

2014 年

我国互联网 网络安全态势报告



国家计算机网络应急技术处理协调中心

2015 年 4 月



P 前言 > Preface

前言 | Preface

安全形势 Security situation

2014 年是我国接入国际互联网 20 周年，也是我国网络安全和信息化国家战略迈出重要步伐的一年。党中央高度重视网络安全工作，成立中央网络安全和信息化领导小组，党的十八届四中全会明确提出加强互联网领域立法，政府工作报告首次出现“维护网络安全”表述，相关管理办法和指导意见先后出台，各类宣传和竞赛活动接连开展，提高了各行业各领域对网络安全的关注和重视，网络安全意识水平逐年提高，投入逐年增大，在各方共同努力下，我国互联网网络安全状况总体平稳。

近年来，我国互联网市场规模和用户体量高速增长，截至 2014 年 12 月底，网站总量保持规模化发展，为 364.7 万个，网站使用的独立域名为 481.2 万余个，互联网接入服务商达 1068 家^①，网民规模达 6.49 亿，手机网民规模达 5.57 亿，互联网普及率达到 47.9%^②，“宽带中国”战略持续推进实施，互联网全面升级提速，4G 商用全力推进，带动移动应用、智能终端等整个产业链条创新，促进信息消费快速增长。但与此同时，信息化的迅猛发展也带来诸多网络安全威胁等伴生性问题。我国基础网络仍存在较多漏洞风险，云服务日益成为网络攻击的重点目标。域名系统面临严峻的拒绝服务攻击，针对重要网站的域名解析篡改攻击频发。网络攻击威胁日益向工业互联网领域渗透，已发现我国部分地址感染专门针对工业控制系统的恶意程序事件。分布式反射型的拒绝服务攻击日趋频繁，大量伪造攻击数据包来自境外网络。针对重要信息系统、基础应用和通用软硬件漏洞的攻击利用活跃，漏洞风险向传统领域、智能终端领域泛化演进。网站数据和个人信息泄露现象依然严重，移动应用程序成为数据泄露的新主体。移动恶意程序不断发展演化，环境治理仍然面临挑战。

在工业和信息化部通信保障局的具体支持和指导下，CNCERT 基于 2014 年互联网行业网络安全信息通报数据和自主监测数据编制了本报告。报告分析和总结了 2014 年我国互联网网络安全态势，提出了 2015 年值得关注的网络安全热点问题。报告旨在为互联网行业和社会各界做好网络安全工作提供参考。

① 中国互联网协会《中国互联网网站发展状况及其安全报告（2015）》数据。

② CNNIC《第 35 次中国互联网络发展状况统计报告》数据。





2014 年我国互联网网络安全形势

| (一) 网络基础设施 |

◎ 基础网络

2014 年，“宽带中国”战略继续推进实施，我国基础网络建设不断升级完善，安全防护水平进一步提升，但基础网络相关设备仍存在安全风险，日益普及的云服务经常发生因系统故障、网络攻击导致的安全问题，影响业务运行和用户使用。

• 基础网络安全防护水平进一步提升

2014 年，工业和信息化部重点围绕网络安全防护措施落实、网络数据安全、用户个人电子信息保护等内容，继续推进基础通信网络安全防护工作。基础电信企业不断加大网络安全投入，加强体系、制度和手段建设，推动工作系统化、规范化和常态化。根据抽查结果，各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 2013 年下降 72%，检查发现问题的难度也逐年加大。截至 2014 年底，各企业已对 80% 以上的漏洞完成修复，并对其余漏洞采取了应急措施，制定了整改计划。



S 安全形势 >
Security
situation

• 基础网络设备仍存在较多安全漏洞风险

随着基础网络安全防护工作的深入推进，发现和处置的深层次安全风险和事件逐渐增多。2014 年，CNCERT 协调处置涉及基础电信企业的漏洞事件 1578 起，是 2013 年的 3 倍。CNVD^③收录与基础电信企业软硬件资产相关的漏洞 825 个，其中与路由器、交换机等网络设备相关的漏洞占比达 66.2%，主要包括内置后门、远程代码执行等类型，这些漏洞将可能导致网络设备或节点被操控，出现窃取用户信息、传播恶意代码、实施网络攻击、破坏网络稳定运行等安全事件。

• 云服务日益成为网络攻击的重点目标

我国基础电信企业和许多大型互联网服务商纷纷加快云平台部署，大力推广云服务，大量金融、游戏、电子商务、电子政务等业务迁移至云平台。2014 年先后发生了多起因电力、机房线路和网络故障导致的云服务宕机事件，针对云平台的攻击事件也逐年增多，仅由 CNCERT 协助处置的大规模攻击事件就达十余起，涉及 Ucloud 公司、浙江宁波某 IDC 机房等国内云平台。据有关单位报告，2014 年 12 月中旬，某大型互联网服务商的云平台上一家知名游戏公司遭受拒绝服务攻击，攻击峰值流量超过 450Gbps。云平台运行的稳定性直接影响业务的可用性和连续性，而且针对云平台上某一目标的攻击，还可能导致其它业务受到牵连，造成大面积用户无法访问或使用。



^③ CNVD 全称为国家信息安全漏洞共享平台（CHINA NATIONAL VULNERABILITY DATABASE），是由 CNCERT 联合国内重要信息系统单位、基础电信企业、网络安全厂商、软硬件厂商和互联网企业建立的信息安全漏洞信息共享知识库，网址为 www.cnvd.org.cn。

◎ 域名系统

域名是网站的入口，其解析安全直接影响网站的正常访问。域名系统承担域名解析工作，面临严重拒绝服务攻击威胁，一些重要网站频繁发生域名解析被篡改事件。

• 域名系统面临的拒绝服务攻击威胁进一步加剧

据抽样监测，2014 年针对我国域名系统的流量规模达 1Gbps 以上的拒绝服务攻击事件日均约 187 起，约为 2013 年的 3 倍，攻击目标上至国家顶级域名系统，下至 CDN 服务商的域名解析系统。与往年相比，攻击发生频率更高、流量规模更大。6 月，我国某权威新闻网站的权威域名服务器遭受拒绝服务攻击，峰值流量达 1.6Gbps，CNCERT 对攻击进行追溯分析，为公安部门破案提供了重要线索。同月，国内某主要 CDN 服务商的域名服务器遭大规模异常流量攻击，由于其承载国内大量重要网站的 CDN 加速服务，导致对这些网站的访问均受到严重影响。10 月，国家 .CN 顶级域名系统继 2013 年 8 月 25 日之后再次遭受大规模流量攻击，由于系统加强了安全防护措施，未受到严重影响，但在一定程度上反映出我国顶级域名系统面临的严峻外部威胁。12 月，我国多个省份的递归域名解析服务器受到攻击，造成部分地区的互联网使用受到影响。

• 针对重要网站的域名解析篡改事件频发

2014 年发生了多起国内政府网站、重要媒体或企事业单位网站的域名解析被篡改的事件。某省重要新闻网站在短时间内连续数次遭受域名解析被恶意篡改的攻击，黑客入侵该网站域名注册服务商的业务系统，直接篡改数据库中相应数据，获取该网站的域名管理权限，将其域名解析服务器改为专门提供免费域名解析的 DNSPOD 服务器地址，并将其域名指向境外地址。经 CNCERT 对我国政府网站（以 .gov.cn 结尾）域名解析情况监测分析，在 10 月期间测试的 870 万余个域名中，约有 107 万余个域名被解析到境外 IP 地址，其中有 2.9 万个域名的 Web 端口能够访问，部分指向推广游戏、色情、赌博等内容的异常页面，还有部分页面被植入恶意代码，不仅影响网站管理方形象，甚至可能造成大面积网络安全危害。



◎ 工业互联网

随着互联网的推进和制造业的转型升级，工业互联网成为推动制造业向智能化发展的重要支撑，将工业领域的生产、研发、管理、销售等各个环节与互联网紧密相连，网络安全风险逐渐累积和延伸，威胁扩展至传统工业基础设施。

• 网络攻击威胁日益向工业互联网渗透

针对工业控制系统的攻击方法和手段已逐渐成熟，并有能力影响物理生产运行环境。根据国际有关机构披露，2014 年 9 月出现一种远程木马“Havex”，它利用了 OPC^④ 工业通信技术，具有很强的针对性，其主要功能是扫描发现工业系统联网设备，收集工控设备详细信息并秘密回传，预置后门并在必要时接收、执行控制端发送的恶意代码，全球能源行业的数千个工业控制系统曾被其入侵。据监测，我国境内已有部分 IP 地址感染了该恶意程序，所对应的控制端均位于境外，并存在部分 IP 地址持续向控制端发送信息的情况。

^④ 一种开放、通用的工业数据交换协议，能够实现基于 Windows 平台的工业控制系统应用程序与过程控制硬件之间的交互通信。

| (二) 公共互联网网络安全环境 |

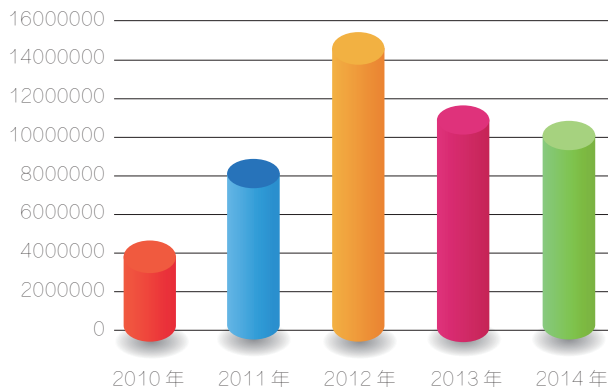
◎ 木马僵尸网络

2014 年，我国境内木马僵尸网络控制服务器和感染主机数量继续呈下降趋势，治理工作成效明显。

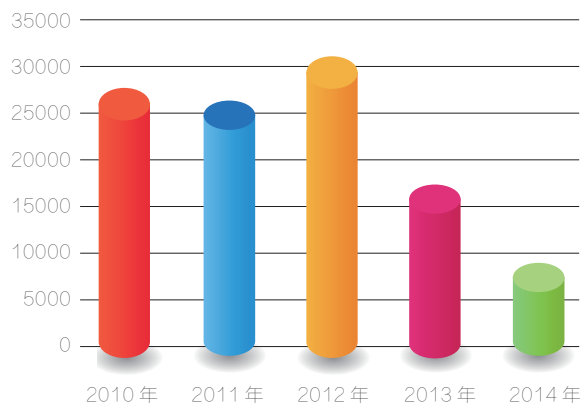
• 我国境内木马僵尸网络感染主机数量稳步下降

据抽样监测，2014 年我国境内感染木马僵尸网络的主机为 1108.8 万余台，较 2013 年下降 2.3%，境内木马僵尸控制服务器 6.1 万余个，较 2013 年大幅下降 61.4%。2014 年，在工业和信息化部的指导下，CN-CERT 协调基础电信企业、域名服务机构等成功关闭 744 个控制规模较大的僵尸网络，累计处置 767 个恶意控制服务器和恶意域名，成功切断黑客对 98 万余台感染主机的控制，有力净化了公共互联网网络安全环境。随着我国持续加大公共互联网环境监管和治理力度，大量僵尸网络控制服务器向境外迁移，2014 年抽样监测发现境外 4.2 万个控制服务器控制了我国境内 1081 万余个主机，境外控制服务器数量较 2013 年增长 45.3%。

近五年来我国境内木马僵尸网络感染主机数量



近五年来我国境内木马僵尸网络控制服务器数量



◎ 拒绝服务攻击

传统拒绝服务攻击主要依托木马僵尸网络，通过控制大量主机或服务器（俗称“肉鸡”）对受害目标发起攻击，近年来，拒绝服务攻击的方式和手段在不断发展变化，分布式反射型的拒绝服务攻击日趋频繁。

• 分布式反射型攻击逐渐成为拒绝服务攻击的重要形式

分布式反射型攻击是指黑客不直接攻击目标，而利用互联网的一些网络服务协议和开放服务器，伪造被攻击目标地址向开放服务器发起大量请求包，服务器向攻击目标反馈大量应答包，间接发起攻击。这种方式能够隐藏攻击者来源，以较小代价实现攻击规模放大，且攻击目标难以防御，在我国呈现出三个明显特点：一是频繁发生且流量规模大。仅 2014 年 10 月，我国就有数十个重要政府的网站和邮件系统遭受到此类攻击，部分攻击流量规模达到

10Gbps 以上。二是攻击方式复杂多样。攻击者综合运用 DNS 协议、NTP 协议^⑤、UPnP 协议^⑥、CHARGEN 协议^⑦等多种协议进行攻击，防御困难。三是攻击包来源以境外为主。在 2014 年发现的分布式反射型攻击中，绝大部分伪造的请求包来自境外，这一方面是由于我国基础网络持续开展虚假源地址流量整治工作，攻击者难以从境内网络发出此类伪造包，另一方面也从一定程度上反映出境外对我攻击频繁。

⑤ NTP 协议，即网络时间协议（Network Time Protocol）。

⑥ UPnP 协议，即通用即插即用（Universal Plug and Play）协议。

⑦ CHARGEN 协议，即字符发生器协议（Character General Protocol）。

◎ 安全漏洞

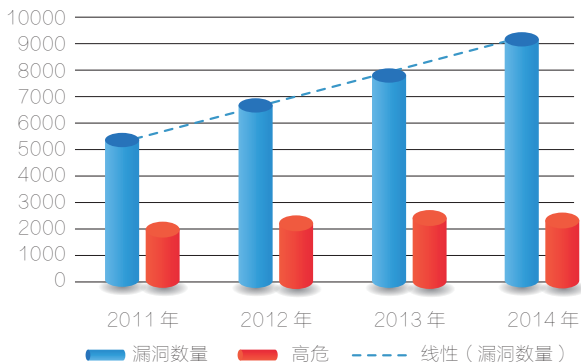
2014 年，安全漏洞信息共享工作持续推进，重要行业和政府部门信息系统的漏洞事件备受关注，“心脏出血”、“破壳”等漏洞展现了基础应用和通用软硬件面临的高危风险，漏洞威胁向传统领域和智能设备领域演化延伸。

• 涉及重要行业和政府部门的高危漏洞事件增多

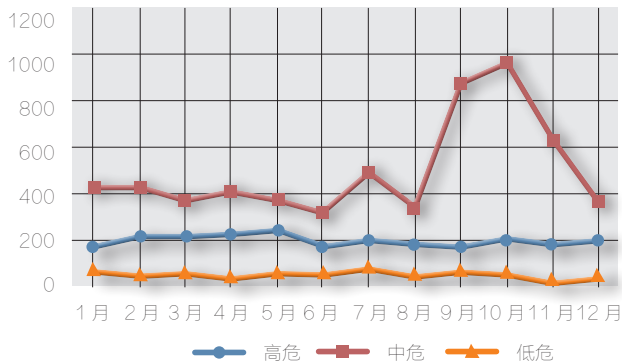
近年来，CNVD 新增收录漏洞数量年均增长率在 15% 至 25% 之间，针对漏洞的挖掘和利用研究日趋活跃。2014 年，CNVD 收录并发布各类安全漏洞 9163 个，较 2013 年增长 16.7%，平均每月新增收录漏洞 763 个；其中高危漏洞 2394 个，占 26.1%，可诱发零日攻击的漏洞 3266 个（即披露时厂商未提供补丁），占 35.6%。漏

洞研究者对重要企事业单位信息系统安全问题的关注程度日益提升，在 2014 年收录的漏洞中，涉及电信行业的占 9%，涉及工控系统的占 2.0%，涉及电子政务的占 1.9%，CNCERT 全年向政府机构和重要信息系统部门通报漏洞事件 9068 起，较 2013 年增长 3 倍。

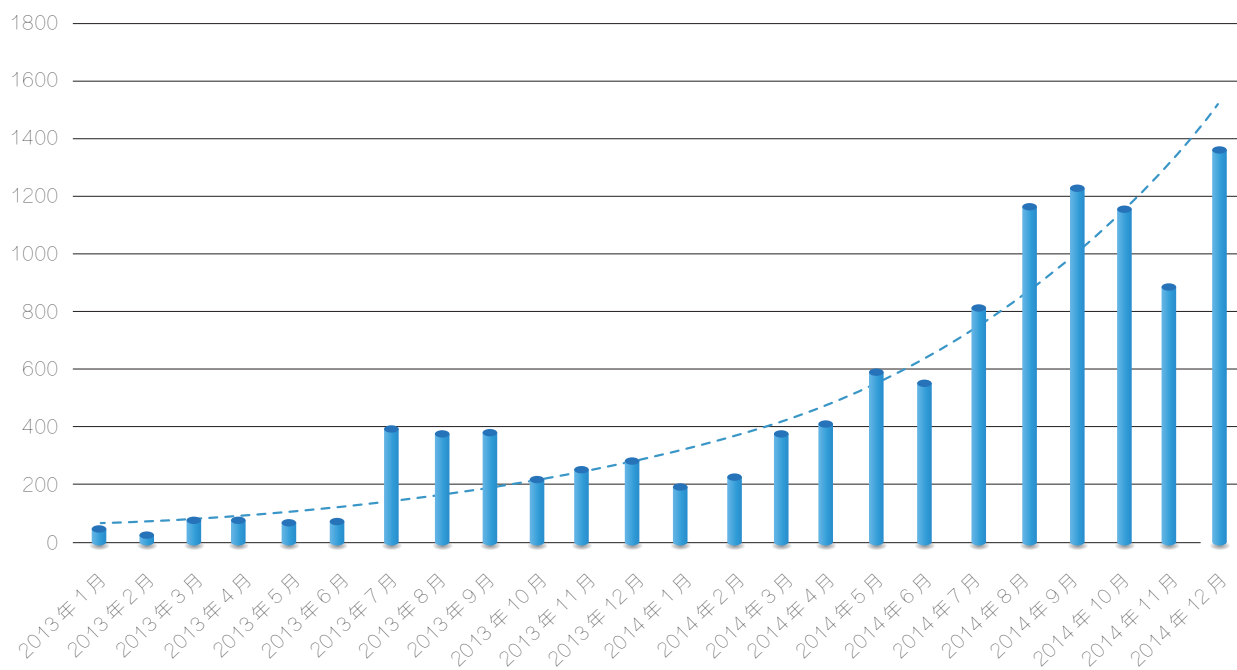
近年来 CNVD 收录漏洞和高危漏洞数量



2014 年 CNVD 收录漏洞数量月度统计



2013 年 – 2014 年向重要单位通报漏洞事件数量



• 基础应用或通用软硬件漏洞风险凸显

2014 年 CNCERT 通报处置通用软硬件漏洞事件 714 起，较 2013 年增长 1 倍。由于基础应用和通用软硬件产品部署广泛，漏洞容易被批量利用，而且定位和修复困难，影响范围可能波及全网，危害程度远大于一般漏洞。4 月 8 日，开源加密协议 OpenSSL 被披露存在内存泄露高危漏洞^⑧，又称“心脏出血（Heartbleed）”漏洞，利用该漏洞可窃取服务器敏感信息，实时获取用户的账号和密码，危害波及大量互联网站、电子商务、网上支付、即时聊天、办公系统、邮件系统等，据抽样统计，我国境内受该漏洞影响的 IP 地址超过 3 万个。9 月 25 日，GNU Bash 组件被披露存在远程代码执行高危漏洞^⑨，又称“破壳（Bash Shellshock）”漏洞，Redhat、Fedora、CentOS、Ubuntu、Debian、MAC OS 等几乎目前所有主流 UNIX/Linux 操作系统平台、使用 ForceCommand

功能的 OpenSSH sshd、使用 mod_cgi 或 mod_cgid 的 Apache 服务器、DHCP 客户端和其它使用 Bash 作为解释器的应用均受到影响，不仅是服务器系统，还包括交换机、防火墙、网络设备以及摄像头、IP 电话等许多基于 Linux 的定制系统，影响范围比“心脏出血”漏洞更为严重。根据对部分漏洞的持续监测来看，漏洞修复的速度总体较为缓慢。“心脏出血”漏洞披露 3 个月后发现仍有约 16% 尚未修复，而知名度相对较低的 Nginx 文件解析漏洞（影响 Web 应用）在披露 1 年后未修复率仍高达 55%。此外，4 月 8 日微软公司正式停止对 Windows XP 系统的支持服务，而从 4 月底至 8 月中旬的抽样监测统计发现，在我国使用微软操作系统的用户中，超过半数仍在 Windows XP 系统，这些用户在未来相当长的一段时间内将面临严重的“零日攻击”风险。



⑧ 编号 CNVD-2014-02175, CVE-2014-0160。

⑨ 编号 CNVD-2014-06345, CVE-2014-6271。



• 漏洞威胁向传统领域泛化演进

随着信息化发展，传统广播电视、公共管理、社会服务等领域与互联网紧密融合，漏洞威胁也在演化跟进。2014 年 CNCERT 处置多起公共服务管理系统存在漏洞风险的事件，涉及公共场所 LED 信息管理、高速公路视频监控、区域车辆 GPS 调度监控等，这些漏洞一旦被利用，将直接影响日常交通管理和公众生活。

• 漏洞威胁向新兴智能设备领域延伸

2014 年，移动互联网与传统产业结合催生智能硬件新业态，智能手环、智能手表等可穿戴设备、互联网电视等产品成为市场热点，智能汽车、智能家居、智慧城市成为新时尚，随着终端设备的功能和性能大幅提升，面临的安全威胁增大。国外某著名电动汽车车载控制系统存在安全漏洞，导致攻击者可远程控制车辆，实现开锁、鸣笛、闪灯、开启天窗等操作。2014 年已经发现一些 ADSL 终端、智能监控设备、智能路由器、网络摄像头、机顶盒等联网智能设备被黑客控制发起网络攻击，这些联网智能设备普遍存在弱口令、配置不当等安全问题，很容易被攻击者安装木马变成“肉鸡”长期进行控制。



◎ 网络数据泄露

自 2011 年 CSDN 社区信息泄露事件后，近年来网站数据泄露事件不断发生，2014 年网站拖库^⑩、撞库^⑪攻击现象仍然严重。

• 网站数据和个人信息泄露仍呈高发态势

网站管理者对数据保护的重视程度日益提升，但在网站数据和个人信息利益价值凸显的背景下，数据泄露事件仍频繁出现，有的依然是由于技术漏洞或管理问题导致的拖库事件，有的则来自撞库攻击。2014 年我国多家知名电商、快递公司、招聘网站、考试报名网站等发生数据泄露事件。5 月中旬，工业和信息化部处理一起某知名手机厂商论坛数据泄露事件，由于此前使用的用户管理模块存在漏洞，导致包括账号、密码和社交账号等的 800 万用户信息泄露，其中有 140 万用户的密码从未修改过（包括开通了云平台账号的 130 万用户），是此次泄露事件受威胁对象，存在黑客针对特定用户实施密码暴力破解的风险。12 月 25 日，国内某著名交通购票网站遭受撞库攻击，导致包括用户账号、明文密码、身份证号码、手机号码和电子邮箱等在内的 13 万多条用户数据在互联网上流传。针对所泄露的数据分析发现，“123456”、“a123456”、“123456a”等弱口令高居榜首，用户的密码安全意识仍有待提高。

• 移动应用程序成为数据泄露的新主体

2014 年，订票、社交、点评、论坛、浏览器等国内多种知名移动应用发生用户数据泄露事件。一些移动应用开发者经验不足，安全意识和水平不够，网站服务器对移动端的访问控制机制较弱，黑客利用移动应用程序与网站服务器之间的接口漏洞，对网站服务器发起攻击，能够轻易获得相应服务器的地址和接口信息，再通过挖掘接口漏洞，直接获取服务器中所有信息，造成信息泄露。2014 年 CNVD 收录 1710 个涉及移动互联网终端设备或软件产品的漏洞，这都可能成为黑客攻击获取用户信息新的入口。

^⑩ 拖库指黑客入侵网站，将网站的用户资料数据库全部盗走的行为。

^⑪ 撞库是指黑客利用从某些网站或渠道获取的用户账号和密码，在其它网站上进行登录尝试。这主要是由于目前有相当一部分互联网用户喜欢在不同网站上使用统一的用户名和密码。

◎ 移动互联网恶意程序

在工业和信息化部指导下，通信行业各方共同努力，积极开展移动互联网环境治理，国内主流应用商店的安全状况有所改善，但移动互联网恶意程序不断发展演化，给治理工作带来挑战。

• 移动互联网网络安全威胁治理取得明显成效

2014 年 4 月至 9 月，工业和信息化部联合公安部、工商总局开展打击治理移动互联网恶意程序专项行动，CNCERT、基础电信企业、域名注册服务机构、安全企业、应用商店和数字认证服务企业等多家单位积极参与，取得明显成效。专项行动期间，及时有效处置了“XX 神器”病毒大规模传播事件，协调处置移动恶意程序控制服务器和传播源链接 1.01 万个；开办主体主动关停或监管部门依法关停应用商店 283 家；中国互联网协会反网络病毒联盟（ANVA）、电子认证服务机构、应用商店、手机安全软件厂商和手机终端生产企业等多方力量联合，试点开展移动应用程序开发者第三方数字证书签名与验证，以实现移动应用程序的防篡改和可溯源；持续推进自律黑名单共享工作，发布移动恶意程序黑名单 4.9 万条、传播地址黑名单 1187 条，发布中国农业银行、奇虎 360、百付宝、搜房等 4 张移动互联网应用自律白名单证书。

• 移动恶意程序逐渐从主流应用商店向小型网站蔓延

2014 年，根据工业和信息化部《移动互联网恶意程序监测与处置机制》，CNCERT 每周协调应用商店下架移动恶意程序，累计通知 139 家应用商店、网盘、下载站点等下架恶意程序 4.1 万个，实际下架 3.9 万余个，下架率达到 95.5%。经过连续两年的治理，国内 30 余家主流应用商店的安全意识均有提高，审核制度和检测手段逐步改善，恶意程序数量由 2013 年的 3.73 万个大幅下降至 0.93 万个，安全状况明显改善。移动恶意程序逐渐向个人网站、广告平台等小型网站蔓延，2014 年监测发现 100 余个小型网站传播移动恶意程序 3 万余个，其中单个网站传播移动恶意程序的数量最多超过 2000 个，针对这类网站的监测处置将是未来移动互联网环境治理工作的重点。

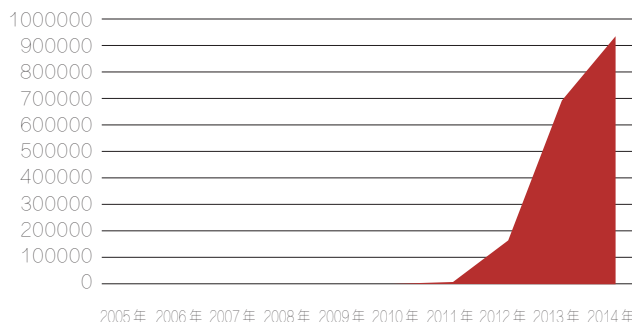
• 移动恶意程序治理打击对抗性初显

2014 年，CNCERT 通过自主监测和交换捕获的移动互联网恶意程序样本达 95.1 万余个。按行为属性分类^②，恶意扣费类的恶意程序数量居首位，占 55.0%，其次是资费消耗类和信息窃取类，分别占 15.3% 和 12.9%，信息

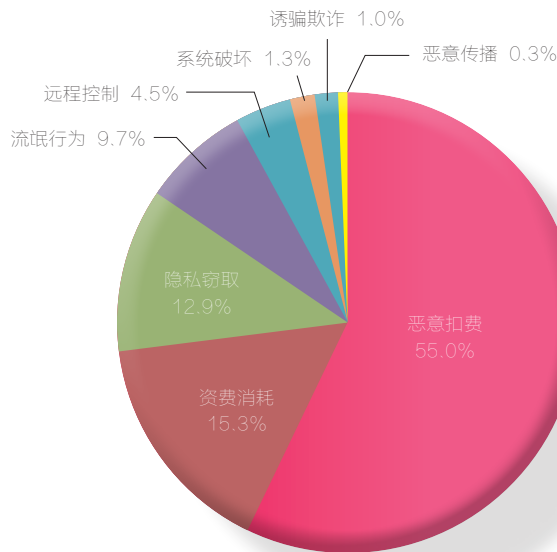
② 如果单个恶意程序具有多重恶意行为属性，统计时根据标准 YD / T 2439-2012《移动互联网恶意代码描述格式》中对恶意行为属性的恶意性等级划分，按其等级最高的恶意行为属性进行统计。

窃取类所占比例较 2013 年的 3.2% 大幅上升。据抽样监测, 2014 年我国感染移动恶意程序的用户数量达 2292 万, 其中感染安卓平台恶意程序的用户数量最多, 达 1575 万余个, 也发现约 30 万用户感染基于苹果 iOS 平台的恶意程序, 如“Panda”、“Wirelurker”等。移动恶意程序的对抗性明显增强, 制作者普遍采用“加固”技术对抗安全检测, 2014 年发现的移动恶意程序样本中有 2.2% 经过“加固”处理, 检测发现难度加大, 给治理工作带来新的挑战。

2005 年 - 2014 年移动互联网恶意程序走势



2014 年移动互联网恶意程序数量按行为属性统计



• 具有短信拦截功能的移动恶意程序大量爆发

目前网银、网购等普遍通过短信验证码方式对用户身份进行校验, 2014 年具有拦截、转发手机短信功能的移动恶意程序数量大幅增长。黑客从短信中获取用户的重要个人信息, 如姓名、身份证号码、银行卡账号、支付验证码、各种登录账号密码等, 再结合其它钓鱼欺诈手段, 窃取用户资金或实施诈骗活动, 威胁用户财产安全。这类恶意程序开发成本低、更新速度快, 一般还带有隐私窃取、远程控制、诱骗欺诈、资费消耗等其它功能。据抽样监测分析, 此类恶意程序最早出现于 2013 年 5 月, 2014 年起开始流行爆发, 目前已发现该类样本 16 万余个, 8 月爆发的“XX 神器”移动恶意程序通过拦截和转发短信, 感染全国用户数量达到 11 万, 波及国内 31 个省 (自治区、直辖市), 在工业和信息化部指导下, CNCERT 及时完成对该样本的分析, 并协调进行处置, 有效控制了其传播态势。

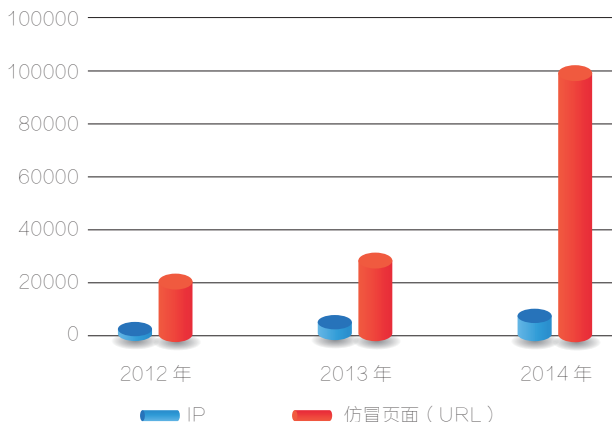
◎ 网络仿冒

2014 年，针对金融、电信行业的网页仿冒事件大幅增长，大量钓鱼站点向云平台迁移，加大事件处置难度，影响用户经济安全和信息消费。

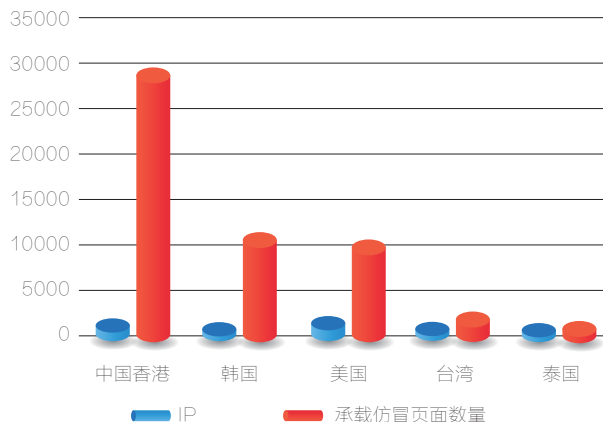
• 针对金融、电信行业的仿冒事件大幅增长

2014 年抽样监测发现，针对我国境内网站的仿冒页面（URL 链接）近 10 万个，较 2013 年增长 2.3 倍，涉及 IP 地址 6844 个，较 2013 年增长 61.4%。在针对我国境内网站的钓鱼站点（IP 地址）中，89.4% 位于境外，承载仿冒页面 9 万余个，较 2013 年增长 2.1 倍，主要是位于香港地区的钓鱼页面数量将近 3 万个，较 2013 年大幅增长。从被仿冒对象来看，针对第三方支付机构、网上银行等金融机构的仿冒页面占比超过 80%，主要是诱骗用户提交银行卡号、密码、身份证号码等信息，同时发现大量针对电信企业的仿冒页面，主要是一些虚假的充值页面，占比达 12%，已超过仿冒知名电视节目或大型互联网站进行虚假抽奖的页面数量。网页仿冒与移动应用结合日益紧密，许多仿冒页面仅能通过移动智能终端访问，针对手机网银、微信等移动应用仿冒事件频发。

近年来针对我国境内网站的仿冒站点和页面数量



2014 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



• 钓鱼站点逐渐向云平台迁移

云服务申请和使用方便、成本低廉、安全审核不严，且云平台同时承载多种不同类型的业务，传统基于 IP 地址的追踪处置手段难以适用，日益成为钓鱼网站栖息的“温床”。针对 2014 年处置的银行类钓鱼网站分析，按所承载的钓鱼网站数量（按域名统计）排序，排名前 10 的 IP 地址有 4 个属于云服务提供商。



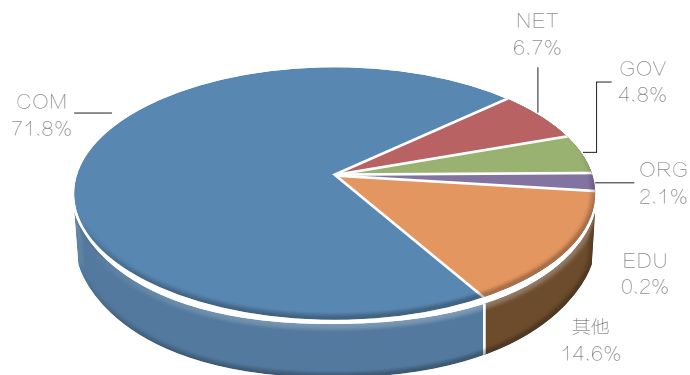
◎ 网站攻击

“匿名者”等黑客组织对我国政府部门和重要企事业单位网站的攻击依然频繁，出现了向网站中植入钓鱼页面、针对性地实施拒绝服务攻击、窃取网站数据等情况。

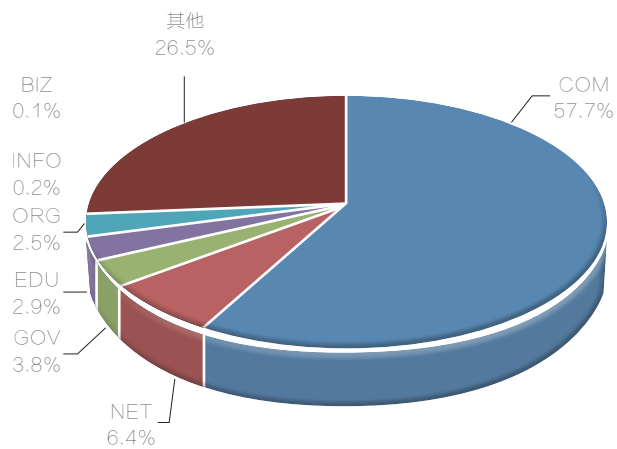
• 针对政府部门和重要行业单位网站的网络攻击频度、烈度和复杂度加剧

据监测，2014 年我国境内被篡改的政府网站 1763 个，被植入后门的政府网站 1529 个，分别占全部被篡改网站的 4.8% 和全部被植入后门网站的 3.8%，据通信行业信息，出现的一个新特点是大量政府和教育类网站的子页面被篡改并植入钓鱼页面。黑客组织对我国政府部门网站的攻击依然频繁。“匿名者”等黑客组织先后篡改了我国 400 余个网站，在针对中国大陆和中国香港政府网站的所谓“OpHongKong”攻击行动中，黑客组织宣称对我国 150 余个重要政府部门的网站发动大规模攻击，并公布了大量攻击目标的 URL 链接、网站服务器类型、IP 地址等详细信息，据 CNCERT 监测其攻击成功的网站达到 40 余个，除网页篡改和植入后门外，还发现许多技术手段复杂、流量规模大的拒绝服务攻击，以及入侵窃取网站内存储的用户信息并公布的情况，严重影响网站的正常运行。

2014 年境内被篡改网站按类型分布



2014 年境内被植入后门的网站数量按域名类型分布







2015 年值得关注的热点问题

根据对 2014 年我国互联网网络安全形势特点的分析，我们认为 2015 年需重点关注的一些热点问题主要如下：

◎ 拒绝服务攻击威胁将继续升级，影响基础网络稳定运行

分布式反射型攻击将继续是实施拒绝服务攻击的重要形式，攻击者将不断分析挖掘更多可被利用的网络协议，增加攻击威力，突破防护措施，大量联网智能设备将成为发起攻击的重要工具。随着拒绝服务攻击与防护的对抗日趋激烈，攻击流量规模可能进一步增大，单个攻击事件的峰值流量甚至可能突破 1Tbps。针对域名系统的攻击将继续呈频繁态势，不仅影响受害目标，而且波及整个基础网络。此外由于网络攻击软件的工具化和平台化、网络攻击服务的商业化等因素，大大降低发起攻击的难度和成本，攻击门槛将越来越低。

◎ 移动恶意程序借助“加固”手段对抗安全检测的情况将更加普遍，利用仿冒应用实施钓鱼欺诈的现象将更为猖獗

随着安卓应用免费“加固”服务市场的发展，“加固”技术手段将不断升级，移动恶意程序制作者利用代码加密、加壳等手段对抗安全检测的现象将更加流行，这将导致经过“加固”处理的恶意程序数量大幅增长，



H 热点问题 > Hot issues

进一步加大移动恶意程序治理工作难度。由于移动应用制作成本较低、追溯较困难等因素影响，黑客制作假冒手机网银、运营企业客户端、热门游戏等的应用程序、通过钓鱼短信或小型网站、社交平台、广告平台等渠道散播、以窃取用户钱财的现象将更加猖獗。

◎ 云平台普及加大数据泄露和网络攻击风险，防护措施和管理机制有待完善

一是云平台的数据安全保护问题。云计算技术的发展推动数据的集中化，在大数据时代，海量数据既是企业和用户的核心资产，也成为网络攻击瞄准的目标，以窃取数据为主要目的的攻击事件将越来越多，云平台自身的网络安全防护特别是对海量数据安全的防护将面临挑战。二是云平台的安全审核和管理机制问题。目前大多数云服务商的安全审核机制并不完善，用户租用后作何用途，云服务商并不清楚知晓，也未作严格审核或周期性检查，因此出现黑客在云平台部署钓鱼网站、传播恶意代码或发动攻击的情况，如不及时加强管理，未来这种现象将继续增多。

◎ 针对基础应用、通用软硬件和国产软硬件的漏洞挖掘将增多，应对机制和披露管理面临挑战

2015 年，黑客将更加关注应用广泛的网站应用框架、开源软件、集成组件、网络协议等的安全问题，随着服务器、



芯片、操作系统、数据库、办公软件等信息产业各个领域的自主可控深入推进，国产软硬件产品应用增多，其安全问题将受到更多重视。由于基础应用、通用软硬件或国产软硬件的影响范围广泛，一旦漏洞信息提前披露或不客观披露，容易造成社会公众心理恐慌，并引发大面积攻击事件，针对这类应用或产品的漏洞信息披露和应对处置面临挑战。

◎ 智能终端将成为新的攻击入口，物联网面临安全挑战

设备智能化的浪潮席卷各行业，智能终端具有带宽较高、全天候在线、系统升级慢、配置较少变动等特点，但由于技术不完善、忽视安全性等原因，大量智能终端设备存在弱口令或安全配置不当等漏洞，安全威胁也随之而来。随着物联网产业的发展和智慧城市的建设，智能生活逐渐推广，连接一切将日益成为现实，智能终端自身安全以及

终端间连接或通信的安全问题，都是物联网面临的安全挑战。

◎ 智能制造面临的网络攻击威胁将凸显，工业互联网发展面临挑战

以智能制造为主攻方向的“中国制造 2025”计划，旨在充分利用信息通信（ICT）技术与制造技术的结合，推动新一轮科技革命和产业变革，实现智能制造、网络制造、绿色制造、服务性制造，促进制造业的数字化、网络化、智能化发展。工业互联网是实现智能制造的必备基础，是智能制造生产体系中必不可少的环节。随着传统工业基础设施加快向工业互联网基础设施演进升级，其所面临的网络攻击威胁也将日益凸显。从近几年的实际案例和统计数据可以看出，针对工业基础设施的网络攻击行为发生频率总体呈逐年增高趋势，攻击手段日益复杂高级，且带有显著 APT 特征，攻击危害逐渐加大，网络攻击威胁将成为工业互联网发展过程中无法回避的问题。





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“863-917 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

I 简介 Introduction

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。

◎ 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：+8610 82990999（CN），
82991000（EN）
- 传真：+8610 82990399

2014

我国互联网 网络安全态势报告



网址: <http://www.cert.org.cn/>

电子邮件: cncert@cert.org.cn

热线电话: +861082990999 (CN), 82991000 (EN)

传真: +861082990399