2013 年我国互联网网络安全态势综述

——CNCERT 观点

习近平总书记指出：“没有网络安全，就没有国家安全”。以互联网为核心的网络空间已成为继陆、海、空、天之后的第五大战略空间，各国均高度重视网络空间的安全问题。2013 年，斯诺登披露的“棱镜门”事件如同重磅炸弹，更是引发了国际社会和公众对网络安全的空前关注。

在我国，随着“宽带中国”战略推进实施，互联网升级全面提速，用户规模快速增长，移动互联网新型应用层出不穷，4G 网络正式启动商用，虚拟运营商牌照陆续发放，网络化和信息化水平显著提高，极大促进传统产业转型升级，带动信息消费稳步增长。

维护互联网网络安全，是保障各领域信息化工作持续稳定发展的先决条件。我国政府相关部门、互联网服务机构、网络安全企业和广大网民对网络安全的重视程度日益提高，不断加强自身防护水平，加大网络安全威胁治理力度，积极参与网络安全国际合作，以期建立安全可信的网络环境，确保基础网络和重要信息系统安全运行，促进产业经济稳定发展。

在各方共同努力下，2013 年我国互联网网络安全状况总体平稳。然而，根据 CNCERT 监测数据和通信行业报送信息，我国互联

网仍然存在较多网络攻击和安全威胁，不仅影响广大网民利益，妨碍行业健康发展，甚至对社会经济和国家安全造成威胁和挑战。本综述着重分析和总结2013年我国互联网面临的安全形势和威胁。

态势要点

◆ 基础信息网络运行总体平稳，域名系统依然是影响安全的薄弱环节

- 基础网络安全防护水平和防范意识进一步提高，符合性评测达标率在97%以上。
- CNVD通报基础网络相关漏洞事件518起，较2012年增长超过一倍，涉及的信息系统超过一半属于基础电信企业省（子）公司。
- 安全漏洞多次引发域名劫持事件，2013年8月25日我国国家.CN顶级域名遭攻击瘫痪。
- 微信断网、宽带接入商路由劫持等事件反映出基础网络承载的互联网业务发展带来的新风险。

◆ 公共互联网治理初见成效，打击黑客地下产业链任重道远

- 我国境内感染木马僵尸网络的主机数量首次下降，降幅22.5%，治理初见成效。
- CNVD分析发现涉及通信网络设备的软硬件漏洞数量较2012年增长1.5倍，友讯等众多网络设备存在后门，被黑客利用劫持用户流量。
- 越来越多与人们生活密切相关的信息汇聚到网络，存在严重泄露风险，并可能给传统社会的信任机制带来挑战。

◆ 移动互联网环境有所恶化，生态污染问题亟待解决

- 安卓平台恶意程序数量呈爆发式增长，2013年新增移动互联网恶意程序样本达70.3万个，较2012年增长3.3倍，其中99.5%针对安卓平台。
- 手机应用商店、论坛、下载站点、经销商等生态系统上游环节污染，下游用户感染速度加快。

◆ 经济信息安全威胁增加，信息消费面临跨平台风险

- 跨平台钓鱼攻击出现并呈增长趋势，针对我国银行等境内网站的钓鱼页面数量和涉及的IP地址数量分别较2012年增长35.4%和64.6%，全年接收的钓鱼事件投诉和处置数量高达10578起和10211起，分别增长11.8%和55.3%。
- 互联网交易平台和手机支付客户端等存在漏洞，威胁用户资金安全，安全风险可能传导到与之关联的其他行业，产生连锁反应。

◆ 政府网站面临的威胁依然严重，地方政府网站成为“重灾区”

- 地方政府网站是黑客攻击的“重灾区”，2013 年我国境内被篡改和被植入后门的政府网站中，超过 90%是省市级以下的地方政府网站。
- 我国政府网站频繁遭受黑客组织攻击，其中“匿名者”等黑客组织至少入侵我国境内超过 600 个网站。继央行明确不认可比特币后，央行官方网站和新浪官方微博遭受黑客攻击。

◆ 国家级有组织攻击频发，我国面临大量境外地址攻击威胁

- 国家级有组织网络攻击频发，我国部分重要网络信息系统遭受渗透入侵，2013 年 CNCERT 监测发现境内 1.5 万台主机被 APT 木马控制。
- 2013 年，境内 6.1 万个网站被境外通过植入后门实施控制，较 2012 年大幅增长 62.1%；针对境内网站的钓鱼站点有 90.2%位于境外；境内 1090 万余台主机被境外控制服务器控制，主要分布在美国、韩国和中国香港，其中美国占 30.2%，控制主机数量占被境外控制主机总数的 41.1%。

一、我国互联网网络安全形势

（一）基础信息网络运行总体平稳，域名系统依然是影响安全的薄弱环节。2013 年，我国基础网络安全防护水平有较大提升，但仍然发现较多信息系统安全风险，尤其是域名系统作为互联网运行的关键基础设施，面临安全漏洞和拒绝服务攻击等多种威胁，是影响网络稳定运行的薄弱环节。基础网络承载的互联网业务类型日益增多，引发一些安全风险。

基础网络安全防护水平进一步提高。2013 年，在工业和信息化部指导下，基础电信企业高度重视网络安全防护工作，在全网开展网络单元和业务系统的定级备案调整工作，对 3000 余个三级及以上网络单元开展符合性评测和风险评估，各企业符合性评测达标率均在 97%以上，与 2012 年基本持平。在检测中还侧重加大对用户个人信息保护工作的检查力度，通过对安全隐患的测试和修复，有效降低了通信网络的安全风险。

基础网络信息系统仍存在较多安全风险。2013 年，国家信息安全漏洞共享平台（CNVD）向基础电信企业通报漏洞风险事件 518 起，较 2012 年增长超过一倍。按漏洞风险类型分类，其中通用软硬件、信息泄露、权限绕过、SQL 注入、弱口令等类型较多，分别占比 42.1%、15.3%、12.7%、12.0%和 11.2%。这些漏洞风险事件涉及的信息系统达 449 个，其中基础电信企业省（子）公司所属信息系统占 54.6%，集团公司所属信息系统占 37.2%。对此，各企业均积极响应，及时进行修复加固处理。但是，2013 年仍发现有

部分企业的接入层网络设备被攻击控制，网络单元稳定运行以及用户数据安全受到威胁，我国基础网络整体防御国家级有组织攻击风险的能力仍较为薄弱。

域名系统依然是影响互联网稳定运行的薄弱环节。域名解析服务是互联网重要的基础应用服务，其安全问题直接影响网络的稳定运行。由于域名注册服务机构的域名管理系统存在漏洞，攻击者能随意篡改域名解析记录，2013 年曾发生多起由此引发的政府部门网站和提供互联网服务的网站域名被劫持的事件，导致用户访问受到严重影响。此外，域名系统遭受拒绝服务攻击的情况日益严重。2013 年 8 月 25 日，黑客为攻击一个以.CN 结尾的网游私服网站，对我国家.CN 顶级域名系统发起大规模的拒绝服务攻击，导致大量政府网站、新浪微博等重要网站无法访问或访问缓慢。同年 8 月，域名注册服务机构爱民网（22.cn）的域名服务器在一周内连续遭受数十 Gbit/s 级的拒绝服务攻击，数万个域名受到影响。据 CNCERT 监测，2013 年针对我国域名系统的较大规模拒绝服务攻击事件日均约有 58 起。直接针对域名系统发起攻击，不仅能使目标网站瘫痪，还会导致大量无辜网站受到牵连，从而造成严重后果。

对此，CNCERT 联合基础电信企业，积极配合政府部门，大力推进虚假源地址流量整治工作，将我国互联网虚假源地址流量占全部流量的比例控制在 1%以内，有效提高了攻击源追溯能力，为国家.CN 域名系统遭受攻击等重大事件查处提供了有力支撑。但与

此同时，还监测发现大量来自境外的虚假源地址攻击流量，这给事件处置和攻击追溯带来很大困难。

2013 年 3 月，国际反垃圾邮件组织 Spamhaus 遭受攻击，攻击峰值达 300Gbit/s，堪称互联网史上最大流量的拒绝服务攻击。攻击者借助互联网庞大的开放域名解析服务器群，利用 DNS 反射技术发送大量伪造的 DNS 解析请求，使服务器向目标网站发送大量长字节应答包，从而对目标网站形成放大约 100 倍的攻击流量。互联网上大量存在的开放递归查询域名服务器，有可能成为黑客实施攻击的“军火库”。

基础信息网络承载的互联网业务频现安全问题。随着基础网络设施不断完善，其所承载的互联网业务类型日益增多，引入新的安全风险。2013 年 7 月 22 日，腾讯微信业务出现故障，全国多地有 6000 多万用户无法正常使用，用户感知强烈。微信属于目前较为流行的 OTT（Over The Top）业务模式，通过基础电信企业的网络发展自己的音视频和数据服务业务，但其安全保障水平和业务承载级别不匹配，一条线路的故障就能导致涉及多家基础电信企业的用户受到影响。2013 年，部分互联网公司的网站域名在某些地区被劫持，甚至被强行插入广告窗口，某些宽带接入商在小区路由器上对部分网站进行劫持跳转等事件，严重影响用户体验，损害互联网企业和网民利益。CNCERT 收到上述事件投诉后，及时协调相关单位进行处置。互联网业务的不断创新导致安全问题不断演化，如何及时、有效应对，需要互联网服务商和基础电信企

业共同努力。

（二）公共互联网治理初见成效，打击黑客地下产业链任重道远。2013 年工业和信息化部组织开展防范治理黑客地下产业链专项行动，及时处置木马僵尸网络等网络攻击威胁，取得一定成效。但网络设备后门、个人信息泄露等事件频繁出现，表明公共互联网环境仍然存在较多安全问题。

近年来我国境内感染木马僵尸网络主机数量首次下降。据 CNCERT 监测，2013 年我国境内感染木马僵尸网络的主机为 1135 万个,控制服务器为 16 万个,分别较 2012 年下降 22.5%和 44.1%，为近 5 年首次出现下降。这反映出我国持续开展的木马僵尸网络专项治理行动和日常处置工作已初见成效。

2013 年，在工业和信息化部组织开展的防范治理黑客地下产业链专项行动中，CNCERT 会同基础电信企业、域名注册服务机构共开展 8 次恶意程序专项打击工作，清理木马僵尸网络控制服务器 3.4 万余台，受控主机近 72 万个，重点处理控制规模较大的僵尸网络 1455 个，切断了黑客对 375 万余台感染主机的控制，有力净化公共互联网环境。虽然我国境内感染主机数量总体有所下降，但感染远程控制类木马的主机数量较 2012 年小幅上涨 4.4%,这类木马能对用户主机实施远程控制、窃取重要文件和敏感信息或发起网络攻击，具有极大的危害性。

分析发现 D-LINK 等众多网络设备存在后门。2013 年，CNVD 共收录各类安全漏洞 7854 个,其中高危漏洞 2607 个,分别较 2012

年增长 15.1%和 6.8%。涉及通信网络设备的软硬件漏洞数量为 505 个，较 2012 年增长 1.5 倍，占 CNVD 收录漏洞总数的比例由 2012 年的 2.9%增长至 6.4%。同时，CNVD 分析验证 D-LINK、Cisco、Linksys、Netgear、Tenda 等多家厂商的路由器产品存在后门，黑客可由此直接控制路由器，进一步发起 DNS 劫持、窃取信息、网络钓鱼等攻击，直接威胁用户网上交易和数据存储安全，使得相关产品变成随时可被引爆的安全“地雷”。以 D-LINK 部分路由器产品为例，攻击者利用后门可取得路由器的完全控制权，CNVD 分析发现受该后门影响的 D-LINK 路由器在互联网上对应的 IP 地址至少有 1.2 万个，影响大量用户。CNVD 及时向相关厂商通报威胁情况，向公众发布预警信息，但截至 2014 年 1 月底，仍有部分厂商尚未提供安全解决方案或升级补丁。路由器等网络设备作为网络公共出口，往往不引人注意，但其安全不仅影响网络正常运行，而且可能导致企业和个人信息泄露。

个人信息泄露问题挑战现有社会信任机制。云计算、移动互联网、社交网络等互联网新技术新业务正在改变个人信息的收集和使用方式，个人信息的可控性逐步削弱，姓名、住址、电话、身份证号、消费记录等重要生活信息越来越多地出现网络泄露问题。

2013 年 10 月，“查开房”网站公开曝光 2000 万条客户酒店入住信息，据比对，该信息是往年泄露的，但其中涉及大量个人隐私信息，严重影响公众生活。该事件发生后，CNCERT 立即联系协

调美国计算机应急响应组织（US-CERT）和相关域名注册服务机构对之进行处置，有效阻止了信息进一步泄露和扩散。2013 年 7 月，Apache Struts 2 被披露存在远程代码执行高危漏洞，可直接导致服务器被远程控制或数据被窃取，多家大型电商和互联网企业以及大量政府、金融机构网站受到影响，上亿用户信息面临严重泄露风险。由于信息管理制度不完善，保险订单、航班订单、网购订单和快递物流单据等包含的用户个人信息被大量滥用，甚至公开售卖，也是个人信息泄露的重要原因之一。这些传统社会中的姓名、身份证号、电话等信息的真实性极高，被黑客广泛用来实施欺诈和社会工程学攻击，给现有社会信任机制带来严重挑战。

（三）移动互联网环境有所恶化，生态污染问题亟待解决。2013 年，移动互联网恶意程序数量继续大幅增长，恶意程序的制作、发布、预装、传播等初步形成一条完整的利益链条，移动互联网生态系统环境呈恶化趋势，亟须加强管理。

针对安卓平台的恶意程序数量呈爆发式增长。2013 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 70.3 万个，较 2012 年增长 3.3 倍，其中针对安卓平台的恶意程序占 99.5%。按照恶意程序行为属性统计，恶意扣费类数量仍居第一位，占 71.5%，较 2012 年的 39.8%有大幅增长；其次是资费消耗类（占 15.1%）、系统破坏类（占 3.2%）和隐私窃取类（占 3.2%），与用户经济利益密切相关的恶意扣费类和资费消耗类恶意程序占总数的 85%以上，表明黑客在制作恶意程序时带有明显的逐利倾向。按

恶意程序的危害等级分类，高危占 1.0%，中危占 29.0%，低危占 70.0%。其中，高危恶意程序所占比例较 2012 年大幅下降，反映出黑客为降低风险，从制作恶意性明显的木马或病毒转向制作恶意广告、恶意第三方插件等灰色应用，以达到既逃避监管又获取经济利益的目的。

手机恶意程序传播渠道多样化。2013 年 CNCERT 监测发现移动互联网恶意程序传播次数达到 1296 万余次，移动互联网恶意程序下载链接 120.7 万个，用于传播移动互联网恶意程序的域名 15247 个、IP 地址 60976 个，分别是 2012 年的 23 倍、33 倍、32 倍和 11 倍。这些域名包括移动应用商店、论坛、网盘、博客等众多类型，其中仅移动应用商店的数量就超过 300 家。移动应用商店的审核机制不完善、安全检测能力差等问题，使得恶意程序得以发布和扩散，仅“安丰市场”就有数千个流行的移动应用被植入木马程序，下载次数超过 200 万次。2013 年发现某电商出售的行货手机，被第三方预置隐私窃取类手机病毒，能静默上传手机号、IMEI 号、联网 IP 地址、位置信息、程序列表等，累计感染人数超过两百万。移动应用商店、手机经销商等移动互联网生态系统的上游环节被污染，导致下游用户感染恶意程序的速度加剧。

对此，CNCERT 按照工业和信息化部发布的《移动互联网恶意程序监测与处置机制》，组织开展了 8 次移动互联网恶意程序治理行动，累计协调应用商店下架恶意应用软件 37507 个。2013 年，中国反网络病毒联盟（ANVA）建立了“移动互联网应用自律白名

单”机制，组织安全企业和应用商店成立白名单工作组和应用商店自律组，形成有序的白名单审核流程和执行机制，并公布了首批“移动互联网应用自律白名单”，以帮助应用商店、移动应用开发人员和广大用户推广或使用安全可信的“白应用”。

（四）经济信息安全威胁增加，信息消费面临跨平台风险。2013 年，互联网与金融行业深度融合，以余额宝、现金宝、理财通等为代表的互联网金融产品市场火爆，在线经济活动日趋活跃。但与此同时，钓鱼攻击呈现跨平台发展趋势，在线交易系统防护稍有不慎即可能引发连锁效应，影响金融安全和信息消费。

跨平台钓鱼攻击出现并呈增长趋势。2013 年，在传统互联网的钓鱼网站之外，黑客还结合移动互联网，利用仿冒移动应用、移动互联网恶意程序、伪基站等多种手段，实施跨平台的钓鱼欺诈攻击，危害用户经济利益。2013 年，黑客利用安卓系统的“签名验证绕过”高危漏洞，制作散播大量仿冒国内主流银行等金融机构的移动应用，诱导用户安装，盗取用户银行账户信息。一些钓鱼网站在盗取用户银行账号和密码等信息时，还大量传播仿冒相应手机银行安全插件的恶意程序，劫持用户收到的短信验证码，从而使黑客进一步完成网银支付、转账等交易操作，牟取经济利益。此外,2013 年利用伪基站进行欺诈的活动呈爆发趋势，一类是仿冒金融机构官方服务号码向周围用户发送钓鱼短信，致使一些大型银行被迫调整部分手机银行业务；另一类是冒充基础电信企业客服电话或手机充值号码联系用户，实施充值诈骗。此类事件

不仅严重破坏了企业形象，也对相关行业的健康发展造成了不良影响。

2013 年钓鱼网站数量继续迅速增长，CNCERT 共监测发现针对我国银行等境内网站的钓鱼页面 30199 个，涉及 IP 地址 4240 个，分别较 2012 年增长 35.4%和 64.6%。CNCERT 全年接收到网络钓鱼类事件举报 10578 起，处置事件 10211 起，分别较 2012 年增长 11.8%和 55.3%，为广大网民挽回数亿元损失。

在线交易系统安全问题易引发连锁效应。2013 年，互联网金融市场火爆，互联网和移动通信技术降低了使用门槛，在带来便利的同时也引入新的安全风险。2013 年 12 月，支付宝钱包客户端 iOS 版被披露存在手势密码漏洞，连续输错 5 次手势密码后可导致密码失效，使得攻击者可以任意进入手机支付宝账户，免密码进行小额支付。此后淘宝网被披露存在认证漏洞，可登录任意淘宝账户，给用户资金安全造成威胁。此类互联网公司通过所运营的在线交易信息系统，掌握大量用户资金、真实身份、经济状况、消费习惯等信息，系统出现安全问题后，风险也随之传导至关联的银行、证券、电商等其他行业，产生连锁反应。2013 年，CNCERT 监测发现银行、证券等行业联网信息系统的安全漏洞、网站后门、网页篡改等各类安全事件超过 500 起，存在交易信息被篡改、投资信息被泄露等诸多高危风险。此外，银行信息系统本身的故障也可能对经济活动造成影响。2013 年，国内两家主流银行的信息系统先后出现全国性大面积故障，导致柜面、ATM、网银、电话语

音系统等瘫痪，相关业务受到严重影响。

（五）政府网站面临威胁依然严重，地方政府网站成为“重灾区”。政府网站因其公信力高、影响力大，容易成为黑客攻击目标。2013 年，我国政府网站被篡改和植入后门的情况依然严重，相对部委网站而言，地方政府网站是遭受攻击的“重灾区”，影响政府形象及电子政务工作。

地方政府网站是黑客攻击的“重灾区”。据 CNCERT 监测，2013 年，我国境内被篡改网站数量为 24034 个，较 2012 年增长 46.7%，其中政府网站被篡改数量为 2430 个，较 2012 年增长 34.9%；我国境内被植入后门的网站数量为 76160 个，较 2012 年增长 45.6%，其中政府网站 2425 个，较 2012 年下降 19.6%。在被篡改和植入后门的政府网站中，超过 90%是省市级以下的地方政府网站，超过 75%的篡改方式是在网站首页植入广告黑链。由于地方政府网站存在技术和管理水平有限、网络安全防护能力薄弱、人员和资金投入不足等问题，其网站服务器成为黑客控制的资源节点。2013 年，CNCERT 共通报和处置超过 1600 起涉及政府部门的网站漏洞事件。一些部门收到 CNCERT 预警通报后置之不理，导致安全威胁长期存在；另一些部门则只针对安全事件简单清除，未对网站进行详细检测和加固处理，导致反复多次遭受攻击。相对于地方政府网站，国务院部委门户网站安全状况较好，未监测发现网页篡改和网站后门事件，不过部分子站和业务系统仍然存在较多安全漏洞和风险点，可能成为黑客进一步实施攻击的跳板。

境外黑客组织频繁攻击我国政府网站。2013 年，境外“匿名者”、“阿尔及利亚黑客”等多个黑客组织曾对我国政府网站发起攻击。其中，“反共黑客”组织较为活跃，持续发起针对我国境内党政机关、高校、企事业单位以及知名社会组织网站的攻击，2013 年该组织对我国境内 120 余个政府网站实施篡改。据监测，该组织利用网站漏洞预先植入后门，对网站实施控制后遂发起攻击，目前至少入侵 600 余个境内网站，并平均每三天在其社交网站发布一起篡改事件。另有“匿名者”、“阿尔及利亚黑客”等组织先后篡改我国 187 个政府网站。此外，还出现黑客为报复国家出台的政策，对我国政府网站实施攻击的新苗头。2013 年 12 月 19 日下午，继央行明确宣布不认可比特币，要求国内第三方支付机构停止为比特币交易平台提供充值和支付服务之后，央行官方网站和新浪官方微博遭到黑客网络攻击，出现间歇性访问困难和大量异常评论。

（六）国家级有组织攻击频发，我国面临大量境外地址攻击威胁。国家级有组织网络攻击行为显著增多，给国家关键基础设施和重要信息系统带来严重威胁和挑战。据 CNCERT 监测，我国面临大量来自境外地址的网站后门、网络钓鱼、木马和僵尸网络等攻击。

具有国家背景的有组织攻击频发。2013 年 6 月以来，斯诺登曝光“棱镜计划”等多项美国家安全局网络监控项目，披露美国情报机构对多个国家和民众长期实施监听和网络渗透攻击，引起

国际社会强烈反响。根据曝光信息，美国投入巨额资金，分别通过互联网、通信网、企业服务器等多种渠道以及采用网络入侵手段，实施信息监听和收集，监听内容包括互联网元数据、互联网通信内容、社交网络资料、电话和短信息等多种数据类型，监控对象包括多国政要、外交系统、媒体网络、大型企业网络和国际组织等。我国属于其重点监听和攻击目标，国家安全和互联网用户隐私安全面临严重威胁。

2013 年，越来越多的有组织高级持续性威胁（APT）攻击事件浮出水面，APT 攻击成为国家间网络对抗的新型有力武器。2013 年 3 月 20 日，美、韩军事演习期间，韩国多家广播电视台和银行等金融机构遭受历史上最大规模的恶意代码攻击，导致系统瘫痪，引发韩国社会一度混乱。CNCERT 获知消息后，第一时间与韩国计算机应急响应组织（KrCERT）联系，并协助调查，及时消除攻击来自中国的误会。迈克菲公司、卡巴斯基实验室等先后曝光持续多年、具有极强隐蔽性的“特洛伊行动”、“红色十月”、“Icefog”等一系列 APT 攻击，曾大量窃取政府部门、科研机构和重点行业单位的重要敏感信息。我国同样面临严重的 APT 攻击威胁，一些国家利用信息化技术优势，大力推动研发计算机病毒武器，破解互联网加密算法，或直接在标准算法中放置后门，持续对我国实施 APT 攻击。我国政府机构、基础电信企业、科研院所、大型商业机构的网络信息系统遭受攻击和渗透入侵。2013 年，CNCERT 监测发现我国境内 1.5 万台主机被 APT 木马控制，对我国关键基础

设施和重要信息系统安全造成严重威胁。

我国仍面临大量来自境外地址的攻击威胁。2013 年，境外有 3.1 万台主机通过植入后门对境内 6.1 万个网站实施远程控制，虽然境外控制主机数量较 2012 年下降 4.3%，但所控制的境内网站数量却大幅增长 62.1%。从所控制的境内网站数量看，位于美国的主机居首位，共有 6215 台主机控制着境内 15349 个网站，平均每个主机控制 2.5 个境内网站，较 2012 年（约 1.4 个）增长 78.6%。其次是中国香港，控制境内 13116 个网站，较 2012 年大幅增长 179.5%。排名第三的是韩国，控制境内 7052 个网站，较 2012 年下降 11.1%。

在网络钓鱼攻击方面，针对我国的钓鱼站点有 90.2%位于境外，共有 3823 个境外 IP 地址承载 29966 个针对我国境内网站的仿冒页面，分别较 2012 年增长 54.3%和 27.8%。从承载的钓鱼页面数量看，美国仍居首位，共有 2043 台主机承载 12573 个钓鱼页面，中国香港和韩国列第二、三位，分别承载 4500 个和 1093 个钓鱼页面。

在木马僵尸网络方面，我国境内 1090 万余台主机被境外 2.9 万余个控制服务器控制，其中位于美国的 8807 个控制服务器控制了我国境内 448.5 万余台主机，控制主机数量占被境外控制主机总数的 41.1%。从控制服务器占全部境外控制服务器比例来看，美国占比由 2012 年的 17.6%增长至 30.2%，仍居首位；韩国和中国香港分列第二、三位，占比分别为 7.8%和 7.7%。就所控制的境内

主机数量而言，美国居首位，葡萄牙和韩国分列第二、三位，分别控制我国境内 398.8 万和 83.9 万台主机。

CNCERT 不断加强与国际 CERT 组织间的网络安全合作，完善跨境网络安全事件处置协作机制。截至 2013 年底，已与 59 个国家和地区、127 个组织建立联系机制，全年共协调境外安全组织处理涉及境内的安全事件 5498 起，较 2012 年增长 35.3%。

二、2014 年值得关注的热点问题

2014 年，我国互联网面临的安全形势将更为复杂，值得关注的热点问题主要如下。

（一）设备智能化促使网络安全威胁向物联网延伸。随着工业控制系统、医疗器械、办公及家用设备的逐步智能化，物联网产业蓬勃发展。然而，新兴技术发展的不完善和对网络安全问题的忽视，往往导致智能设备设计存在漏洞缺陷。黑客利用这些漏洞，可以轻易实施网络攻击。2013 年，美国“黑帽子”大会展示 10 多项针对电网、智能家居、汽车等控制系统智能设备的攻击或监控技术，同时出现大规模“冰箱僵尸网络”等针对智能家电的恶意攻击事件，表明针对物联网中智能设备的攻击技术已取得突破。此外，由于安卓系统已成为智能设备的主流平台，针对安卓系统的攻击威胁也会迅速从移动互联网辐射至物联网。2014 年，物联网的脆弱性将伴随其应用和发展而更加凸显。

（二）社交网络成为黑客攻击和网络犯罪的新途径。实施网络攻击的重要手段之一，便是利用社会工程学（社工库）。而逐渐

深入人们生活的社交网络，成为黑客实施社会工程攻击的“温床”。由于大多数社交网络基于人与人之间的信任关系构成，包含的信息内容和用户生活密切相关，带有很强的真实性。黑客通过社交网络广泛收集挖掘用户个人信息，形成社工库，并基于用户网络习惯实施高效的定向攻击，散播恶意程序、钓鱼欺诈信息等，命中率极高。受经济利益驱使，2014 年基于社交网络的恶意程序攻击将增多，甚至可能出现利用社交网络发布命令、实施控制的新型僵尸网络，社交网络免费开放的第三方应用接口将成为黑客进行违法犯罪活动的突破口。

（三）云平台的应用普及加大信息泄露风险和事件处置难度。随着云平台的应用普及和大数据技术的发展，涵盖互联网行业、金融服务业、医疗保健业、制造业的大量行业数据快速增长，越来越多的用户数据从个人电脑转向云平台。一方面，集成大量同类数据的云端如同“地下宝藏”，吸引攻击者的目光，其一旦发生信息泄露，将对整个行业造成影响。另一方面，由于云平台使用方便、成本低廉，黑客将大量利用云平台进行钓鱼网站部署、恶意程序传播控制和网络攻击跳板，而云平台的使用给传统基于 IP 地址的追踪溯源带来困难，事件处置难度进而增大。

（四）实施 APT 攻击的手段将更加多维化。随着网络空间对抗的日益加剧，APT 攻击以其精准高效的特点，将成为黑客组织乃至国家间网络对抗的主要方式。APT 攻击将综合运用多种技术手段协作互补，形成一体化监视和攻击体系，除传统的恶意程序、软

硬件漏洞等技术外，还包括多种新型的手段和技术。2013 年 12 月 30 日，斯诺登披露美国家安全局研制出数十种间谍工具，包括通过直接将后门嵌入主板、硬盘驱动器、SIM 卡等硬件设备，实现物理入侵；将后门植入固件以保障攻击连续性，避免受到更换系统平台、升级系统和程序、安装查杀软件的影响；通过无线射频技术破解传统局域网的物理隔离问题，实现远距离隔空攻击等。这些手段将提高 APT 攻击渗透的广度和深度，增强间谍行动的隐蔽性和可持续性，对 APT 攻击检测能力也提出了更高要求。

（五）移动支付安全和移动终端漏洞成为移动互联网发展的新挑战。2014 年，随着 4G 网络的大面积商用、移动互联网带宽的提速和 Wi-Fi 热点普及，智能手机和移动应用在日常生活中日益普及，人们将更习惯使用移动支付方式，这将进一步推动各类金融、证券、电商等移动应用的普及。受经济利益驱使，黑客将更多地把移动互联网作为主阵地，这也将导致针对移动互联网应用的仿冒 APP 和恶意插件增多，并可能引发更多移动互联网经济犯罪事件。此外，针对智能终端设备硬件、操作系统、应用程序等的安全漏洞挖掘将增多，移动互联网零日漏洞数量将迅速增长，这将导致针对移动互联网和智能终端的攻击增多。大量智能终端设备通过家用无线路由器、公用 Wi-Fi 等接入互联网，但路由器后门、通过公用 Wi-Fi 进行网络劫持和网络钓鱼等事件的曝光，暴露出诸多安全隐患，这将加深移动互联网面临的攻击威胁。

（六）分布式反射拒绝服务攻击规模呈持续增大趋势。2014

年，依靠僵尸网络和带宽构造大规模攻击流量的传统方式已无法达到预想的攻击效果，黑客将更多地运用 DNS、NTP（Network Time Protocol，网络时钟协议）和 CHARGEN（Character Generator Protocol，字符发生器协议）等进行分布式反射放大拒绝服务攻击，能轻易把攻击流量放大几十倍到几百倍，耗尽有限的服务器、路由器和带宽资源，隐藏了攻击僵尸主机 IP 地址的攻击方式也给追踪溯源带来难度。此外，攻击者还将不断寻找更多类似的新技术手段，以最小代价实现攻击流量的放大，增加攻击威力，实现“借刀杀人”的目的，使拒绝服务攻击与防护的对抗进一步激烈。

（七）微软停止对 Windows XP 系统的服务支持可能导致零日漏洞攻击增多。2014 年 4 月 8 日，微软将正式停止对 Windows XP 系统的技术支持与更新，不再提供对该操作系统的安全补丁、升级、杀毒软件更新以及其他相关服务，这意味着此后针对该系统的病毒与漏洞攻击，微软将不再负责。由于 Windows XP 系统市场占有份额高，据统计在我国安装和使用该系统的计算机将近 2 亿台，一旦系统支持与更新停止，这些计算机将面临严重安全风险，黑客可能会加强对该系统的零日漏洞挖掘，用于对高价值目标计算机攻击或控制，造成信息泄露、系统瘫痪、经济损失等严重后果。

（八）传统短信验证和新兴二维码扫描方式背后均面临安全风险。当前进行网购和网络支付时经常会用到短信验证码。2014 年通过手机木马劫持支付验证码短信，窃取用户账户信息的活动

将呈高发态势。黑客利用手机木马拦截验证码短信，并进一步套取用户网络支付账号和密码，使得用户的个人财产面临巨大损失。此外，随着二维码的日益普遍使用，由于隐蔽性高，制作成本低，二维码背后未经安全认证的网站链接和应用程序逐步成为黑客的青睐对象。缺乏安全意识的手机用户在扫描来历不明或无法确认安全的二维码后，进入黑客预先埋伏的网站链接或下载应用程序，导致手机被植入病毒或恶意插件，造成个人信息泄露和经济损失。

三、对策建议

（一）加快推动制定网络安全战略和相关政策，统筹规划网络安全保障能力。在“棱镜门”和国家级 APT 事件频现的背景下，建议尽快制定我国国家级网络信息安全战略，明确应对网络安全威胁的战略目标、指导思想和方针，为维护国家网络空间安全提供战略指导；同时，制定相关的配套法规政策，明确相关主体工作内容和责任义务。此外，建议加强网络安全保障工作的顶层设计，继续健全跨部门、跨行业、跨地域的网络安全保障协作机制，实现各部门现有网络安全资源的对接，在各负其责的基础上，实现国家全局网络安全能力的协同联动和专业支撑，有效应对国家级的网络攻击行为。

（二）加大网络安全工作投入，提高网络安全防护意识。建议相关行业、企业和政府部门，加大在网络设备和技术研发方面的投入，强化安全防护和管理，提高自身应对网络安全新风险的能力，以减少技术不断发展引起的网络安全隐患。同时，建议各

单位进一步加强对网络安全的重视程度和安全意识，全面落实安全组织、安全制度和技术防范措施，建立和完善安全防范机制，建立完备的应急响应预案，定期排查安全管理和技术实施环节的隐患和漏洞，确保联网重要信息系统的安全。

（三）加强网络安全技术手段建设，提高对网络攻击主体的追溯能力。针对网络钓鱼、木马、移动互联网恶意程序、APT 攻击以及互联网新技术新业务可能引发的新问题、新风险，建议加强实现网络安全技术手段的研究和建设，进一步提高对网络攻击的威胁监测、全局感知、预警防护、应急处置、协同联动等能力；建议进一步提高对网络攻击的追踪溯源能力，对正在发生的网络攻击行为，能够准确判断网络攻击来源、目标和真实意图，提取数据线索，还原攻击场景，并找到攻击源头，从而形成一定的震慑力。

（四）提高核心设备国产化水平，加快完善信息安全审查制度。建议加强网络关键设备和核心技术的研发和推广，提高重点行业和重要信息系统中联网设备软硬件的国产化水平，提升软硬件产品和服务的自主可控能力。在较长一段时间内，我国各部门仍然不可避免地要使用国外主流网络设备和互联网服务，建议加强对联网系统的安全防护检查和动态监测能力，提高对系统漏洞的发现能力，及时修复安全漏洞，确保联网系统的安全可靠运行。同时，建议尽快完善信息安全审查制度框架，明确信息产品的审查范围和审查内容，对相关信息产品，根据产品的来源、可靠性、

可监督性和安全性进行审查，规范其使用范围，可有计划地开展信息安全审查试点，进一步增强国家信息和网络安全保护水平。

（五）加强移动互联网恶意程序治理，维护良性的移动生态环境。建议政府主管部门加大移动互联网监管力度，督促企业落实各项责任，加强对移动互联网应用商店、增值电信企业经营者的网络安全管理，建立健全标准规范以明确应用程序制作者和应用商店的责任，从制作、发布、传播环节加大对恶意程序的打击力度，在源头上遏制移动互联网地下黑色产业链的蔓延。同时，建议通信行业、互联网行业、软硬件厂商等充分发挥优势，加强行业联动和信息技术共享，提升对移动互联网恶意程序的监测能力，提高处置效率，积极配合政府主管部门，净化公共互联网环境，努力为广大网民营造绿色健康的移动互联网环境。

（六）加强对网民网络安全意识的宣传教育，推动全民网络安全防护能力提升。建议政府、企业、安全厂商和社会组织等共同努力，提升网民的网络安全防范意识和技能。通过电视、广播、网站等多种渠道提醒网民做好个人数据资料的保护，谨慎进行电子交易、网上支付等涉及经济利益的操作，及时修复安全漏洞，防范个人主机或移动终端被木马僵尸网络操控，防止个人信息泄露和财产损失。