CNCERT/CC
国家互联网应急中心

2012年我国互联网网络安全态势综述

态势要点 Situational points

- 2012 年，网络基础设施运行总体平稳，但安全形势不容乐观。国家信息安全漏洞共享平台（CNVD）向基础电信运营企业通报其所属信息系统或设备的漏洞风险 339 个，针对网络基础设施的探测、渗透和攻击事件时有发生。
- 网站被植入后门等隐蔽性攻击事件呈增长态势，网站用户信息成为黑客窃取重点。2012 年 ,CNCERT 共监测发现我国境内 52324 个网站被植入后门，其中政府网站 3016 个，较 2011 年月均分别增长 213.7% 和 93.1%。
- 网络钓鱼日渐猖獗，严重影响在线金融服务和电子商务的发展，危害公众利益。2012 年，CNCERT 共监测发现针对我国境内网站的钓鱼页面 22308 个，接收到网络钓鱼类事件投诉 9463 起，约占总接收事件数量的一半。
- 移动互联网恶意程序数量急剧增长，Android 平台成为重灾区。2012 年，CNCERT 监测和网络安全企业通报的移动互联网恶意程序样本有 162981 个，较 2011 年增长 25 倍，其中约有 82.5% 针对 Android 平台。
- 2012 年，据 CNCERT 监测，我国境内日均发生攻击流量超过 1G 的较大规模拒绝服务攻击事件 1022 起，约为 2011 年的 3 倍，但常见虚假源地址攻击事件所占比例由 2011 年的 70% 下降至 49%。
- 利用“火焰”病毒、“高斯”病毒、“红色十月”病毒等实施的高级可持续攻击（APT 攻击）活动频现，对国家和企业的数据安全造成严重威胁。2012 年 ,我国境内至少有 4.1 万余台主机感染了具有 APT 特征的木马程序。
- 2012 年，CNVD 每月新增收集发布的漏洞数量平均超过 550 个。同时，多种原因导致漏洞修复的周期较长、进程缓慢。日益增多的存量漏洞和每日新增漏洞是基础信息网络和重要信息系统的主要安全隐患。
- 我国面临的境外攻击威胁依然严重。从控制服务器数量、控制我国境内主机的数量、钓鱼网站托管地来看，美国均居首位。“匿名者”等黑客组织活动频繁，多次声称或实施针对我国政府网站的网络攻击。

O 概述 verview

2012 年我国互联网网络安全态势综述

2012 年，我国互联网快速融合发展，宽带普及提速工程稳步推进，移动互联网、云计算、电子商务、网络媒体、微博客等新技术新业务相互促进、快速发展。在政府相关部门、互联网服务机构、网络安全企业和广大网民的共同努力下，我国相关单位和网民的网络安全防范意识进一步提高，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。

但总体上看，黑客活动仍然日趋频繁，网站后门、网络钓鱼、移动互联网恶意程序、拒绝服务攻击事件呈大幅增长态势，直接影响网民和企业权益，阻碍行业健康发展；针对特定目标的有组织高级可持续攻击（APT 攻击）日渐增多，国家、企业的网络信息系统安全面临严峻挑战。本综述着重对2012年互联网安全威胁的特点和未来发展趋势进行了分析和总结。

Security situation 安全形势

我国互联网网络安全形势

网络基础设施运行总体平稳，但依然面临严峻挑战

在政府主管部门的指导下，各基础电信运营企业认真开展网络安全防护工作。根据工信部 2012 年通信网络安全防护检查的情况，基础电信企业对网络安全防护工作的重视程度进一步提高，网络安全风险意识和防护水平显著提升。2012 年，CNVD 共向基础电信运营企业发布漏洞预警信息 211 份，通报了其所属信息系统或设备的漏洞风险事件 339 个，各基础电信运营企业均快速响应、积极处置，及时消除了安全隐患。路由器、交换机等通信网络设备是网络基础设施的基本组成部分。据 CNVD 收录的漏洞信息统计，2012 年发现涉及通信网络设备的通用软硬件漏洞数量为 199 个，较 2011 年下降 2.0%。但不容忽视的是，涉及通信网络设备的通用软硬件高危漏洞为 95 个，较 2011 年大幅增长了 30.1%。总体来看，2012 年我国网络基础设施运行基本平稳，未发生重大网络安全事件。然而，针对我国网络基础设施的探测、渗透和攻击事件时有发生，虽尚未造成严重危害，但高水平、有组织的网络攻击给网络基础设施安全保障带来严峻挑战。

- 在政府主管部门的指导下，基础电信运营企业认真开展网络安全防护工作。

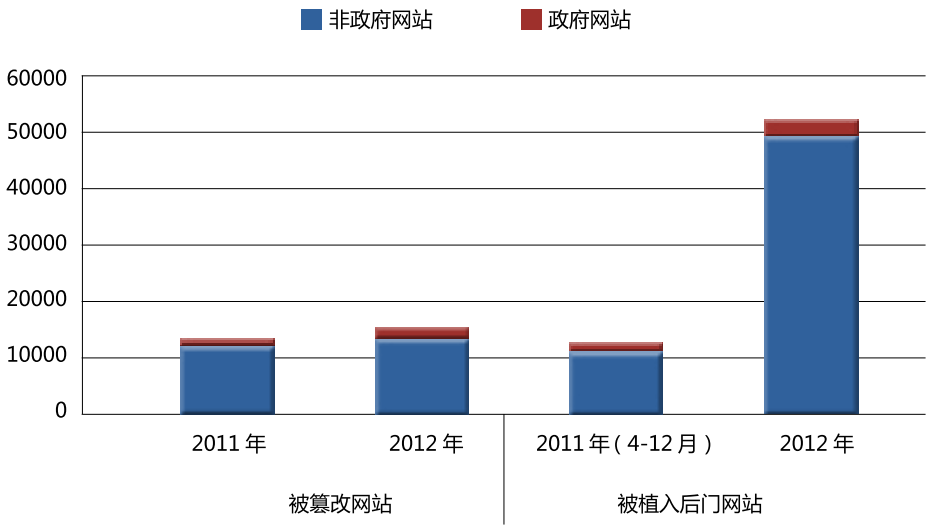
- 2012 年，CNVD 共向基础电信运营企业发布漏洞预警信息 211 份，通报了其所属信息系统或设备的漏洞风险事件 339 个。各企业均积极响应、迅速处置。
- 据 CNVD 收录的漏洞信息统计，2012 年发现涉及路由器、交换机等通信网络设备的软硬件漏洞 199 个，较 2011 年下降 2.0%

- 但涉及通信网络设备的通用软硬件高危漏洞数量为 95 个，较 2011 年大幅增长 30.1%。
- 针对我国网络基础设施的探测、渗透和攻击事件时有发生，高水平、有组织的网络攻击给网络基础设施安全保障带来严峻挑战。

网站被植入后门等隐蔽性攻击事件呈增长态势，网站用户信息成为黑客窃取的重点

与以往通过明显篡改网页内容以表达诉求或炫耀技术不同的是，2012 年，黑客倾向于通过隐蔽的危害更大的后门程序，获得经济利益和窃取网站内存储的信息。据 CNCERT 监测，2012 年，我国境内被篡改网站数量为 16388 个，其中政府网站有 1802 个，较去年分别增长了 6.1% 和 21.4%；被暗中植入后门的网站有 52324 个，其中政府网站有 3016 个，较去年月均分别大幅增长 213.7% 和 93.1%。此外，据不完全统计，2012 年，约有 50 余个我国网站用户信息数据库在互联网上公开流传或通过地下黑色产业链进行售卖，其中已证实确为真实信息的数据近 5000 万条。同时，由于网民习惯在不同网站使用同样的账号密码，受 2011 年底发生的 CSDN、天涯社区等网站信息泄露事件的影响，2012 年又有多个电商网站和论坛被披露由此导致用户个人信息泄露。网站安全尤其是网站中用户个人信息和数据的安全问题，仍然面临严重威胁。

2012 年我国境内被篡改和被植入后门的网站数量统计

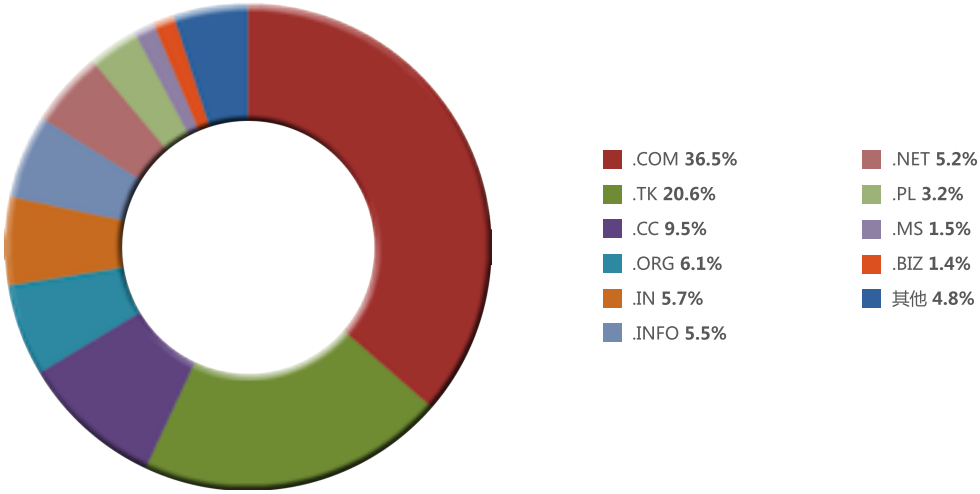


Security situation 安全形势

网络钓鱼日渐猖獗，严重影响在线金融服务和电子商务的发展，危害公众利益

2012 年，互联网用户通过网络开展的经济活动持续增多，在线销售和支付总额增长迅速，窃取经济利益成为黑客实施网络攻击的主要目标之一。2012 年，CNCERT 共监测发现针对我国境内网站的钓鱼页面 22308 个，涉及 IP 地址 2576 个，从钓鱼站点使用域名的顶级域分布来看，以 .COM 最多，占 36.5%，其次是 .TK 和 .CC，分别占 20.6% 和 9.5%；接收到网络钓鱼类事件举报 9463 起，较 2011 年大幅增长 73.3%，约占总接收事件数量的一半（49.5%）。这些钓鱼网站中，仿冒中国工商银行等网上银行的约占 54.8%，仿冒中央电视台、腾讯、淘宝等进行虚假抽奖或中奖活动、虚假新奇特或低价物品销售活动的约占 44.7%。钓鱼网站的主要目的是骗取用户的银行帐号、密码等网上交易所需信息。2012 年，仅 CNCERT 监测发现被黑客骗取的用户银行卡信息就达 1.8 万条，这些信息的失窃很可能会给用户带来巨额财产损失。值得注意的是，除骗取用户经济利益外，一些钓鱼页面还会套取用户的个人身份、地址、电话等信息，导致用户个人信息泄露。

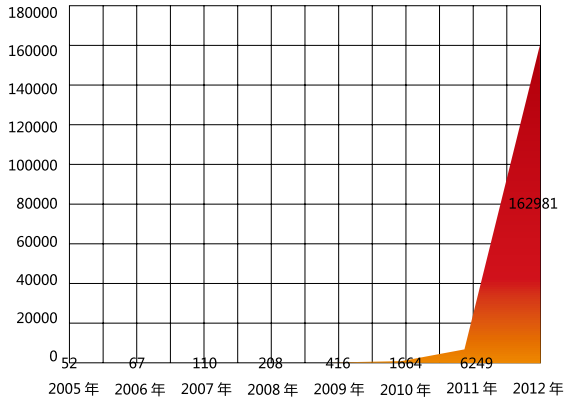
2012 年 CNCERT 监测发现的钓鱼站点所用域名按顶级域分布



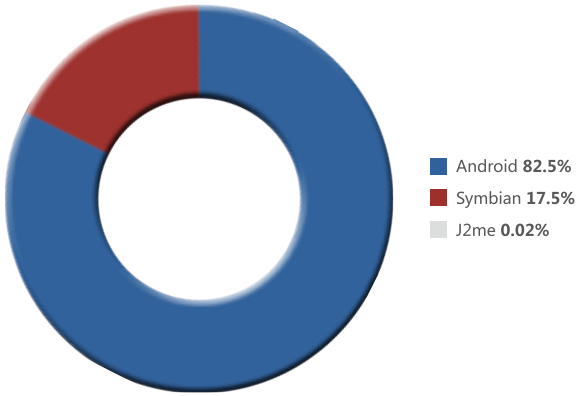
移动互联网恶意程序数量急剧增长，Android 平台成为安全重灾区

2012 年，我国移动用户数量稳步增长，新增智能设备数量跃居世界首位，应用程序商店下载量快速增长。在移动互联网快速发展的同时，移动互联网恶意程序也在快速繁衍和扩散。以 2012 年 CNCERT 监测发现的一个名为 A.privacy.NetiSend.d 的手机恶意程序为例，其存在于国内水货手机固件 ROM 中，平均每月感染规模约 15 万，安装后伪装成系统组件，于后台运行并窃取手机 IMEI 号、手机型号、版本信息以及手机内其它个人信息发送到指定控制服务器上，危害用户隐私安全。CNCERT 监测发现的另一个名为 A.remote.Wangdou.a 的手机恶意程序感染了约 117 万手机用户，其能够根据控制服务器指令向大量指定号码发送带垃圾广告的短信，一方面造成了垃圾短信的泛滥，另一方面也给感染用户造成话费损失。2012 年，CNCERT 监测和网络安全企业通报的移动互联网恶意程序样本有 162981 个，较 2011 年增长 25 倍，其中约有 82.5% 的样本针对 Android 平台，已超过 Symbian 平台跃居首位，这主要是缘于 Android 平台的用户数量快速增长和 Android 平台的开放性。按照恶意程序的行为属性统计，恶意扣费类的恶意程序数量仍居第一位，占 39.8%，流氓行为类（占 27.7%）、资费消耗类（占 11.0%）分列第二、三位。2012 年，CNCERT 组织通信行业开展了多次移动互联网恶意程序专项治理行动，所重点打击的远程控制类和信息窃取类恶意程序所占比例分别较 2011 年的 17.59% 和 18.88% 大幅度下降至 8.5% 和 7.4%。

2005 年 -2012 年移动互联网恶意程序数量走势



2012 年移动互联网恶意程序数量按操作系统统计

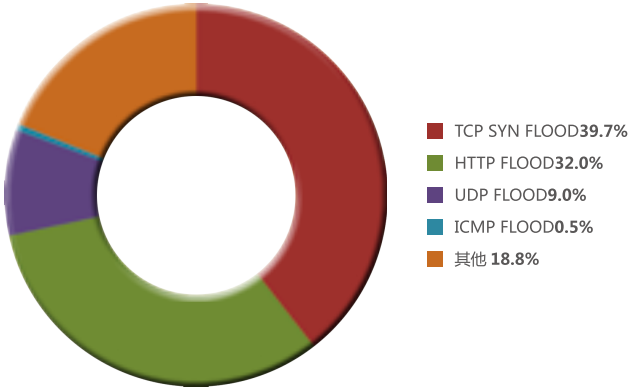


安全形势 Security situation

拒绝服务攻击仍然是影响互联网运行安全最主要的威胁之一

据 CNCERT 抽样监测，2012 年我国境内日均发生攻击流量超过 1G 的较大规模拒绝服务攻击事件有 1022 起，约为 2011 年的 3 倍，但与 2011 年不同的是，常见虚假源地址攻击事件所占比例由约 70% 下降至 49%。在监测发现的拒绝服务攻击事件中，约有 88.8% 的被攻击目标位于境内。拒绝服务攻击所采用的技术手段日趋综合化复杂化，从攻击网站本身逐渐转为攻击网站所使用的权威域名解析服务器，使得其所承载的大量其它网站的域名解析都间接受到影响，甚至对我国互联网的整体运行安全造成严重威胁。2012 年，在 CNCERT 处理过的一起拒绝服务攻击事件中，攻击者为使受害网站无法提供正常服务，针对其权威域名解析服务器进行了混合多种攻击方式的大流量攻击，导致全网 DNS 流量异常激增，流量峰值达 90Gbps，对部分省份的用户正常使用互联网造成了一定影响。

2012 年 CNCERT 监测发现的 DDOS 攻击事件类型分布



我国境内日均发生攻击流量超过 1G 的较大规模 DDOS 事件 1022 起，约为 2011 年的近 3 倍。

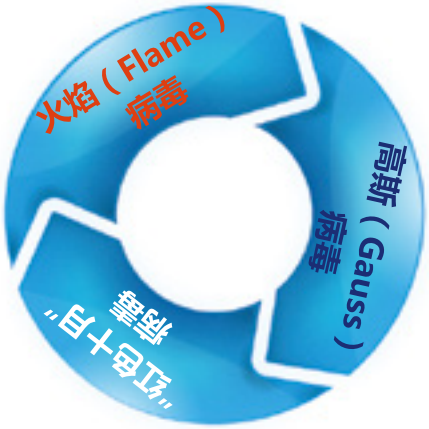
在监测发现的拒绝服务攻击事件中，约有 88.8% 的被攻击目标位于境内

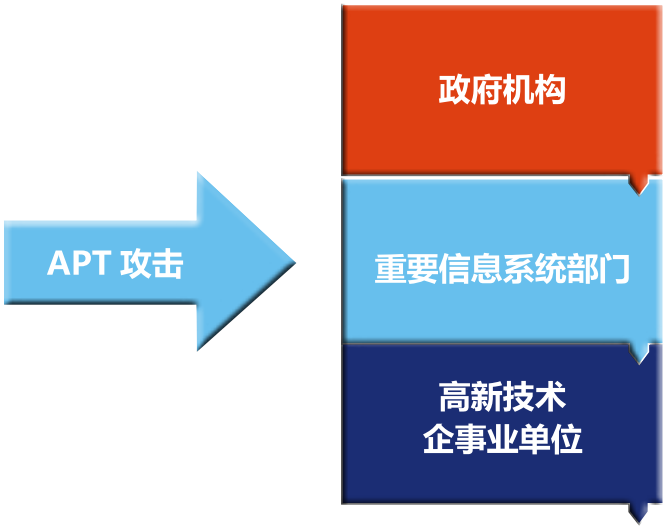
与 2011 年不同的是，常见虚假源地址攻击事件所占比例由约 70% 下降至 49%。

采用的技术手段日趋综合化复杂化，从攻击网站本身逐渐转为攻击网站所使用的权威域名解析服务器，使其承载的大量其它网站的域名解析间接受到影响，甚至对互联网整体运行安全造成严重威胁。

实施 APT 攻击的恶意程序频被披露，国家和企业的数据安全面临严重威胁

2012 年，“火焰（Flame）”病毒、“高斯（Gauss）”病毒、“红色十月”病毒等实施复杂 APT 攻击的恶意程序频现，其功能以窃取信息和收集情报为主，且均已隐蔽工作了数年。据 CNCERT 监测，2012 年我国境内至少有 4.1 万余台主机感染了具有 APT 特征的木马程序，涉及多个政府机构、重要信息系统部门以及高新技术企事业单位，且绝大多数这类木马的控制服务器位于境外。由于上述单位的网络信息系统中传输或存储的信息以及其自身的正常运行往往关系国家事务和经济社会运行，所以容易成为带有一定背景的组织或团体重点关注的目标，其数据安全面临严重威胁，需要各方高度重视。

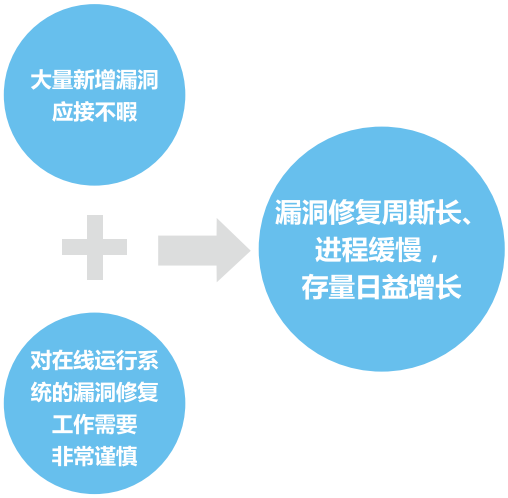




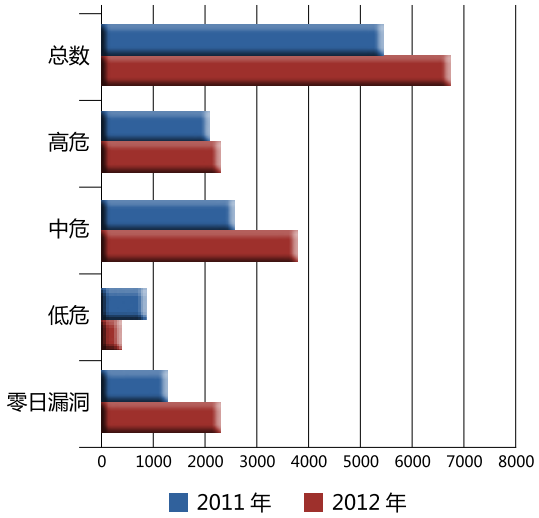
Security situation 安全形势

安全漏洞旧洞未补新洞迭出，留下安全隐患

2012 年，CNVD 共收集整理并公开发布信息安全漏洞 6824 个，较 2011 年增长 23.0%，每月新增漏洞数量平均超过 550 个。其中，高危漏洞 2440 个，较 2011 年增长 12.8%；零日漏洞 2439 个，较 2011 年大幅增长 82.0%。一方面，大量新增的安全漏洞让网络维护人员应接不暇，另一方面，对在线运行系统的漏洞修复工作需要非常谨慎，避免造成业务中断而带来更大影响，这些原因导致安全漏洞修复的周期较长、进程缓慢。例如，2012 年 1 月初，Web 网站常用框架软件 Apache Struts Xwork 被披露存在一个远程代码执行高危漏洞（CNVD-2012-09285），CNCERT 随后通过网站发布了该漏洞预警信息，并向监测发现存在该漏洞的近 300 个政府和重要信息系统网站管理部门通报了情况，但截至 2013 年 2 月底，从 CNCERT 抽样检查的数据看，仍有约 20% 的采用该框架软件的政府网站未及时修复。多年来日益累积的存量漏洞和每日不断出现的新漏洞对信息系统安全带来严重威胁。



2011 年和 2012 年 CNVD 收录的漏洞情况比较



CNCERT/CNVD 通过网站发布了 Web 网站常用框架软件 Apache Struts Xwork 的远程代码执行漏洞预警信息，陆续对监测发现存在该漏洞的近 300 个政府和重要信息系统网站管理部门通报了情况。

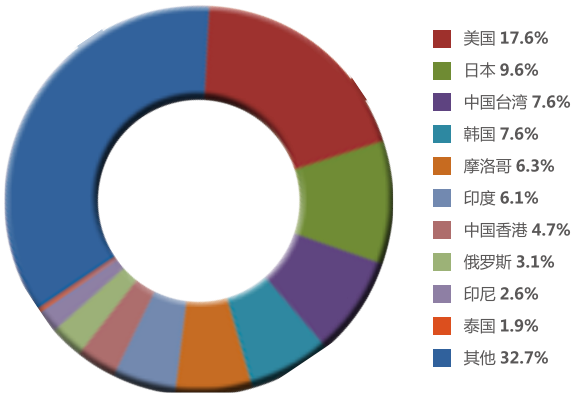
但截止到 2013 年 2 月底，从 CNCERT 抽样检查的数据看，仍有约 20% 的采用该框架软件的政府网站未及时修复。

我国面临的境外攻击威胁依然严重

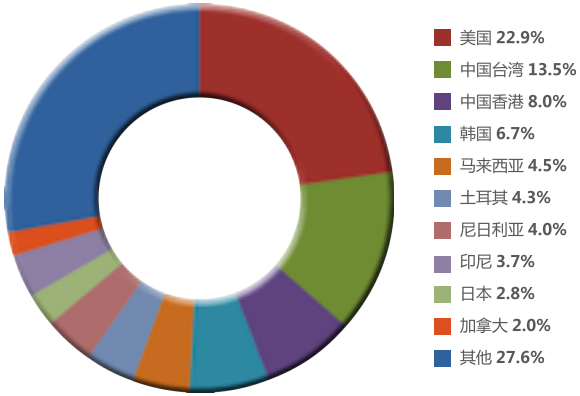
2012 年，CNCERT 抽样监测发现，境外约有 7.3 万个木马或僵尸网络控制服务器控制了我国境内 1419.7 万余台主机，较 2011 年分别大幅增长 56.9% 和 59.6%；其中位于美国的 12891 个控制服务器（占境外控制服务器的 17.6%）控制了我国境内 1051.2 万余台主机（占受境外控制的境内主机的 74.0%），控制服务器数量和所控制的我国境内主机数量均居首位；从控制服务器所占比例来看，日本和中国台湾分列第二、三位，占比分别为 9.6% 和 7.6%；从所控制的我国境内主机数量来看，韩国和德国分列第二、三位，分别控制了我国境内 78.5 万和 77.8 万台主机。这些受控主机因被黑客远程操控，一方面会导致用户计算机上存储的信息被窃取，另一方面则可能成为黑客借以向他人发动攻击的跳板，同时大量受到黑客集中控制的受控主机还可能构成僵尸网络，成为黑客发动大规模网络攻击的工具和平台。2012 年，我国某 CDN 服务商、某 IDC 机房等多次遭到持续性的拒绝服务攻击，以致无法正常提供服务，经分析发现这些攻击都是由位于多个省份的 IDC 机房内的主机因被黑客远程操控而发起的。

在网站后门攻击方面，境外有 3.2 万台主机通过植入后门对境内 3.8 万个网站实施远程控制，按照所控制的境内网站数量统计，位于美国的 7370 台主机控制着境内 10037 个网站，位居第一，其次是位于韩国和中国香港的主机，分别控制了境内 7931 个和 4692 个网站。2012 年 CNCERT 监测发现我国某高校、某高新技术科研院所、某上市公司等的邮件服务器被境外入侵并植入后门，三千多个用户的邮件账号与密码哈希值以及大量数据被通过加密方式上传至境外服务器。

2012 年境外木马或僵尸程序控制服务器 IP 按国家和地区分布



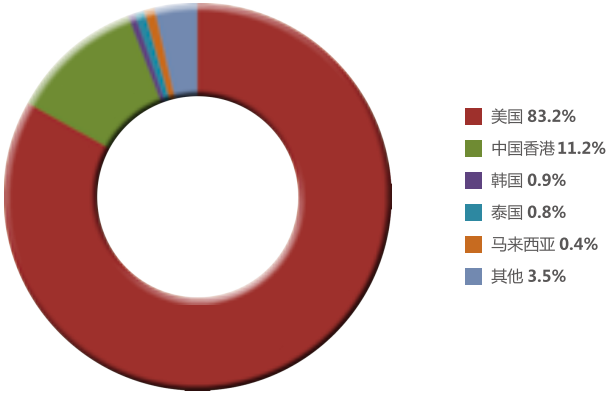
2012 年向境内网站植入后门的境外 IP 按国家和地区分布



Security situation 安全形势

在网络钓鱼攻击方面，针对我国的钓鱼站点有96.2%位于境外，其中位于美国的 2062 台主机承载了 18230 个针对境内网站的钓鱼页面，位于美国的钓鱼站点数量在全部位于境外的钓鱼站点中占比高达 83.2%，位居第一。

2012 年仿冒境内网站的境外 IP 按国家和地区分布



2012 年，“匿名者”、“幽灵躯壳”、“反共黑客”、“阿尔及利亚 Barbaros-DZ”等黑客组织频繁发动对我国的网络攻击。其中，“匿名者”组织于 2012 年 3 月、4 月、11 月多次宣称要针对我国多家政府和大型企业发动攻击。据 CNCERT 监测，我国部分网站已经遭到其篡改攻击。“幽灵躯壳”组织在 2012 年 6 月声称要针对中国发动名为“蜻蜓计划”的网络战，并在互联网上公布了大量其已获取的我国境内数十家网站的部分账户信息。“反共黑客”组织持续发起针对我国境内党政机关、高校以及社会组织网站的网页篡改攻击，留下恶毒攻击中国共产党、具有煽动性的政治言论，并在攻击成功后通过社交网站等网络媒介进行传播以扩大影响。截止到 2012 年底，CNCERT 共监测到涉及 90 个部门的 142 个网站被“反共黑客”组织篡改。名为 Barbaros-DZ 的阿尔及利亚黑客组织自 2012 年 3 月以来声称对我国境内超过 1250 个政府网站页面进行了篡改。

Our 实践工作 Practices

CNCERT 开展的相关工作

支撑政府主管部门开展网络安全监管和检查，维护基础网络和重要信息系统安全

2012 年，CNCERT 配合工信部开展互联网虚假源地址整治工作，制定虚假源地址治理技术指南，中国电信、中国移动等电信运营企业按照工信部要求和技术指南，在全网数万台设备上部署和完善虚假源地址过滤策略，有效遏制了虚假源地址攻击势头。据 CNCERT 监测统计，常见的 TCP SYN FLOOD、UDP FLOOD 等虚假源地址攻击事件所占比例已从 2011 年的 70% 下降至 49%。配合工信部开展针对国务院部委网站的外部网络安全检查，发现涉及多个部门的 46 个网站信息系统存在 263 处不同程度的安全风险，并针对发现的问题及时提出了整改加固措施和建议。

加大公共互联网环境治理力度，遏制恶意代码生存空间

2012 年，在工信部的指导下，CNCERT 及各地分中心会同基础电信运营企业、域名注册服务机构开展了 14 次木马和僵尸网络专项打击行动，共成功处置了 3690 个控制规模较大的木马和僵尸网络控制端和恶意程序传播源，切断了黑客对 3937 万余台感染主机的远程操控。此外，CNCERT 各分中心在当地通信管理局的指导下，共协调地方基础电信运营企业分公司清理木马和僵尸网络控制服务器 5.4 万个、受控主机 65 万个，有效净化了公共互联网环境。

贯彻落实《移动互联网恶意程序监测与处置机制》，大力推动移动互联网恶意程序治理工作

2012 年，在工信部的指导下，CNCERT 积极组织开展移动互联网恶意程序专项治理，维护移动互联网安全。一是组织基础电信运营企业、12321 举报中心、中国反网络病毒联盟（ANVA）成员单位、手机应用下载站点和论坛先后开展了 6 次移动互联网恶意程序专项打击行动，共接收各单位报送的恶意样本 4644 个，处置恶意控制和传播 URL 链接 1805 条，对恶意程序传播起到良好遏制作用。二是组织基础电信运营企业完善疑似恶意样本报送接口规范和监测处置管理平台数据接口规范，进一步推动移动互联网恶意程序的监测与处置工作。

完善网络安全事件处置体系，提高事件处置能力和应急水平

2012 年，CNCERT 继续完善与电信运营企业、域名注册管理和服务机构等通信行业相关单位建立的事件处置协作体系，全年共处置各类网络安全事件 18805 起，较 2011 年的 10924 起大幅增长 72.1%。其中，处置数量位列前三的分别是安全漏洞事件（7657 起）、网络钓鱼事件（6575 起）和网页篡改事件（2204 起），网络钓鱼和网页篡改事件处置数量均较 2011 年增长近 2.5 倍。面对网络钓鱼攻击成本低、变化快、时效性强等特点，CNCERT 与电信运营企业和域名注册机构建立了快速处置机制，有效打击了利用我国主机和域名资源从事网络钓鱼的活动。2012 年，CNCERT 积极参加了工信部组织通信行业开展的

互联网网络安全应急演练，演练模拟重要通信基础设施和信息系统遭受网络攻击，CNCERT 及相关单位迅速对事件进行分析，采取措施消除威胁和影响，保障通信网络和重要信息系统安全运行。演练有效检验了互联网网络安全应急预案和处置流程，切实提高了通信行业的网络安全事件应急响应能力。

充分发挥行业联动合力，不断加强信息共享和技术合作

2012 年，由 CNCERT 发起并负责管理的 CNVD 在各成员单位的积极贡献和众多科研机构、个人的大力支持下，与近 200 家国内应用软件生产厂商以及企事业单位建立了处置联络机制，向 100 余位漏洞研究者颁发了超过 500 份的 CNVD 漏洞证书，漏洞和补丁信息的报送、验证、发布等工作机制高效运转，极大地提高了漏洞预警能力和修复速度。同时，依托 CNCERT 事件处置体系，CNVD 根据收录整理的安全漏洞，共向国内政府、电力、证券、金融等重要信息系统、电信行业、教育机构等单位和部门发布漏洞预警信息近 1000 份。由 CNCERT 发起成立的中国反网络病毒联盟（ANVA）积极开展联盟内恶意程序样本和恶意程序传播链接的共享工作，全年共享恶意样本 21.3 万个、传播恶意程序的 URL 链接 4.1 万条，共享流行移动互联网恶意样本 1.8 万个、传播移动互联网恶意程序的 URL 链接 0.9 万余条。ANVA 经汇总后共向公众发布恶意 URL 链接黑名单 3.2 万余条。

深化网络安全国际合作，进一步强化跨境网络安全事件处置协作机制

作为我国互联网网络安全应急体系对外合作窗口，2012 年 CNCERT 继续实施“国际合作伙伴计划”，目前已与 51 个国家和地区的 91 个组织建立了联系机制，与其中的 12 个组织正式签订网络安全合作备忘录或达成了一致，进一步完善和加强了跨境网络安全事件处置的协作机制，全年共协调境外安全组织处理涉及境内的网络安全事件 4063 起，较 2011 年增长近 3 倍，协助境外机构处理跨境事件 961 起，较 2011 年增长 69.2%。其中包括针对境内的 DDoS 攻击、网络钓鱼等事件，也包括针对美国银行、澳大利亚国家银行、PayPal 等境外银行和大型公司的网络安全事件。2012 年 10 月，CNCERT 接到美国 US-CERT 投诉，称部分位于我国的主机被恶意程序控制参与针对美国某银行和大型公司的拒绝服务攻击，请求协助处理。CNCERT 对相关情况进行核实后，对其提供的 75 个位于我国境内的 IP 地址进行了及时处理。CNCERT 还与微软公司联手打击了一个名为 Nitol 的僵尸网络，针对被其利用来进行恶意程序传播和控制的 3322.org 域名进行清理，关停了其中 7 万余个恶意域名。

2013 年值得关注的网络安全热点问题

在“宽带中国 2013 专项行动”稳步实施、移动互联网快速发展、应用终端不断丰富、信息系统云端化、资源大数据化以及国际政治经济新形势等环境因素的综合作用下，网络攻击将越来越呈现入侵渠道多、威力强度大、实施门槛低等特点，2013 年我国互联网面临的情况将更为复杂，网络安全形势将更加严峻。

恶意代码和漏洞技术不断演进，针对“高价值”目标的 APT 攻击风险持续加深，严重威胁我国网络空间安全

一是恶意代码将越来越多的具备零日漏洞攻击能力，黑客发现漏洞和利用漏洞进行攻击的时间间隔将越来越短。二是恶意代码的针对性、隐蔽性和复杂性将进一步提升，针对目标环境中特定配置的计算机可进行精准定位攻击。三是我国金融、能源、商贸、工控、国防等拥有高价值信息或对国家经济社会运行意义重大的信息系统将面临更多有组织或有国家支持背景的复杂 APT 攻击风险，轻则影响涉事企业的生存和发展，重则影响国家经济在全球的核心竞争力，甚至可能危及国家安全。

信息窃取和网络欺诈将继续成为黑客攻击的重点

2012 年 12 月 28 日，全国人大常委会通过《关于加强网络信息保护的决定》，网络信息保护立法已翻开新篇章，然而，在法律法规细化、管理措施落实、技术手段建设等诸多方面还有大量细致工作亟待完善。由于用户的网上活动所留下的大量私密信息已成为互联网的“新金矿”，唾手可得的经济利益将吸引黑客甘于冒险追逐。黑客将继续大肆通过钓鱼网站、社交网站、论坛等，结合社会工程学对用户自身或其生活圈实施攻击。网络平台的安全漏洞和安全管理的缺位，以及用户的不安全上网习惯将继续导致用户个人信息“裸奔”事件呈现频发态势，用户信息的窃取、贩卖和网络欺诈地下产业将逐步形成规模。

移动互联网恶意程序数量将持续增加并更加复杂

随着移动互联网的发展和应用的不断丰富，用户通过移动终端进行社交和经济活动的时间越来越长，而移动终端具备的实时在线、与用户互动紧密、能够对用户精确定位的特点，使得不法分子将更倾向于通过移动终端和移动互联网收集和售卖用户信息、强行推送广告、攻击移动在线支付等来获取经济利益，催生移动互联网黑色产业链发展。通过基于位置的服务（LBS）收集用户地理位置信息，还可能会

成为犯罪活动的重要信息来源。二维码技术的应用，从视觉上改变了原有信息传递的方式，得到用户的追捧，同时也为恶意程序提供了隐身之机。还有一些应用软件开发方和软件平台管理方为一己私利，给软件功能滥用和恶意软件传播留下方便之门。

大数据和云平台技术的发展引入新的安全风险，面临数据安全和运行安全双重考验

一是数据安全威胁。首先，大数据意味着大风险，存储大量高价值数据的信息系统将吸引更多的潜在攻击者；其次，越来越多的组织和个人将信息移入云中，一旦云平台在传输和存储信息时遭到窃取、篡改、破坏等攻击，则其影响范围将呈几何级增长；再有，大数据时代的数据处理技术日益提升，黑客利用数据挖掘和关联分析技术也将获得更多有价值的信息。二是云服务运行安全威胁。一方面，分布式拒绝服务攻击如造成云服务中断，则将影响众多组织和大量的用户；另一方面，云服务汇集了大量计算机和网络资源，一旦被控制用于实施网络攻击等违法犯罪行为，将给网络信息安全和用户合法权益带来不可估量的威胁，同时，攻击隐藏在云中，给安全事件的追踪分析增加了困难。此外，随着多元化智能终端的发展，用户使用各类智能终端通过移动互联网接入云端，也为网络攻击带来了更多的攻击渠道。

Countermeasures 对策建议

对策建议

针对当前我国面临的网络安全威胁和热点问题，提出以下对策建议：

加强网络空间立法，加大网络违法犯罪打击力度

建议加快出台国家信息安全战略，明确应对网络攻击、网络窃密、网络犯罪和网络恐怖主义等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制订整体规划。针对政府机构、重要信息系统运行单位、互联网企业等各方责任划分，重要信息系统安全防护，网上重要敏感信息监管以及个人隐私保护等难题和重点，分步骤出台或细化法律法规，细化网络违法犯罪的法律界定范围和量刑标准，确保我国网络空间有法可依。同时，建议执法机构加大网络违法犯罪的惩治力度，做到执法必严、违法必究，从而形成有效震慑。

构建国家网络空间安全综合防御体系，形成安全保障合力

建议不断健全跨部门、跨行业、跨地域的网络安全保障协作机制，整合政府部门、重要信息系统部门、电信运营企业、社会组织、公众等多方力量，逐步构建起国家网络空间安全综合防御体系。加强网络安全国际合作，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，为维护整个互联网安全做出贡献。

加强对新型网络安全威胁和应对措施的研究和投入，提高网络安全保障技术水平

针对木马和僵尸网络、网络钓鱼、移动互联网恶意程序、安全漏洞、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，建议有关部门加大科研投入，研究跨部门协同、多层次协作的保障技术、标准和体系架构，提高网络安全保障基础技术能力。同时，建议各基础信息网络和重要信息系统的运行单位加大网络安全保障投入，强化安全防护和管理，坚持做到安全防护设施的同步规划、同步建设和同步运行。

加强公共互联网网络安全环境的治理

建议政府主管部门加大互联网监管力度，落实企业责任，加强对移动互联网应用商店、增值电信业务经营者的网络安全管理，继续开展针对木马和僵尸网络、移动互联网恶意程序、网络钓鱼、拒绝服务攻击等安全威胁的清理和处置；通信行业、互联网企业、软硬件厂商等充分发挥行业优势，加强行业自律，积极配合政府主管部门，净化公共互联网网络环境。

加强对网民网络安全意识和防范知识的宣传和教育

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、宣传册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或僵尸网络操控，防范个人信息泄露和财产损失。

简介 Introduction

关于国家互联网应急中心（CNCERT）

国家互联网应急中心的全称是国家计算机网络应急技术处理协调中心（英文简称为 CNCERT 或 CNCERT/CC），成立于 1999 年 9 月，是工业和信息化部领导下的国家级网络安全应急机构，致力于建设国家级的网络安全监测中心、预警中心和应急中心，以支撑政府主管部门履行网络安全相关的社会管理和公共服务职能，支持基础信息网络的安全防护和安全运行，支援重要信息系统的网络安全监测、预警和处置。

2003 年，CNCERT 在我国大陆 31 个省、自治区、直辖市成立分中心，完成了跨网络、跨系统、跨地域的公共互联网网络安全应急技术支撑体系建设，形成了全国性的互联网网络安全信息共享、技术协同能力。目前，CNCERT 作为国家互联网安全应急体系的核心技术协调机构，在协调国内网络安全应急组织（CERT）共同处理互联网安全事件方面发挥着重要作用。

CNCERT 的业务能力主要包括：

监测发现：依托“863-917 网络安全监测系统”实现网络安全事件的监测发现。863-917 网络安全监测系统是一个全程全网、多层次、多渠道延伸的网络安全综合监测平台，目前已具备对安全漏洞、恶意代码、网页篡改、网页挂马、拒绝服务攻击、域名劫持、路由劫持等各种网络威胁或攻击的监测发现能力。

通报预警：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。此外，按照 2009 年工业和信息化部颁布实施的《互联网网络安全信息通报实施办法》承担通信行业互联网网络安全信息通报工作。

应急处置：依托与运营商、域名注册商、安全服务厂商等相关部门的快速工作机制和与涉及国计民生的重要信息系统部门及执法机关密切合作机制实现网络安全事件的快速处置；同时作为国际著名网络安全合作组织 FIRST 和 APCERT 的重要成员，与国内外多个国家级应急响应组织和知名网络安全机构建立了网络安全事件处理合作机制。面向国内外用户受理网络安全事件报告，及时掌握和处置突发重大网络安全事件。

热线电话：+8610 82990999（中文），82991000（英文）
传　　真：+8610 82990399
电子邮件：cncert@cert.org.cn
PGP Key：http://www.cert.org.cn/cncert.asc
网　　址：http://www.cert.org.cn/

热线电话：+8610 82990999（中文）82991000（英文）
传真：+8610 82990399　电子邮件：cncert@cert.org.cn
PGP Key：http://www.cert.org.cn/cncert.asc
网址：http://www.cert.org.cn/