1 2011 年网络安全状况综述

1.1 总体状况

2011 年，在政府相关部门、互联网服务机构、网络安全企业和网民的共同努力下，我国互联网网络安全状况继续保持平稳状态，未发生造成大范围影响的重大网络安全事件，基础信息网络防护水平明显提升，政府网站安全事件显著减少，网络安全事件处置速度明显加快，但以用户信息泄露为代表的与网民利益密切相关的事件，引起了公众对网络安全的广泛关注。本综述着重对 2011 年互联网安全威胁的一些新特点和趋势进行了分析和总结。

一、我国互联网网络安全形势

（一）基础网络防护能力明显提升，但安全隐患不容忽视。根据工信部组织开展的 2011 年通信网络安全防护检查情况，基础电信运营企业的网络安全防护意识和水平较 2010 年均有所提高，对网络安全防护工作的重视程度进一步加大，网络安全防护管理水平明显提升，对非传统安全的防护能力显著增强，网络安全防护达标率稳步提高，各企业网络安全防护措施总体达标率为 98.78%，较 2010 年的 92.25%、2009 年的 78.61%呈逐年稳步上升趋势。

但是，基础电信运营企业的部分网络单元仍存在比较高的风险。据抽查结果显示，域名解析系统（DNS）、移动通信网和 IP 承载网的网络单元存在风险的百分比分别为 6.8%、17.3%和 0.6%。涉及基础电信运营企业的信息安全漏洞数量较多。据国家信息安全漏洞共享平台（CNVD）收录的漏洞统计，2011 年发现涉及电信运营企业网络设备（如路由器、交换机等）的漏洞 203 个，其中高危漏洞 73 个；发现直接面向公众服务的零日 DNS 漏洞 23 个，应用广泛的域名解析服务器软件 Bind9 漏洞 7 个。涉及基础电信运营企业的攻击形势严峻。据国家计算机网络应急技术处理协调中心（CNCERT）监测，2011 年每天发生的分布式拒绝服务攻击（DDoS）事件中平均约有 7%的事件涉及到基础电信运营企业的域名系统或服务。2011 年 7 月 15 日域名注册服务机构三五互联 DNS 服务器遭受 DDoS 攻击，导致其负责解析的大运会官网域名在部分地区无法解析。8 月 18 日晚和 19 日晚，新疆某运营商 DNS 服务器也连续两次遭到拒绝服务攻击，造成局部用户无法正常使用互联网。

（二）政府网站篡改类安全事件显著减少，网站用户信息泄漏引发社会高度关注。据 CNCERT 监测，2011 年中国大陆被篡改的政府网站为 2807 个，比 2010

年大幅下降 39.4%；从 CNCERT 专门面向国务院部门门户网站的安全监测结果来看，国务院部门门户网站存在低级别安全风险的比例从 2010 年的 60%进一步降低为 50%。但从整体来看，2011 年网站安全情况有一定恶化趋势。在 CNCERT 接收的网络安全事件(不含漏洞)中，网站安全类事件占到 61.7%；境内被篡改网站数量为 36612 个，较 2010 年增加 5.1%；4 月-12 月被植入网站后门的境内网站为 12513 个。CNVD 接收的漏洞中，涉及网站相关的漏洞占 22.7%，较 2010 年大幅上升，排名由第三位上升至第二位。网站安全问题进一步引发网站用户信息和数据的安全问题。2011 年底， CSDN、天涯等网站发生用户信息泄露事件引起社会广泛关注，被公开的疑似泄露数据库 26 个，涉及帐号、密码信息 2.78 亿条，严重威胁了互联网用户的合法权益和互联网安全。根据调查和研判发现，我国部分网站的用户信息仍采用明文的方式存储，相关漏洞修补不及时，安全防护水平较低。

（三）我国遭受境外的网络攻击持续增多。2011 年，CNCERT 抽样监测发现，境外有近 4.7 万个 IP 地址作为木马或僵尸网络控制服务器参与控制我国境内主机，虽然其数量较 2010 年的 22.1 万大幅降低，但其控制的境内主机数量却由 2010 年的近 500 万增加至近 890 万，呈现大规模化趋势。其中位于日本（22.8%）、美国（20.4%）和韩国（7.1%）的控制服务器 IP 数量居前三位，美国继 2009 年和 2010 年两度位居榜首后，2011 年其控制服务器 IP 数量下降至第二，以 9528 个 IP 控制着我国境内近 885 万台主机，控制我国境内主机数仍然高居榜首。在网站安全方面，境外黑客对境内 1116 个网站实施了网页篡改；境外 11851 个 IP 通过植入后门对境内 10593 个网站实施远程控制，其中美国有 3328 个 IP（占 28.1%）控制着境内 3437 个网站，位居第一，源于韩国（占 8.0%）和尼日利亚（占 5.8%）的 IP 位居第二、三位；仿冒境内银行网站的服务器 IP 有 95.8%位于境外，其中美国仍然排名首位——共有 481 个 IP（占 72.1%）仿冒了境内 2943 个银行网站的站点，中国香港（占 17.8%）和韩国（占 2.7%）分列二、三位。总体来看，2011 年位于美国、日本和韩国的恶意 IP 地址对我国的威胁最为严重。另据工业和信息化部互联网网络安全信息通报成员单位报送的数据，2011 年在我国实施网页挂马、网络钓鱼等不法行为所利用的恶意域名约有 65%在境外注册。此外，CNCERT 在 2011 年还监测并处理多起境外 IP 对我国网站和系统的拒绝服务攻击事件。这些情况表明我国面临的境外网络攻击和安全威胁越来越严重。

（四）网上银行面临的钓鱼威胁愈演愈烈。随着我国网上银行的蓬勃发展，广大网银用户成为黑客实施网络攻击的主要目标。2011 年初，全国范围大面积爆发了假冒中国银行网银口令卡升级的骗局，据报道此次事件中有客户损失超过

百万元。据 CNCERT 监测，2011 年针对网银用户名和密码、网银口令卡的网银大盗、Zeus 等恶意程序较往年更加活跃，3 月-12 月发现针对我国网银的钓鱼网站域名 3841 个。CNCERT 全年共接收网络钓鱼事件举报 5459 件，较 2010 年增长近 2.5 倍，占总接收事件的 35.5%；重点处理网页钓鱼事件 1833 件，较 2010 年增长近两倍。

（五）工业控制系统安全事件呈现增长态势。继 2010 年伊朗布舍尔核电站遭到 Stuxnet 病毒攻击后，2011 年美国伊利诺伊州一家水厂的工业控制系统遭受黑客入侵导致其水泵被烧毁并停止运作，11 月 Stuxnet 病毒转变为专门窃取工业控制系统信息的 Duqu 木马。2011 年 CNVD 收录了 100 余个对我国影响广泛的工业控制系统软件安全漏洞，较 2010 年大幅增长近 10 倍，涉及西门子、北京亚控和北京三维力控等国内外知名工业控制系统制造商的产品。相关企业虽然能够积极配合 CNCERT 处置安全漏洞，但在处置过程中部分企业也表现出产品安全开发能力不足的问题。

（六）手机恶意程序现多发态势。随着移动互联网生机勃勃的发展，黑客也将其视为攫取经济利益的重要目标。2011 年 CNCERT 捕获移动互联网恶意程序 6249 个，较 2010 年增加超过两倍。其中，恶意扣费类恶意程序数量最多，为 1317 个，占 21.08%，其次是恶意传播类、信息窃取类、流氓行为类和远程控制类。从手机平台来看，约有 60.7%的恶意程序针对 Symbian 平台，该比例较 2010 年有所下降，针对 Android 平台的恶意程序较 2010 年大幅增加，有望迅速超过 Symbian 平台。2011 年境内约 712 万个上网的智能手机曾感染手机恶意程序，严重威胁和损害手机用户的权益。

（七）木马和僵尸网络活动越发猖獗。2011 年，CNCERT 全年共发现近 890 万余个境内主机 IP 地址感染了木马或僵尸程序，较 2010 年大幅增加 78.5%。其中，感染窃密类木马的境内主机 IP 地址为 5.6 万余个，国家、企业以及网民的信息安全面临严重威胁。根据工业和信息化部互联网网络安全信息通报成员单位报告，2011 年截获的恶意程序样本数量较 2010 年增加 26.1%，位于较高水平。黑客在疯狂制造新的恶意程序的同时，也在想方设法逃避监测和打击，例如，越来越多的黑客采用在境外注册域名、频繁更换域名指向 IP 等手段规避安全机构的监测和处置。

（八）应用软件漏洞呈现迅猛增长趋势。2011 年，CNVD 共收集整理并公开发布信息安全漏洞 5547 个，较 2010 年大幅增加 60.9%。其中，高危漏洞有 2164 个，较 2010 年增加约 2.3 倍。在所有漏洞中，涉及各种应用程序的最多，占 62.6%，涉及各类网站系统的漏洞位居第二，占 22.7%，而涉及各种操作系统的漏洞则排

到第三位，占 8.8%。除发布预警外，CNVD 还重点协调处置了大量威胁严重的漏洞，涵盖网站内容管理系统、电子邮件系统、工业控制系统、网络设备、网页浏览器、手机应用软件等类型以及政务、电信、银行、民航等重要部门。上述事件暴露了厂商在产品研发阶段对安全问题重视不够，质量控制不严格，发生安全事件后应急处置能力薄弱等问题。由于相关产品用户群体较大，因此一旦某个产品被黑客发现存在漏洞，将导致大量用户和单位的信息系统面临威胁。这种规模效应也吸引黑客加强了对软件和网站漏洞的挖掘和攻击活动。

（九）DDoS 攻击仍然呈现频率高、规模大和转嫁攻击的特点。2011 年，DDoS 仍然是影响互联网安全的主要因素之一，表现出三个特点。一是 DDoS 攻击事件发生频率高，且多采用虚假源 IP 地址。据 CNCERT 抽样监测发现，我国境内日均发生攻击总流量超过 1G 的较大规模的 DDoS 攻击事件 365 起。其中，TCP SYN FLOOD 和 UDP FLOOD 等常见虚假源 IP 地址攻击事件约占 70%，对其溯源和处置难度较大。二是在经济利益驱使下的有组织的 DDoS 攻击规模十分巨大，难以防范。例如 2011 年针对浙江某游戏网站的攻击持续了数月，综合采用了 DNS 请求攻击、UDP FLOOD、TCP SYN FLOOD、HTTP 请求攻击等多种方式，攻击峰值流量达数十个 Gbps。三是受攻击方恶意将流量转嫁给无辜者的情况屡见不鲜。2011 年多家省部级政府网站都遭受过流量转嫁攻击，且这些流量转嫁事件多数是由游戏私服网站争斗引起。

二、国内网络安全应对措施

（一）相关互联网主管部门加大网络安全行政监管力度，坚决打击境内网络攻击行为。针对工业控制系统安全事件愈发频繁的情况，工信部在 2011 年 9 月专门印发了《关于加强工业控制系统信息安全管理的通知》，对重点领域工业控制系统信息安全管理提出了明确要求。2011 年底，工信部印发了《移动互联网恶意程序监测与处置机制》，开展治理试点，加强能力建设。6 月起，工信部组织开展 2011 年网络安全防护检查工作，积极将防护工作向域名服务和增值电信领域延伸。另外还组织通信行业开展网络安全实战演练，指导相关单位妥善处置网络安全应急事件等。公安部门积极开展网络犯罪打击行动，破获了 2011 年 12 月底 CSDN、天涯社区等数据泄漏案等大量网络攻击案件；国家网络与信息安全信息通报中心积极发挥网络安全信息共享平台作用，有力支撑各部门做好网络安全工作。

（二）通信行业积极行动，采取技术措施净化公共网络环境。面对木马和僵尸程序在网上的横行和肆虐，在工信部的指导下，2011 年 CNCERT 会同基础电信运营企业、域名从业机构开展 14 次木马和僵尸网络专项打击行动，次数比去

年增加近一倍。成功处置境内外 5078 个规模较大的木马和僵尸网络控制端和恶意程序传播源。此外，CNCERT 全国各分中心在当地通信管理局的指导下，协调当地基础电信运营企业分公司合计处置木马和僵尸网络控制端 6.5 万个、受控端 93.9 万个。根据监测，在中国网民数和主机数量大幅增加的背景下，控制端数量相对 2010 年下降 4.6%，专项治理工作取得初步成效。

（三）互联网企业和安全厂商联合行动，有效开展网络安全行业自律。2011 年 CNVD 收集整理并发布漏洞信息，重点协调国内外知名软件商处置了 53 起影响我国政府和重要信息系统部门的高危漏洞。中国反网络病毒联盟（ANVA）启动联盟内恶意代码共享和分析平台试点工作，联合 20 余家网络安全企业、互联网企业签订遵守《移动互联网恶意程序描述规范》，规范了移动互联网恶意代码样本的认定命名，促进了对其的分析和处置工作。中国互联网协会于 2011 年 8 月组织包括奇虎 360 和腾讯公司在内的 38 个单位签署了《互联网终端软件服务行业自律公约》，该公约提倡公平竞争和禁止软件排斥，一定程度上规范了终端软件市场的秩序；在部分网站发生用户信息泄露事件后，中国互联网协会立即召开了“网站用户信息保护研讨会”，提出安全防范措施建议。

（四）深化网络安全国际合作，切实推动跨境网络安全事件有效处理。作为我国互联网网络安全应急体系对外合作窗口，2011 年 CNCERT 积极推动“国际合作伙伴计划”，已与 40 个国家、79 个组织建立了联系机制，全年共协调国外安全组织处理境内网络安全事件 1033 起，协助境外机构处理跨境事件 568 起。其中包括针对境内的 DDoS 攻击、网络钓鱼等网络安全事件，也包括针对境外苏格兰皇家银行网站、德国邮政银行网站、美国金融机构 Wells Fargo 网站、希腊国家银行网站和韩国农协银行网站等金融机构，加拿大税务总局网站、韩国政府网站等政府机构的事件。另外 CNCERT 再次与微软公司联手，继 2010 年打击 Waledac 僵尸网络后，2011 年又成功清除了 Rustock 僵尸网络，积极推动跨境网络安全事件的处理。2011 年，CNCERT 圆满完成了与美国东西方研究所（EWI）开展的为期两年的中美网络安全对话机制反垃圾邮件专题研讨，并在英国伦敦和我国大连举办的国际会议上正式发布了中文版和英文版的成果报告“抵御垃圾邮件 建立互信机制”，增进了中美双方在网络安全问题上的相互了解，为进一步合作打下基础。

1.2 数据导读

多年来，国家互联网应急中心对我国网络安全宏观状况进行了持续监测，以下是 2011 年抽样监测获得的主要数据分析结果。

- 木马和僵尸程序监测
  - 2011 年木马或僵尸程序控制服务器 IP 总数为 300407 个，较 2010 年下降 39.1%。其中，境内木马或僵尸程序控制服务器 IP 数量为 253684 个，较 2010 年下降 4.6%；境外木马或僵尸程序控制服务器 IP 数量为 46723 个，较 2010 年大幅下降 79.5%。
  - 2011 年木马或僵尸程序受控主机 IP 总数为 27275399 个，较 2010 年大幅增长 71.1%。其中，境内木马或僵尸程序受控主机 IP 数量为 8895123 个，较 2010 年大幅增长 78.5%；境外木马或僵尸程序受控主机 IP 数量为 18380276 个，较 2010 年大幅增长 67.8%。
- “飞客”蠕虫监测
  - 2011 年全球互联网平均每月有超过 3500 万个主机 IP 感染“飞客”蠕虫。其中，境内感染“飞客”蠕虫的主机 IP 月均超过 400 万个。
- 移动互联网安全监测
  - 2011 年累计捕获移动互联网恶意程序 6249 个，其中有控制域名的 3060 个，占 49.0%。
  - 移动互联网恶意程序按行为属性统计，排名前三的分别是：具有恶意扣费行为的恶意程序占 21.1%；具有恶意传播行为的恶意程序占 19.8%；具有信息窃取行为的恶意程序占 18.9%。
  - 按操作系统统计，捕获 Symbian 平台的恶意程序最多，占 60.7%；Android 平台恶意程序占到 39.3%，呈迅速增长态势。
- 网站安全监测情况
  - 2011 年境内被篡改网站数量累计为 36612 个，较 2010 年略增 5.1%。其中，境内被篡改政府网站（gov.cn 域名网站）数量累计为 2807 个，与 2010 年相比下降 39.4%，去重后为 1484 个，在 CNCERT 监测的政府网站列表中所占比例达到 3.4%。
  - 2011 年 3 月-12 月监测到仿冒境内银行网站的域名有 3841 个；仿冒境内银行网站的服务器 IP 有 667 个，其中 95.8%位于境外，美国（72.1%）、

中国香港（17.8%）和韩国（2.7%）居前三位。

- 2011 年 4 月-12 月监测到境内 12513 个网站被植入网站后门，其中政府网站 1167 个。位于境外的攻击 IP 有 11851 个，主要位于美国（28.1%）、韩国（8.0%）和尼日利亚（5.8%）。

■ 信息系统安全漏洞公告及处理

- 2011 年，CNVD 共收集整理并公开发布信息安全漏洞 5547 个，较 2010 年大幅增加 60.9%。其中，高危漏洞 2164 个，较 2010 年增加约 2.3 倍。
- 按漏洞影响对象类型统计，排名前三位的是应用程序漏洞（占 62.6%），涉及网站相关的漏洞（占 22.7%），操作系统漏洞（占 8.8%）。
- 2011 年，CNVD 共收录漏洞补丁 3707 个。

■ 网络安全事件接收与处理

- 2011 年，CNCERT 共接收国内外报告网络安全事件 15366 起，较 2010 年增加了 47.3%；其中，国外报告的网络安全事件数量为 2100 起，较 2010 年下降了 58.6%。所报告的网络安全事件集中在信息系统漏洞（占 36.3%）、网页仿冒（占 35.5%）、恶意程序（占 23.4%）等类型。
- 2011 年，CNCERT 共成功处理各类网络安全事件 10924 件，较 2010 年增长约 63.5%。其中，信息系统漏洞事件（占 51.0%）、恶意程序事件（占 22.8%）、网页仿冒事件(占 16.8%)处置较多。

■ 网络安全信息发布情况

- 2011 年 CNCERT 共收到通信行业各单位报送的网络安全月度信息 619 份，事件信息和预警信息 962 份。全年共编制并向各单位发送《互联网网络安全信息通报》46 期。
- 2011 年 CNCERT 通过发布网络安全专报、周报、月报、年报和在期刊杂志上发表文章等多种形式面向行业外发布报告 139 个。