将继续影响 2016

2015 年上半年，Hacking Team 的 400G“网络核武”泄漏事件爆发，从下半年的挂马网址及 APT、DDoS 攻击情况来看，本次事故流出的许多 0Day 漏洞及新型漏洞利用工具已经被黑客广泛使用。

瑞星安全专家指出，Hacking Team“网络核武”的泄漏，并不是一起单纯的信息泄漏事件。它是全球安全局势恶化所带来必然的结果。未来，带有经济及政治目的的黑客攻击还将继续在以下几个方面影响 2016 年的信息安全局势：

- 企业、事业单位、政府乃至国家的核心机密信息泄漏。
- 大量高危 0Day 漏洞被公开，挂马网址有可能在 2016 年继续呈上升趋势。
- 随着先进的黑客工具在网上疯传，APT 攻击、DDoS、黑色产业链可能在 2016 年更为猖獗。
- 近年来，病毒与反病毒技术没有实质性的改变，但受到本次事件的影响，病毒与反病毒的对抗将更加激烈，反病毒技术也必将在未来出现颠覆性的革新。
- 需求催生创新，本次事件可能会催生大量以前从未想到过的高级信息安全技术。

（二）APT、DDoS 已常态化 全球安全威胁将持续高危等级

2015 年的 APT、DDoS 攻击在数量和频率上都有了进一步发展，量级超过 100 Gbps 的 DDoS 攻击峰值达到 12 次/季度。越来越多的传染型病毒开始带有文件收集、文件破坏乃至屏幕监控功能。此外，从网络上公开流传着的海量黑客工具可看出，该类工具已完成从复杂操作到“傻瓜式”操作的进化。受此影响，越来越多的不法分子开始具备黑客能力，带有经济目的或政治目的 DDoS 和 APT 攻击已成常态。从上述发展趋势来看，未来随着“互联网+”计划的实施，黑客将更多的瞄准企业，类似超级工厂、Duqu、Duqu2 这样的超级病毒及 APT 攻击还会再次出现，任何重要的企业、机构都应该具备专业的计算机安全保障机制，并进行周期性的计算机安全普查。

（三）“互联网+”将进一步促进虚拟化安全技术发展

3 月 5 日，国家总理在政府工作报告中提出了“互联网+”计划，该计划是要推动互联网和传统行业的融合。这不仅意味着我国今后将快速向互联网化发展，也意味着云计算、大

数据将成为未来支撑企业日常办公、运营的重要组成部分。

云计算和大数据几乎满足了企业对办公系统、数据存储系统及网站运营系统所有的美好愿景：更高效的资源利用、更强的稳定性、更低廉的运营成本和更便捷的管理。这两类技术有一个共同特点，那就是以虚拟化平台为基础。其中，云计算是将计算能力依托于虚拟化平台，对硬件资源进行统筹管理，使资源利用率达到最大化。大数据则是将数据存储依托于虚拟化平台，个人用户可以在不同时间、不同地点、不同终端上，对同一数据进行读写并保存，企业用户可以利用大数据对碎片化的信息进行整合分析或集中处理，从而达到简化办公、提取商业数据等目的。

然而，作为云计算和大数据的支撑，虚拟化平台的安全问题一直在业界存在争论。一种说法是，虚拟化平台——尤其是桌面虚拟化，不存在安全问题，因为数据是集中管理的，连操作系统都具备极强的流动性，随时可能在不同主机上进行迁移，依托先进的双机热备技术，可保证虚拟化平台上运行的终端处于绝对安全的状态。

瑞星安全专家指出，这种说法过于片面。相对于普通的 PC 操作系统，虚拟化平台固然有它的先天优势，然而正是这些优势，同时也带来了致命的弊端。众所周知，虚拟化平台的资源整合能力来自于资源的集中和再分配，企业的数据、服务都维系在一组服务器上，因此一旦虚拟化平台遭遇到严重的病毒感染、黑客入侵等攻击时，有可能整个服务器组直接受到影响，在这种情况下，即使是双机热备也无法解决问题，届时企业办公将受到牵连，严重时还可能使整个系统瘫痪。

瑞星安全专家警告，虽然虚拟化技术还是一种新型技术，黑客针对虚拟化平台的挖掘受到成本限制，目前还不多见。然而就 2015 年曝出的重大漏洞来看，未来会有大批黑客重点关注虚拟化平台的漏洞挖掘。同时，在“互联网+”计划的引导下，智慧城市、智慧家庭、企业智能化办公等项目会成为必然趋势，虚拟化平台将更多的承载企业乃至国家的核心业务和数据。因此，云计算、大数据在国内普及以后，必将有大批黑客在大数据的诱惑下铤而走险。

附录：部分案例与参考资料

瑞星：一年八起重大事故 大数据安全保障迫在眉睫
http://it.rising.com.cn/dongtai/17928.html

正版未至病毒先行 Google Play 遭遇李鬼
http://it.rising.com.cn/dongtai/17924.html

瑞星：病毒仿冒中国移动 中秋国庆出行查流量小心中毒
http://it.rising.com.cn/dongtai/17922.html

护航 BTV 瑞星打造国内首例云存储安全项目
http://www.rising.com.cn/about/news/rising/2015-03-31/17217.html

XcodeGhost 爆发 中国 APP 开发者正遭遇最严重水坑攻击
http://www.rising.com.cn/about/news/rising/2015-09-23/17830.html

本报告贡献者如下*（排名不分先后）*：

超哥、丰哥、bfish、阿启、阿森、Kimbel、阿领、DE、阿成
撰写人：墨嘉