2011 年网络安全挑战与工作展望

■ 2011 年网络安全趋势预测

随着我国互联网新技术、新应用的快速发展，2011 年的网络安全形势将更加复杂，可能呈现以下特点：

（一）网络安全形势日益严峻，针对我国互联网基础设施和金融、证券、交通、能源、海关、税务、工业、科技等重点行业的联网信息系统的探测、渗透和攻击将逐渐增多。

（二）黑客地下产业将更加专注于网络钓鱼、攻击勒索、网络刷票[1]、个人隐私窃取等能够直接获利或易于获利的攻击方式；大型商业网站将成为攻击的热点目标。

（三）网络安全技术对抗将不断升级。恶意代码的变种数量将激增，“免杀”[2]能力将进一步增强；窃密木马将不断演变升级，木马投放方式将更加隐蔽和具有欺骗性，木马抗查杀能力将更加强大；网络攻击的规模将进一步扩大，对公共互联网安全运行带来严重影响；为躲避处置和打击，网络攻击的跨境特点将更加突出。

（四）随着智能终端的迅速普及，移动互联网的安全问题凸显，手机恶意程序数量将急剧增加，其功能将集中在恶意扣费、弹出广告、垃圾短信和窃听窃取方面，手机用户的经济利益和个人隐私安全面临挑战。

（五）网络新技术、新应用蓬勃发展，随着三网融合、IPv6、云计算、物联网等技术的试用和推广，新的安全问题将不断出现。

■ 对策建议

为有效保障国家网络空间安全，促进互联网健康发展，维护互联网安全，保护网民权益，我国政府主管部门、互联网企业和互联网用户都应高度重视网络安全问题，从各自职能和能力出发，发挥不同层面的作用，上下联动，共同提高互联网网络安全水平。

（一）加强网络安全立法工作。解决当前网络安全立法层级低的问题，加强高层次立法。加大网络犯罪惩治、量刑力度，尽快出台打击计算机信息系统犯罪的司法解释，形成有效震慑。适应新技术、新业务发展，提高法律的适用性和时

[1] 网络刷票是指利用代理和不同账号等手段突破网络投票系统限制，采用非公平的方式为某投票选项投票，以获取利益的行为。

[2] 免杀是指一种能使木马等恶意代码避免被防病毒软件查杀的技术。

效性。

（二）进一步加大网络安全行政监管力度。抓好《通信网络安全防护管理办法》、《公共互联网网络安全应急预案》、《域名系统安全专项应急预案》、《木马和僵尸网络监测与处置机制》和《互联网网络安全信息通报实施办法》等网络安全相关政策文件的落实，在继续做好基础电信运营企业安全监管的基础上，重点加强对增值电信运营企业的安全管理，建立健全移动互联网安全保障和用户隐私数据保护等工作机制，并在软件安全标准规范、漏洞检测和处置机制等方面加强管理。金融、证券、交通、能源、海关、税务、工业、科技等重要联网信息系统主管部门应加强网络安全管理和保障工作。高度重视我国工业控制系统的安全管理。

（三）各重要联网信息系统单位、互联网企业等应提高自身网络安全防护水平，落实安全防护措施，提高抵御外部攻击入侵的能力，加强对关键敏感数据的保护力度。加大安全投入，培养网络安全队伍，建设必要的网络安全技术手段。建立完善监测预警和应急响应机制，提高应急处置和联动能力。

（四）广大网民要提高对网络安全威胁的认识及网络安全防护意识。做好个人计算机和手机的安全防护，养成良好的安全上网习惯，避免访问不安全的网站或安装无法确定安全性的软件。国家工作人员要提高保密意识，严格落实保密规定，防止发生网络失窃密事件。

（五）加强网络安全国际合作。从政府部门、互联网企业和技术机构等多个层面推进网络安全国际合作，推动建立跨境网络安全事件的通报、处置机制，提高对跨境网络安全事件的处置能力。