2016 年我国互联网网络安全态势综述

国家计算机网络应急技术处理协调中心

2017 年 4 月

目　录

前　言

2016 年，是我国在网络空间法制化进程迈出实质性步伐的一年，《网络安全法》正式表决通过和《国家网络空间安全战略》正式发布进一步强化了我国网络安全顶层设计，为实现我国网络强国战略保驾护航。习近平总书记“419”等一系列讲话明确要求树立正确的网络安全观，为网络安全工作指明了主攻方向和行动理念。

《中华人民共和国国民经济和社会发展第十三个五年规划纲要》（以下简称“十三五规划”）发布，明确提出实施网络强国战略，要求加快建设数字中国，推动信息技术与经济社会发展深度融合，加快推动信息经济发展壮大。2016 年，作为“十三五规划”开局之年，网络经济空间发展大幅拓展趋势明显，推动信息技术服务向更为智能、与传统领域全面融合的阶段发展。然而，信息技术创新发展伴随的安全威胁与传统安全问题相互交织，使得网络空间安全问题日益复杂隐蔽，面临的网络安全风险不断加大，各种网络攻击事件层出不穷。2016 年，我国互联网网络安全状况总体平稳，未出现影响互联网正常运行的重大网络安全事件，但移动互联网恶意程序数量持续高速上涨且具有明显趋利性；来自境外的针对我国境内的网站攻击事件频繁发生；联网智能设备被恶意控制，并用于发起大流量分布式拒绝服务攻击的现象更加

严重；网站数据和个人信息泄露带来的危害不断扩大；欺诈勒索软件在互联网上肆虐；具有国家背景黑客组织发动的高级持续性威胁(APT)攻击事件直接威胁了国家安全和稳定。

国家互联网应急中心（以下简称“CNCERT”）在对我国互联网宏观安全态势监测的基础上，结合网络安全预警通报、应急处置工作实践成果，着重分析和总结了 2016 年我国互联网网络安全状况，并预测 2017 年网络安全热点问题。

一、2016 年我国互联网网络安全监测数据分析

CNCERT 持续对我国网络安全宏观状况开展抽样监测，2016 年，移动互联网恶意程序捕获数量、网站后门攻击数量以及安全漏洞收录数量较 2015 年有所上升，而木马和僵尸网络感染数量、拒绝服务攻击事件数量、网页仿冒和网页篡改页面数量等均有所下降。

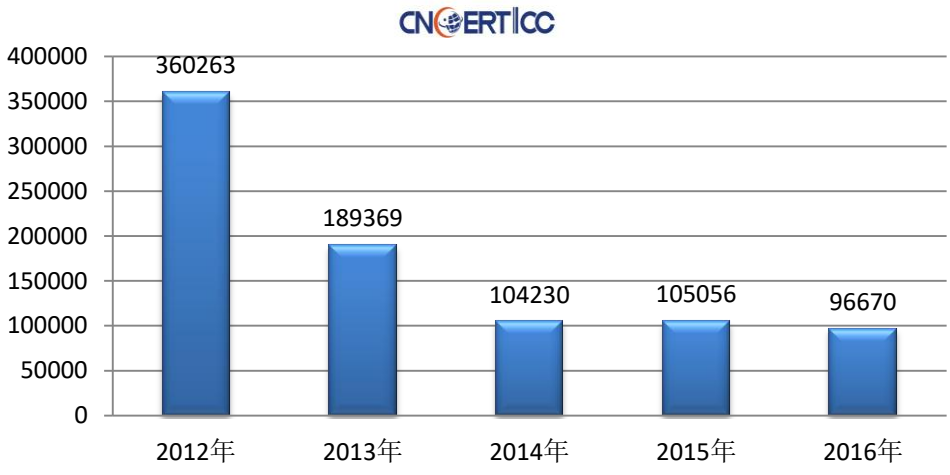
（一）木马和僵尸网络

据抽样监测，2016 年约 9.7 万个木马和僵尸网络控制服务器控制了我国境内 1699 万余台主机，控制服务器数量较 2015 年下降 8.0%，境内感染主机数量较 2015 年下降了 14.1%。。其中，来自境外的约 4.8 万个控制服务器控制了我国境内 1499 万余台主机，来自美国的控制服务器数量居首位，其次是中国香港和日本。就所控制我国境内主机数量来

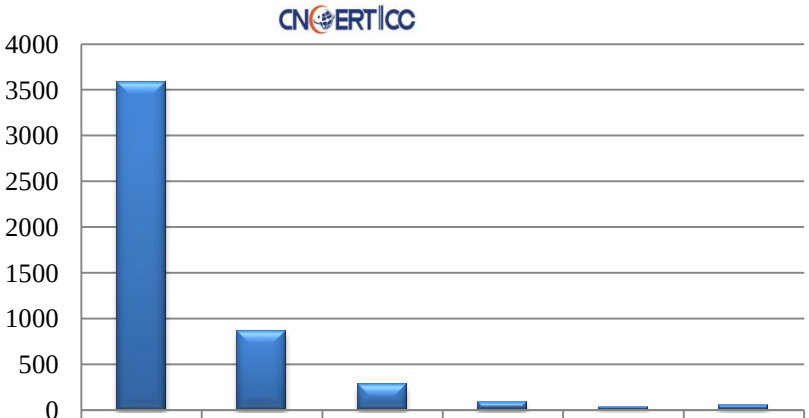
看，来自美国、中国台湾和荷兰的控制服务器控制规模分列前三位，分别控制了我国境内约 475 万、182 万、153 万台主机。在监测发现的因感染恶意程序而形成的僵尸网络中，规模在 100 台主机以上的僵尸网络数量 4896 个，其中规模在 10 万台以上的僵尸网络数量 52 个。

从我国境内感染木马和僵尸网络主机按地区分布数量分析来看，排名前三位的分别是广东省（占我国境内感染数量的 13.4%）、江苏省（占 9.2%）和山东省（占 8.3%）。为有效控制木马和僵尸网络感染主机引发的危害，2016 年，在工业和信息化部指导下，根据《木马和僵尸网络监测与处置机制》，CNCERT 组织基础电信企业、域名服务机构等成功关闭 1011 个控制规模较大的僵尸网络。

2012年至2016年木马和僵尸网络控制端数量对比

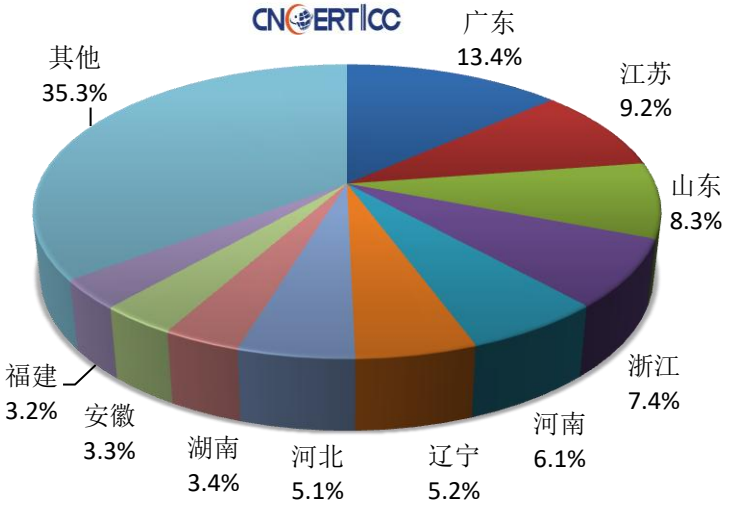


2016年僵尸网络的规模分布



	100-1000	1000-5000	5000-20000	2-5万	5-10万	>10万
僵尸网络数目	3578	865	279	90	32	52

2016年境内木马或僵尸程序受控主机数量按地区分布



（二）移动互联网安全

1. 移动互联网恶意程序捕获情况

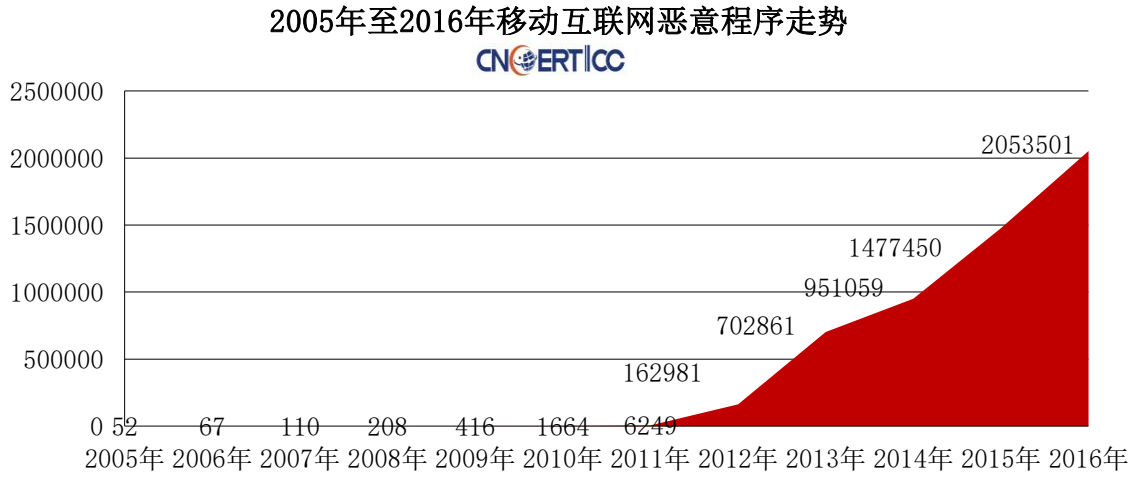
2016 年，CNCERT 通过自主捕获和厂商交换获得移动互联网恶意程序数量 205 万余个，较 2015 年增长 39.0%，近 7 年来持续保持高速增长趋势。按其恶意行为进行分类，前三

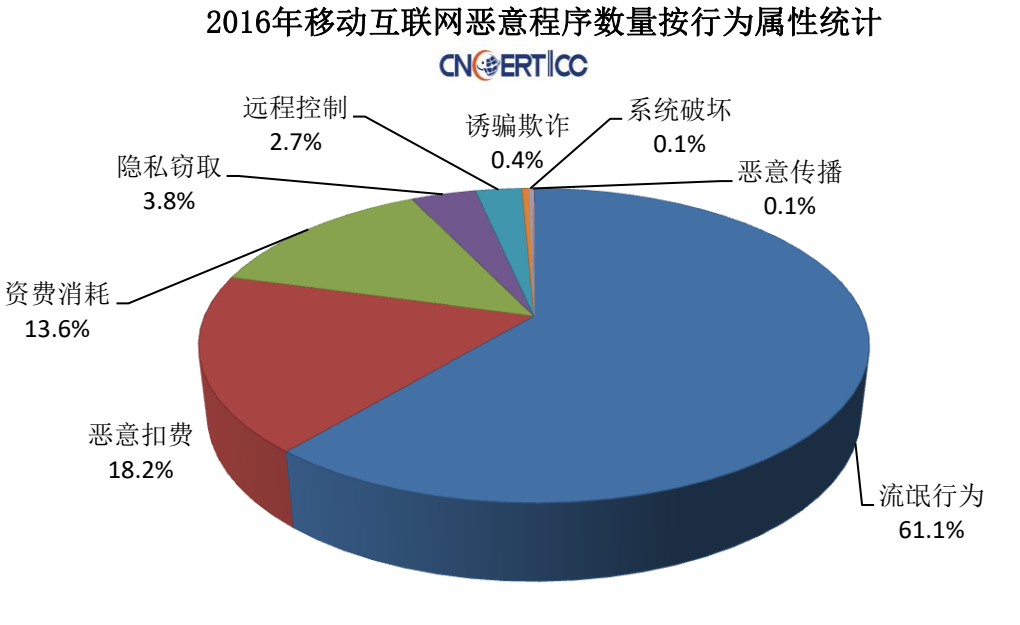
位分别是流氓行为类、恶意扣费类和资费消耗类[1]，占比分别为 61.1%、18.2%和 13.6%。CNCERT 发现移动互联网恶意程序下载链接近 67 万条，较 2015 年增长近 1.2 倍，涉及的传播源域名 22 万余个、IP 地址 3 万余个，恶意程序传播次数达 1.24 亿次。

2016 年，CNCERT 重点对通过短信传播，且具有窃取用户短信和通信录等恶意行为的“相册”类[2]安卓恶意程序及具有恶意扣费、恶意传播属性的色情软件进行监测，并开展协调处置工作。全年共发现此类恶意程序 47316 个，累计感染用户超过 101 万人，用于传播恶意程序的域名 6045 个，用于接收用户短信和通讯录的恶意邮箱账户 7645 个，用于接收用户短信的恶意手机号 6616 个，泄露用户短信和通讯录的邮件 222 万封，严重危害用户个人信息安全和财产安全。在工业和信息化部指导下，根据《移动互联网恶意程序监测与处置机制》，CNCERT 组织邮箱服务商、域名注册商等积极开展协调处置工作，对发现的恶意邮箱账号、恶意域名等进行关停处置。

[1] 分类方法参照通信行业标准《移动互联网恶意程序描述格式》（YD/T2439-2012）。

[2] “相册”类安卓恶意程序是指一类针对安卓系统的，主要通过短信进行传播的移动互联网恶意程序，黑客通过发送带有恶意程序下载链接的短信，诱骗用户点击安装，导致感染手机的个人信息泄露。

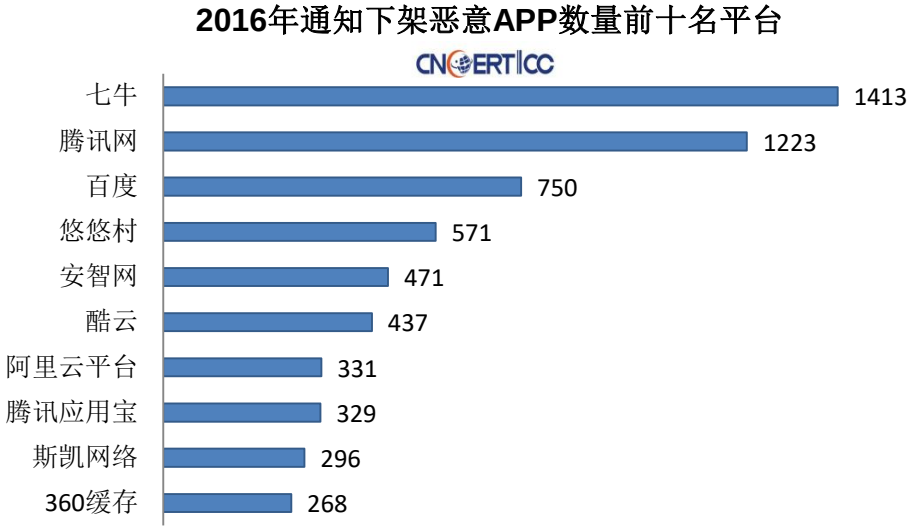




2. 移动互联网恶意 APP 监测情况

目前，移动互联网 APP 传播途径多样，包括应用商店、网盘、云盘和广告宣传等平台，且大量的未备案网站也在提供 APP 下载服务。在工业和信息化部指导下，经过连续 4 年的治理，要求国内的应用商店、网盘、云盘和广告宣传等平台积极落实安全责任，不断完善安全检测、安全审核、社会监督举报、恶意 APP 下架等制度，积极参与处置响应与反

馈，严格控制恶意 APP 传播途径。2016 年，CNCERT 累计向 141 家已备案的应用商店、网盘、云盘的广告宣传等网站运营者通报恶意 APP 事件 8910 起，较 2015 年减少了 47.8%，表明在移动互联网恶意程序持续快速增长的情况下，恶意 APP 在正规网站上传播的途径得到有效控制，但通过非正规应用商店途径传播恶意 APP 的数量还在继续增长。



（三）拒绝服务攻击

2016 年，CNCERT 牵头组织通信行业和安全行业单位，宣布成立了中国互联网网络安全威胁治理联盟，并着力开展分布式拒绝服务攻击（以下简称“DDoS 攻击”）防范打击工作。经过协同治理，有效缓解了 DDoS 攻击的危害，2016 年 CNCERT 监测到 1Gbps 以上 DDoS 攻击事件日均 452 起，比 2015 年下降 60%。但同时发现，2016 年大流量攻击事件数量全年持续增加，10Gbps 以上攻击事件数量第四季度日均攻

击次数较第一季度增长 1.1 倍，全年日均达 133 次，占日均攻击事件的 29.4%，另外 100Gbps 以上攻击事件数量日均达到 6 起以上，并监测发现某云平台多次遭受 500Gbps 以上的攻击。从攻击目的来看，67%涉及互联网地下黑色产业链；从攻击方式来看，反射攻击依旧占据主流；从攻击源 IP 地址对应设备来看，除了传统的 PC“肉鸡”和 IDC 服务器外，智能设备也逐渐被利用为 DDoS 攻击工具。

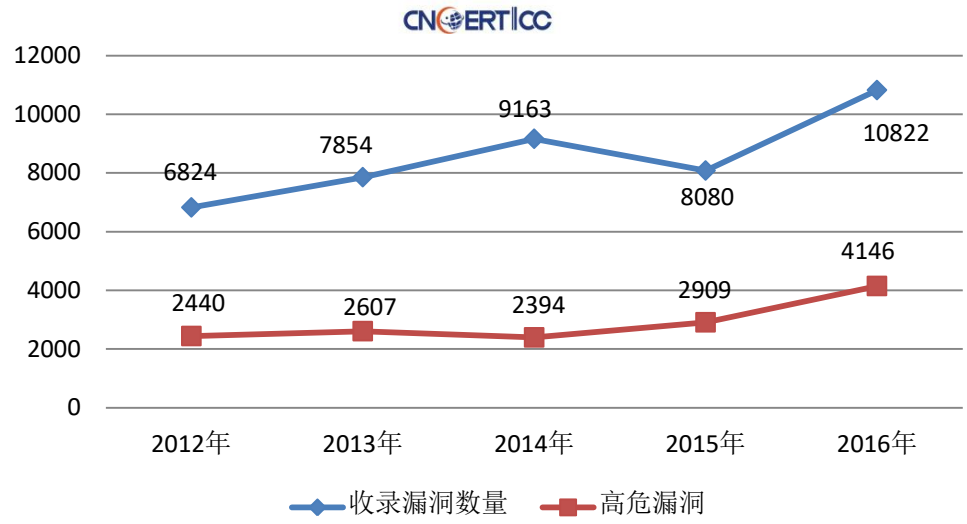
（四）安全漏洞

2016 年，国家信息安全漏洞共享平台（CNVD）共收录通用软硬件漏洞 10822 个，较 2015 年增长 33.9%。其中，高危漏洞收录数量高达 4146 个（占 38.3%），较 2015 年增长 29.8%；“零日”漏洞[3]2203 个，较 2015 年增长 82.5%。漏洞主要涵盖 Google、Oracle、Adobe、Microsoft、IBM、Apple、Cisco、Wordpress、Linux、Mozilla、Huawei 等厂商产品，其中涉及 Google 产品（含操作系统、手机设备以及应用软件等）的漏洞最多，达到 819 个，占全部收录漏洞的 7.6%；按影响对象类型分类，应用程序漏洞占 59.97%，Web 应用漏洞占 16.8%，操作系统漏洞占 13.2%，网络设备漏洞（如路由器、交换机等）占 6.47%，数据库漏洞占 1.97%，安全产品漏洞（如防火墙、入侵检测系统等）占 1.59%。2016 年，CNVD

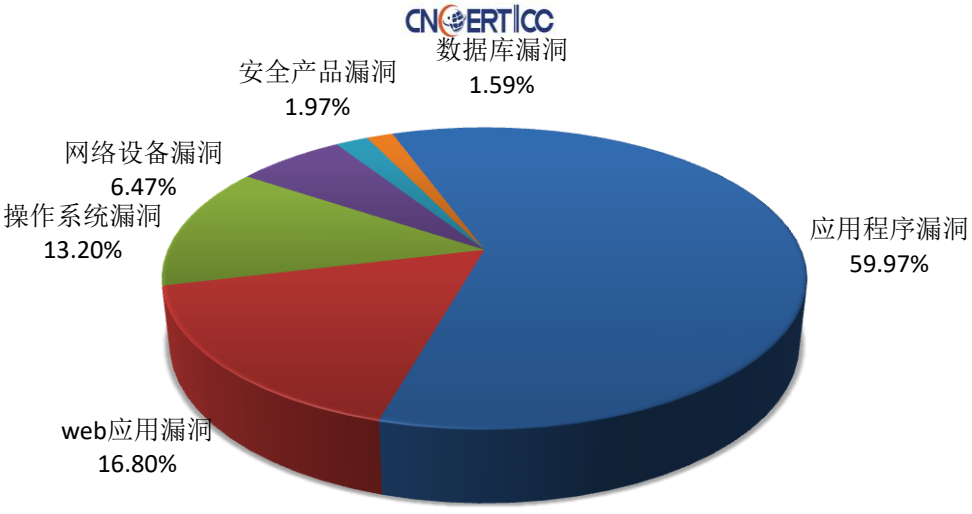
[3] CNVD 收录时还未公布补丁。

加强了原创通用软硬件漏洞的收录工作，成为全年漏洞收录数量的一个新增长点，全年接收白帽子、国内漏洞报告平台、安全厂商等报送相关漏洞 1926 个，占全年收录总数的 17.8%。

2012年至2016年CNVD收录漏洞数量对比



2016年CNVD收录漏洞按影响对象类型分类统计



表：2016 年 CNVD 收录漏洞涉及厂家情况统计

漏洞涉及产品	漏洞数量（单位：个）	占全年收录数量百分比
Google	819	7.6%
Oracle	689	6.4%
Adobe	561	5.2%
Microsoft	522	4.8%
IBM	500	4.6%
Apple	439	4.1%
Cisco	356	3.3%
Wordpress	233	2.2%
Linux	218	2.0%
Mozilla	183	1.7 %
Huawei	155	1.4%
其他	6147	56.8%

CNVD 对现有漏洞进行了进一步整理，建立了基于重点关注方向的子漏洞库，目前已建立有移动互联网、电信行业、电子政务和工业控制系统 4 类子漏洞库。2016 年这 4 类子漏洞库分别收录漏洞 985 个（占 9.1%）、640 个（占总收录比例 5.9%）、344 个（占 3.1%）和 172 个（占 1.5%）。

表：2016 年重点关注方向的子漏洞库漏洞数量收录情况统计

子漏洞库	收录漏洞数量（单位：个）	占全年收录数量百分比
移动互联网子漏洞库	985	9.1%
电信行业子漏洞库	640	5.9%
电子政务子漏洞库	344	3.1%
工业控制系统子漏洞库	172	1.5%

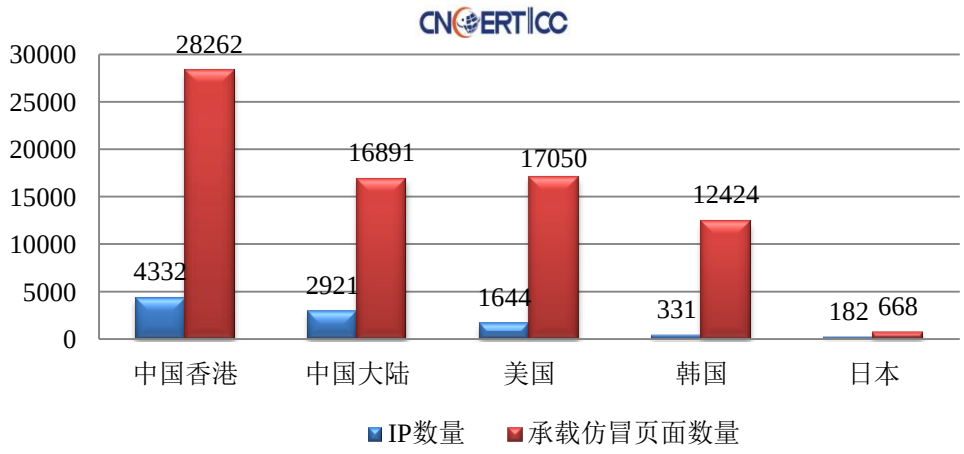
CNVD 针对重点关注方向子漏洞库的安全漏洞影响情况进行巡查，全年通报涉及政府机构、重要信息系统部门以及行业安全漏洞事件 24246 起，较 2015 年上升 3.1%。

（五）网站安全

1. 网页仿冒

2016 年，CNCERT 监测发现约 17.8 万个针对我国境内网站的仿冒页面，页面数较 2015 年下降 3.6%。约 2 万个 IP 地址承载了上述仿冒页面，其中位于境外的 IP 地址占 85.4%。从承载的仿冒页面数量来看，来自中国香港的数量最多，4332 个 IP 地址共承载了仿冒页面 2.8 万余个，其次是中国大陆和美国，承载的仿冒页面均约 1.7 万个。为有效防止网页仿冒引起的网民经济损失，CNCERT 重点针对金融行业、电信行业网上营业厅的仿冒页面进行重点处置，全年共协调处置仿冒页面 52836 个。从处置的页面类型来看，积分兑换和用户登录仿冒页面数量最多，分别占处置总数的 32%。从承载仿冒页面 IP 地址归属情况来看，绝大多数 IP 地址位于境外，主要分布在中国香港、美国及中国台湾，其中位于中国香港的 IP 地址超过境外总数的一半。针对跨境仿冒页面的处置，CNCERT 继续与国际网络安全组织加强合作，全年协调境外安全组织处置跨境网页仿冒事件 14515 起。

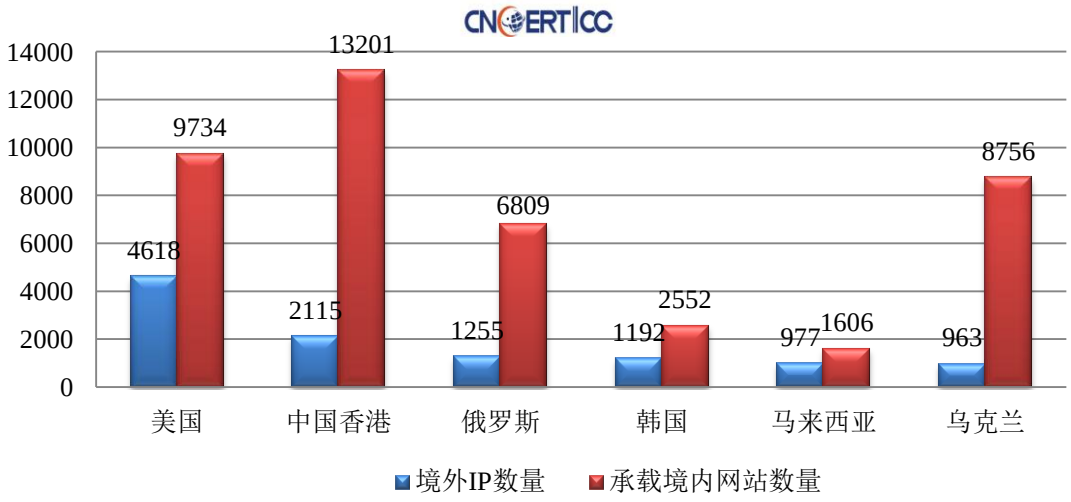
2016年仿冒境内网站的境外IP地址及其承载的仿冒页面数量
按国家或地区分布TOP5



2. 网站后门

2016 年，CNCERT 监测发现约 4 万个 IP 地址对我国境内 8.2 万余个网站植入后门，网站数量较 2015 年增长 9.3%。境外有约 3.3 万个（占全部 IP 地址总数的 84.9%）IP 地址通过向网站植入后门对境内约 6.8 万个网站进行远程控制。其中，来自美国的 IP 地址最多，占比 14.0%，其次是来自中国香港和俄罗斯的 IP 地址。从控制我国境内网站总数来看，来自中国香港的 IP 地址控制数量最多，有 1.3 万余个，其次是来自美国和乌克兰的 IP 地址，分别控制了 9734 个和 8756 个网站。

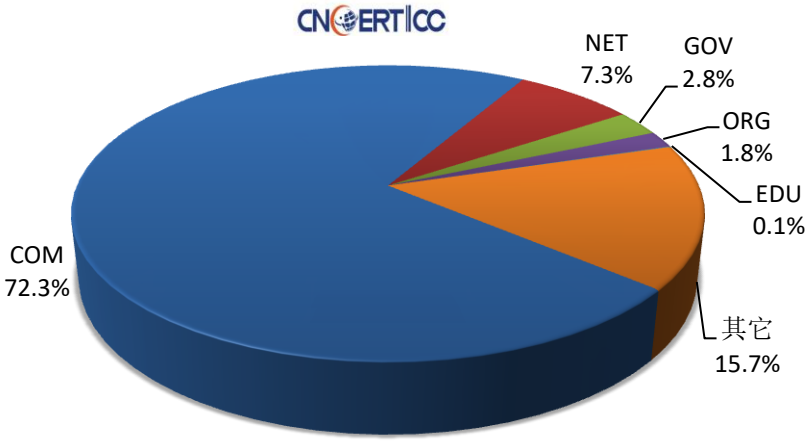
2016年境外向我国境内网站植入后门IP地址所属国家或地区TOP6



3. 网页篡改

2016 年，CNCERT 监测发现，我国境内约 1.7 万个网站被篡改，较 2015 年减少 31.7%，其中被篡改政府网站有 467 个，较 2015 年减少 47.9%。从网页篡改的方式来看，被植入暗链的网站占全部被篡改网站的比例高达 86%，是我国境内网站被篡改的主要方式。从境内网页被篡改类型分布来看，以.com 为后缀的商业网站被篡改网站数量最多，占总数的 72.3%，其次是以.net 为后缀的网络服务公司网站和以.gov 为后缀的政府网站，分别占总数的 7.3%和 2.8%。

2016年境内被篡改网站按类型分布



二、2016 年我国互联网网络安全状况

近年来，随着我国网络安全法律法规、管理制度的不断完善，我国在网络安全技术实力、人才队伍、国际合作等方面取得了明显的成效。2016 年，我国互联网网络安全状况总体平稳，网络安全产业快速发展，网络安全防护能力得到提升，网络安全国际合作进一步加强。但随着网络空间战略地位的日益提升，世界主要国家纷纷建立网络空间攻击能力，国家级网络冲突日益增多，我国网络空间面临的安全挑战日益复杂。

（一）域名系统安全状况良好，防攻击能力明显上升

2016 年，我国域名服务系统安全状况良好，无重大安全事件发生。据抽样监测，2016 年针对我国域名系统的流量规模达 1Gpbs 以上的 DDoS 攻击事件日均约 32 起，均未对我

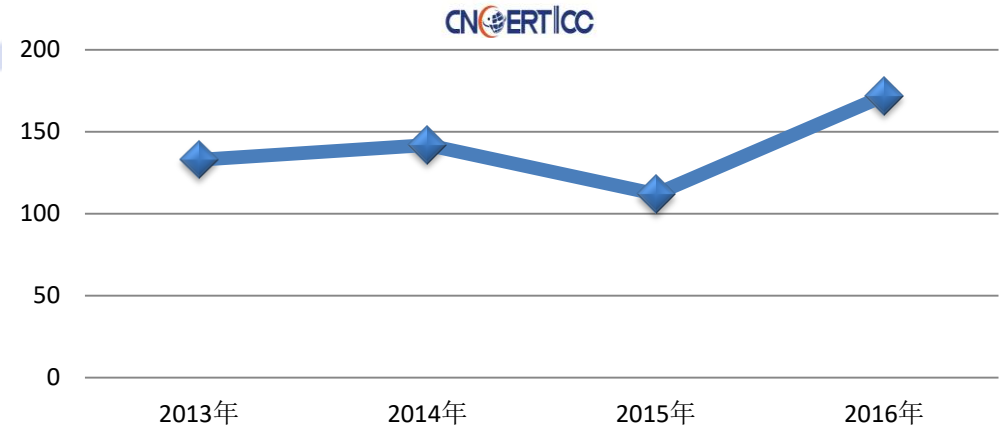
国域名解析服务造成影响，在基础电信企业侧也未发生严重影响解析成功率的攻击事件，主要与域名系统普遍加强安全防护措施，抗 DDoS 攻击能力显著提升相关。2016 年 6 月，发生针对全球根域名服务器及其镜像的大规模 DDoS 攻击，大部分根域名服务器受到不同程度的影响，位于我国的域名根镜像服务器也在同时段遭受大规模网络流量攻击。因应急处置及时，且根区顶级域缓存过期时间往往超过 1 天，此次攻击未对我国域名系统网络安全造成影响。

（二）针对工业控制系统的网络安全攻击日益增多，多起重要工控系统安全事件应引起重视

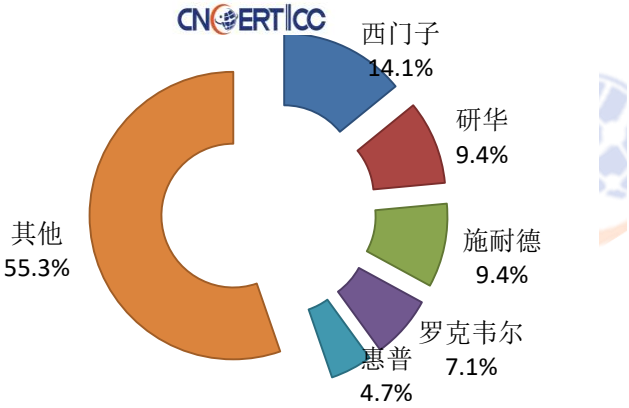
2016 年，全球发生的多起工控领域重大事件值得我国警醒。3 月，美国纽约鲍曼水坝的一个小型防洪控制系统遭攻击；8 月，卡巴斯基安全实验室揭露了针对工控行业的“食尸鬼”网络攻击活动，该攻击主要对中东和其他国家的工业企业发起定向网络入侵；12 月，乌克兰电网再一次经历了供电故障，据分析本次故障缘起恶意程序“黑暗势力”的变种。我国工控系统规模巨大，安全漏洞、恶意探测等均给我国工控系统带来一定安全隐患。截至 2016 年年底，CNVD 共收录工控漏洞 1036 条，其中 2016 年收录了 173 个，较 2015 年增长了 38.4%。工控系统主要存在缓冲区溢出、缺乏访问控制机制、弱口令、目录遍历等漏洞风险。同时，通过联网

工控设备探测和工控协议流量监测，2016 年 CNCERT 共发现我国联网工控设备 2504 个，协议主要涉及 S7Comm、Modbus、SNMP、EtherNetIP、Fox、FINS 等，厂商主要为西门子、罗克韦尔、施耐德、欧姆龙等。通过对网络流量分析发现，2016 年度 CNCERT 累计监测到联网工控设备指纹探测事件 88 万余次，并发现来自境外 60 个国家的 1610 个 IP 地址对我国联网工控设备进行了指纹探测。

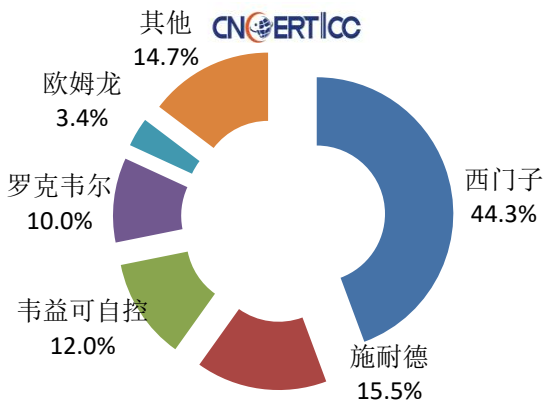
2013年至2016年CNVD收录工控系统漏洞情况



工控系统高危漏洞涉及厂商情况



发现的联网工控设备厂商分布情况



（三）高级持续性威胁常态化，我国面临的攻击威胁尤为严重

截止到 2016 年底，国内企业发布高级持续性威胁（APT）研究报告共提及 43 个 APT 组织，其中针对我国境内目标发动攻击的 APT 组织有 36 个[4]。从攻击实现方式来看，更多 APT 攻击采用工程化实现，即依托商业攻击平台和互联网黑色产业链数据等成熟资源实现 APT 攻击。这类攻击不仅降低了发起 APT 攻击的技术和资源门槛，而且加大了受害方溯源分析的难度。2016 年，多起针对我国重要信息系统实施的 APT 攻击事件被曝光，包括 “白象行动[5]”、“蔓灵花攻击行动”等，主要以我国教育、能源、军事和科研领域为主要攻击目标。2016 年 8 月，黑客组织 “影子经纪人（Shadow Brokers）”公布了方程式组织[6]经常使用的工具包，包含各种防火墙的漏洞利用代码、黑客工具和脚本，涉及 Juniper、飞塔、思科、天融信、华为等厂商产品。CNCERT 对公布的 11 个产品漏洞（有 4 个疑似为 0day 漏洞）进行普查分析，发现全球有约 12 万个 IP 地址承载了相关产品的网络设备，其中我国境内 IP 地址有约 3.3 万个，占全部 IP 地址的 27.8%，对我国网络空间安全造成严重的潜在威胁。2016 年 11 月，黑客组织“影子经纪人”又公布一组曾受美国国家安全局网络攻击与控制的 IP 地址和域

[4] 360 威胁情报中心发布的《2016 中国高级持续性威胁（APT）研究报告》。
[5] 又名“摩诃草”黑客组织或“丰收行动”。
[6] 方程式组织（Equation Group），世界上最尖端的网络攻击组织之一，疑似与美国国家安全局（NSA）有联系。

名数据，中国是被攻击最多的国家，涉及我国至少 9 所高校，12 家能源、航空、电信等重要信息系统部门和 2 个政府部门信息中心。

（四）大量联网智能设备遭恶意程序攻击形成僵尸网络，被用于发起大流量 DDoS 攻击

近年来，随着智能可穿戴设备、智能家居、智能路由器等终端设备和网络设备的迅速发展和普及利用，针对物联网智能设备的网络攻击事件比例呈上升趋势，攻击者利用物联网智能设备漏洞可获取设备控制权限，或用于用户信息数据窃取、网络流量劫持等其他黑客地下产业交易，或用于被控制形成大规模僵尸网络。CNCERT 对车联网系统安全性进行在线监测分析，发现部分车联网信息服务商及相关产品存在安全漏洞，可导致车辆、位置及车主信息泄露和车辆被远程控制等安全风险。2016 年底，因美国东海岸大规模断网事件和德国电信大量用户访问网络异常事件，Mirai 恶意程序受到广泛关注。Mirai 是一款典型的利用物联网智能设备漏洞进行入侵渗透以实现对设备控制的恶意代码，被控设备数量积累到一定程度将形成一个庞大的“僵尸网络”，称为“Mirai 僵尸网络”。又因物联网智能设备普遍是 24 小时在线，感染恶意程序后也不易被用户察觉，形成了“稳定”的攻击源。CNCERT 对 Mirai 僵尸网络进行抽样监测显示，截至 2016 年年底，共发现 2526 台控制

服务器控制了 125.4 万余台物联网智能设备，对互联网的稳定运行形成了严重的潜在安全威胁。此外，CNCERT 还对 Gafgyt 僵尸网络进行抽样检测分析，在 2016 年第四季度，共发现 817 台控制服务器控制了 42.5 万台物联网智能设备，累计发起超过 1.8 万次的 DDoS 攻击，其中峰值流量在 5Gpbs 以上的攻击次数高达 72 次。

（五）网站数据和个人信息泄露屡见不鲜，“衍生灾害”严重

由于互联网传统边界的消失，各种数据遍布终端、网络、手机和云上，加上互联网黑色产业链的利益驱动，数据泄露威胁日益加剧。2016 年，国内外网站数据和个人信息泄露事件频发，对政治、经济、社会的影响逐步加深，甚至个人生命安全也受到侵犯。在国外，美国大选候选人希拉里的邮件泄露，直接影响到美国大选的进程；雅虎两次账户信息泄露涉及约 15 亿的个人账户，致使美国电信运营商威瑞森 48 亿美元收购雅虎计划搁置甚至可能取消。在国内，我国免疫规划系统网络被恶意入侵，20 万儿童信息被窃取并在网上公开售卖；信息泄露导致精准诈骗案件频发，高考考生信息泄露间接夺去即将步入大学的女学生徐玉玉的生命；2016 年公安机关共侦破侵犯个人信息案件 1800 余起，查获各类公民个人信息 300 亿余条。此外，据新闻媒体报道，俄罗斯、墨西哥、土耳其、菲律宾、叙利亚、肯尼亚等多个国家政府的网站数据发生了泄漏。

（六） 移动互联网恶意程序趋利性更加明确，移动互联网黑色产业链已经成熟

2016 年，CNCERT 通过自主捕获和厂商交换获得移动互联网恶意程序数量 205 万余个，较 2015 年增长 39.0%，近 6 年来持续保持高速增长趋势。通过恶意程序行为分析发现，以诱骗欺诈、恶意扣费、锁屏勒索等攫取经济利益为目的的应用程序骤增，占恶意程序总数的 59.6%，较 2015 年增长了近三倍。从恶意程序传播途径发现，诱骗欺诈行为的恶意程序主要通过短信、广告和网盘等特定传播渠道进行传播，感染用户数达到 2493 万人，造成重大经济损失。从恶意程序的攻击模式发现，通过短信方式传播窃取短信验证码的恶意程序数量占比较大，全年获得相关样本 10845 个，表现出制作简单、攻击模式固定、暴利等特点，移动互联网黑色产业链已经成熟。

（七）敲诈勒索软件肆虐，严重威胁本地数据和智能设备安全

根据 CNCERT 监测发现，2016 年在传统 PC 端，捕获敲诈勒索类恶意程序样本约 1.9 万个，数量创近年来新高。对敲诈勒索软件攻击对象分析发现，勒索软件已逐渐由针对个人终端设备延伸至企业用户，特别是针对高价值目标的勒索情况严重。针对企业用户方面，勒索软件利用安全漏洞发起攻击，对企业数据库进行加密勒索，2016 年底开源 MongoDB 数据库遭一轮勒索软件攻击，大量的用户受到影响。针对个人终端设备

方面，敲诈勒索软件恶意行为在传统 PC 端和移动端表现出明显的不同特点：在传统 PC 端，主要通过“加密数据”进行勒索，即对用户电脑中的文件加密，胁迫用户购买解密密钥；在移动端，主要通过“加密设备”进行勒索，即远程锁住用户移动设备，使用户无法正常使用设备，并以此胁迫用户支付解锁费用。但从敲诈勒索软件传播方式来看，传统 PC 端和移动端表现出共性，主要是通过邮件、仿冒正常应用、QQ 群、网盘、贴吧、受害者等传播。

三、2017 年值得关注的热点

根据对 2016 年我国互联网网络安全形势特点的分析，CNCERT 预测 2017 年值得关注的热点方向主要如下。

（一）网络空间依法治理脉络更为清晰

2016 年 11 月 7 日第十二届全国人大常委会第二十四次会议表决通过《网络安全法》，并将于 2017 年 6 月 1 日起施行。该法有 7 章 79 条，对网络空间主权、网络产品和服务提供者的安全义务、网络运营者的安全义务、个人信息保护规则、关键信息基础设施安全保护制度和重要数据跨境传输规则等进行了明确规定。预计 2017 年各部门将更加重视《网络安全法》的宣传和解读工作，编制出台相关配套政策法规，落实各项配套措施，网络空间依法治理脉络将更为清晰。

（二）利用物联网智能设备的网络攻击事件将继续增多

2016 年 CNVD 收录物联网智能设备漏洞 1117 个，主要涉及网络摄像头、智能路由器、智能家电、智能网关等设备。漏洞类型主要为权限绕过、信息泄露、命令执行等，其中弱口令（或内置默认口令）漏洞极易被利用，实际影响十分广泛，成为恶意代码攻击利用的重要风险点。随着无人机、自动驾驶汽车、智能家电的普及和智慧城市的发展，联网智能设备的漏洞披露数量将大幅增加，针对或利用物联网智能设备的网络攻击将更为频繁。

（三）互联网与传统产业融合引发的安全威胁更为复杂

随着我国“互联网 + ”、“中国制造 2025”行动计划的深入推进，我国几乎所有的传统行业、传统应用与服务都在被互联网改变，给各个行业带来了创新和发展机会。在融合创新发展的过程中，传统产业封闭的模式逐渐转变为开放模式，也将以往互联网上虚拟的网络安全事件转变为现实世界安全威胁。互联网金融、工业互联网等融合的新兴行业快速发展，但引发的新的网络安全威胁也不容忽略，互联网金融整合了信息流和资金流，信息流的风险很可能引发资金流损失；工业控制系统更为智能化、网络化，开放互联带来的恶意嗅探行为增多，被恶意攻击的风险不断加大。传统互联网安全与现实世界安全问题相交织引发的安全威胁更为复杂，产生的后果也更为严重。

（四）个人信息和重要数据保护将更受重视

近年来，互联网技术的发展极大的方便和丰富了我们的生活和工作，网上购物、网上求职、社交平台、政府服务等平台上充斥着大量的个人详细隐私信息。自 2011 年以来我国关于严重个人信息泄露的事件不绝于耳，特别是近年来的网络诈骗案件中，受害人的详细信息都被诈骗分子所掌握，给社会安定带来严重危害。2013 年 “斯诺登事件”及后续相继爆出的美国政府大范围监听项目，刺激着各国加强重要数据的保护措施，严格规范互联网数据的收集、使用、存储等。我国在《网络安全法》中对个人信息保护规则、重要数据跨境传输进行了明确规定，预计关于个人信息和重要数据信息保护的详细规范性文件将制定出台，切实落实保护措施。

（五）网络安全威胁信息共享工作备受各方关注

及时全面获取和分析网络安全威胁，提前做好网络安全预警和部署应急响应措施，充分体现了一个国家网络安全综合防御能力。通过网络安全威胁信息共享，利用集体的知识和技术能力，是实现全面掌握网络安全威胁情况的有效途径。美国早在 1998 年的克林顿政府时期就签署了总统令，鼓励政府与企业开展网络安全信息共享，到奥巴马政府时期更是将网络安全信息共享写入了政府法案。近年来，我国高度重视网络安全信息共享工作，在《网络安全法》中明确提出了促进有关部门、

关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享。但面对纷繁复杂的、多维度的数据源信息，如何高效地开展共享和深入分析，需建立一套基于大数据分析的网络安全威胁信息共享标准。目前，我国很多机构已经在开展网络安全威胁信息共享的探索与实践，相关国家标准和行业标准已在制定中，CNCERT 也建立了网络安全威胁信息共享平台，在通信行业和安全行业内进行相关共享工作。

（六）有国家背景的网络争端受关注度将继续升温

目前，我国互联网普及率已经达到 53.2%[7]，民众通过互联网获得的新闻资讯越来越快捷方便，民众关注全球政治热点的热度也不断高涨。2016 年美国总统大选“邮件门”事件、俄罗斯黑客曝光世界反兴奋剂机构丑闻事件等，都让网民真切感受到有组织、有目的的一场缜密的网络攻击可以对他国政治产生严重的影响，将有国家背景的网络争端从行业领域关注视角延伸到了全体网民。随着大量的国家不断强化网络空间军事能力建设，有国家背景的网络争端事件将会热点不断、危机频出，全民讨论的趋势将会持续升温。

（七）基于人工智能的网络安全技术研究全面铺开

在第三届世界互联网大会“世界互联网领先科技成果发布

[7] 中国互联网络信息中心第 39 次《中国互联网络发展状况统计报告》

活动”现场，微软、IBM、谷歌三大国际科技巨头展示了基于机器学习的人工智能技术，为我们描绘了人工智能美好的未来。目前，网络攻击事件层出不穷、手段多样、目的复杂，较为短缺的网络安全人才难以应对变化过快的网络安全形势，而机器学习在数据分析领域的出色表现，人工智能被认为在网络安全方面将会“大有作为”。有研究机构[8]统计发现，2016 年“网络安全”与“人工智能”两词共同出现在文章中的频率快速上升，表明越来越多的讨论将二者联系在一起共同关注。以网络安全相关的大数据为基础，利用机器学习等人工智能技术，能够在未知威胁发现、网络行为分析、网络安全预警等方面取得突破性进展。

结　语

2016 年，我国不断完善网络安全保障措施，网络安全防护水平进一步提升，有力保障了“G20 杭州峰会”、“第三届世界互联网大会”等多项重要活动的顺利举办。近年来，我国在持续推进依法治理网络空间安全进程和不断完善网络安全人才培养机制，新《国家安全法》、《反恐怖主义法》、《网络安全法》和《国家网络空间安全战略》等多项网络空间法律法规或战略制定并发布，首批优秀网络安杰出人才、优秀人才和优秀教师受到表彰。当前，我国已明确提出实施网络强国战略，但

[8] CB Insights 在 2016 年 11 月 2 日发布的分析报告，参考链接为：https://www.cbinsights.com/blog/cybersecurity-artificial-intelligence/。

不管是来自互联网黑色产业链的网络安全威胁还是来自国家级之间的网络安全对抗，我国面临的网络空间安全问题越来越复杂、隐蔽。希望我们共同努力，不断攀登网络安全技术高峰，维护我国网络空间安全，为我国第五大战略空间竖起一道坚实的堡垒。