CNCERT/CC

2015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

2016年4月

前 言
Preface

2015年，党中央、国务院加大了对网络安全的重视，我国网络空间法制化进程不断加快，网络安全人才培养机制逐步完善，围绕网络安全的活动蓬勃发展。我国新《国家安全法》正式颁布，明确提出国家建设网络与信息安全保障体系；《刑法修正案（九）》表决通过，加大打击网络犯罪力度；《反恐怖主义法》正式通过，规定了电信业务经营者、互联网服务提供者在反恐中应承担的义务；《网络安全法（草案）》向社会各界公开征求意见；高校设立网络空间安全一级学科，加快网络空间安全高层次人才培养；政府部门或行业组织围绕网络安全举办的会议、赛事、宣传活动等丰富多样。

2015年是我国“十二五”规划收官之年，我国实现了半数中国人接入互联网，网民规模达6.88亿，手机网民规模达6.2亿，域名总数为3102万[1]。2015年，我国陆续出台了“互联网+”行动计划、“宽带中国2015专项行动”等，加快建设网络强国。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。然而，层出不穷的网络安全问题仍然难以避免。基础网络设备、域名系统、工业互联网等我国基础网络和关键基础设施依然面临着较大安全风险，网络安全事件多有发生。木马和僵尸网络、移动互联网恶意程序、拒绝服务攻击、安全漏洞、网页仿冒、网页篡改等网络安全事件表现出了新的特点：利用分布式拒绝服务攻击（以下简称“DDoS攻击”）和网页篡改获得经济利益现象普遍；个人信息泄露引发的精准网络诈骗和勒索事件增多；智能终端的漏洞风险增大；移动互联网恶意程序的传播渠道转移到网盘或广告平台等网站。

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，着重分析和总结2015年我国互联网网络安全状况，并预测2016年网络安全热点问题。

[1] 数据来自《第37次中国互联网络发展状况统计报告》。

基础网络和关键基础设施

基础通信网络安全防护水平进一步提升

基础电信企业逐年加大网络安全投入，加强通信网络安全防护工作的体系、制度和手段建设，推动相关工作系统化、规范化和常态化。2015年，工业和信息化部以网络安全管理、技术防护、用户个人电子信息和数据安全保护、应急工作、网络安全问题整改等为检查重点，对电信和互联网行业落实网络安全防护工作进行抽查。根据抽查结果，各基础电信企业符合性测评平均得分均达到90分以上，风险评估检查发现的单个网络或系统的安全漏洞数量较2014年下降20.5%。

我国域名系统抗拒绝服务攻击能力显著提升

CNCERT监测发现，2015年针对我国域名系统的DDoS攻击流量进一步增大。4月，我国某重要新闻网站的域名服务器多次遭受DDoS攻击，峰值流量达8Gbit/s，经分析发现此次攻击主要为利用NTP❷ 和UPnP❸ 进行的反射攻击，主要攻击源均来自境外；8月，我国顶级域名系统先后遭受2次大流量DDoS攻击，峰值流量超过10Gbit/s。2015年发生的多起针对重要域名系统的DDoS攻击均未对相关系统的域名解析服务造成严重影响，反映出我国重要域名系统普遍加强了安全防护措施，抗DDoS攻击能力显著提升。

❷ NTP，即网络时间协议（Network Time Protocol）。
❸ UPnP，即通用即插即用（Universal Plug and Play）协议。

工业互联网面临的网络安全威胁加剧

新一代信息技术与制造业深度融合，工业互联网成为推动制造业向智能化发展的重要支撑。近年来，国内外已发生多起针对工业控制系统的网络攻击，攻击手段也更加专业化、组织化和精确化。2015年，国家信息安全漏洞共享平台（以下简称“CNVD”）共收录工控漏洞125个，发现多个国内外工控厂商的多款产品普遍存在缓冲区溢出、缺乏访问控制机制、弱口令、目录遍历等漏洞风险，可被攻击者利用实现远程访问。据监测，2015年境外有千余个IP地址对我国大量使用的某款工控系统进行渗透扫描，有数百个IP地址对我国互联网上暴露的工控设备进行过访问。2015年12月，因遭到网络攻击，乌克兰境内近三分之一的地区发生断电事故。据分析，此次网络攻击利用了一款名为“黑暗力量”的恶意程序，获得了对发电系统的远程控制能力，导致电力系统长时间停电。此次事件的发生，再次对我国提出警示，我国工业互联网也可能面临着严峻的网络安全威胁。

针对我国重要信息系统的高强度有组织攻击威胁形势严峻

据监测，2015年我国境内有近5000个IP地址感染了窃密木马，存在失泄密和运行安全风险。针对我国实施的APT[4]攻击事件也在不断曝光，例如境外“海莲花”黑客组织多年以来针对我国海事机构实施APT攻击；国内安全企业发现了一起名为APT-TOCS的长期针对我国政府机构的攻击事件。2015年7月发生的Hacking Team公司信息泄露事件，揭露了部分国家相关机构雇佣专业公司对我国重要信息系统目标实施网络攻击的情况。

[4] APT（Advanced Persistent Threat，高级持续性威胁）：利用先进的攻击手段对特定目标进行长期持续性网络攻击的形式。

公共互联网

公共互联网网络安全环境

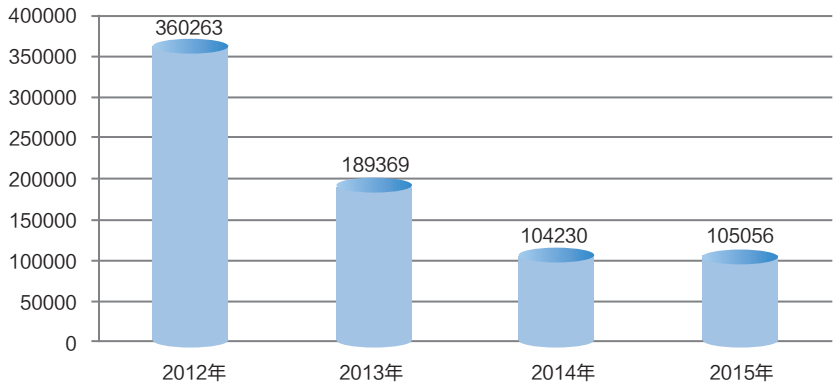
2015年，根据CNCERT自主监测数据，我国公共互联网网络安全状况总体平稳，位于境内的木马和僵尸网络控制端数量保持下降趋势、主流移动应用商店安全状况明显好转，但个人信息泄露、网络钓鱼等方面的安全事件数量呈上升趋势。

● *木马和僵尸网络*

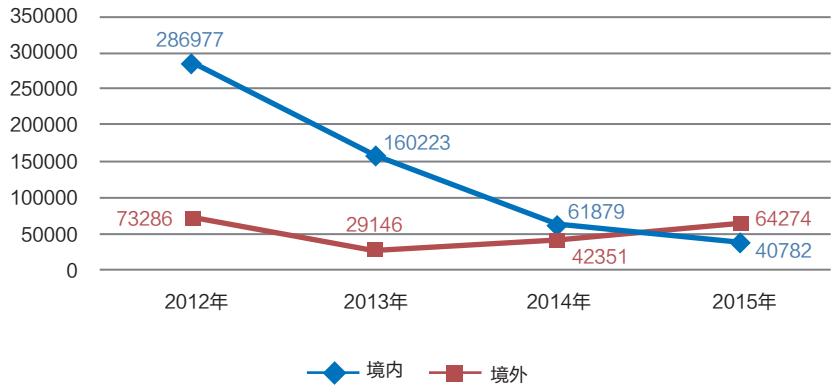
◎ **我国境内木马和僵尸网络控制端数量再次下降　首次出现境外木马和僵尸网络控制端数量多于境内的现象**

据抽样监测，2015年共发现10.5万余个木马和僵尸网络控制端，控制了我国境内1978万余台主机。其中，位于我国境内的控制端近4.1万个，较2014年下降34.1%，继续保持下降趋势。以上情况的出现主要与行业内相关单位近年来持续开展木马和僵尸网络治理有关。2015年，在工业和信息化部指导下，按照《木马和僵尸网络监测与处置机制》的有关规定，CNCERT组织基础电信企业、域名服务机构等成功关闭678个控制规模较大的僵尸网络，累计处置690个恶意控制服务器和恶意域名，成功切断黑客对154万余台感染主机的控制。随着我国境内持续开展木马和僵尸网络治理工作，大量木马和僵尸网络控制端向境外迁移。2015年抽样监测发现境外6.4万余个木马和僵尸网络控制端，较2014年大幅增长51.8%，占全部控制端数量的61.2%，首次出现境外木马和僵尸网络控制端多于境内的现象。

2012－2015年木马和僵尸网络控制端总数



2012-2015年木马和僵尸网络控制端境内外数量变化情况



安全形势

Security Situation

● 个人信息泄露

◎ 个人信息泄露事件频发

2015年我国发生多起危害严重的个人信息泄露事件。例如某应用商店用户信息泄露事件、约10万条应届高考考生信息泄露事件、酒店入住信息泄露事件、某票务系统近600万用户信息泄露事件等。针对安卓平台的窃取用户短信、通讯录、微信聊天记录等信息的恶意程序爆发。安卓平台感染此类恶意程序后，大量涉及个人隐私的信息被通过邮件发送到指定邮箱。2015年，CNCERT抽样监测发现恶意程序转发的用户信息邮件数量超过66万封。CNCERT在判定此类恶意程序的恶意行为后，立即协调处置了涉及的URL、域名和邮箱，有效防止影响范围进一步扩大。此外，个人信息泄露事件频繁被媒体报道，反映出社会对此类事件的关注度不断提升。

◎ 个人信息泄露引发网络诈骗和勒索等“后遗症”

2015年发生多起因网购订单信息泄露引发的退款诈骗事件，犯罪分子利用遭泄露的收件地址和联系方式等用户购物信息，向用户发送虚假退款操作信息，迷惑性很强，造成财产损失。由于许多网民习惯在不同网站使用相同账号密码，个人隐私信息易被“撞库”[5]等黑客行为窃取，进而威胁到网民财产安全。2015年，CNCERT多次接到网民投诉苹果手机被锁遭敲诈勒索事件。据查，此类事件大多因用户个人隐私泄露，攻击者利用用户账户密码等信息结合苹果手机的防遗失功能，对用户进行锁机勒索，勒索不成则远程删除用户手机数据，给用户带来了严重损失。

[5] 撞库是黑客通过收集互联网已泄露的用户和密码信息，生成对应的字典表，尝试批量登录其他网站后，得到一系列可以登录的用户。

● 移动互联网恶意程序

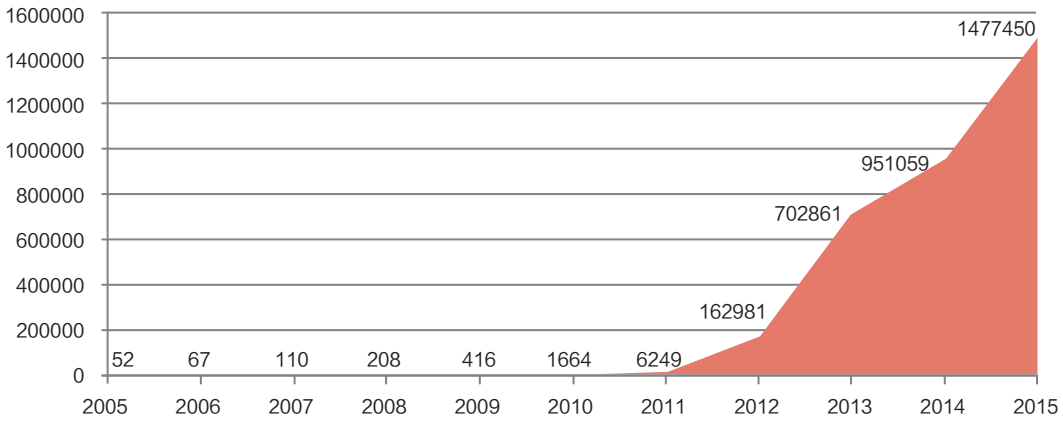
◎ 移动互联网恶意程序数量仍大幅增长

2015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近148万个，较2014年增长55.3%，主要针对安卓平台。按恶意行为进行分类，排名前三位的恶意行为分别是恶意扣费类、流氓行为类和远程控制类，占比分别为23.6%、22.2%和15.1%。CNCERT发现移动互联网恶意程序下载链接30万余条，同比增长7.2%，涉及的传播源域名4万余个、IP地址近2万个，恶意程序传播次数达8384万余次，较2014年增长了9.8%。

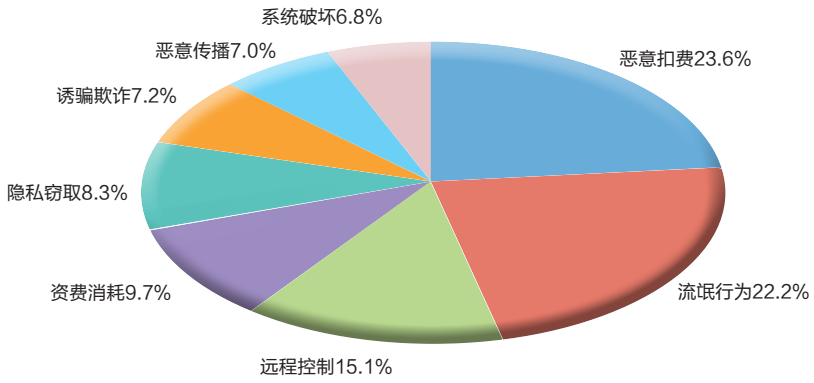
◎ 主流移动应用商店安全状况明显好转　大量移动恶意程序的传播渠道转移到网盘或广告平台等网站

在工业和信息化部指导下，经过连续三年的治理，国内主流应用商店积极落实安全责任，不断完善安全检测、安全审核、社会监督举报、恶意程序下架等制度，积极参与处置响应与反馈，恶意APP下架数量连续保持下降趋势，2015年较2014年下降了57.3%。2015年，CNCERT累计向302家应用商店、云盘、网盘或广告宣传网站等平台通报恶意APP事件1.7万余起，要求对通报的恶意APP进行下架，全年下架率达97.2%。按各平台接到通报数量来看，排名前6的平台接到的通报次数占全年总通报次数的50.2%。经确认发现，这6家主要是提供云盘、网盘、广告宣传等业务的网站，反映出大量的恶意程序传播源已发生转移。

2005－2015年移动互联网恶意程序数量走势



2015年移动互联网恶意程序按行为类型分布



◎ 应用软件供应链安全问题凸现

2015年先后曝出多起应用软件开发工具被植入恶意代码，导致使用这些工具开发的应用软件出现安全问题的事件。9月，CNCERT监测发现，苹果开发工具Xcode被植入XcodeGhost恶意代码，导致使用该工具开发的苹果APP被植入恶意代码。国内数百款知名的APP均受到感染，这些恶意APP绕过苹果AppStore安全审核机制供用户下载。截至9月18日，全国受感染用户达2140万。10月，网上披露了“WormHole”漏洞，该漏洞存在于国内某公司开发的一款公共开发套件中，影响集成此套件的该公司系列APP及其他20余款APP。CNCERT及时完成了事件的样本分析、处置和预警，要求涉事单位及时修复相关APP并通知用户更新，有效遏制了恶意代码传播蔓延势头。

● *拒绝服务攻击*

◎ DDoS攻击仍然是我国互联网面临的严重安全威胁之一

近年来，DDoS攻击的方式和手段不断发生变化。自2014年起，利用互联网传输协议的缺陷发起的反射型DDoS攻击日趋频繁，增加了攻击防御和溯源的难度。几乎不需要技术基础即可使用的DDoS攻击服务平台在互联网上大量出现，DDoS攻击以服务形式在互联网上公开叫卖，这些平台的出现极大地降低了DDoS攻击技术门槛，使攻击者可以轻易发起大流量攻击。2015年前三季度，攻击流量在1Gbit/s以上的DDoS攻击次数近38万次，日均攻击次数达到了1491次。为遏制DDoS攻击事件数量继续增长，减少DDoS攻击带来的危害，CNCERT于2015年第四季度组织电信和互联网行业单位集中开展了互联网网络安全威胁治理行动，日均DDoS攻击数量明显下降。

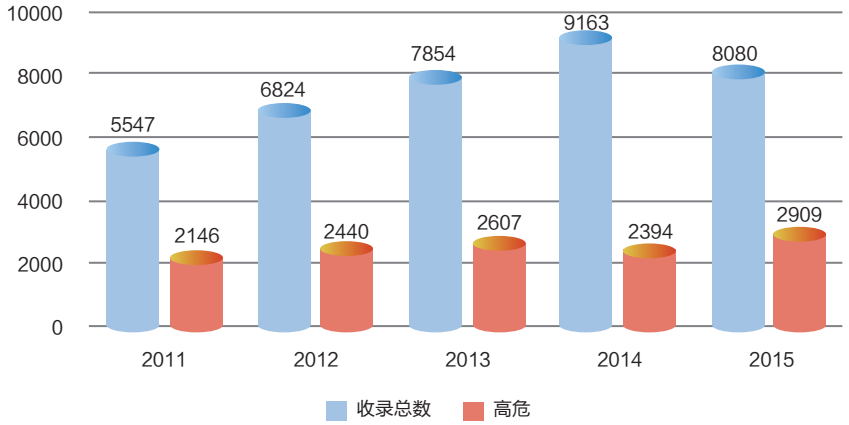
● 安全漏洞

◎ 网络安全高危漏洞频现 网络设备安全漏洞风险依然较大

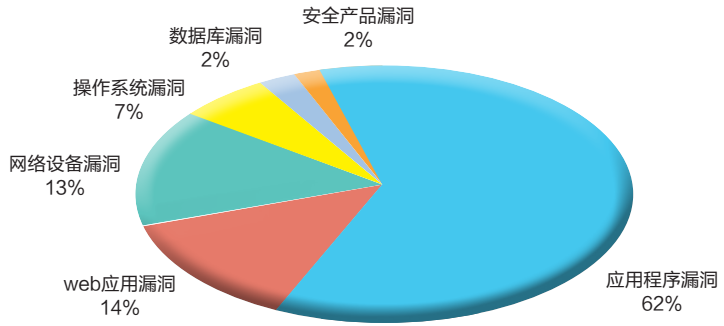
2015年，CNVD共收录安全漏洞8080个，较2014年减少11.8%。其中，高危漏洞收录数量高达2909个，较2014年增长21.5%；可诱发零日攻击的漏洞1207个（即收录时厂商未提供补丁），占14.9%。2015年曝出了Juniper Networks ScreenOS后门漏洞[6]、Java反序列化远程代码执行漏洞[7]、Redis未授权执行漏洞[8]、HTTP.sys远程代码执行漏洞[9]和GNU glibc函数库缓冲区溢出漏洞[10]（又称为“Ghost”幽灵漏洞）等多个涉及基础软件的高危漏洞。基础软件广泛应用在我国基础应用和通用软硬件产品中，若不及时修复，容易被批量利用，造成严重危害。从CNVD行业漏洞收录数量统计分析发现，电信行业漏洞库收录漏洞数量为657个，其中网络设备（如路由器、交换机等）漏洞占54.3%，可见网络设备安全风险依然较大。值得注意的是，如果骨干路由器等关键节点网络设备的漏洞被攻击利用，可能导致网络设备或节点被操控、破坏网络稳定运行、窃取用户信息、传播恶意代码、实施网络攻击等问题，需引起高度重视。2015年，CNVD共向基础电信企业通报2447份漏洞风险通报，较2014年增长61.9%；通报涉及的基础电信企业门户网站及业务系统漏洞风险事件2530起，较2014年增长60.3%。

⑥ 编号 CNVD-2015-08306、CNVD-2015-08307，CVE-2015-7756。
⑦ 编号 CNVD-2015-07556。
⑧ 编号 CNVD-2015-07557。
⑨ 编号 CNVD-2015-02422，CVE-2015-1635。
⑩ 编号 CNVD-2015-00719，CVE-2015-0235。

2011－2015年CNVD漏洞收录情况



2015年CNVD收录漏洞按影响对象类型分布



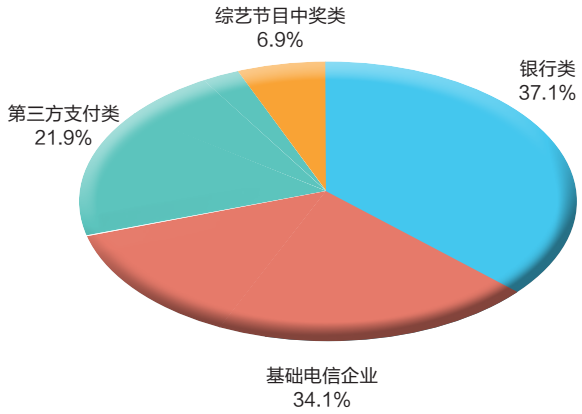
◎ 涉及重要行业和政府部门的高危漏洞事件持续增多 修复进度未跟上步伐

政府机构和重要信息系统的网络系统上承载了大量有价值的数据信息，广泛被漏洞挖掘者关注。2015年，CNCERT通报了涉及政府机构和重要信息系统部门的事件型漏洞近2.4万起，约是2014年的2.6倍，继续保持快速增长态势。然而，部分通报漏洞未及时修补，为相关系统带来严重安全隐患。CNCERT抽取2015年12月通报的安全漏洞事件进行修复验证，发现政府部门网站系统漏洞隔月修复率仅为52.7%，涉及网络基础设施的漏洞隔月修复率为81.3%，可见部分漏洞修复不及时。

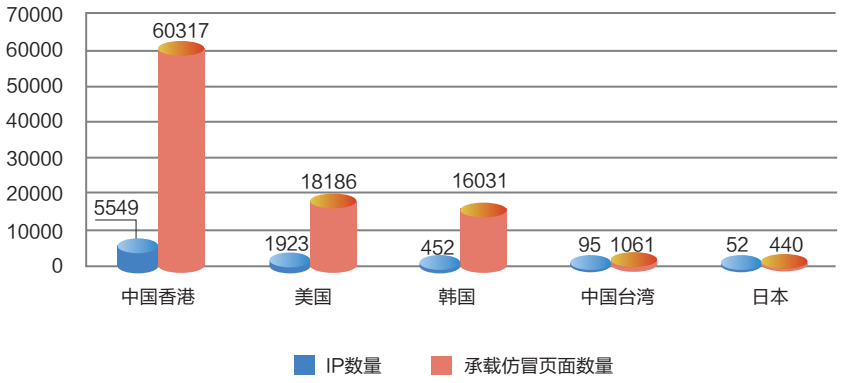
◎ 智能联网设备暴露出的安全漏洞问题严重

乘着“互联网＋”的新机遇，各行业与互联网深度融合，智能联网设备也逐渐在各行业广泛使用，漏洞威胁也在逐步增加。2015年，CNVD共收录了739个移动互联网设备或软件产品漏洞；通报了多款智能监控设备、路由器等存在被远程控制高危风险漏洞的安全事件。2015年年初，政府机关和公共行业广泛使用的某型号监控设备被曝存在高危漏洞，并已被利用植入恶意代码，导致部分设备被远程控制并可对外发动网络攻击。CNCERT核查发现，我国主要厂商生产的同类型设备，普遍存在类似安全问题，亟需进行大范围整改。

2015年仿冒境内网站按仿冒对象分布



2015年仿冒境内网站的境外IP及其承载的仿冒页面数量
按国家或地区分布TOP5



● 网页仿冒

◎ 网页仿冒事件数量暴涨

CNCERT监测发现，2015年针对我国境内网站的仿冒页面数量达18万余个，较2014年增长85.7%。其中，针对金融支付的仿冒页面数量上升最快，较2014年增长6.37倍；针对娱乐节目中奖类的网页仿冒页面数量也较2014年增长1倍。大量仿冒银行或基础电信企业积分兑换的仿冒网站链接由伪基站发送。2015年，CNCERT共处置各类网络安全事件近12.6万起，其中网页仿冒事件数量位居第一，达7.5万余起，同比增长近3.2倍。由于我国加大了对网页仿冒的打击力度，大量的网页仿冒站点迁移到境外。在针对我国境内网站的仿冒站点中，83.2%位于境外，其中位于香港的IP地址承载的仿冒页面最多，达6万余个。

● 网页篡改

◎ 植入暗链[1]是网页篡改的主要攻击方式

CNCERT监测发现，2015年我国境内近2.5万个网站被篡改，其中被篡改政府网站有898个，较2014年减少49.1%。从网页篡改的方式来看，我国被植入暗链的网站占全部被篡改网站的比例高达83%，在被篡改的政府网站中，超过85%的网页篡改方式是植入暗链。植入暗链已成为黑客地下产业链牟利方式之一，2015年CNCERT处置参与网页篡改攻击的博彩、私服等非法网站链接6320个，通知5609个被植入暗链网站用户单位对网站进行修复。

[1] 暗链就是页面上看不见网站链接，主要指向博彩、私服等非法网站链接。

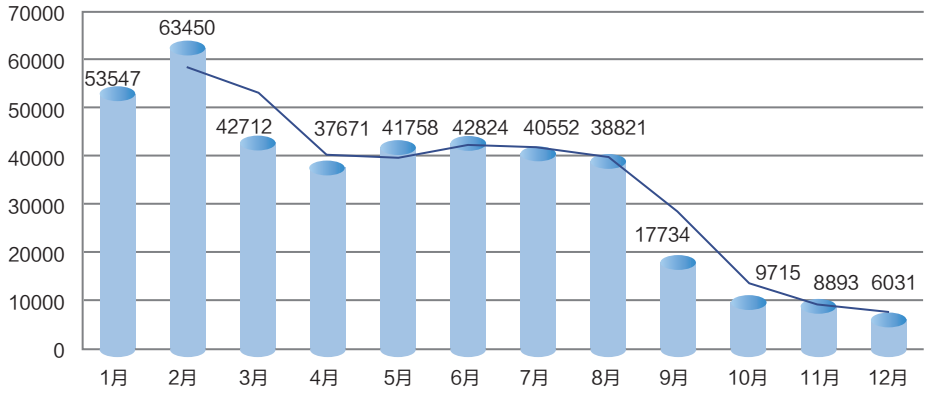
公共互联网网络安全合作

网络空间具有开放互联等特性，网络安全问题涉及面广。首先，网络安全威胁往往是涉及多行业、多领域的交叉问题，需要跨部门、跨行业、跨地域的多方力量共同协作才能有效应对。其次，跨境网络安全事件频发，需要加强国际对话合作，建立高效的网络安全信息共享和跨境网络安全事件处置协作机制。2015年，我国网络安全领域的国内外合作均进一步加强。在国内，电信和互联网行业积极发挥行业自律作用，共同应对网络安全威胁；在国际合作方面，协作处置的跨境网络安全事件数量显著增加。

● *互联网网络安全威胁治理行动*

2015年7月31日，CNCERT联合中国互联网协会网络与信息安全工作委员会组织开展互联网网络安全威胁治理行动。共56家企业参与此次行动，包括基础电信企业、互联网企业、域名注册服务机构、应用商店等。该行动以加强行业自律为目的，通过投诉举报、信息共享、威胁认定、协同处置、信息发布等多项措施环环相扣，取得了显著治理效果。此次行动重点针对DDoS攻击、网页篡改等与互联网黑产密切相关的事件进行处置。截至2015年年底，CNCERT共接到广大网民举报的网络安全事件54937起，处置网络安全事件52950起，发布URL黑名单地址47061条。DDoS攻击事件次数由行动启动前的日均1491起下降到日均358起，大幅下降76.7%；境内被篡改网站相比行动启动前月均下降8.6%，其中被篡改政府网站月均下降了44%，国内主流浏览器、搜索引擎对共享的URL黑名单地址进行拦截或提示次数达千万余次。

2015年攻击流量在1Gbit/s以上DDoS攻击事件数量月度统计

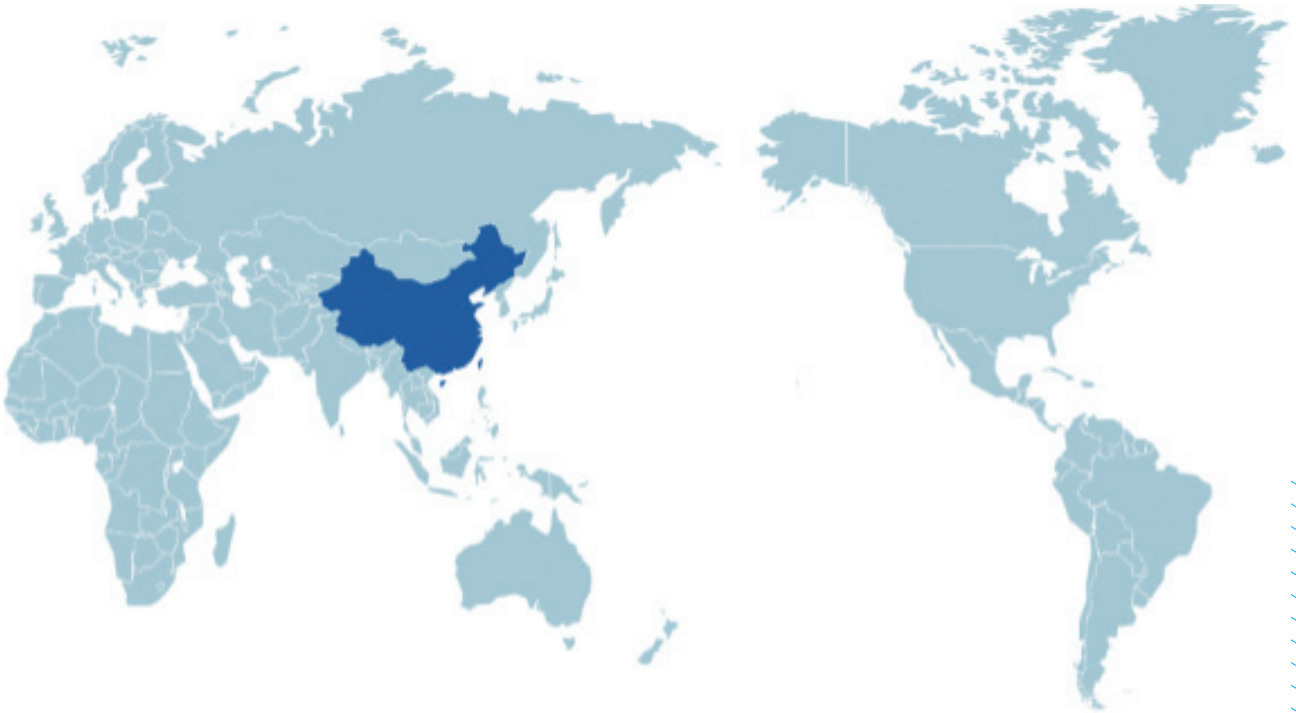


● 安全漏洞披露和处置规范

为方便涉事单位在漏洞披露前得到通知并及时修复漏洞、避免漏洞信息描述不准确或漏洞披露信息夸大其词造成社会恐慌、或漏洞披露信息过于详细而被黑客利用等，CNCERT与乌云、补天、漏洞盒子等多家民间漏洞平台建立了工作联系，并于2015年6月，组织国内32家单位在北京共同签署了《中国互联网协会漏洞信息披露和处置自律公约》，首次以行业自律的方式共同规范漏洞信息的接收、处置和发布方面的行为。协议签署后，相关单位漏洞披露、处置方式的规范性得到了有效提升。

● 网络安全国际合作

2015年，CNCERT继续与国际网络安全组织加强合作，完善跨境网络安全事件协作处置机制。截至2015年年底，已与66个国家和地区的165个组织建立了联系机制，与其中的16个国家或地区的CERT组织、7个网络安全组织签署了网络安全合作谅解备忘录，全年协调境外安全组织处置了涉及我国境内的安全事件近1.9万起，比2014年增长1倍多。CNCERT还推动落实中国-东盟国家计算机应急响应组织合作机制的行动计划、加强中日韩区域网络安全协作，积极发挥在FIRST、APCERT等国际组织中作用，并支撑开展上合组织、APEC-TEL、ITU以及双边网络安全对话国际合作活动。



2016年值得关注的热点问题

根据对2015年我国互联网网络安全形势特点的分析，CNCERT预测2016年值得关注的热点问题主要如下。

将有更多APT攻击事件被曝光

近年来，针对我国的网络窃密、监听等攻击事件频发，网络空间的网络安全攻防对抗日趋激烈。据行业报告显示，2015年对我国发起APT攻击的黑客组织近30个，主要针对我国境内科研教育、政府机构等。随着行业对APT攻击事件的了解加深，“仍有众多APT攻击事件尚未被识别”这一观点已是业内共识。同时，我国安全行业在技术、人才等多方面加大了投入，对APT攻击发现能力提高。因此，预计在2016年，更多APT攻击组织、事件和手段将被披露。

云平台和大数据的安全防护能力将是关注重点

随着云计算、大数据等新技术、新业务的应用与发展，更多政府和企业将系统部署到云平台，大量涉及国计民生、企业运营的数据以及用户个人信息存储在云上，吸引了攻击者的目光。攻击者不断挖掘云平台自身可能存在的安全漏洞，一旦发现漏洞并加以利用，可能导致严重的大规模信息泄露事件发生。此外，攻击者也可以利用云平台实施网络攻击，例如在云平台上部署网络攻击控制端、仿冒站点或发动DDoS攻击等。因此，云平台和大数据的安全防护将成为行业重点关注的问题。


SECURITY

行业合作和国际合作需求继续加强

威胁互联网网络安全的黑客行为涉及多个环节，例如，黑客需要连接互联网、注册域名、托管用于攻击的服务器、发布推广攻击工具和服务，涉及基础电信企业、非经营性互联单位、域名注册服务机构、互联网和安全企业、数据中心、应用商店等。为有效应对网络威胁、改善公共互联网网络安全环境，需在共享威胁信息、完善合作机制、成立产业联盟等方面加强行业合作。此外，随着我国境内互联网网络安全环境治理的持续深入推进，来自境外的网络攻击事件数量上涨趋势明显，预计2016年关于跨境网络安全事件处置的合作需求将继续上升。

物联网智能设备将面临更多网络安全威胁

随着物联网技术的发展，智能穿戴设备、智能家电、智能交通等产品逐渐普及。然而，智能设备安全防护能力普遍较弱，弱口令、安全配置不当、升级维护机制不健全等问题导致智能设备普遍存在安全隐患且难以修复。2016年，随着我国“互联网＋”行动计划、“中国制造2025”计划、智慧城市建设等的不断推进，大量的物联网智能设备不断涌现，在还未建立完善的网络安全保障措施情况下，物联网智能设备的安全问题将更为突出，可能面临更多的网络安全威胁。

精准网络诈骗和勒索敲诈行为将更加猖獗

2015年已发生多起精准网络诈骗和敲诈勒索事件。预计2016年，此类事件将会越来越多。黑客将大量制作伪装成正常应用的恶意程序，通过钓鱼短信、小型网站、社交平台等渠道散播，欺骗用户安装并窃取用户个人信息，进而实施精准网络诈骗。此外，低成本高收益的勒索软件将大量出现，且针对移动智能终端的敲诈勒索行为将更为盛行。

国家计算机网络应急技术处理协调中心基本情况

工作职责

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称是CNCERT或CNCERT/CC），成立于2002年9月，为非政府非盈利的网络安全技术中心，是我国网络安全应急体系的核心协调机构。

作为国家级应急中心，CNCERT的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

业务范围及能力

事件发现：CNCERT依托“公共互联网网络安全监测平台”开展对基础信息网络、金融证券等重要信息系统、移动互联网服务提供商、增值电信企业等安全事件的自主监测。同时还通过与国内外合作伙伴进行数据和信息共享，以及通过热线电话、传真、电子邮件、网站等接收国内外用户的网络安全事件报告等多种渠道发现网络攻击威胁和网络安全事件。

预警通报：CNCERT依托对丰富数据资源的综合分析和多渠道的信息获取实现网络安全威胁的分析预警、网络安全事件的情况通报、宏观网络安全状况的态势分析等，为用户单位提供互联网网络安全态势信息通报、网络安全技术和资源信息共享等服务。

应急处置：对于自主发现和接收到的危害较大的事件报告，CNCERT及时响应并积极协调处置，重点处置的事件包括：影响互联网运行安全的事件、波及较大范围互联网用户的事件、涉及重要政府部门和重要信息系统的事件、用户投诉造成较大影响的事件，以及境外国家级应急组织投诉的各类网络安全事件等。

测试评估：作为网络安全检测、评估的专业机构，按照“支撑监管，服务社会”的原则，以科学的方法、规范的程序、公正的态度、独立的判断，按照相关标准为政府部门、企事业单位提供安全评测服务。CNCERT还组织通信网络安全相关标准制定，参与电信网和互联网安全防护系列标准的编制等。

同时，作为我国非政府层面开展网络安全事件跨境处置协助的重要窗口，CNCERT积极开展国际合作，致力于构建跨境网络安全事件的快速响应和协调处置机制。CNCERT为著名网络安全合作组织FIRST正式成员以及亚太应急组织APCERT的发起人之一。截至2015年，CNCERT与66个国家和地区的165个组织建立了“CNCERT国际合作伙伴”关系。

联系方式

CNCERT建立了7×24小时的网络安全事件投诉机制，国内外用户可通过网站、电子邮件、热线电话、传真4种主要渠道向CNCERT投诉网络安全事件。

- 网　　址：http://www.cert.org.cn/
- 电子邮件：cncert@cert.org.cn
- 热线电话：+861082990999（CN），+861082991000（EN）
- 传　　真：+861082990399

CNCERT CC
国家互联网应急中心

CNCERT/CC
国家互联网应急中心

- 网　　址：http://www.cert.org.cn/
- 电子邮件：cncert@cert.org.cn
- 热线电话：+861082990999（CN）
  +861082991000（EN）
- 传　　真：+861082990399

2015年
我国互联网
网络安全态势综述