瑞星 2016 年中国信息安全报告

北京瑞星信息技术股份有限公司

2017 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、瑞星反病毒实验室、瑞星互联网攻防实验室、瑞星威胁情报平台等部门的统计、研究数据和分析资料，仅针对中国 2016 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

- 2016 年瑞星“云安全”系统共截获病毒样本总量 4,327 万个，病毒总体数量比 2015 年同期上涨 16.47%。报告期内，病毒感染次数 5.6 亿次，感染机器总量 1,356 万台，平均每台电脑感染 40.96 次病毒。

- 2016 年瑞星“云安全”系统在全球范围内共截获恶意网址（URL）总量 1.38 亿个，其中挂马网站 8,804 万个，诈骗网站 4,977 万万个。美国恶意 URL 总量为 7,001 万个，位列全球第一，其次是中国 695 万个，德国 526 万个，分别为二、三位。

- 2016 年瑞星“云安全”系统共截获手机病毒样本 502 万个，隐私窃取类病毒占比 32%，位列第一位，资费消耗类病毒占比 16%，位列第二位，流氓行为类与恶意扣费类并列第三，占比 15%。

- 2016 年移动安全事件：病毒伪装“交行安全控件”盗取用户敏感信息；Android 木马冒充“公安”电信诈骗；“一条短信偷光银行卡”骗子实施补卡截码诈骗；数百万台安卓智能手机暴露于 DRAMMER Android 攻击之下。

- 2016 年移动安全趋势分析：手机 web 浏览器攻击将倍增；Android 系统将受到远程设备劫持、监听；物联网危机将不断加深；

- 2016 年企业面临的安全问题逐渐凸显，特别是自斯诺登事件后互联网出现了大规模信息泄露事件，其中雅虎为信息泄露最大的受害者，影响个人信息超过 10 亿。同时，企业还面临着勒索软件的攻击以及 APT 攻击等，这将使企业成为网络威胁中的最大受害者。

- 趋势展望：敲诈软件依然会是低成本高收益网络犯罪的主流；IoT（物联网）安全隐患正在凸显；全新的网络攻击模式——网络流量监控；

- 专题 1：勒索软件年度分析报告。2016 年是勒索软件繁荣发展的一年，在这一年里除了针对 Windows 系统勒索软件，针对 Linux、Mac OX 等勒索软件都已出现。同时移动平台 Android 和 IOS 系统也未能幸免。勒索软件为了躲避查杀不断发展，用上了各种手段。脚本 JS 开发、python 开发、Autoit 开发的勒索软件都在今年出现。2017 年注定还是勒索软件猖獗的一年。

- 专题 2：SEO 诈骗分析报告。瑞星安全专家针对诈骗网址进行了深入分析，分析过程中发现该网址不仅具有欺诈性质，而且还利用黑帽手段进行关键词排名推广，当用户利用搜索引擎搜索到黑客设置的关键词时，就会弹出黑客预先修改过的“正规网站”，让受害者误以为是官方网站，从而导致用户上当受骗。

- 专题 3：不法分子如何利用伪基站盈利。瑞星安全专家通过对伪基站深入的分析发现，诈骗者通过雇佣其他人员携带伪基站在街道和小区周边进行大范围发送诈骗短信、广告、诈骗网址，木马 APK 程序等，一旦用户点击诈骗链接，用户的银行卡、支付账户等

个人信息将有可能泄露。诈骗者通过购买大量黑卡进行洗钱，将可用账户中的金额进行消费变现，然后转账到黑卡账户中。

- 专题 4：2016 路由安全分析。路由安全一直是网络安全里的热门事件，几乎所有路由品牌都曝出过漏洞，黑客正是利用这些漏洞对用户的路由进行入侵和劫持，将用户访问的网站定向到诈骗网站，然后盗取用户个人隐私，如果是企业级路由被黑客攻击，将会造成更大的影响。

一、病毒与恶意网址

（一）病毒和木马

1. 2016 年病毒概述

（1）病毒疫情总体概述

2016 年瑞星“云安全”系统共截获病毒样本总量 4,327 万个，病毒总体数量比 2015 年同期上涨 16.47%。报告期内，病毒感染次数 5.6 亿次，感染机器总量 1,356 万台，平均每台电脑感染 40.96 次病毒。

在报告期内，新增木马病毒占总体数量的 48.6%，依然是第一大种类病毒。灰色软件病毒（垃圾软件、广告软件、黑客工具、恶意壳软件）为第二大种类病毒，占总体数量的 17.54%，第三大种类病毒为后门病毒，占总体数量的 12.77%。

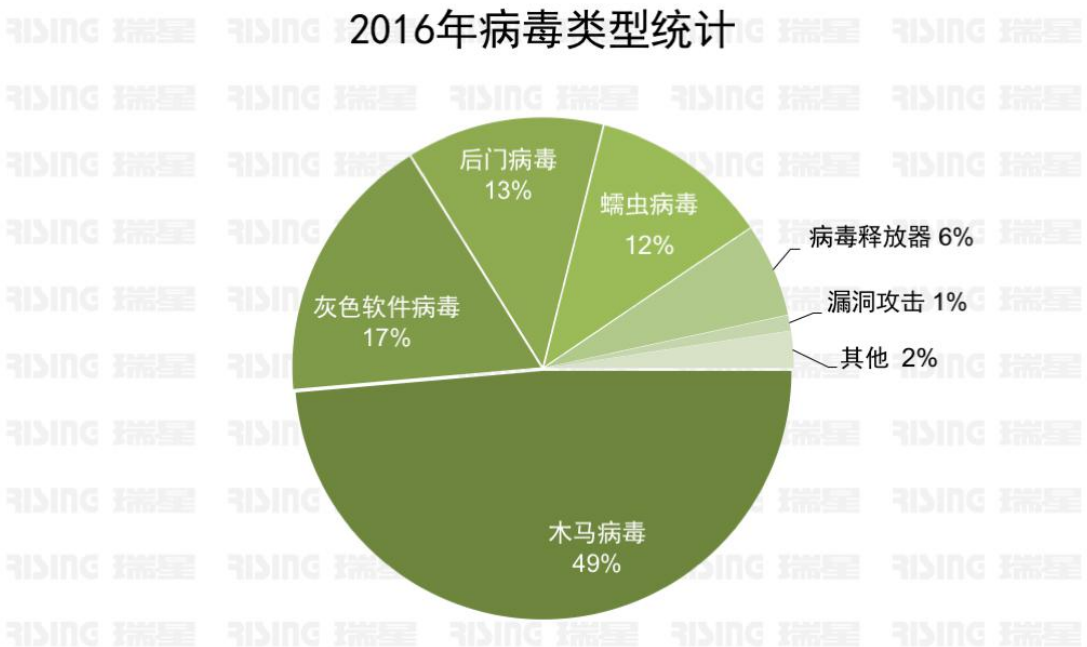

图 1：2016 年病毒类型统计

（2）病毒感染地域分析

在报告期内，广东省病毒感染 6,051 万人次，依然位列全国第一，其次为北京市 3,657 万人次及河南省 2,477 万人次。与 2015 年同期相比，北京排进前三，江苏则由第二名降到

第五。

图 2：2016 年病毒感染地域 TOP10

2. 2016 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 2016 年病毒 TOP10：

2016年病毒TOP10

1	PUA.Generic	不被需要的灰色软件，例如：软件下载/推广器、具备流量劫持功能的无用软件等
2	LNK:Worm.LnkBased	通常是由蠕虫释放的恶意快捷方式文件
3	Trojan.Crypto	采用了混淆、膨胀等技术对抗安全软件检测的恶意软件，例如：Zbot, Urausy等
4	Virus.Ramnit	感染型病毒
5	Trojan.Generic	窃取隐私信息、盗取帐号、密码，远程控制
6	Rootkit.HtmlInject	释放驱动、通过HTTPS劫持流量牟取利益
7	Ransom.Locky	勒索软件Locky家族，会加密200种以上的数据文件，支付赎金后才能解密
8	Backdoor.Overie	后门程序，感染后计算机会被黑客完全控制，成为“肉鸡”
9	Adware.BrowseFox	恶意广告软件，会劫持浏览器，大量消耗计算机资源
10	Trojan.OddCode/JS	经过混淆、加密的JS下载器，例如：勒索病毒下载器

图 3：2016 年病毒 TOP10

3. 2016 年中国勒索软件感染现状

在报告期内，瑞星“云安全”系统共截获勒索软件样本 26.5 万个，感染共计 1,311 万次，其中北京市感染 143 万次，位列全国第一，其次为广东省 100 万次、浙江省 73 万次及安徽省 68 万次。

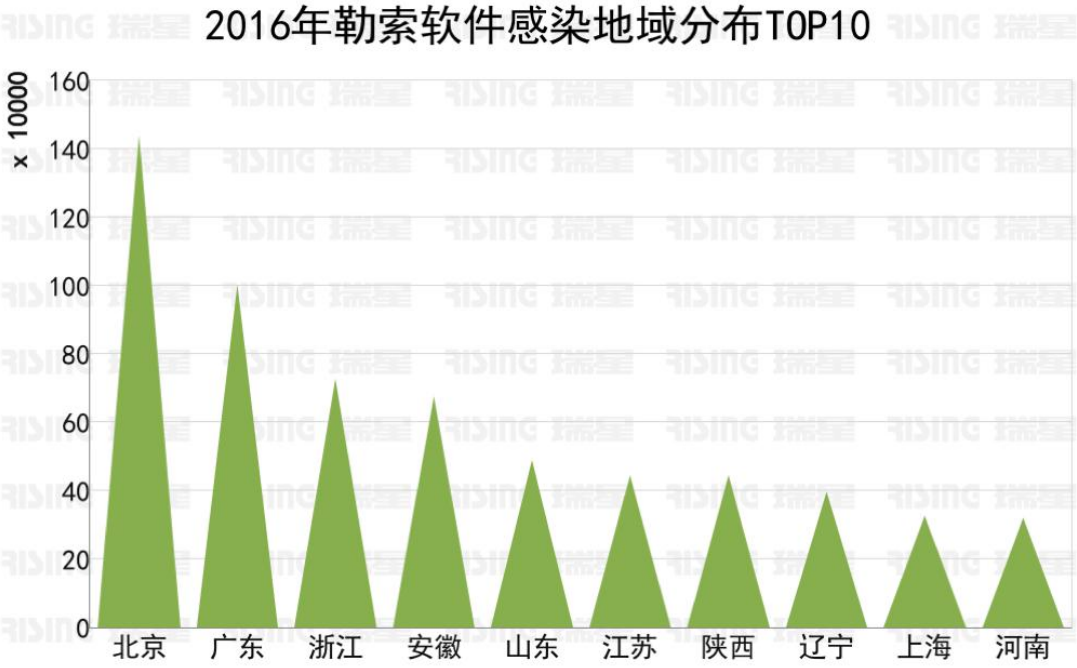

图 4：2016 勒索软件感染地域分布 TOP10

2016年热门勒索软件

勒索软件名称	具体恶意行为
TeslaCrypt	针对游戏平台，利用Flash Player漏洞(CVE-2015-0311)或者一个古老的IE浏览器漏洞将TeslaCrypt勒索软件植入目标系统上。然后对受害者文件进行加密
CTB-Locker	远程加密用户电脑文件
Cryptowall	一旦受害者感染了这些病毒，它们会立即对机器上的所有文件加密
Locky	黑客向受害者邮箱发送带有恶意word文档的Email，word文档中包含有黑客精心构造的恶意宏代码，受害者打开word文档并运行宏代码后，locky恶意代码会被加载执行，下载加密密钥，加密本地的所有磁盘和文件
cuteRansomware	cuteRansomware的特征是只弹出中文书写的文本文件。此外，所有加密文件的末尾有“.encrypted”（中文的）扩展名

图 5：2016 年热门勒索软件

4. 2016 年 CVE 漏洞 TOP10

2016年CVE漏洞TOP10

漏洞名称	漏洞内容
PHPMailer RCE 漏洞	远程攻击者利用该漏洞，可实现远程任意代码在web服务器账户环境中执行，并使web应用陷入威胁中。
OpenSSH远程代码执行漏洞	漏洞出现在ssh-agent中，该进程默认不启动、只在多主机间免密码登录时才会用到。
Joomla未授权创建特权漏洞	Joomla被披露存在账号创建和权限提升漏洞，综合利用上述两个漏洞，远程攻击者可在不允许注册的情况下注册账号，并可进一步提升权限至管理员特权。
Apache Tomcat远程代码执行漏洞	此漏洞在严重程度上被定义为Important，而非Critical，主要是因为采用此listener的数量并不算大，而且即便此listener被利用，此处JMX端口访问对攻击者而言也相当不寻常。
Jenkins 反序列化漏洞	通过低权限用户构造一个恶意的 XML 文档发送至服务端接口，使服务端解析时调用 API 执行外部命令。
BadTunnel漏洞	当WPAD协议回退到目标系统上易受攻击的代理发现进程时，该漏洞可能会允许特权提升，但这个漏洞的精髓实则是利用NetBIOS的协议缺陷实现跨网段的广播协议劫持。
Wget重定向漏洞	当使用wget 下载文件时，如果服务器将下载资源重定向到ftp服务时，wget 会默认信赖http服务器重定向的 ftp 链接地址和文件名，而不做二次验证。
Struts 2命令执行漏洞	无论是否在开启动态方法调用（Dynamic Method Invocation）的情况下，攻击者使用REST插件调用恶意表达式均可以远程执行代码。
Image Magick 命令执行漏洞	漏洞产生的原因是 ImageMagick 使用 system() 指令调用来处理 HTTPS 请求，而对用户传入的 shell 参数没有做好过滤，导致能注入任意指令执行。
脏牛（Dirtycow）漏洞	一个低权限的本地用户能够利用此漏洞获取其他只读内存映射的写权限，并且可以进一步导致提权漏洞。

图 6：2016 年 CVE 漏洞 TOP10

（二）恶意网址

1. 2016 年全球恶意网址总体概述

2016 年瑞星“云安全”系统在全球范围内共截获恶意网址（URL）总量 1.38 亿个，其中挂马网站 8,804 万个，诈骗网站 4,977 万个。美国恶意 URL 总量为 7,001 万个，位列全球第一，其次是中国 695 万个，德国 526 万个，分别为二、三位。

图 7：2016 年全球恶意 URL 地域分布 TOP10

2. 2016 年中国恶意网址总体概述

在报告期内，香港恶意网址（URL）总量为 117 万个，位列中国第一，其次是浙江省 104 万个，以及北京市 95 万个，分别为二、三位。

注：上述恶意 URL 地址为恶意 URL 服务器的物理地址。

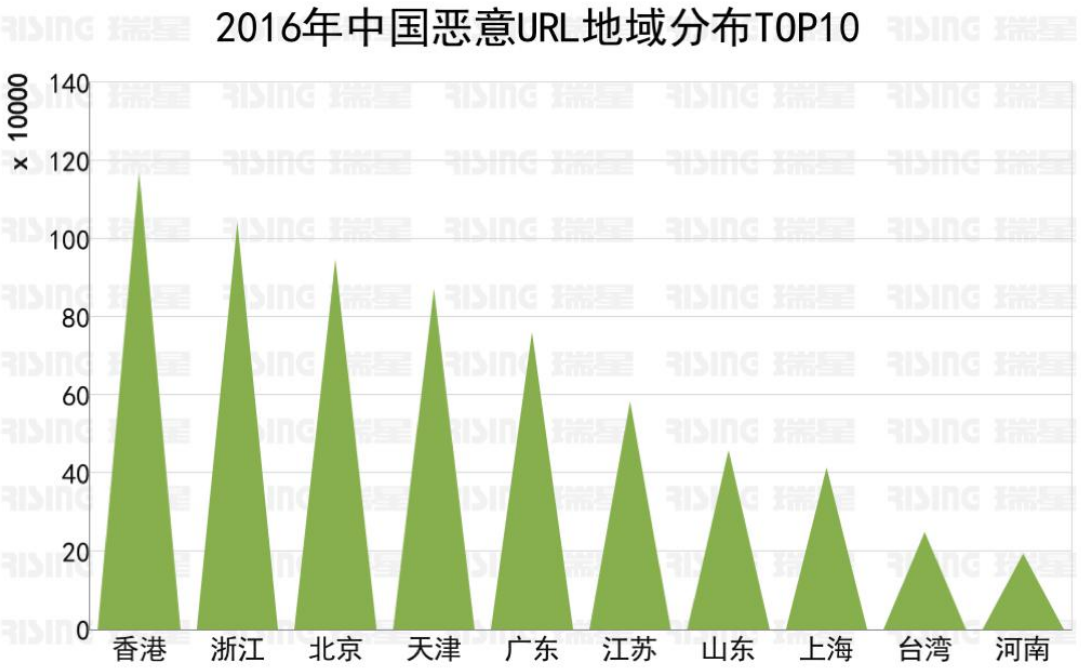

图 8：2016 年中国恶意 URL 地域分布 TOP10

3. 2016 年中国诈骗网站概述

2016 年瑞星“云安全”系统共拦截诈骗网站攻击 4,399 万余次，攻击机器总量 327 万台，平均每台机器被攻击 13.43 次。

在报告期内，广东省受诈骗网站攻击 733 万次，位列第一位，其次是北京市受诈骗网站攻击 608 万次，第三名是浙江省受诈骗网站攻击 340 万次。

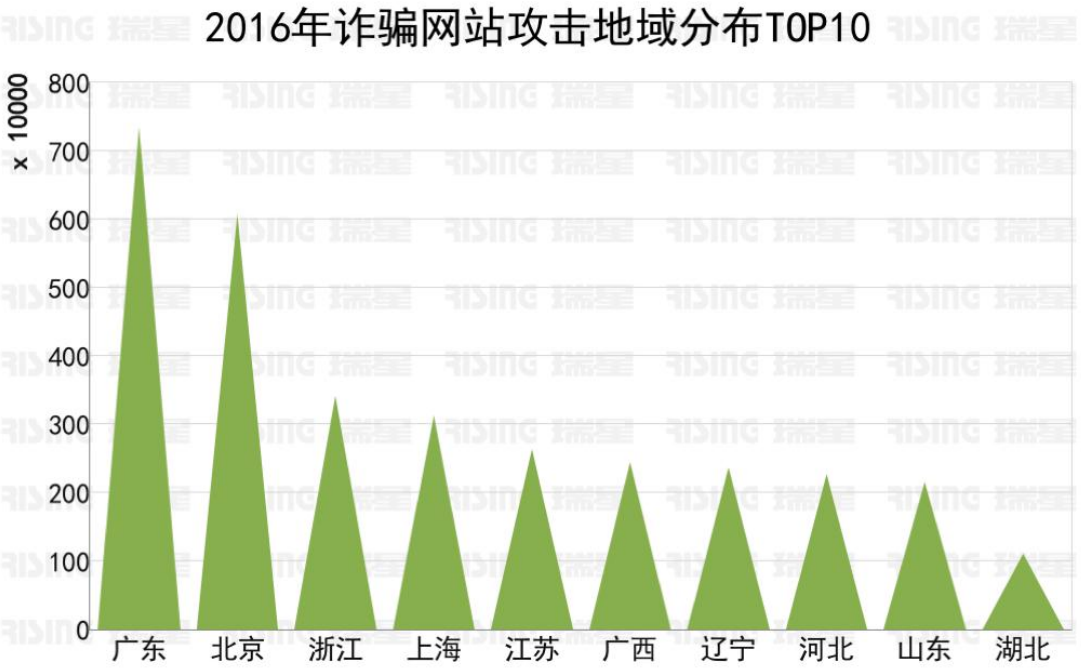

图 9：2016 年诈骗网站攻击地域分布 TOP10

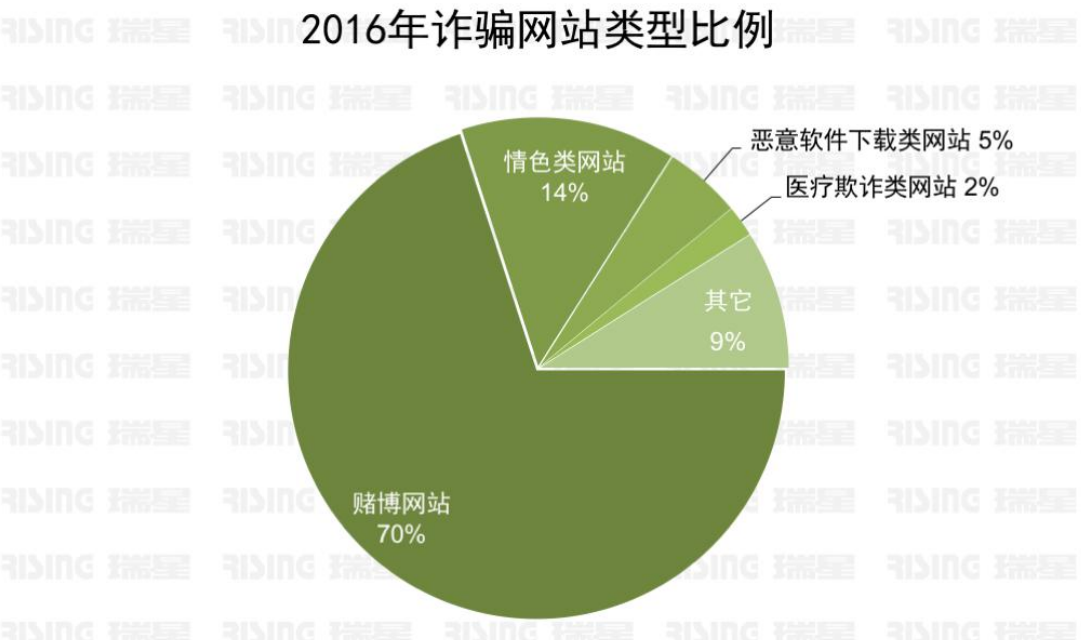

图 10：2016 年诈骗网站类型比例

4. 2016 年中国主要省市访问诈骗网站类型

在报告期内，浙江省、上海市等访问的诈骗网站类型主要以网络赌博为主，而湖北省、天津市则以色情论坛为主。

2016年中国主要省市访问诈骗网站类型

浙江	网络赌博
上海	网络赌博
北京	六合彩
陕西	私服网游
广东	网络赌博
湖北	色情论坛
天津	色情论坛
江西	网络赌博
广西	保健会所
江苏	网络赌博
山东	恶意软件下载类网站
四川	网络赌博
重庆	网络赌博
河南	网络赌博

图 11：2016 年中国主要省市访问诈骗网站类型

5. 诈骗网站趋势分析

2016 年赌博和情色类诈骗网站占比较多，这类网站会诱使用户下载恶意 APP 程序，窃取用户隐私信息。有些甚至通过木马病毒盗取用户银行卡信息，进行恶意盗刷、勒索等行为。诈骗攻击主要通过以下手段进行攻击：

- 利用 QQ、微信、微博等聊天工具传播诈骗网址。
- 利用垃圾短信“伪基站”推送诈骗网址给用户进行诈骗。
- 通过访问恶意网站推送安装恶意 APP 程序窃取用户隐私信息。
- 通过第三方下载网站对软件进行捆绑木马病毒诱使用户下载。

6. 2016 中国挂马网站概述

2016 年瑞星“云安全”系统共拦截挂马网站攻击 2,749 万余次，攻击机器总量 181 万台，平均每台机器被攻击 15.16 次。

在报告期内，北京市受挂马攻击 588 万次，位列第一位，其次是上海市受挂马攻击 551 万次，第三名是辽宁省受挂马攻击 528 万次。

图 12：2016 年挂马攻击地域分布 TOP10

7. 挂马网站趋势分析

2016 年挂马攻击相对减少，攻击者所使用的工具倾向于使用 2015 年下半年由 hacking team 泄露的网络工具包。攻击者一般是自建一些导航类或色情类的网站，吸引用户主动访问。也有一些攻击者会先购买大型网站上的广告位，然后在用户浏览广告的时候悄悄触发。如果不小心进入挂马网站，则会感染木马病毒，导致丢失大量的宝贵文件资料和账号密码，其危害极大。挂马防护手段主要为：

- 拒绝接受陌生人发来的链接地址。
- 禁止浏览不安全的网站。
- 禁止在非正规网站下载软件程序。
- 安装杀毒防护软件。

二、移动互联网安全

（一）手机安全

1.手机病毒概述

2016 年瑞星“云安全”系统共截获手机病毒样本 502 万个，隐私窃取类病毒占比 32%，位列第一位，资费消耗类病毒占比 16%，位列第二位，流氓行为类与恶意扣费类并列第三，占比 15%。

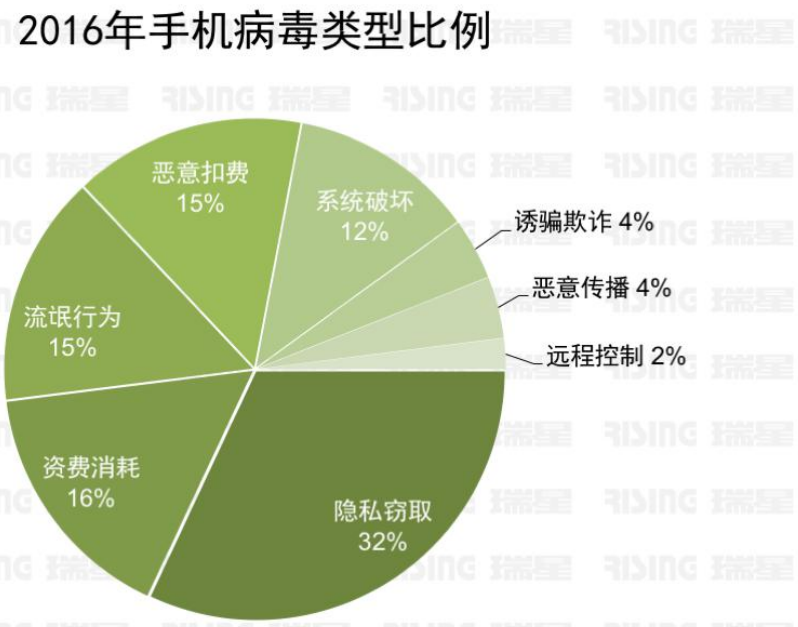

图 13：2016 年手机病毒类型比例

2016年手机病毒TOP5

1	Trojan.SMSreg!8.2DFC	具有通过私自拨打电话、私发短信、彩信、邮件、频繁连接网络、窃取用户短信收件箱等行为。
2	Dropper.Shedun/Android!8.3F4	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	Dropper.Agent/Android!8.37E	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。
4	Trojan.Agent/Android!8.358	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	Trojan.SMSSend!8.2DF7	具有通过私自发送短信、彩信、获取用户隐私内容等行为。

图 14：2016 年手机病毒 TOP5

2. 2016 年 Android 手机漏洞 TOP5

2016年Android手机漏洞TOP5

序号	漏洞名	漏洞编号	漏洞概述
1	Quadrooter	CVE-2016-3842	黑客可欺骗用户安装恶意应用，同时并不需要请求任何特别的权限。在应用安装后，黑客可以获得root权限，随后完全控制受影响的Android设备。
2	Dirty COW	CVE-2016-5195	黑客可利用此漏洞获取设备root权限，对只读内存映射进行写访问。
3	BadKernel	CNNVD-201608-414	该漏洞是由于微信V8源码中“observe_accept_invalid”异常类型被误写为“observe_invalid_accept”。通过这个漏洞黑客可获取微信的完全控制权。
4	广升FOTA系统升级服务命令执行漏洞	CNNVD-201611-438	该漏洞是源于服务的系统应用没有限制程序调用系统函数。攻击者可借助恶意代码利用该漏洞以‘SYSTEM’权限执行任意命令。
5	Linux内核漏洞	CVE-2016-0728	该漏洞源于程序没有正确处理特定错误中的对象引用。本地攻击者可借助特制的keyctl命令利用该漏洞造成拒绝服务（整数溢出和释放后重用）。

图 15：2016 年 Android 手机漏洞 TOP5

3.手机垃圾短信概述

2016 年瑞星“云安全”系统共截获手机垃圾短信 328 亿条，广告类垃圾短信占比 82.37%，

居首位。危险程度极高的诈骗短信占比 10.74%，其他类垃圾短信占比 6.89%。

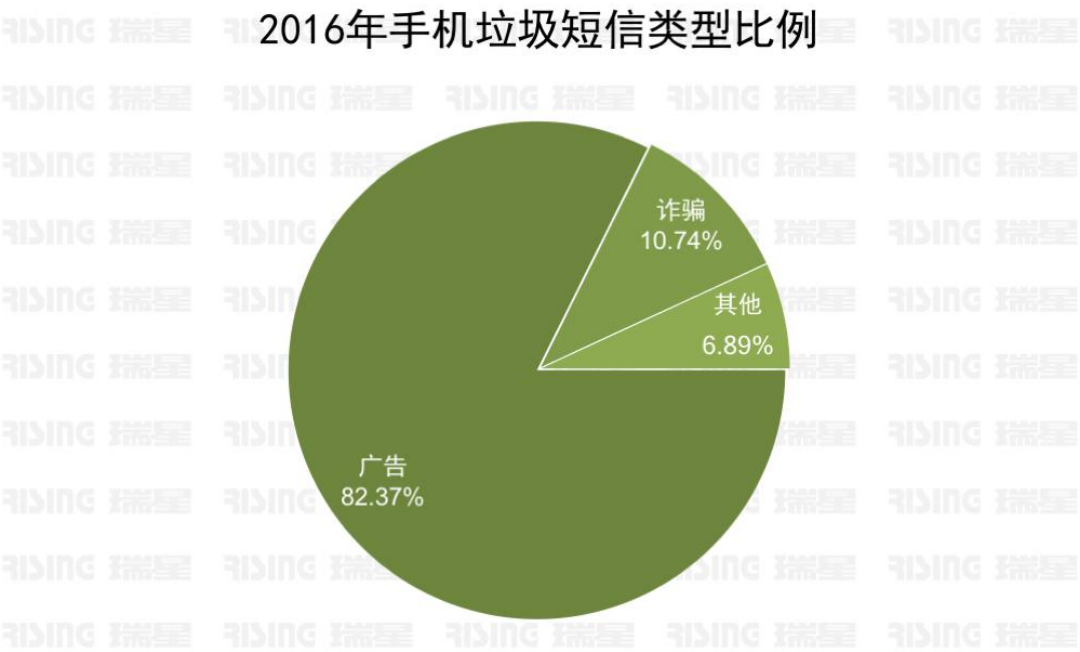

图 16：2016 年手机垃圾短信类型比例

（二）2016 年移动安全事件

1.病毒伪装“交行安全控件”盗取用户敏感信息

2016 年 6 月，一个伪装成“交行安全控件”的病毒潜伏在各大安卓电子市场中，诱导用户下载安装。该病毒运行后，会诱导用户激活系统设备管理器、隐藏自身启动图标、拦截用户短信并将短信内容发送到指定号码、还涉及登陆、支付等相关功能，给用户造成严重的隐私泄露等安全问题。

图 17：病毒伪装“交行安全控件”

2.Android 木马冒充“公安”电信诈骗

2016 年 5 月，全球首款专用于网络电信诈骗的 Android 木马被发现，该木马伪装成“公安部案件查询系统”，可实现窃取隐私、网络诈骗和远程控制等多种恶意行为，在受害人不知情的情况下转走其银行账户中的资金，对手机用户造成极大威胁。Android 木马加速实现了电信诈骗手段的 3.0 进化，一般的网络电信诈骗中，诈骗者必须诱导受害人完成转账。而引入了移动场景的 3.0 级别，即使受害人没有自主完成转账，诈骗者也可以依靠植入受害人手机的木马，在其不知情的情况下完成远程转账。

图 18：Android 木马冒充“公安”电信诈骗

3.“一条短信偷光银行卡”骗子实施补卡截码诈骗

2016 年 4 月，一网友爆料，莫名其妙地收到了一条“订阅增值业务”的短信，根据提示回复了“取消+验证码”之后，噩梦就此开启：手机号码失效，半天之内支付宝、银行卡上的资金被席卷一空。这起案件的关键点在于不法分子利用 “USIM 卡验证码”，完成了对受害者手机卡的复制，不法分子复制了网友手机卡，摇身变成网友，然后随意操作资金流向。

图 19：“订阅增值业务”短信

4.数百万台安卓智能手机暴露于 DRAMMER Android 攻击之下

2016 年 10 月，来自谷歌公司 Zero 项目组的安全研究人员们发现了一种名为 DRAMMER 的全新攻击方式，该攻击可劫持运行有 Linux 系统之计算机设备，利用其内存机制中的一项设计漏洞获取 Linux 系统的更高内核权限，可被用于在数百万台 Android 智能手机之上获取“root”访问权限，从而允许攻击者对受感染设备加以控制。

图 20：DRAMMER Attack

（三）移动安全趋势分析

1.手机 web 浏览器攻击将倍增

Android 和 iPhone 平台上的 web 浏览器，包括 Chrome、Firefox、Safari 以及采用类似内核的浏览器都有可能受到黑客攻击。因为移动浏览器是黑客入侵最有效的渠道，通过利用浏览器漏洞，黑客可以绕过很多系统的安全措施。

2.Android 系统将受到远程设备劫持、监听

随着 Android 设备大卖，全球数以亿计的人在使用智能手机，远程设备劫持将有可能引

发下一轮的安全问题，因为很多智能手机里存在着大量能够躲过谷歌安全团队审查和认证的应用软件。与此同时，中间人攻击（MitM）的数量将大增，这是因为很多新的智能手机用户往往缺乏必要的安全意识，例如他们会让自己的设备自动访问不安全的公共 WiFi 热点，从而成为黑客中间人攻击的猎物和牺牲品。

3.物联网危机将不断加深

如今，关于“物联网开启了我们智慧生活”的广告标语不绝于耳，但支持物联网系统的底层数据架构是否真的安全、是否已经完善，却很少被人提及，智能家居系统、智能汽车系统里藏有我们太多的个人信息。严格来讲，所有通过蓝牙和 WiFi 连入互联网的物联网设备和 APP 都是不安全的，而这其中最人命关天的莫过于可远程访问的医疗设备，例如大量的超声波扫描仪等医疗设备都使用的是默认的访问账号和密码，这些设备很容易被不法分子进行利用。

三、企业信息安全

（一）2016 年企业安全总体概述

2016 年企业面临的安全问题逐渐凸显，特别是自斯诺登事件后互联网出现了大规模信息泄露事件，其中雅虎为信息泄露最大的受害者，影响个人信息超过 10 亿。同时，企业还面临着勒索软件的攻击以及 APT 攻击等，这将使企业成为网络威胁中的最大受害者。

（二）2016 年企业安全相关数据

报告期内，通过对国内企业网络安全产品部署情况进行分析，发现企业部署终端安全防护产品占比 81.79%，位列第一位，其次网关安全硬件占比 12.25%，第三名是虚拟化安全占 5.75%，这说明企业对于终端安全更加重视。在调查的企业中，政府、军队、军工、能源等行业安全产品部署相对完善，而中小企业则投入较少，安全意识不足。

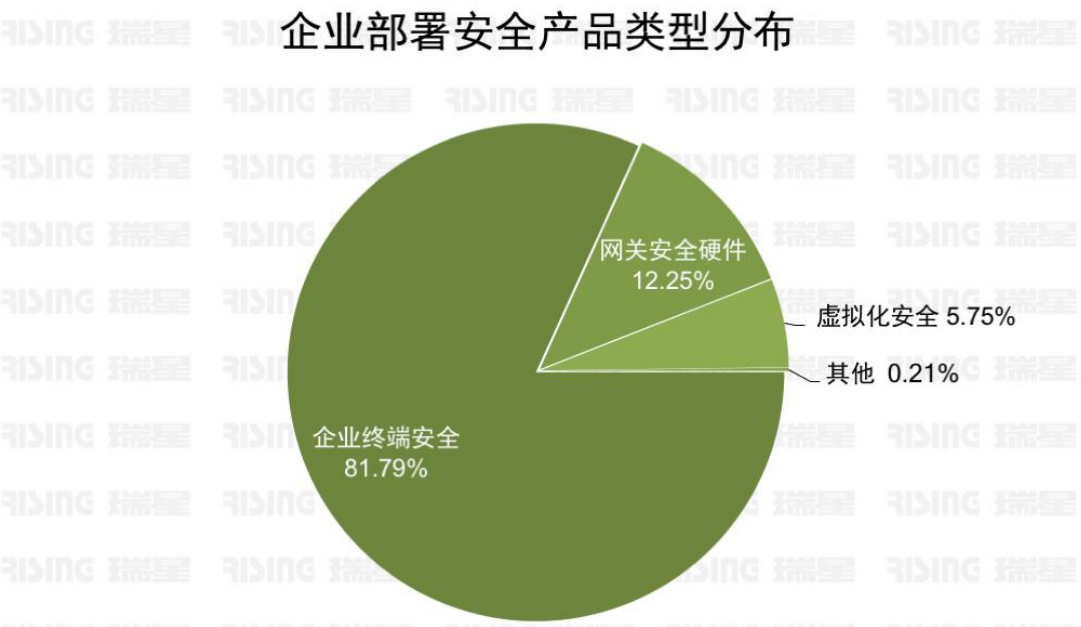

图 21：企业部署安全产品类型分布

（三）企业 APT 攻击中，CVE 漏洞攻击占比最多

在针对企业的 APT 攻击中，利用 CVE 漏洞往往是攻击过程中最重要的手段。攻击者利用 Office，Adobe 漏洞对企业发起攻击。而企业对于第三方软件漏洞修复往往没有做到及时响应，导致企业存在安全漏洞。根据瑞星“云安全”统计“CVE-2010-0188” Adobe Reader 样本超过 4 万个。

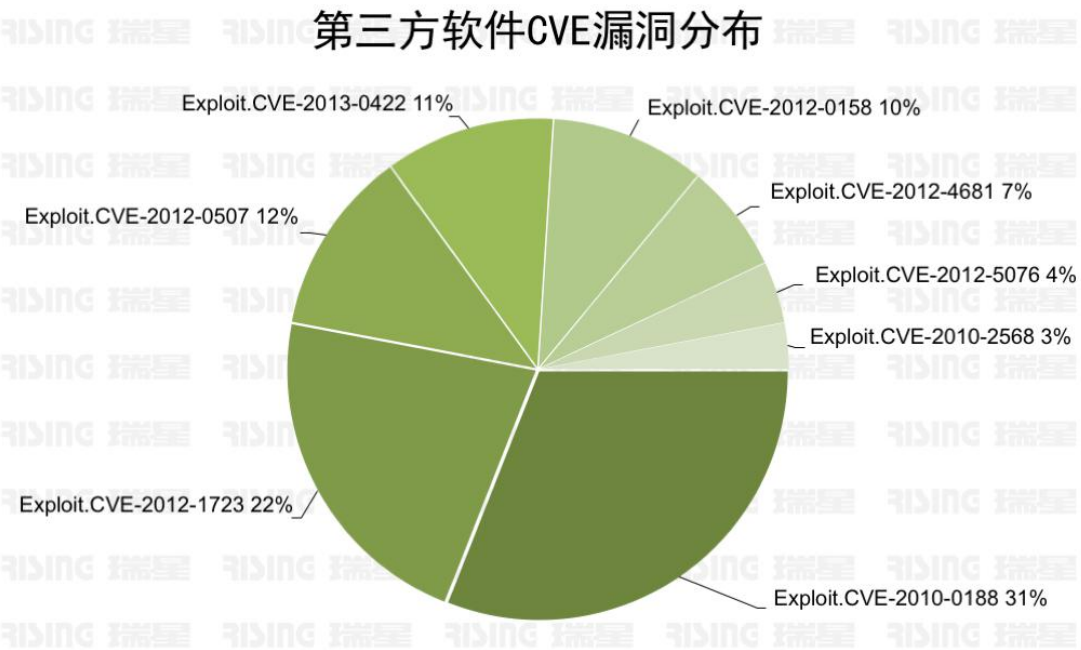

图 22：第三方软件 CVE 漏洞分布

由于企业软件开发大量采用 Java 编程，而 Oracle 官方已经停止对 Java 1.7 的维护，导致很多企业没有及时升级，存在着大量老式 CVE 漏洞。在 2016 年中利用 2015 年 CVE 漏洞最多的是对 Office 的攻击，主要为 CVE-2015-1641，CVE-2015-2545。

（四）2016 年全球网络安全事件 TOP10

2016年全球网络安全事件TOP10

1	Yahoo 邮箱十亿用户信息泄露
2	美国云存储服务Dropbox发生数据泄露事故
3	美国遭史上最大规模DDoS攻击、东海岸网站集体瘫痪
4	希拉里邮件门事件
5	物联网Mirai僵尸网络
6	乌克兰电网攻击事件
7	勒索软件侵袭
8	瑞士电信信息泄露
9	“脏牛”Linux通杀漏洞
10	GitHub 800 万用户信息泄露

图 23：2016 年全球网络安全事件 TOP10

（五）2016 年全球数据泄露事件 TOP10

2016年全球数据泄露事件TOP10

序号	安全事件	泄露数据量
1	MySpace信息泄露	3.6亿
2	LinkedIn信息泄露	1.7亿
3	VK.com信息泄露	9400万
4	美国云存储服务Dropbox发生数据泄露	6900万
5	雅虎十亿邮箱信息泄露	10亿
6	GitHub 800 万用户信息泄露	800万
7	俄罗斯网络服务门户yandex.ru信息泄露	1350万
8	全球招聘网站巨头PageGroup用户信息泄露	78万
9	Evony游戏公司3300万数据泄露	3300万
10	AdultFriendFinder数据泄露	4.12亿

图 24：2016 年全球十大数据泄露事件 TOP10

（六）2016 年全球网络安全事件解读

1.黑客攻击美国大选

在 2016 年中，黑客对美国大选进行了攻击干扰，通过攻击邮箱、投票机等设备，导致美国“邮件门”事件爆发，在 2016 年 6 月，维基解密泄露出几千封美国民主党委员会（DNC）被盗邮件。直至 7 月，维基解密共泄露 20000 多封被盗邮件和 29 段录音材料，间接性干扰了选民的决策。“邮件门”事件成为黑客攻击影响史上的里程碑。

2.NSA 方程式组织内部工具泄露

在 2016 年中，NSA 内部组织遭到网络攻击并泄露了大量的文件。在泄露的文件夹中 NSA 对全球进行网络攻击活动，其中包括了 32 个来自中国教育机构的域名，其他的主要为三大移动运营商以及部分电子科技企业和研究机构。从泄露的文件可以看出，NSA 对中国的科技和研究企业的网络安全攻击成为了企业的重灾区。

3.雅虎 10 亿数据泄露

雅虎作为一个全球知名搜索引擎，旗下的服务同样是多元化。雅虎邮箱作为老牌提供商，

用户量过亿。在 2016 年中，雅虎内部遭到网络攻击导致超过 10 亿的数据泄露，不仅对用户造成了不可挽回的影响，同样对雅虎自身也造成了不可估量的经济损失。

（七）安全建议

1. 实时关注漏洞公告，对漏洞的重要性及影响范围进行评估。
2. 企业内部软件资产评估，对于老旧的软件进行及时升级。
3. 建立合理的企业内部安全架构，定期进行安全评估。
4. 企业内部人员安全意识培训，避免遭到 APT 攻击。

四、趋势展望

（一）敲诈软件依然会是低成本高收益网络犯罪主流

敲诈软件在过去取得了巨大的“成功”，使得敲诈软件的种类、攻击范围、攻击目标越来越多，受害者数量也持续上升。同时，2016 年出现的敲诈软件中，充斥着大量使用了对称加密算法的变种，被它们加密的文件实际上是可以还原的。这类犯罪者，仅仅是想借 Locky/CryptXXX 等知名敲诈软件给人们带来 “文件无法解密还原”的主观判定，以更低的成本和技术难度，达到成功勒索的目的。

同时，敲诈软件似乎已经盯上了企业，同个人数据相比，企业数据显得更加重要，勒索成功率会大幅上升。为了遏制敲诈软件带来的危害，产品提供商、安全提供商、政府都在做出相应的努力。例如：安卓系统将采用新的机制来遏制锁屏（Trojan.SLocker）类敲诈软件的攻击，政府和安全厂商有都在尝试追踪比特币交易来定位犯罪者。未来，敲诈软件也一定会因为法律的震慑作用而有所收敛。

（二）IoT（物联网）安全隐患正在凸显

2016 年是 IoT（物联网）安全开始正式走进我们视野的一年，随着物联网的日渐成熟，IoT 的安全隐患正在凸显出来。

图 25：IOT 存在的安全隐患

诸如 2016 年的“物联网 Mirai 僵尸网络”、“乌克兰电网攻击事件”、“索尼摄像头后门事件”、“德国电信用户超 90 万台路由器遭黑客破坏”等多起安全事件，都说明了 IoT 安全的建设迫在眉睫，相对传统的传统的互联网安全，IoT 安全涉及范围更广，破坏力更大。

（三）全新的网络攻击模式——网络流量监控

在 NSA 泄露的工具中，从安全从业者角度来看是一个全新的网络攻击模式，他脱离了传统企业内部安全攻击，而是对运营商网络设备的攻击。在泄露的文件 Firewall 目录中涉及了思科，华为，Juniper 等知名厂商的产品，在 EXPLOITS 文件夹中，攻击脚本涉及了思科，天融信，Fortigate 等安全防火墙产品。NSA 通过对设备的网络攻击，将数据流量进行收集。对于这类利用安全产品自身的漏洞攻击手法，可以从海量数据中进行定向分析某一个企业网络活动，直接窥探企业内部安全。

专题 1：勒索软件年度分析报告

1. 什么是勒索软件？

勒索软件（也称密锁病毒）是一类以加密电脑和移动设备中用户文件为目的的恶意软件。用户一旦感染，用户设备中的各类文件将会被加密无法使用，用户必须按照恶意软的指示缴纳赎金才有可能解密文件。

2. 勒索软件历史

最早的一批勒索软件病毒大概出现在 8、9 年前，那时候的勒索软件作者还没有现在那么恶毒大胆，敲诈的形式还比较温和，主要通过一些虚假的电脑检测软件，提示用户电脑出现了故障或被病毒感染，需要提供赎金才能帮助用户解决问题和清除病毒，期间以 FakeAV 为主。

图 26：FakeAV 勒索截图

随着人们安全意识的提高，这类以欺骗为主的勒索软件逐渐的失去了它的地位，慢慢消失了。伴随而来的是一类 locker 类型的勒索软件。此类病毒不加密用户的数据，只是锁住用户的设备，阻止对设备的访问，需提供赎金才能帮用户进行解锁。期间以 LockScreen 家族占主导地位。由于它不加密用户数据，所以只要清除了病毒就不会给用户造成任何损失。由于这种病毒带来危害都能够很好的被解决，所以该类型的敲诈软件也只是昙花一现，很快也消失了。

LockScreen勒索截图

图 27：LockScreen 勒索截图

FakeAV 和 LockScreen 都因自身不足逐渐消失了，随之而来的是一种更恶毒的以加密用户数据为手段勒索赎金的敲诈软件。由于这类敲诈软件采用了一些高强度的对称和非对称的加密算法对用户文件进行加密，在无法获取私钥的情况下要对文件进行解密，以目前的计算水平几乎是不可能完成的事情。正是因为有这一点，该类型的勒索软件能够带来很大利润，各种家族如雨后春笋般出现了，比较著名的有 CTB-Locker、TeslaCrypt、CryptoWall、Cerber 等等。

Tesla勒索截图

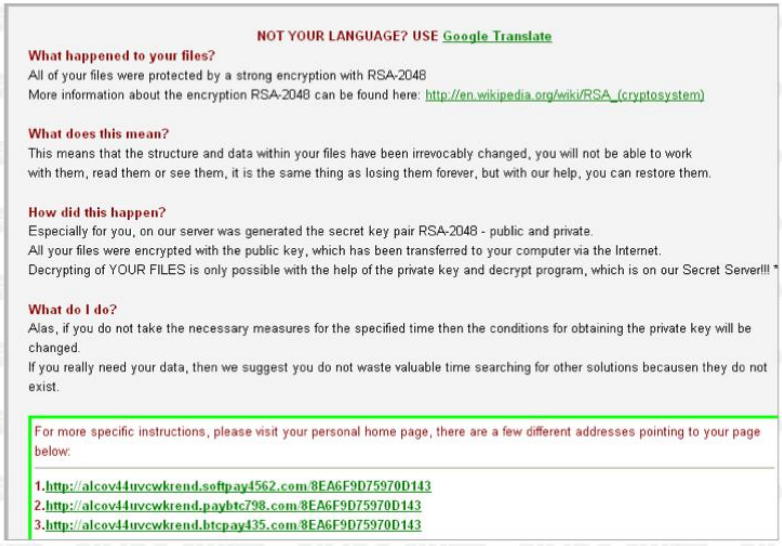

图 28：Tesla 勒索截图

3. 勒索软件的传播途径

1）垃圾邮件

勒索软件的传播途径和其他恶意软件的传播类似，垃圾邮件是最主要的传播方式。攻击者通常会用搜索引擎和爬虫在网上搜集邮箱地址，然后利用已经控制的僵尸网络向这些邮箱发有带有病毒附件的邮件。垃圾邮件投毒的方式有以下几种：

a. 附件中包含压缩包，压缩包中包含病毒的可执行程序和下载器。
b. 附件中包含压缩包，压缩包中包含有 js 脚本和 wsf 脚本等，运行脚本会从网上下载勒索软件的可执行程序或下载器执行。
c. 附件中包含压缩包，压缩包中包含 doc 文档，执行文档后会加载 doc 中的宏并运行，释放出脚本并执行，接着会下载勒索软件或下载器执行。

图 29：垃圾邮件传播

2）Exploit Kit

Exploit Kit 是一种漏洞利用工具包，里面集成了各种浏览器、Flash 和 PDF 等软件漏洞代码。攻击流程通常是：在正常网页中插入跳转语句或者使用诈骗页面和恶意广告等劫持用户页面，触发漏洞后执行 shellcode 并下载恶意病毒执行。常见比较著名的 EK 有 Angler、Nuclear、Neutrino 和 RIG 等。勒索软件也会利用 EK 去投毒，当用户机器没有及时打补丁的情况下被劫持到攻击页面的话，中毒的概率是比较高的。

3）定向攻击

定向攻击在勒索软件传播的过程中使用的也越来越多。攻击者有针对性的对某些互联网

上的服务器进行攻击，通过弱口令或者一些未及时打补丁的漏洞对服务器进行渗透，获得相应的权限后在系统执行勒索病毒，破坏用户数据，进而勒取赎金。

4.勒索软件家族种类

2016 年是勒索软件繁荣昌盛的一年，这一年出现了许多新的家族，也有很多老的家族从人们的视线中消失。整年中瑞星“云安全”系统截获的勒索家族有七十多种。其中以下几种在今年影响比较大。

1）Cerber

Cerber 家族是年初出现的一款新型勒索软件。从年初的 1.0 版本一直更新到现在的 4.0 版，是今年最活跃的勒索软件之一。传播方式主要是垃圾邮件和 EK 挂马。索要赎金为 1-2 个比特币。到目前为止加密过后的文件没有公开办法进行解密。

图 30：Cerber 勒索信息

2）Locky

Locky 家族也是 2016 年流行的勒索软件之一，和 Cerber 的传播方式类似，主要采用垃圾邮件和 EK。勒索赎金 0.5-1 个比特币。

图 31：Locky 勒索信息图

3）CryptoWall

CryptoWall 家族也是 2016 年较流行的一款勒索软件，勒索赎金 1.5 个比特币。最主要的传播方式是垃圾邮件和 EK 传播。垃圾邮件附件中通常包含一个 doc 文档，文档打开后会加载宏释放 wsf 文件并执行，从网上下载勒索病毒运行。

图 32：CryptoWall 勒索信息

4）TeslaCrypt

TeslaCrypt 是今年消失的一款勒索软件。其家族在 2015 年底到 2016 年初仍然大规模的传播。但是在 2016 年 5 月份，该家族幕后组织突然发布道歉声明宣布停止传播，并公布出一个主解密密钥。随即 TeslaCrypt 就慢慢淡出人们的视野了。

图 33：TeslaCrypt 关闭信息

5. 勒索软件受害人群

为了能够获取最大的利润，攻击者通常是不区分受害者对象的。就目前勒索软件最主要的传播途径来看，个人用户比企事业组织受害比例要高。随着各人市场攻击的饱和，必然会使攻击者转向企事业单位和政府组织，企事业面临的风险也会越来越大。

6. 勒索软件爆发原因

1）加密手段有效，解密成本高

勒索软件都采用成熟的密码学算法，使用高强度的对称和非对称加密算法对文件进行加密。除非在实现上有漏洞或密钥泄密，不然在没有私钥的情况下是几乎没有可能解密。当受害者数据非常重要又没有备份的情况下，除了支付赎金没有什么别的方法去恢复数据，正是因为这点勒索者能源源不断的获取高额收益，推动了勒索软件的爆发增长。

互联网上也流传有一些被勒索软件加密后的修复软件，但这些都是利用了勒索软件实现上的漏洞或私钥泄露才能够完成的。如 Petya 和 Cryptxxx 家族恢复工具利用了开发者软件实现上的漏洞，TeslaCrypt 和 CoinVault 家族数据恢复工具利用了 key 的泄露来实现的。

2）使用电子货币支付赎金，变现快追踪困难

几乎所有勒索软件支付赎金的手段都是采用比特币来进行的。比特币因为他的一些特点:匿名、变现快、追踪困难，在加上比特币名气大，大众比较熟知，支付起来困难不是很大而被攻击者大量使用。可以说比特币很好的帮助了勒索软件解决赎金的问题，进一步推动了勒索软件的繁荣发展。

3）Ransomware-as-a-server 的出现

勒索软件服务化，开发者提供整套勒索软件的解决方案，从勒索软件的开发、传播到赎金的收取都提供完整的服务。攻击者不需要任何知识，只要支付少量的租金及可租赁他们的服务就可以开展勒索软件的非法勾当。这大大降低了勒索软件的门槛，推动了勒索软件大规模爆发。

7.勒索软件幕后黑手

勒索软件的幕后黑手都有哪些呢。瑞星抽样分析了下 2016 年比较著名的勒索软件家族，统计了下他们的控制服务器(C&C)的地址和传毒地址。从统计结果中不难看出美国和俄罗斯不管是在控制服务器和传毒端都占有很大比例。

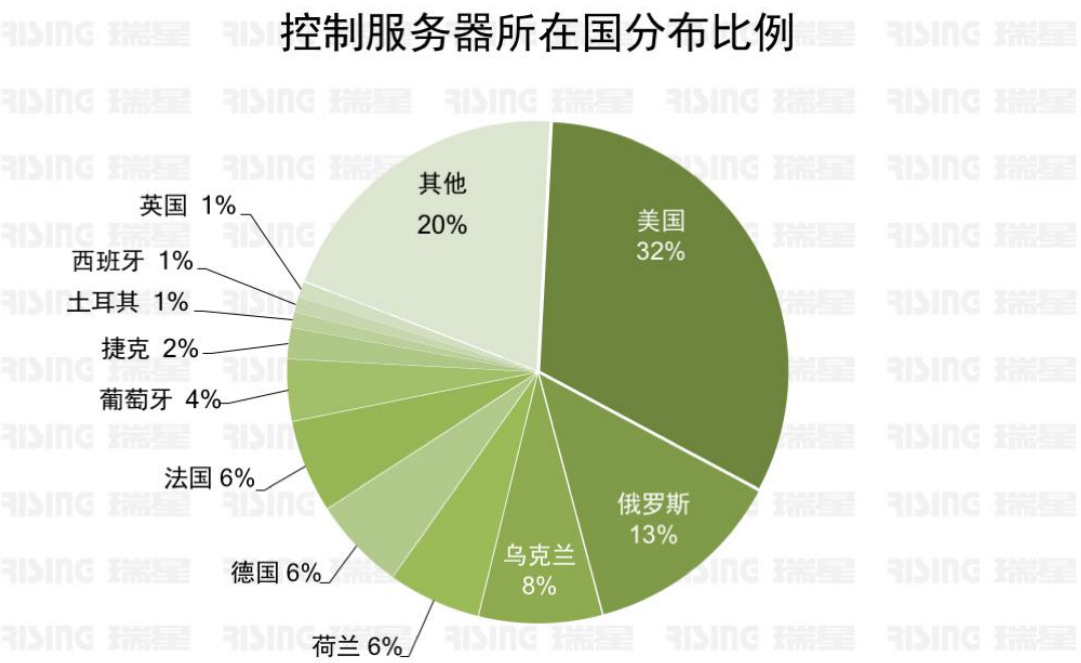

图 34：控制服务器所在国分布比例

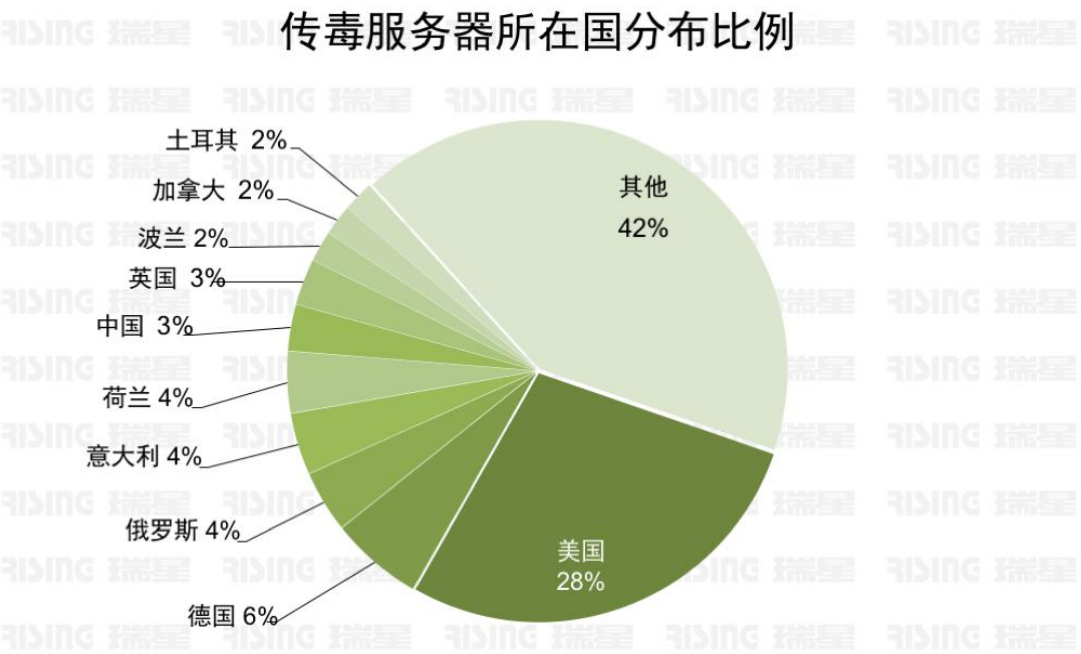

图 35：传毒服务器所在国分布比例

8. 勒索软件发展的新形势

2016 年是勒索软件繁荣发展的一年，在这一年里除了针对 Windows 系统勒索软件，针对 Linux、Mac OX 等勒索软件都已出现。同时移动平台 Android 和 IOS 系统也未能幸免。勒索软件为了躲避查杀不断发展，用上了各种手段。脚本 JS 开发、python 开发、Autoit 开发的勒索软件都在今年出现。2017 年注定还是勒索软件猖獗的一年。

1）现有各种平台仍将持续发展

由于勒索软件能够给攻击者带来巨额的利润，这种攻击手段在短时间内是不会消失的。各平台、各样式的勒索软件仍会繁荣发展。

2）针对企业等组织的攻击将越来越多

随着勒索软件在个人市场的竞争越来越激烈，必然会使越来越多的攻击转向针对企业。虽然针对企业的攻击要更高的技术水平和更长的时间，但是带来的回报也会更多。往往企业中的数据要比个人的数据更有价值。企业面对勒索软件的风险在未来也会越来越大。

3）物联网新兴设备受到的威胁增加

物联网在当下已经越来越普及，这部分设备受到攻击的风险也会越来越大。试想下当你下班回家打开智能电视，看到的不是精彩节目而是某某勒索软件的信息，当你准备发动汽车电子显示屏上显示的是交付赎金的勒索信息你该怎么办？这不是异想天开，这都是可能会发生的事情。

4）工控系统可能成为攻击对象

工控系统受到攻击的最著名的案例当属”震网“了，Stuxnet 蠕虫攻击伊朗核设施。当今的工业社会工控系统是如此普遍，如果他们受到勒索软件的攻击，带来的结果将是难以预料的。

9.瑞星给用户的建议

1）、定期备份系统与重要文件，并离线存储独立设备。
2）、使用专业的电子邮件与网络安全工具，可分析邮件附件、网页、文件是否包括恶意软件，带有沙箱功能。
3）、经常给操作系统、设备及第三方软件更新补丁。
4）、使用专业的反病毒软件、防护系统，并及时更新。
5）、设置网络安全隔离区，确保既是感染也不会轻易扩散。
6）、针对 BYOD 设置同样或更高级别的安全策略。
7）、加强员工（用户）安全意识培训，不要轻易下载文件、邮件附件或邮件中的不明链接。
8)、受感染后尽量不要给勒索者付赎金，不要去纵容勒索者，增加他们的收入去继续破坏更多的人。

专题 2：SEO 诈骗分析报告

1.概述

报告期内，瑞星安全专家在诈骗拦截的网址中发现一个极为可疑的 URL，随后对其进行了深入分析，分析过程中发现该网址不仅具有欺诈性质，而且还利用黑帽手段进行关键词排名推广。

黑客首先利用非法手段入侵正规政府或学校网站，在网站的其他目录下上传恶意文件，当受害者利用搜索引擎搜索到黑客设置的关键词时，就会弹出黑客预先修改过的“正规网站”，让受害者误以为是官方网站，从而导致用户上当受骗。

2.代码分析

通过拦截的诈骗网址进行代码分析，代码如下图：

钓鱼网址部分代码

图 36：诈骗网址部分代码

其中，我们抽取其中一段代码，可以看出，黑客隐藏了一段域名 body=GetHtml("h"&"tt"&"p:"&"/"&"/2"&"2"&"2."&"18"&"6"&"."&"43.1"&"0"&"9")，我们将其中的域名进行拼接，就可以看出该域名为：http://222.186.43.109。然后我们访问该域名，网站显示为客服服务中心，如下图：

诈骗网址页面

图 37：诈骗网址页面

查看最开始诈骗网址 http://www.vdsjg.top 的源文件时发现，黑客在 META 中设置了标

题为“〖余额宝转账到银行卡号上迟迟未到账怎么办〗__百度--知道”的关键字，以此来骗取搜索引擎收录与用户点击，如下图：

图 38：黑客在代码中设置关键字

代码中加载了 uaredirect.js 文件，访问 JS 文件经过加密处理，解密后发现加载了一个 URL 链接框架，其中 IP 与上面拼接的链接中 IP 地址相同，访问该 IP 连接与上面域名显示的页面一致，如下图：

图 39：加载的 URL 链接页面

加密代码中同时还存在一个流量统计的页面 http://js.users.51.la/17459262.js，该流量统计是用来统计页面的访问次数和访客的地区分布等信息。

通过技术分析得到了诈骗网站站长的账户名为 lllppp，网站的名称为“飞升云端”，统计 ID 为“17459262”。

图 40：站长信息

查询 IP：222.186.43.109 的归属地为江苏镇江。

图 41：IP 信息

对诈骗网站的域名进行分析，查询到域名联系人，联系方式，注册时间和过期时间等信息。

图 42：诈骗网站域名分析

继续深入查询，可以了解到注册人注册时所使用的姓名和联系方式，查询手机号码归属地为安徽，这里不排除注册者使用虚假的信息。

图 43：注册人电话信息

诈骗网站域名归属地为香港地区，一般非正规网站所使用服务器多数分布在海外地区。

图 44：IP 地址的地理位置

通过注册人邮箱查询出该注册人名下的其他域名，根据域名信息判断是同一时间注册的多个域名。

域名	注册者	邮箱	注册时间	过期时间
djkvs.top	dachun wei	llfdsgk@qq.com	2016-07-20	2017-07-20
vdsjg.top	wei da chun	llfdsgk@qq.com	2016-07-20	2017-07-20
vndjd.top	wei da chun	llfdsgk@qq.com	2016-07-20	2017-07-20

图 45：注册人名下其他域名

打开其中任意域名查看，发现同 http://www.vdsjg.top 网站内容相同。

图 46：其他域名页面

由此可以推断域名使用者利用关键词推广的形式进行支付宝诈骗，当网民在搜索引擎中输入支付宝客服，支付宝电话，支付宝客服电话，支付宝客服中心等关键词，就会出现诈骗者利用非法手段入侵入侵的网站所挂载的欺诈页面，而不知真相的用户很难对其进行辨别，如果拨打其网站所提供的电话，就会陷入诈骗者所设的圈套，一步步引诱骗取用户钱财。

3. 诈骗手段

整个诈骗过程人员划分可以分为受害者、非法攻击者、诈骗者。

首先，由非法攻击者对网站实施攻击，在获取网站的权限之后，将获取到的权限交给诈骗者，由诈骗者上传诈骗页面等待搜索引擎收录诈骗页面。

其次，受害者在某搜索引擎中搜索支付宝退款等相关关键词，搜索引擎会将诈骗网站提供给用户。

最后，受害者拨打诈骗网页中提供的客服联系方式，诈骗者利用各种手段骗取用户个人信息。

一般诈骗者会发给受害者一个可以退款的诈骗链接地址，要求受害者输入支付宝账号、银行卡等信息，并告诉受害者在一定的时间内就可以将钱退回到账户中。受害者输入完个人信息，诈骗者便会利用这些信息登陆受害者的支付宝账户或银行账户进行转账操作。

4. 防诈骗手段

1、认准官方网站，拨打官方所提供的客服电话。
2、请勿相信索取手机验证码的陌生电话或短信。
3、不要点击以短信、微信等通信方式发来的退款、转账链接。

专题 3：不法分子如何利用伪基站盈利

1. 伪基站简介

“伪基站”即假基站，设备一般由主机和笔记本电脑组成，通过短信群发器、短信发信机等相关设备，能够搜取以其为中心、一定半径范围内的手机卡信息，利用移动通信的缺陷，通过伪装成运营商的基站，冒用他人手机号码强行向用户手机发送诈骗、广告推销等信息。

2. 伪基站组织结构

伪基站的组织结构包括木马程序开发者、伪基站短信发送者、垃圾邮件发送者、诈骗者、

中介或下线组成。

图 47：伪基站组织结构

3. 伪基站运作流程

伪基站首先由诈骗者购买硬件设备进行伪基站部署，然后程序开发者开发伪基站需要的 web 框架平台或应用程序，然后通过域名运营商购买大量域名进行诈骗工作，这些域名周期都是非常短，一般周期为 1-7 天，然后将诈骗程序搭建起来，一般常用的几套诈骗源码为建设银行诈骗、工商银行诈骗、QQ 安全中心诈骗、中国移动诈骗、中国好声音中奖诈骗等。

诈骗者通过雇佣其他人员携带伪基站在街道和小区周边进行大范围发送诈骗短信、广告、诈骗网址，木马 APK 程序等，同时也以邮箱的形式进行发送事先部署好的诈骗网址，通过诈骗网址来获取网民的个人信息、银行卡、支付账户等，诈骗者在收信平台对诈骗网址获取到的信息进行整理和验证。

诈骗者寻找合作方或中介，将整理出来的信息进行变现操作，通过购买大量黑卡进行洗钱，将可用账户中的金额进行消费变现，然后转账到黑卡账户中。

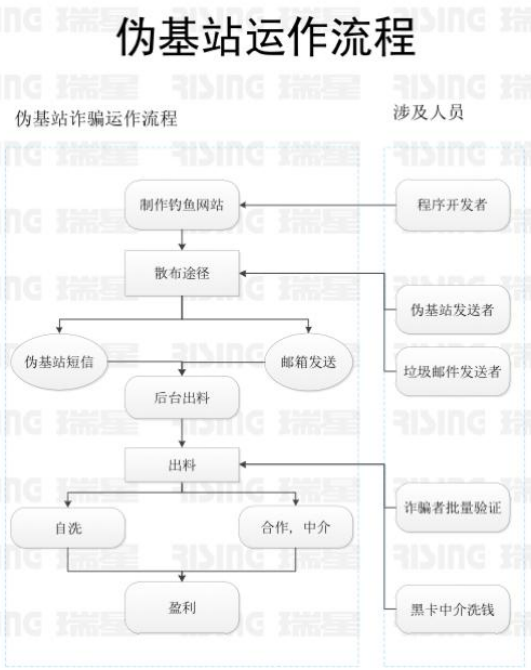

图 48：伪基站运作流程

名词解释：

制作网站：有专人抢注类似于运营商，各大银行机构的域名进行出售或自己用，有专业的人员进行仿站模仿类似于运营商、各个银行的网站，然后购买美国或者香港免备案服务器进行搭建后制作过域名拦截程序。

木马制作：由程序开发人员进行开发后，以几千元不等的价格将源码卖给下级代理进行二次开发出售（根据各大杀毒库的更新情况制作“免杀”），以每周 2000 元进行出售。

伪基站发送诈骗短信：这个一般为线下交易，包吃包住包油钱以每小时 500 元左右为酬劳或以合作分成的方式，让有伪基站设备的人带着伪基站游走在繁华的街区进行大范围的撒网（发送诈骗网站）。

“出料”：将诈骗网站后台收到的数据进行筛选整理（利用各个银行的在线快捷支付功能情况查余额，看看是否可以直接消费进行转账或第三方支付进行消费），自己无法将余额消费的将会以余额的额度以不同的价格出售（大部分会打包起来以每条 1 元的价格进行多次叫卖）余额巨大的有时还会找人合作进行“洗料”。

“洗料”：通过多种方式将“料”进行变现，一般开通快捷支付充值水电、话费、游戏币或者利用其他存在第三方支付转账接口和银行快捷支付漏洞等，将“四大件”变成成现金后通过各种规避追查的手段与合伙人按比例（一般以料的额度按 5：5、 4：6 、3：7 这些比例）进行分账，日均可以赚取 10 万元以上。

4.伪基站影响、危害

（1）诈骗网站涉及行业分布

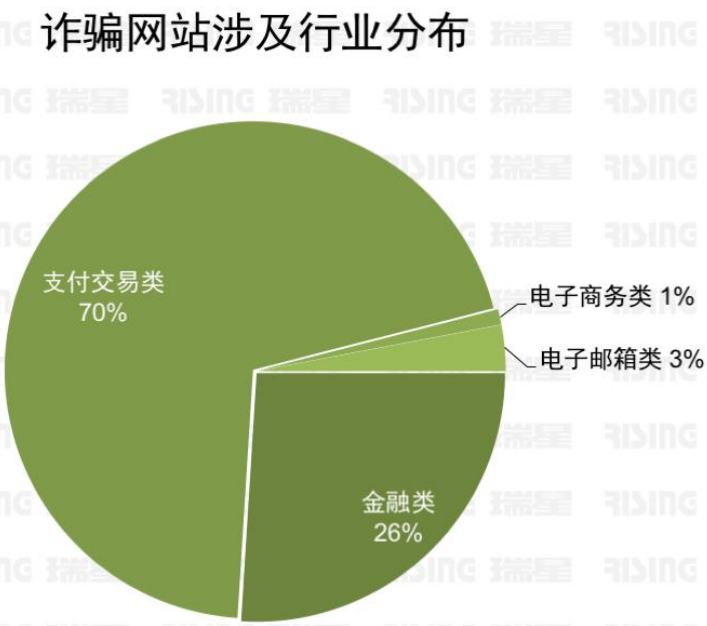

图 49：诈骗网站涉及行业分布

（2）诈骗网站影响的银行分布

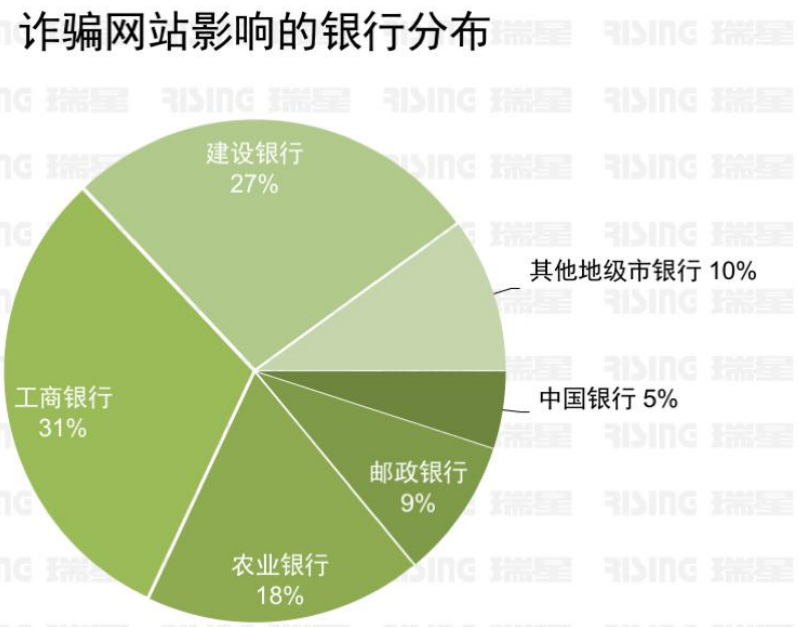

图 50：诈骗网站影响的银行分布

（3）伪基站受害人群年龄分布

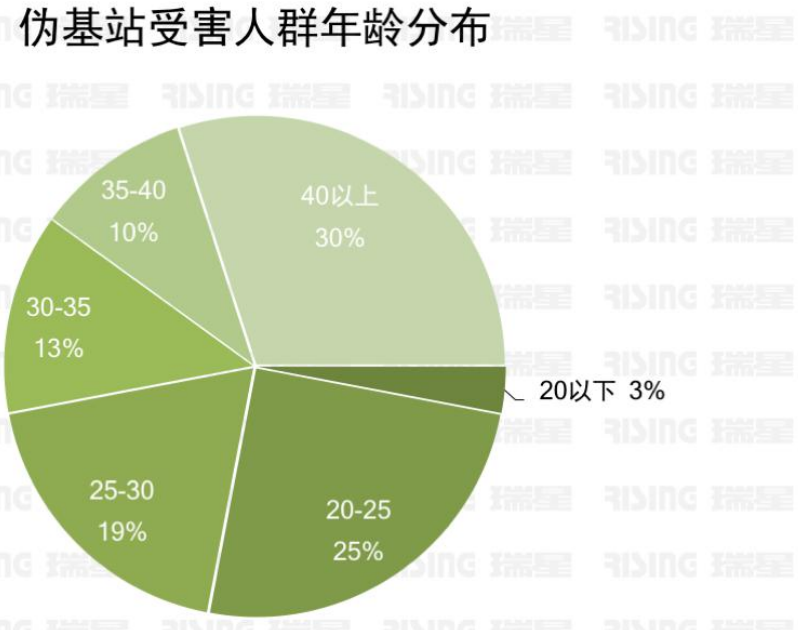

图 51：伪基站受害人群年龄分布

5.伪基站危害：

1、“伪基站”运行时用户手机信号被强制连接到该设备上，无法正常使用运营商提供的服务，手机用户一般会暂时脱网 8-12 秒后恢复正常，部分手机用户则必须开关机才能重新入网。此外，“伪基站”还会导致手机用户频繁地更新位置，使得该区域的无线网络资源紧张并出现网络拥塞现象，影响用户的正常通信。

2、“伪基站”盗用公众无线电通信运营商的频率资源，其大功率发射对周边电磁环境造成强烈干扰。

3、发送病毒短信，机主一旦不慎点击，轻则手机被植入木马病毒，发生手机资费被恶意消耗，被恶意广告骚扰等后果，重则会记录网友在该诈骗网页中输入的任何信息，如涉及银行卡号密码、支付账号密码等，有可能造成财产损失。

6. 伪基站相关数据

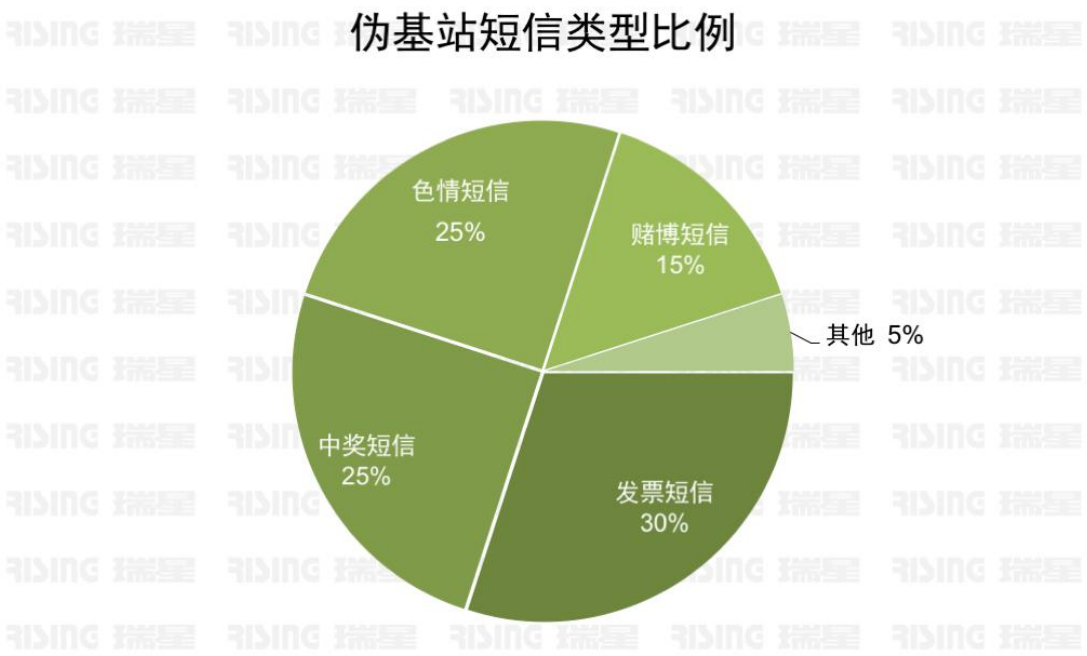

图 52：伪基站短信类型比例

7. 伪基站防范建议

1. 收到可疑短信及时向官方客服电话确认。
2. 收到陌生短信不打开链接，不下载，不安装。
3. 公共场所不使用来历不明的 WIFI 热点。
4. 任何场所下不轻易泄露个人任何信息。
5. 手机安装安全防护软件、定期清理垃圾、查杀木马病毒。

专题 4：2016 路由安全分析

1、概述

路由安全一直是网络安全里的热门事件，几乎所有路由品牌都曝出过漏洞，黑客正是利用这些漏洞对用户的路由进行入侵和劫持，将用户访问的网站定向到诈骗网站，然后盗取用户个人隐私，如果是企业级路由被黑客攻击，将会造成更大的影响。

2、德国电信断网事件

2016 年 11 月德国电信遭遇了一次大范围的网络故障，这次攻击致使多达 90 万宽带用户和 2000 万固定电话用户遭遇了网络中断，中断时间从星期日一直持续到星期一。事件发生后，德国电信连夜与设备供应商生成了新的升级包，并且要求客户如果怀疑受到影响就断电重启路由器，之后利用自动或手动的升级过程来减轻问题。

德国电信还采取了一系列的过滤措施来保证升级过程不受攻击影响。德国电信经过调查发现，此次攻击和此前攻击美国网络的恶意软件 Mirai 存在必然联系，此次攻击同样是从路由器和网络摄像头发起导致德国电信的服务器流量飙升，从而使正常的网络不堪重负。

3、各品牌路由器漏洞情况

截止到 2016 年底包括 D-link、TP-link、Cisco、斐讯、iKuai 等一众国内外知名品牌都相继爆出了高危漏洞，影响上万用户的网络安全，以下是 2016 年中国用户最关注的的路由器品牌占比，以及根据 exploits-db 披露的各品牌路由器漏洞比例。

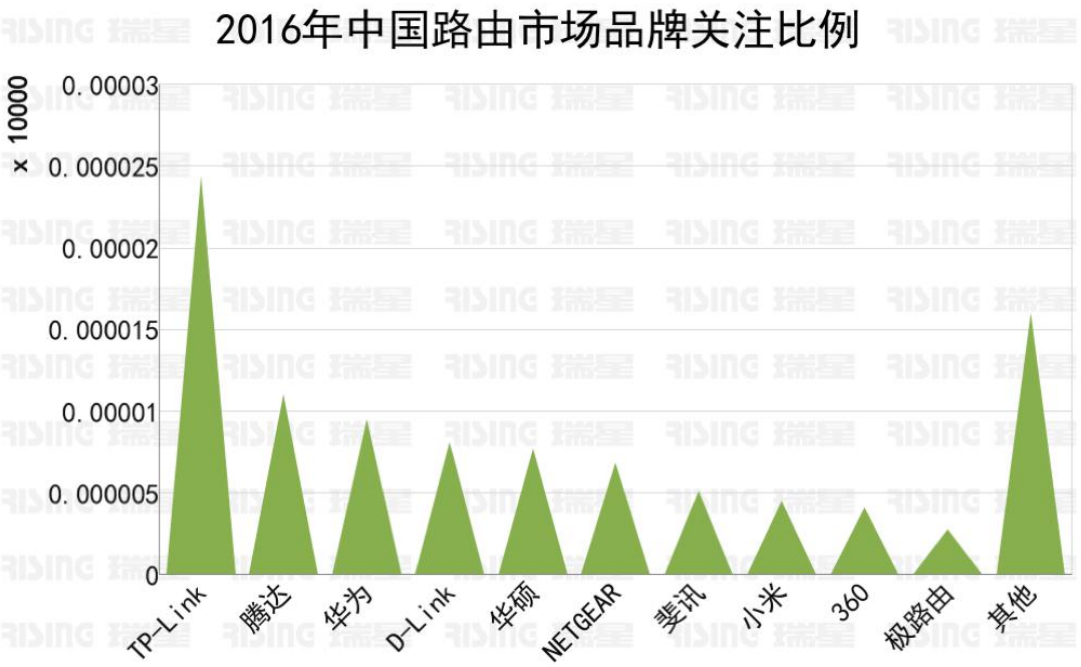

图 53：2016 年中国路由市场品牌关注比例

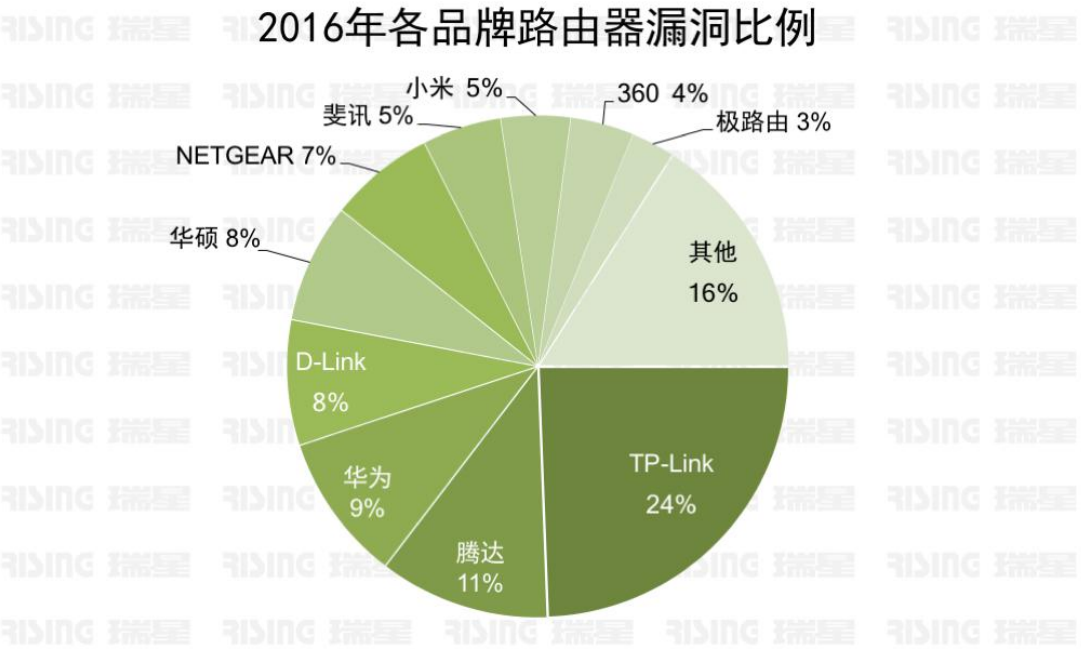

图 54：2016 年各品牌路由器漏洞比例

4、2016 年路由器漏洞类型——僵尸网络成爆发性增长

2016 年路由器漏洞类型包括默认口令、固件漏洞、路由后门等一系列安全问题。通过对 2016 年相关路由器事件进行统计，各种攻击方式中弱口令占比最多，也使得今年的僵尸网络呈现了爆发性的增长。

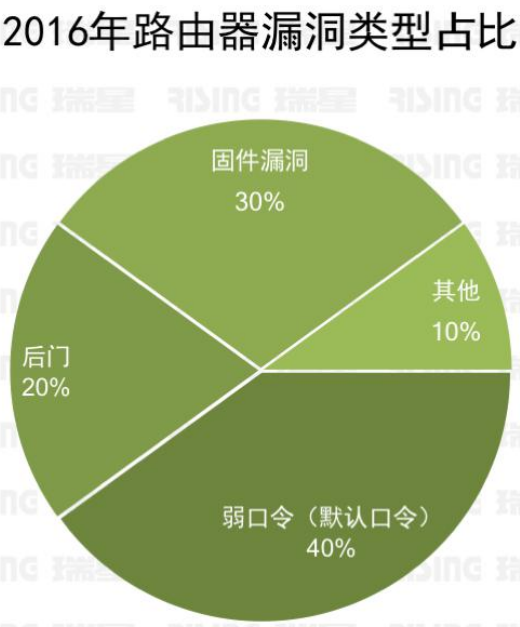

图 55：2016 年路由器漏洞类型占比

当路由器开始使用并运行后，如果用户没有修改设备的默认登录口令，或是因为某些原因将设备的口令设置的极其简单，使得攻击者可以针对这些路由器进行暴力破解，轻而易举的进入设备的管理界面。

然后，攻击者就可以向路由器植入恶意代码，并使之与攻击者的 C&C（远程命令）服务器通讯，将设备变成僵尸网络中的一员。而这些僵尸网络主要以发动 DDos 攻击为主，或作为代理对其他设备进行暴力破解，威胁网络安全。此前威胁美国、新加坡以及德国网络安全的都属于僵尸网络。

2016年中国路由器弱密码TOP10

用户名	密码
admin	admin
admin	12345
root	pass
admin	1234
admin	passwrord
admin	smcadmin
admin	admin1234
admin	123456
guest	12345
Administrator	admin

图 56：2016 年中国路由器弱密码 TOP10

5、提高网民安全意识，加固用户名密码安全

对于像 mirai 这样的僵尸网络，目前还没有十分奏效的方法加以遏制，现在主要采用蜜罐技术通过行为特征分析，在僵尸网络形成的初期发现并采取相关措施。

由于僵尸网络的特性就是控制大量“肉鸡”，所以对于用户来说，就是提高自身的安全意识，修改初始密码以及弱密码，加固用户名和密码的安全性，督促行业对密码策略的进一步加强。