# CNCERT/CC
# 2007 年上半年网络安全工作报告



国家计算机网络应急技术处理协调中心

CNCERT/CC

关于CNCERT/CC 2007年上半年网络安全工作报告



编者按：

谢谢您阅读“CNCERT/CC 2007 年上半年网络安全工作报告”，如果您发现本报告存在任何问题，请您及时与我们联系，电子邮件地址为：cncert@cert.org.cn。我们对此深表感谢。

# 目录

目录 ..... 3
1 关于 CNCERT/CC ..... 4
2 网络安全总体状况分析 ..... 5
3 网络安全事件接收与处理情况 ..... 6
3.1 事件接收情况 ..... 6
3.2 事件处理情况 ..... 7
3.3 事件处理部分案例介绍 ..... 8
4 信息系统安全漏洞公告及处理情况 ..... 10
5 互联网业务流量监测分析 ..... 11
6 木马与僵尸网络监测分析 ..... 13
6.1 木马数据分析 ..... 13
6.2 僵尸网络数据分析 ..... 15
7 被篡改网站监测分析 ..... 16
7.1 我国网站被篡改情况 ..... 17
7.2 我国大陆地区政府网站被篡改情况 ..... 17
8 网络仿冒事件情况分析 ..... 18
9 恶意代码捕获及分析情况 ..... 19
10 CNCERT/CC 网站信息发布 ..... 20
11 网络安全应急组织发展情况 ..... 21
11.1 国内应急组织发展情况 ..... 21
11.2 CNCERT/CC 组织的相关重要活动 ..... 23
12 国际合作与交流 ..... 26
13 结束语 ..... 27

# 1 关于 CNCERT/CC

国家计算机网络应急技术处理协调中心（简称 CNCERT/CC）是在信息产业部互联网应急处理协调办公室的直接领导下，负责协调我国各计算机网络安全事件应急小组（CERT）共同处理国家公共互联网上的安全紧急事件，为国家公共互联网、国家主要网络信息应用系统以及关键部门提供计算机网络安全的监测、预警、应急、防范等安全服务和技术支持，及时收集、核实、汇总、发布有关互联网网络安全的权威性信息，组织国内计算机网络安全应急组织进行国际合作和交流的组织。

CNCERT/CC 成立于 2000 年 10 月，2002 年 8 月成为国际权威组织“事件响应与安全组织论坛（FIRST）”的正式成员。CNCERT/CC 参与组织成立了亚太地区的专业组织 APCERT，是 APCERT 的指导委员会委员和副主席单位。CNCERT/CC 与国外应急小组和其他相关组织建立了互信、畅通的合作渠道，是中国处理网络安全事件的对外窗口。

CNCERT/CC 的主要业务包括:

- 信息沟通: 通过各种信息渠道与合作体系，及时交流获取各种网络安全事件与网络安全技术的相关信息，并通报相关用户或机构;
- 事件监测: 及时发现各类重大网络安全隐患与网络安全事件，向有关部门发出预警信息、提供技术支持;
- 事件处理: 协调国内各应急小组处理公共互联网上的各类重大网络安全事件，同时，作为国际上与中国进行网络安全事件协调处理的主要接口，协调处理来自国内外的网络安全事件投诉;
- 数据分析: 对各类网络安全事件的有关数据进行综合分析，形成权威的数据分析报告;
- 资源建设: 收集整理网络安全漏洞、补丁、攻击防御工具、最新网络安全技术等各种基础信息资源，为各方面的相关工作提供支持;
- 安全研究: 跟踪研究各种网络安全问题和技术，为网络安全防护和应急处理提供基础;
- 安全培训: 提供网络安全应急处理技术以及应急组织建设等方面的培训;
- 技术咨询: 提供网络安全事件处理的各类技术咨询;
- 国际交流: 组织国内计算机网络安全应急组织进行国际合作与交流。

CNCERT/CC 的联系方式:

国家计算机网络应急技术处理协调中心 CNCERT/CC
网址: http://www.cert.org.cn/
电邮: cncert@cert.org.cn
热线: +8610 82990999，82991000（英文）
传真: +8610 82990375
PGP Key: http://www.cert.org.cn/cncert.asc

# 2 网络安全总体状况分析

2007 年 1 月至 6 月期间，公共互联网网络整体上运行基本正常，未出现造成严重后果的大规模网络安全事件。但是，根据今年上半年接收和处理的网络安全事件统计可以看出，目前中国的互联网安全实际状况仍不容乐观。各种网络安全事件与去年同期相比都有明显增加。半年时间内，CNCERT/CC 接收的网络仿冒事件和网页恶意代码事件，已分别超出去年全年总数的 14.6%和 12.5%。我国大陆地区被植入木马的主机 IP 远远超过去年全年，增幅达 21 倍。我国大陆被篡改网站数量比去年同期增加了 4 倍，比去年全年增加了近 16.9%。

从 CNCERT/CC 掌握的半年情况来看，攻击者的攻击目标明确，针对不同网站和用户采用不同的攻击手段，且攻击行为趋利化特点表现明显。对政府类和安全管理相关类网站主要采用篡改网页的攻击形式，以达到泄愤和炫耀的目的，也不排除放置恶意代码的可能，导致政府类网站可能存在安全隐患。对中小企业，尤其是以网络为核心业务的企业，采用有组织的分布式拒绝服务攻击（DDoS）攻击等手段进行勒索，从而迫使企业接受相应条件，影响企业正常业务的开展。对于个人用户，攻击者更多的是通过用户身份窃取等手段，偷取该用户游戏账号、银行账号、密码等，窃取用户的私有财产。如利用网络钓鱼（Phishing）和网址嫁接（Pharming）等对金融机构、网上交易等站点进行网络仿冒，在线盗用用户身份和密码。通过恶意网页、社交工程、电子邮件和信息系统漏洞等方式传播恶意代码，利用间谍软件（spyware）和木马程序窃取用户的私有信息，严重的导致财产损失。而上半年我国大陆被植入木马的主机数量大幅攀升的现象，反映出国内网络安全状况中木马产业链的猖獗，是失泄密、网银账号被窃事件频发的重要原因。

2007 年上半年恶意代码的目的性增强。通过对 CNCERT/CC 蜜网系统所捕获的恶意代码进行分析，可以看出流行的恶意代码侧重于控制用户系统并进而组成僵尸网络或者窃取用户敏感信息等，主要有后门、邮件蠕虫、木马、间谍软件以及利用 MS Windows 系统漏洞和通过即时通讯软件、网络共享进行传播的蠕虫。而以破坏用户数据或影响系统正常使用为主要目标的病毒数量所占比例相对较少。这些恶意代码的传播能力增强、传播途径多样化、隐蔽性更强。如 1 月份出现的“熊猫烧香”蠕虫，可通过局域网、移动硬盘/U 盘、共享文件夹、系统弱口令等多种方式进行传播。当恶意代码被下载到主机上时，通过将自身属性设为隐藏等手段，使得用户难以察觉。与此同时，需要特别注意防范那些盗取网络个人银行账号密码、ADSL 账号密码的木马程序和通过 Skype 软件传播的木马程序。

僵尸网络发展迅速，逐渐成为攻击行为的基本渠道，成为网络安全的最大隐患之一。2007 年上半年 CNCERT/CC 监测到感染僵尸网络的主机总数达 520 多万。攻击者既可以利用僵尸网络发起 DDoS 攻击、发送大量垃圾邮件和传播恶意代码等，又可以通过僵尸系统收集受感染主机中用户的敏感信息或进一步组建成更大的僵尸网络。目前，僵尸网络中僵尸主机的数量一般在 1 千以内，但是也存在规模巨大的僵尸网络。

针对 DNS 服务器和域名转发服务器的攻击数量有明显增多的趋势，且危害严重。4 月份 CNCERT/CC 处理了微软 Windows 域名服务中存在漏洞（MS07-029）的相关事宜。DNS 服务可将主机名映射为具体的 IP 地址，是用户上网常用的服务之一。一旦提供该服务的系统被攻陷，通过网址嫁接方式，可将用户引诱到钓鱼网站或含有恶意代码的网站。对域名服务器的 DDoS 攻击，使其无法正常解析网络地址，往往会造成大量用户无法正常访问网站。所以，对 DNS 和域名转发服务器的安全防护非常重要。

新型网络应用的发展带来了新的安全问题和威胁。除了传统的 Web 浏览、E-Mail 和 DNS 服务外，eMule、clubox、迅雷等 P2P 下载软件占用了大量的网络带宽。利用 Windows 信使服务 MSN 和 QQ 等即时聊天类工具软件进行恶意代码传播的事件日益增多。因此，新型应

用服务的安全应当引起充分的注意。

近半年，各种网络安全事件数量较之以往均有显著增加。说明我国的公共互联网网络面临着更加严重的安全威胁。而以获益为目的的网络攻击事件将为广大用户带来更加直接的经济损失。

# 3 网络安全事件接收与处理情况

为了能够了解和掌握当前互联网的安全运行状态，CNCERT/CC 采用了多种方式来接收公众的网络安全事件报告，如热线电话、传真、电子邮件、网站等。对于其中影响互联网运行安全，涉及政府与重要信息系统部门的网络安全事件，CNCERT/CC 协调各省分中心进行及时、有效处理。网络安全事件的接收与处理数量在宏观上反映了我国互联网网络安全的当前状况，同时也体现出我国及时发现和应急处理安全事件的能力。

## 3.1 事件接收情况

2007 年上半年 CNCERT/CC 接收 1813 件非扫描类网络安全事件报告，其中每月接收非扫描类事件具体数量如图 1 所示。

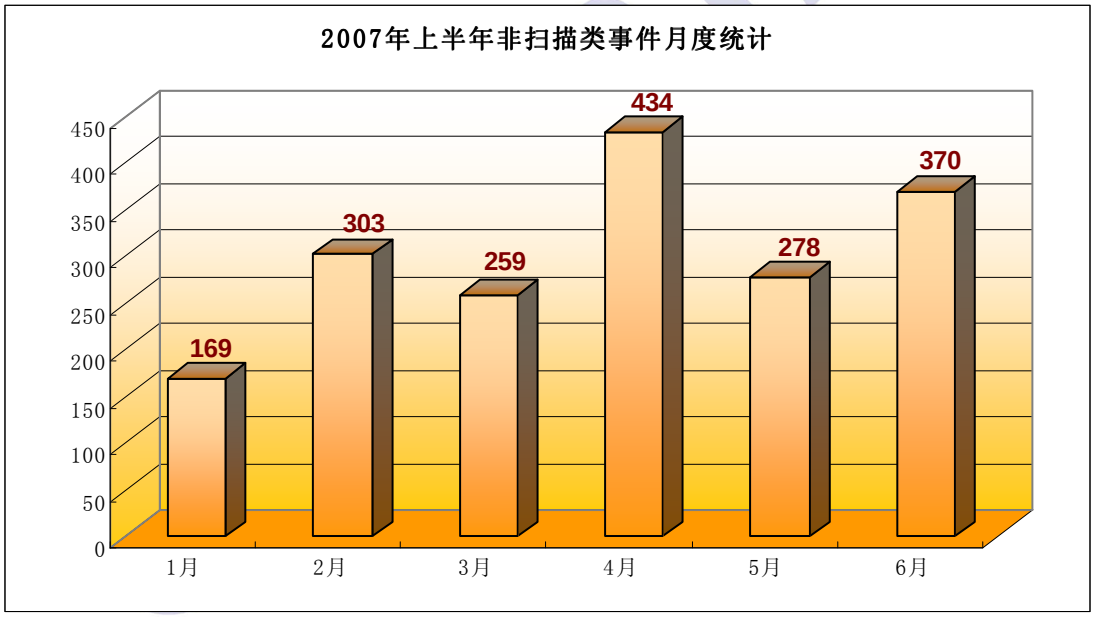



图 1　2007 年上半年非扫描类事件月度统计

所报告的网络安全事件主要有：网络仿冒、垃圾邮件和网页恶意代码事件等。根据报告的事件类型统计，如图 2 所示，网络仿冒事件数量最多，占所有接收事件的 35%，且 07 年上半年的数量便超出 06 年全年该类事件的总和（563 件），共计 645 件。垃圾邮件的数量达 452 件，占 25%。网页恶意代码事件也已超出 2006 年全年的数量（320 件），达到 360 件。漏洞事件为 186 件，占 10%。病毒、蠕虫或木马事件达 157 件，占 9%。拒绝服务攻击事件为 13 件，占 1%。本半年内所接收的网络安全事件大大超出去年同期水平，而网络仿冒事件、网页恶意代码事件尤为突出，甚至超出去年全年总数。

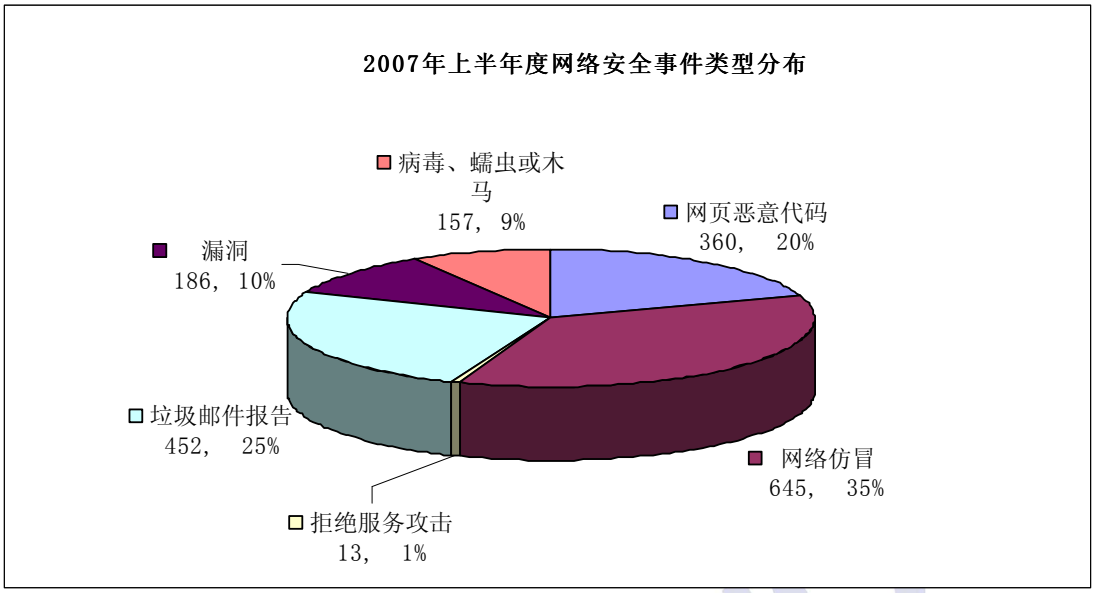



图 2　2007 年上半年网络安全事件类型分布

## 3.2 事件处理情况

2007 年上半年 CNCERT/CC 共成功处理各类网络安全事件 488 件，事件类型主要有网络仿冒、网页篡改、网页恶意代码、拒绝服务攻击等，各类事件处理数量如图 3 所示。在 CNCERT/CC 处理的安全事件中，涉及国内政府机构和重要信息系统部门的网页篡改类事件，以及涉及国外商业机构的网络仿冒类事件数量最多。

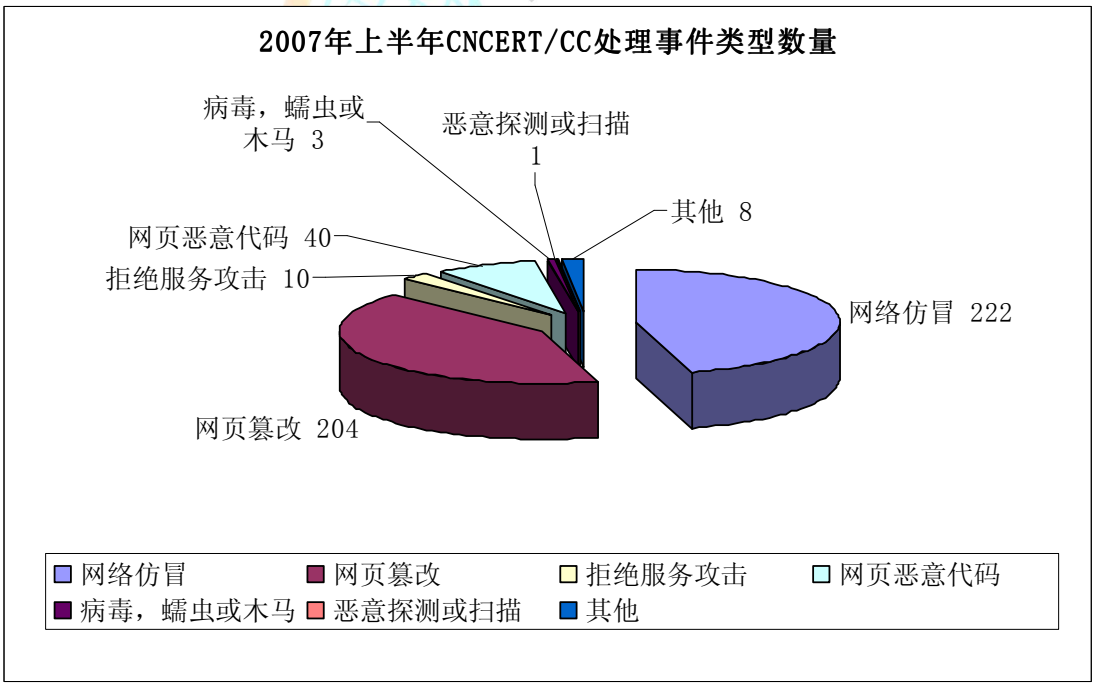



图 3　2007 年上半年 CNCERT/CC 处理网络安全事件数量统计

CNCERT/CC 一般是通过 CNCERT/CC 国家中心（总部）协调其在大陆各省所设分中心来处理安全事件。2007 年上半年各省分中心参与事件处理数目和比例如图 4 所示，其中新疆、北京、上海、广东、和山西处理事件数量居前 5 位。

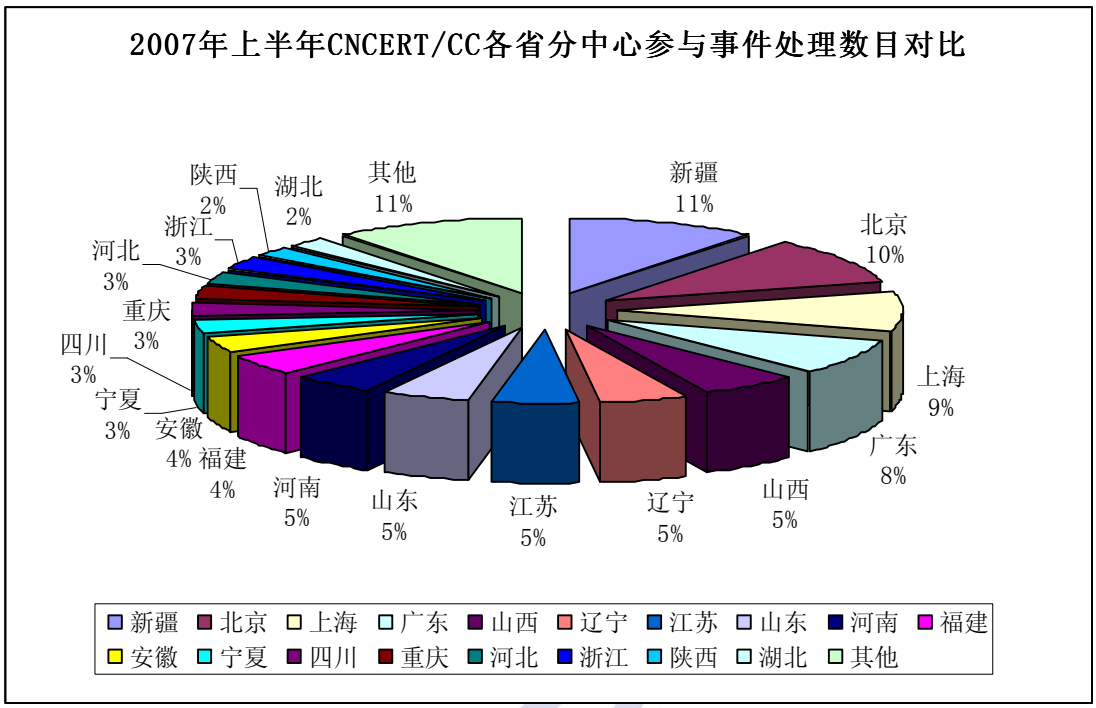



图 4　CNCERT/CC 各省分中心 2007 年上半年参与事件处理数目对比

## 3.3 事件处理部分案例介绍

### 3.3.1 “Nimaya（熊猫烧香）”病毒事件处理

“Nimaya（熊猫烧香）”病毒在 2007 年初出现流行趋势。该病毒具有感染、传播、网络更新、发起分布式拒绝服务攻击（DDoS）等功能。“熊猫烧香”的传播方式同时具备病毒和蠕虫的特性，危害较大。CNCERT/CC 注意到“熊猫烧香”在更新时所采用的机制是定期访问特定的网站，而且这些网站服务器位于国内。为此，CNCERT/CC 于 1 月 19 日开始协调江苏分中心和浙江分中心对用于更新的两台网站服务器进行处理。通过当地运营商，两个分中心先后确定了两台服务器的用户及其联系方式，最终位于江苏的一台服务器于 1 月 29 日删除了有关网页；而位于浙江的服务器用户已于 1 月 20 日重装了系统，故有关网页也已删除。截至到 2 月底，CNCERT/CC 监测发现 11 万个 IP 地址的主机被“熊猫烧香”病毒感染。

### 3.3.2 某招商网遭受分布式拒绝服务攻击

2007 年 1 月 15 日，CNCERT/CC 接到某招商网的事件报告，称该公司网站遭到已持续一个月的 DDoS 攻击，流量峰值达到 1G。接到事件报告后，CNCERT/CC 立即对此事件进行了协调处理。

在对被攻击网站提供的日志进行初步分析后，CNCERT/CC 国家中心协调了北京、广东、河南、湖南、辽宁、四川、安徽、河北、福建、上海等 10 个分中心参与处理，查找到了被黑客控制的部分计算机，但由于这些计算机基本都是属于网吧、局域网和 ADSL 用户，所以定位他们的具体用户比较困难，而且即使与用户取得联系，部分用户对于我们上机分析的请求也不予配合，这使得很难进行后续的深入分析。

2 月初，在上海分中心的协调下，得到了一个 ADSL 用户的积极配合，事件处理取得了重大进展。CNCERT/CC 对该 ADSL 用户的机器进行了深入分析，发现黑客是利用重庆市的一台服务器作为跳板，而最终的控制服务器位于福建省。在重庆分中心和福建分中心的配合下，CNCERT/CC 国家中心对这两台服务器进行了分析，从中得到了两名作案嫌疑人的有关线索，在用户的要求下将线索提供给了北京市公安局丰台分局。

### 3.3.3 某国内著名门户网站被挂马

2007 年 6 月 14 日，CNCERT/CC 收到合作伙伴报告称，某国内著名门户网站首页于 6 月 14 日凌晨被“挂马”（页面被嵌入恶意代码）数小时。CNCERT/CC 接到报告后，立即对事件进行了监测，发现包含该网站在内的国内多个网站，在 6 月 15 日凌晨再次被挂马数小时，而且被挂马网站均将用户访问跳转到 http://6688.89111.cn/m42.htm，导致用户从域名 89111.cn 之下多个恶意链接中下载恶意代码。

CNCERT/CC 立即联系被挂马的重要网站，告知其事件有关的详细情况和分析，建议其做好安全防范工作。与此同时，因 89111.cn 域名注册人所登记的信息及联系方式都是虚假信息，CNCERT/CC 与域名注册单位取得联系，得到对方的积极支持和快速响应，按照国家有关规定关闭了该恶意域名。

### 3.3.4 我国主机被利用为仿冒网站提供域名解析服务

2007 年 6 月，CNCERT/CC 先后收到 IBM 应急响应小组、Brandprotect 公司、CastleCops PIRT 反欺诈组织、RSA Cyota 反欺诈安全公司等多个国外安全组织的投诉，称位于我国大陆的两个 IP 地址自 6 月 6 日起为大量从事网络仿冒活动的域名提供域名解析服务。涉及被仿冒的机构有：PNC bank、bank of american、wash mutual、us bank 等。经查，此两 IP 分别位于上海市和山东省。CNCERT/CC 上海分中心和山东分中心分别联系当地运营商进行处理，其中也与一个用户直接取得了联系，并多次向用户发出了说明此安全事件的传真。在 CNCERT/CC 的努力下，十几天过后，运营商反馈两个用户终于同意暂时脱网，并采取消除安全问题的措施。

在此事件中，被犯罪分子入侵的主机，向大量仿冒网站提供域名解析服务，其所带来的危害，比单独一台运行一个仿冒网站的主机所带来的危害要更为严重。该事件反映近期网络仿冒域名有大量增加的趋势。CNCERT/CC 分析认为，出现这个趋势的原因在于：目前，虽然微软的 IE 7 浏览器和 Mozilla 的火狐 2.0 浏览器都采用了黑名单技术，使得当用户访问已知的仿冒网站（钓鱼网站）时向用户发出警告，然而这些流行的浏览器并没有很大的减少网络仿冒攻击的数量。犯罪分子采用了可以绕过黑名单的策略，他们每一次进行攻击的时候都注册新的域名，这给犯罪分子提供了几个小时的窃取信息的时间，因为从发出消息到网站被添加到黑名单需要一些时间。犯罪分子的新策略导致了仿冒网站域名的爆炸式增长。同时，犯罪分子会入侵一些主机来为大量仿冒网站的域名提供域名解析服务。

因此，近期网络仿冒大为增加的新情况，需要我国有关部门更加紧密合作共同应对，同

时也需要用户的积极配合。

### 3.3.5 某恶意域名处理

2007 年 6 月底，CNCERT/CC 收到澳大利亚应急响应组织（Auscert）的投诉，称一个包含有 3400 台主机的僵尸网络，正在从 http://fafb4c4c.com/session.exe 中下载恶意代码。此外，攻击者还通过在一个国际著名交友网站上以挂马的方式传播此恶意代码，挂马同样涉及域名 fafb4c4c.com。CNCERT/CC 核实后，立即与有关单位取得联系，得到对方的积极支持和快速响应，按照国家有关规定关闭了该恶意域名。

### 3.3.6 北京联众遭分布式拒绝服务攻击

在 CNCERT/CC 的协助与支持下，北京市网监处成功破获北京联众公司遭受分布式拒绝服务攻击案。2007 年 5 月 11 日，北京联众公司向北京市网监处报案称: 该公司自 4 月 26 日以来其托管在上海、石家庄 IDC 机房的 13 台服务器分别遭受到大流量的 DDoS 拒绝服务攻击，攻击一直从 4 月 26 日持续到 5 月 5 日，其攻击最高流量达到瞬时 700M/s。致使服务器全部瘫痪，在此服务器上运行的其经营的网络游戏被迫停止服务，经初步估算其经济损失为 3460 万人民币。在 CNCERT/CC 的支持与配合下，北京市网监处成功的获取了犯罪团伙实施 DDoS 攻击的证据，并及时将 4 名犯罪嫌疑人一举抓获。

## 4 信息系统安全漏洞公告及处理情况

CNCERT/CC 对于漏洞发布予以高度重视，2007 年上半年共整理发布与我国用户密切相关的漏洞公告 65 个。下面列举几个 2007 年上半年 CNCERT/CC 重点处理的漏洞。

#### Cisco IOS 在处理特定 TCP 包、IP 选项和 IPv6 路由包头时存在的三个漏洞

CNCERT/CC 通过国际应急合作组织获知，Cisco 公司在 1 月 24 日发布了三个漏洞公告，分别是“伪造 TCP 包可导致拒绝服务攻击漏洞”、“处理伪造 IP 选项存在的漏洞”、“处理 IPv6 路由包头存在的漏洞”。这 3 个漏洞影响所有运行 Cisco IOS 软件的 Cisco 设备。利用这些漏洞，黑客可对 Cisco 设备发动拒绝服务攻击或者在设备上远程执行攻击代码。对此，CNCERT/CC 紧急通知各运营商应急小组采取应急措施。各运营商在收到关于漏洞情况的通报后，立即对漏洞影响范围进行了排查，并对受漏洞影响的设备采取了紧急措施，包括采用配置访问控制列表的临时解决方式对攻击包进行封堵、与思科进行协商要求厂商提供满足网络业务运行的修复版本、研究和安排后续的版本升级工作从而彻底根除漏洞等。由于措施及时，各运营商除部分网络设备在一定程度上受到影响外，未出现由于这三个安全漏洞导致的异常故障。

#### 微软 Windows 动态游标文件头栈溢出漏洞（MS06-048）

CNCERT/CC 于 3 月 30 日发布了“Microsoft Windows 动态游标文件头栈溢出漏洞（CN-VA07-023）”的公告。攻击者利用该漏洞构建恶意 ANI 文件，并通过恶意网页、电子邮件、或者将动画光标文件拷贝到共享目录等方式来进行入侵，从而能够远程控制受影响的用户系统。CNCERT 接到国内外关于 ANI 网页木马安全事件报告后，及时向广大网民进

行通报，在网站上发布了安全公告，提醒用户谨慎处理来源不明的光标文件其他格式的图片文件。

### 微软 Windows 域名服务远程过程调用接口漏洞（MS07-029）

4 月 CNCERT/CC 重点处理的一个安全漏洞是“Microsoft Windows 域名服务远程过程调用接口漏洞”。微软虽于 4 月 12 日发布了有关的安全通报，但由于在其尚未发布补丁程序时，就已经发现有针对此漏洞的大量攻击行为，因此引起我们的高度重视，及时将有关漏洞信息通报各运营商应急小组和合作伙伴。根据 CNCERT/CC 掌握的数据，我国大陆有 3 千多个 IP 地址对应主机可能受此漏洞影响。这些主机不一定是对外提供 DNS 服务的服务器，但是它们启用了 DNS 服务，故也会受到漏洞影响。从 CNCERT/CC 调查的结果来看，我国主要公共 DNS 服务器并未受到此漏洞影响。

# 5 互联网业务流量监测分析

根据 CNCERT/CC 在 2007 年上半年对互联网业务流量的抽样统计，在 TCP 协议中，占用带宽最多的网络应用有四类：Web 浏览、P2P 下载、电子邮件和即时聊天工具。电子邮件协议使用 TCP 25 号端口，除正常使用外，该端口还充斥着大量的蠕虫和垃圾邮件流量。P2P 软件（例如 eMule、clubox、迅雷等）已成为目前最流行的下载工具，受到大量用户的青睐，且会占用大量网络带宽。因此，我国需重视该类软件的安全问题。同时，防止利用即时聊天类工具（如 Windows 信使服务 MSN 和 QQ 软件）对重要信息的泄密行为。

UDP 协议流量端口前十位如图 5 所示：

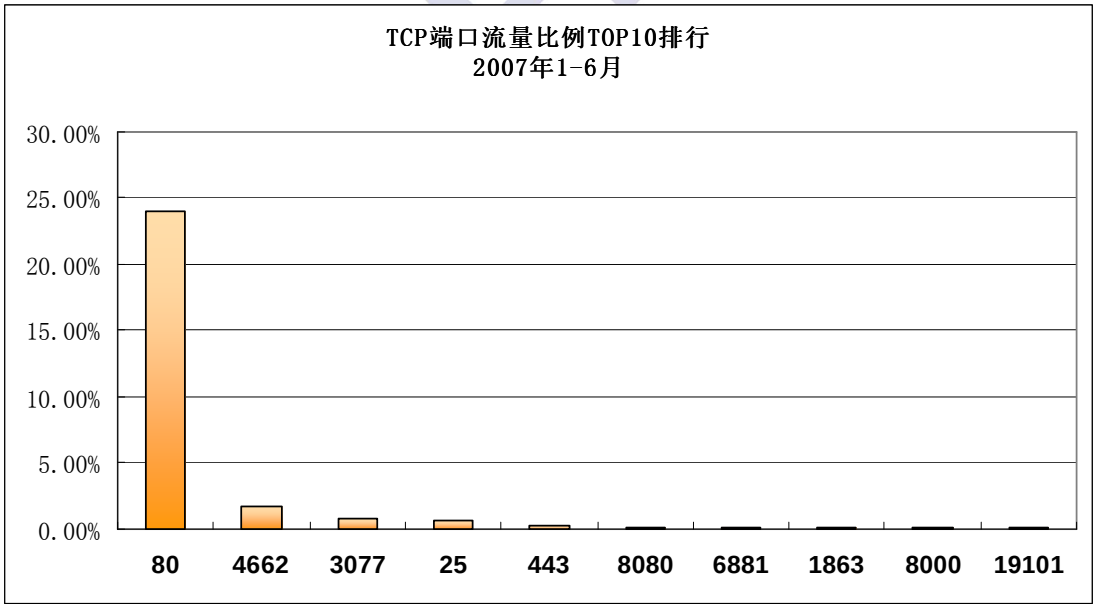



图 5　2007 年上半年 TCP 协议流量端口排名前十位

| TCP 端口 | TCP 流量排名 | 百分比 | 主要的业务种类 |
|---|---|---|---|
| 80 | 1 | 23.97% | 网页服务 |
| 4662 | 2 | 1.79% | eMule 下载工具默认端口 |
| 3077 | 3 | 0.75% | 迅雷下载工具默认端口 |
| 25 | 4 | 0.69% | SMTP 默认端口 |
| 443 | 5 | 0.31% | 网页服务 |
| 8080 | 6 | 0.20% | 网页服务 |
| 6881 | 7 | 0.19% | P2P 下载软件端口 |
| 1863 | 8 | 0.17% | MSN Messenger 协议登陆服务端口 |
| 8000 | 9 | 0.12% | QQ 通讯端口 |
| 19101 | 10 | 0.12% | clubbox 服务开放端口 |

表 1　2007 年上半年 TCP 协议流量端口排名前十位

UDP 协议中当前最占用带宽的是 Windows 信使服务使用的 1026 和 1027 端口，此端口常被滥用发送垃圾信息。此外，P2P 下载软件迅雷和 eMule 占用较多带宽。使用 UDP 协议的 DNS 服务，也占有较大流量，为 1.06%。为了防止黑客利用动态域名等服务来操控僵尸网络，躲避追踪和处置，需要进一步加强对 DNS 服务的监测。

UDP 协议流量端口前十位如图 6 所示。

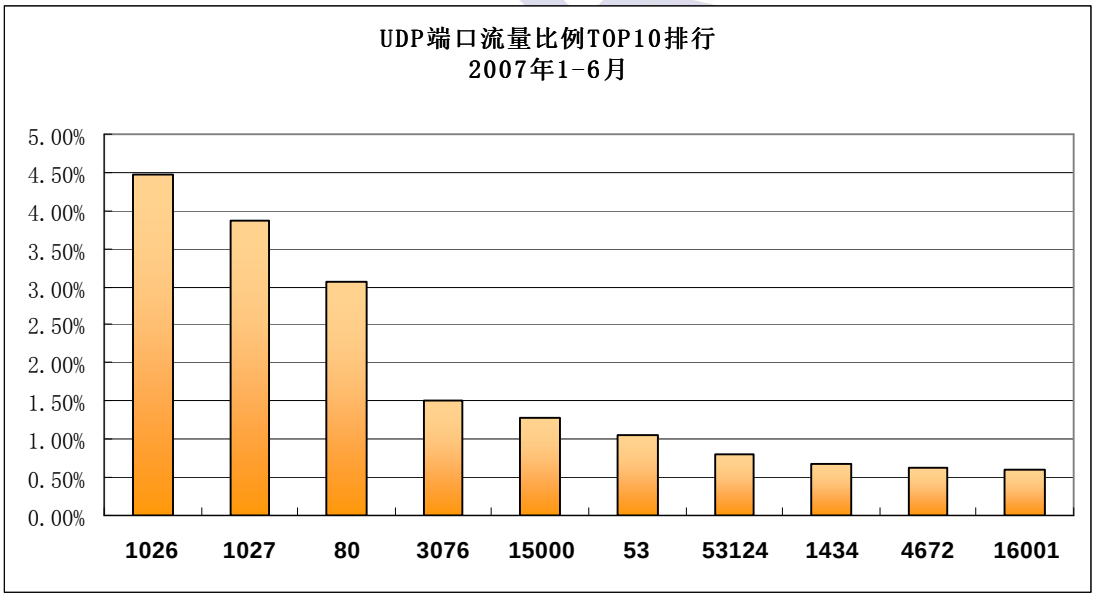



图 6　2007 年上半年 UDP 协议流量端口排名前十位

| UDP 端口 | UDP 流量排名 | 百分比 | 主要的业务种类 |
|---|---|---|---|
| 1026 | 1 | 4% | MS Messenger 端口 |
| 1027 | 2 | 3.87% | MS Messenger 端口 |
| 80 | 3 | 3.06% | 网页服务 |
| 3076 | 4 | 1.50% | 迅雷下载工具默认端口 |
| 15000 | 5 | 1.27% | P2P 下载软件端口 |
| 53 | 6 | 1.06% | DNS 服务端口 |
| 53124 | 7 | 0.81% | 未知 |
| 1434 | 8 | 0.68% | MSSQL 服务端口 |
| 4672 | 9 | 0.63% | eMule 下载工具默认端口 |
| 16001 | 10 | 0.60% | P2P 下载软件端口 |

表 2　2007 年上半年 UDP 协议流量端口排名前十位

# 6　木马与僵尸网络监测分析

木马是一种由攻击者秘密安装在受害者计算机上的窃听及控制程序。计算机一旦被植入木马，其重要文件和信息不仅会被窃取，用户的一切操作行为也都会被密切监视，而且还会被攻击者远程操控实施对周围其他计算机的攻击。木马不仅是一般黑客的常用手段，更是网上情报刺探活动中的主要手段之一。

僵尸网络是指由黑客通过控制服务器间接并集中控制的僵尸程序感染计算机群。僵尸程序一般是由攻击者专门编写的类似木马的控制程序，通过网络病毒等多种方式传播出去。由于受控计算机数目很大，攻击者可利用僵尸网络实施信息窃取、垃圾邮件、网络仿冒、拒绝服务攻击等各种恶意活动，成为当前互联网安全的最大威胁。

比较来看，木马和僵尸网络虽然在控制方式和攻击的针对性、灵活性以及规模上有所区别，但是两者都是非常有效的远程监听和控制手段，尤其是在失窃密方面对国家安全造成了严重危害，因此 CNCERT/CC 对此两类事件进行了重点监测。

## 6.1 木马数据分析

木马特指计算机后门程序，它通常包含控制端和被控制端两部分。被控制端植入受害者计算机，而黑客利用控制端进入受害者的计算机，控制其计算机资源，盗取其个人信息和各种重要数据资料。CNCERT/CC 在 2007 年上半年抽样监测，境内外控制者利用木马控制端对主机进行控制的事件中，木马控制端 IP 地址总数为 209949 个，被控制端 IP 地址总数为 1863753 个。

### 6.1.1 中国大陆地区被木马控制的计算机分布统计

2007年上半年，CNCERT/CC 对常见的木马程序活动状况进行了抽样监测，发现我国大陆地区1000372个IP 地址的主机被植入木马，与去年全年（44717个IP地址）相比有很大增长。我国大陆地区木马活动分布情况如图 7所示，木马被控制端最多的地区分别为上海（17%）、北京(12%)、江苏（9%）、广东（8%）和山东（8%）。

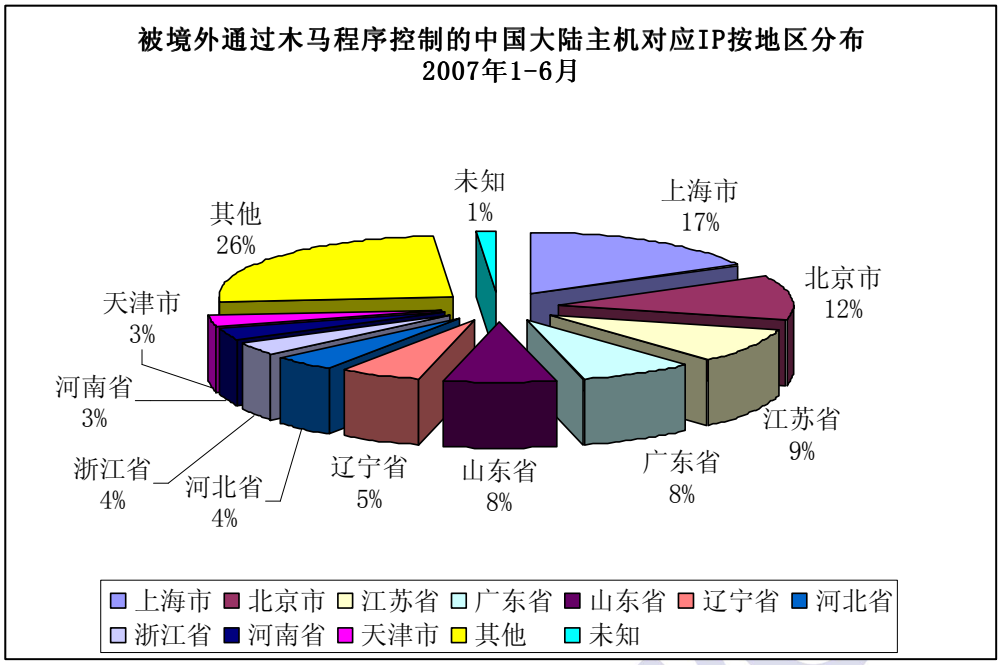
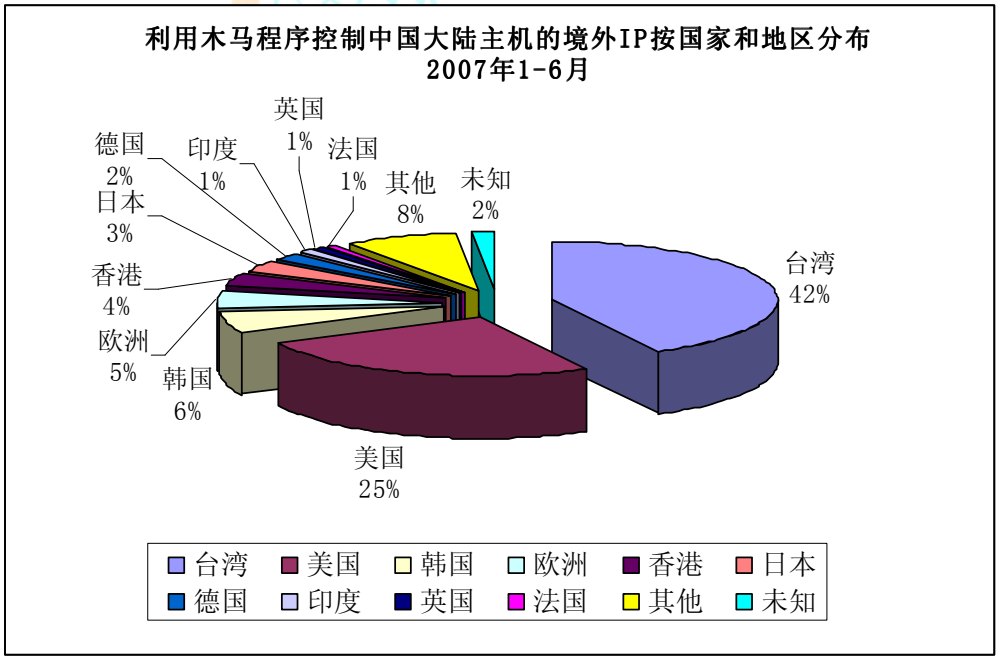



图 7　2007 年上半年中国大陆地区被木马控制的计算机 IP 分布图

### 6.1.2 中国大陆地区外木马控制端分布统计

CNCERT/CC同时发现大陆地区外77703个主机地址参与控制我国大陆被植入木马的计算机，控制端IP按国家和地区分布如图 8所示，其中位于中国台湾（42%）、美国（25%）、韩国（6%）、欧洲（5%）和中国香港(4%）的木马控制端数量居前五位。




注：“欧洲”中具体国家未知。

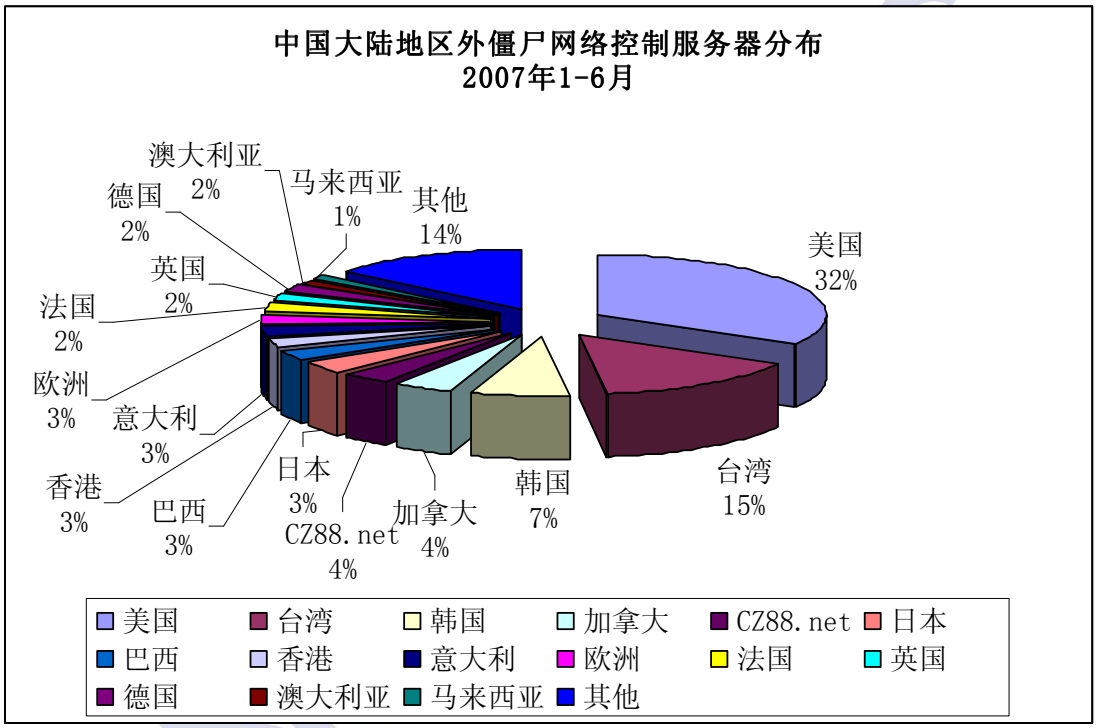
图 8　2007 年上半年通过木马控制我国计算机的境外 IP 分布图

## 6.2 僵尸网络数据分析

CNCERT/CC 每天密切关注着新出现的僵尸网络并跟踪过去出现的大规模僵尸网络，2007 年上半年抽样监测发现我国大陆约有 3 百多万个 IP 地址的主机被植入僵尸程序。

### 6.2.1 僵尸网络控制服务器分布

2007 年上半年，CNCERT/CC 共发现 8361 个境外控制服务器对我国大陆地区的主机进行控制，按国家和地区的分布如图 9 所示，其中位于美国的占 32%、中国台湾占 15%、韩国占 7%。




注：“欧洲”中具体国家未知。

图 9 2007 年上半年中国大陆地区外僵尸网络控制服务器分布图

### 6.2.2 僵尸网络控制服务器使用端口分布

僵尸网络控制端口是指感染僵尸程序的计算机所连接的控制服务器的端口。2007 年上半年，CNCERT/CC 的 Matrix 蜜网系统发现并跟踪的僵尸网络中，基于 IRC 协议的僵尸网络所用控制端口的分布情况如图 10 所示。其中，端口 6667、1863 和 8080 等是僵尸网络最常用的控制端口。

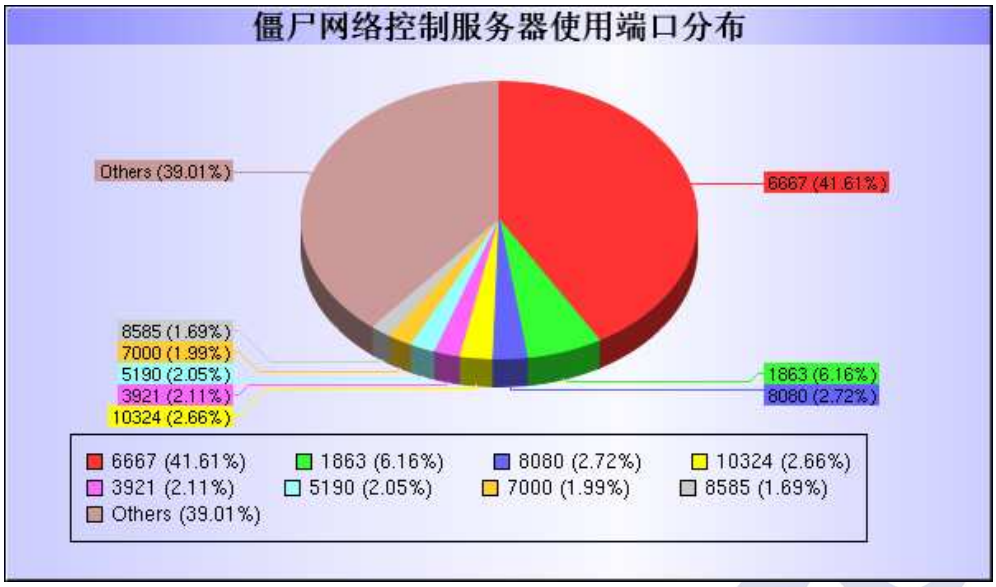



图 10　2007 年上半年僵尸网络控制服务器使用端口分布图

### 6.2.3 僵尸网络规模分布

僵尸网络的规模总体上趋于小型化、局部化和专业化。1千以内规模的僵尸网络居多。2007年上半年监测到僵尸网络各种规模数量如图 11所示。

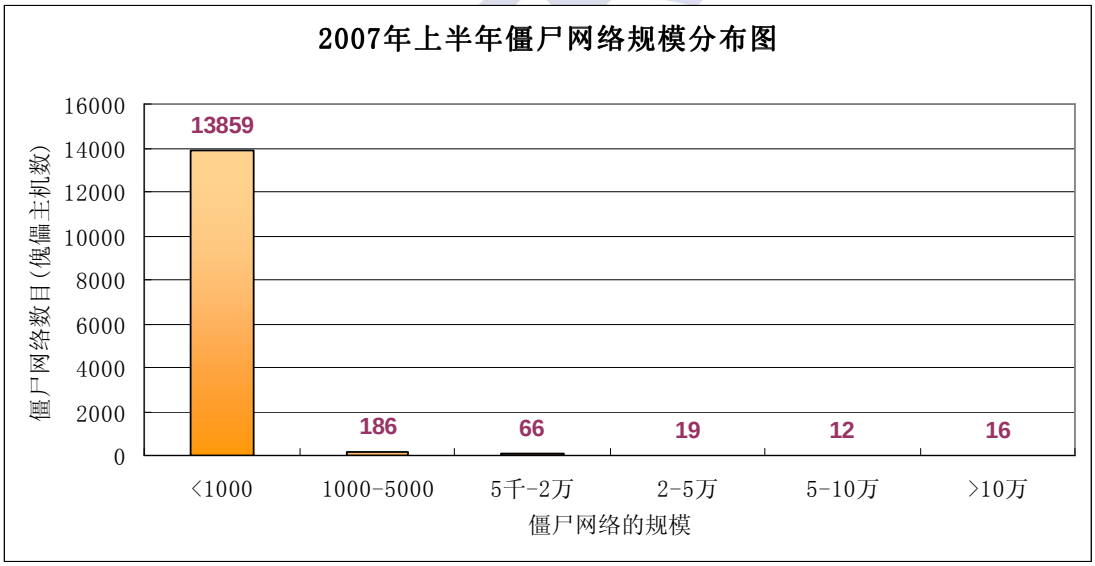



图 11　2007 年上半年僵尸网络规模分布图

# 7 被篡改网站监测分析

从 2003 年 CNCERT/CC 便开始监测我国大陆网站被篡改情况。通过包括自主监测在内的各种手段，每日对中国大陆地区网站被篡改情况进行跟踪监测，在发现被篡改网站后及时通知网站所在省份的分中心协助解决，力保被篡改网站快速恢复。

## 7.1 我国网站被篡改情况

2007 年上半年，中国大陆被篡改网站的数量相比往年处于明显上升趋势。CNCERT/CC 监测到中国大陆被篡改网站总数达到 28367 个，比去年全年增加了近 16%。按月统计情况如图 12 所示。

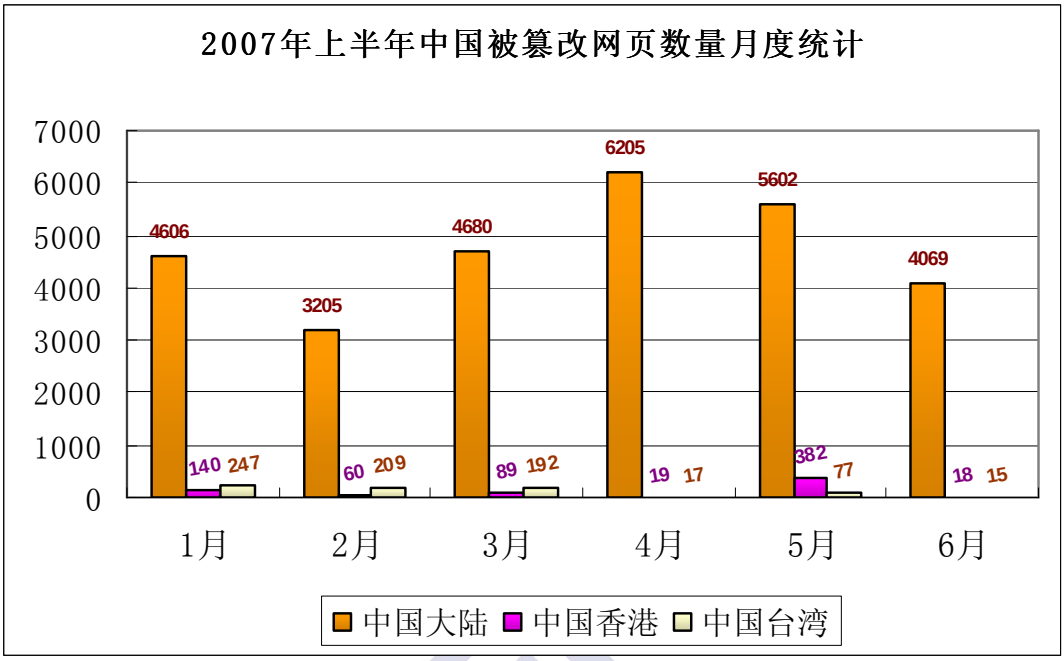



图 12　2007 年上半年被篡改网站数量统计

## 7.2 我国大陆地区政府网站被篡改情况

2007 年 1 月至 6 月期间，中国大陆政府网站被篡改数量基本保持平稳，各月累计达 1585 个。与去年监测情况相比，该数量在中国大陆被篡改的网站总数中所占比例有所下降。上半年中国大陆被篡改的网站中政府网站所占比例月度统计如图 13 所示。从中可以看出，每月被篡改的 gov.cn 域名网站占整个大陆地区被篡改网站的 6%左右。与我国.cn 域名下的政府网站所占的 1.9％比例[1]相比，.gov.cn 网站遭受黑客攻击的比例相对较高，其安全性亟待提高。

[1]注：该数据来自中国互联网络信息中心（CNNIC）2007 年 7 月第 20 次《中国互联网络发展状况统计报告》。

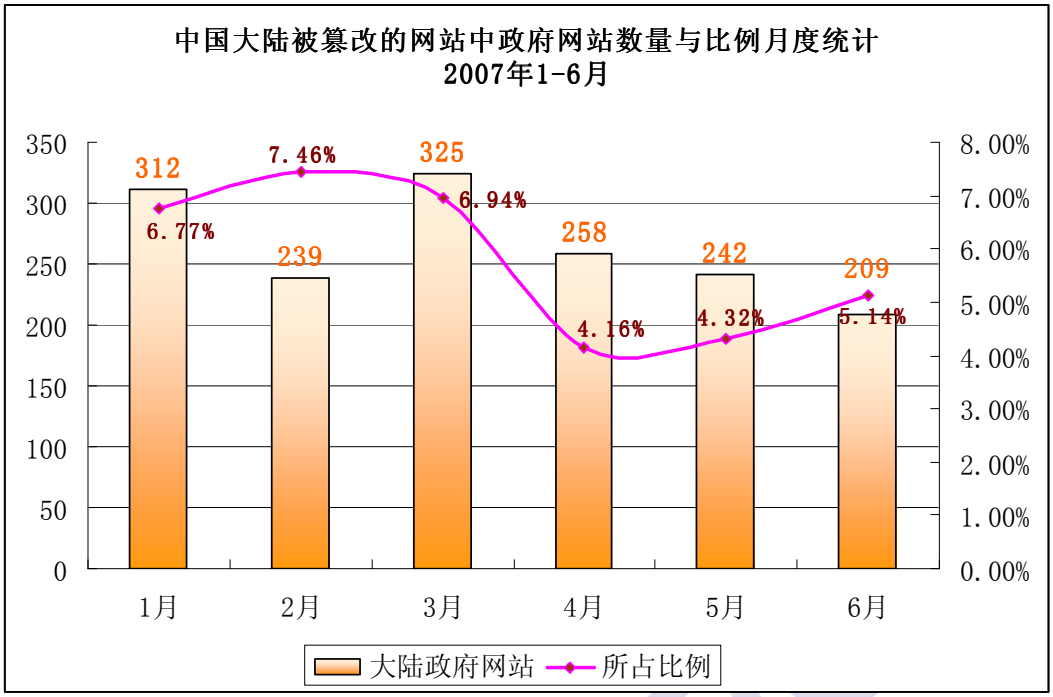



图 13　2007 年上半年中国大陆被篡改的网站中政府网站所占比例月度统计

政府网站易被篡改的主要原因是网站整体安全性差，缺乏必要的经常性维护，某些政府网站被篡改后长期无人过问，还有些网站虽然在接到报告后能够恢复，但并没有根除安全隐患，从而遭到多次篡改。

# 8　网络仿冒事件情况分析

2007 年上半年 CNCERT/CC 共接到网络仿冒事件报告 645 件，具体成功处理了 222 件。被仿冒的网站大都是国外的著名金融交易机构和安全公司。表 3 列出了向 CNCERT/CC 报告网络仿冒事件数量居前 5 名的组织机构。

| 网络仿冒事件报告者 | 数量 |
|---|---|
| VeriSign(美国网络安全公司) | 138 |
| eBay(美国网上交易站点) | 73 |
| RSA Cyota(美国网络安全公司) | 71 |
| Castlecops(美国网络安全机构) | 55 |
| Mark Mornitor(美国网络安全公司) | 44 |

表 3　向 CNCERT/CC 报告网络仿冒事件前 5 名统计

# 9 恶意代码捕获及分析情况

恶意代码是对人为编写制造的计算机攻击程序的总称，包括计算机病毒、网络蠕虫、木马程序、僵尸网络、网页恶意脚本、间谍软件等。通过对恶意代码的捕获和分析，可以评估互联网及信息系统所面临的安全威胁情况，以及掌握黑客的最新攻击手段，通过研究可以对真实应用系统的防护提供建议。

利用专门构造的、可控的、具有多种安全漏洞的网络“陷阱”主机，即“蜜罐”，监测其被扫描、攻击和攻陷的过程，以便掌握各种攻击活动。由于与生产网络隔绝并有保护措施，因此闯入蜜罐的入侵者无法借助蜜罐攻击其他外部系统。蜜网，又称诱捕网络，是蜜罐技术的进一步发展，它构成了一个黑客诱捕网络体系架构，可以包含一个或多个蜜罐，同时保证网络的高度可控性，提供多种工具对攻击信息进行采集和分析。

为了加强对恶意代码的监测处理能力，CNCERT/CC 于 2006 年陆续在我国 15 个省市部署了 Matrix 蜜网系统。通过对 Matrix 系统捕获的恶意代码样本分析，可以掌握目前我国互联网上主动式恶意代码的传播和利用情况。

2007 年 1 月到 6 月，每日平均捕获样本 3041 次，图 14 给出了每日的样本捕获趋势。

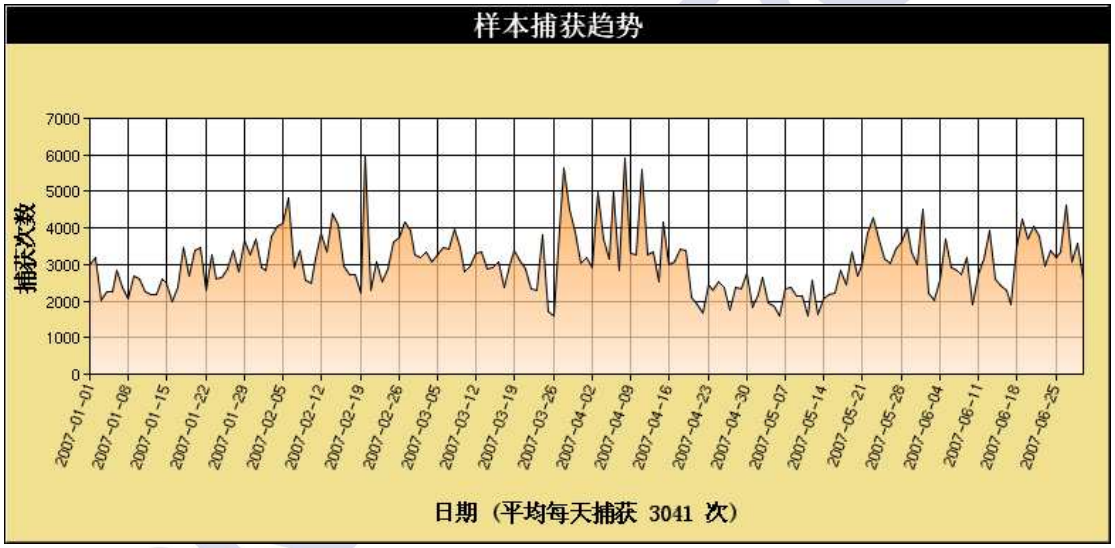



图 14　分布式蜜网样本捕获趋势图

由于蜜网是被动式监测，因此一个恶意代码通常会捕捉到多次。以下是根据每日捕获的不重复的新样本数目绘制的捕获趋势图，据图可见分布式蜜网平均每天捕获恶意代码新样本为 442 个。新的恶意代码层出不穷也是安全形势日益严峻的主要原因之一。

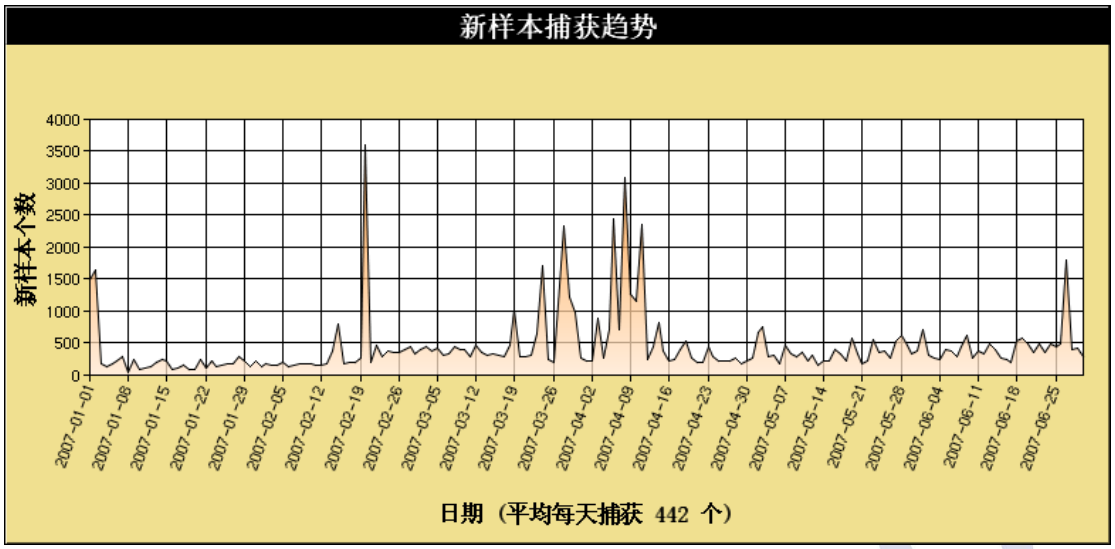



图 15　分布式蜜网新样本捕获趋势图

2007 年 1 月 1 日至 6 月 30 日期间，蜜网共捕获 550421 个恶意代码样本，位于前十位的恶意代码如表 4 所示：

| 排名 | 恶意代码名称 | 总捕获次数 |
|---|---|---|
| 1 | Backdoor.Win32.PoeBot.c | 62203 |
| 2 | Backdoor.Win32.VanBot.ax | 61622 |
| 3 | Net-Worm.Win32.Allaple.b | 42755 |
| 4 | Virus.Win32.Virut.b | 30964 |
| 5 | Backdoor.Win32.SdBot.aad | 17958 |
| 6 | Backdoor.Win32.SdBot.xd | 16156 |
| 7 | Backdoor.Win32.Rbot.gen | 15030 |
| 8 | Virus.Win32.Virut.a | 14236 |
| 9 | Net-Worm.Win32.Allaple.e | 14070 |
| 10 | Backdoor.Win32.IRCBot.ul | 13843 |

表 4　分布式蜜网捕获次数前十名的恶意代码

以上恶意代码，主要利用微软系统的漏洞进行传播，并在感染的机器上留下后门程序，通过 IRC、HTTP 等协议进行远程控制形成僵尸网络。黑客利用僵尸网络能够窃取被感染主机的系统信息，并控制被感染的机器发起新的扫描、DDoS 攻击、发送垃圾邮件或进行远程控制和网络欺诈活动。如：PoeBot（派波）、VanBot、SDBot、Rbot（瑞波）等僵尸程序均具有较高的危害性。

# 10 CNCERT/CC 网站信息发布

CNCERT/CC 网站是 CNCERT/CC 对外公开提供网络安全信息服务的重要窗口。2007 年 1 月至 6 月，CNCERT/CC 通过网站发布了 216 条消息，其中包括安全公告、安全漏洞、病毒预报、安全新闻、安全建议、统计报告等，各类消息具体发布情况见图 16。CNCERT/CC 网站已成为国内外安全组织和网站参考或转载权威信息的重要来源。

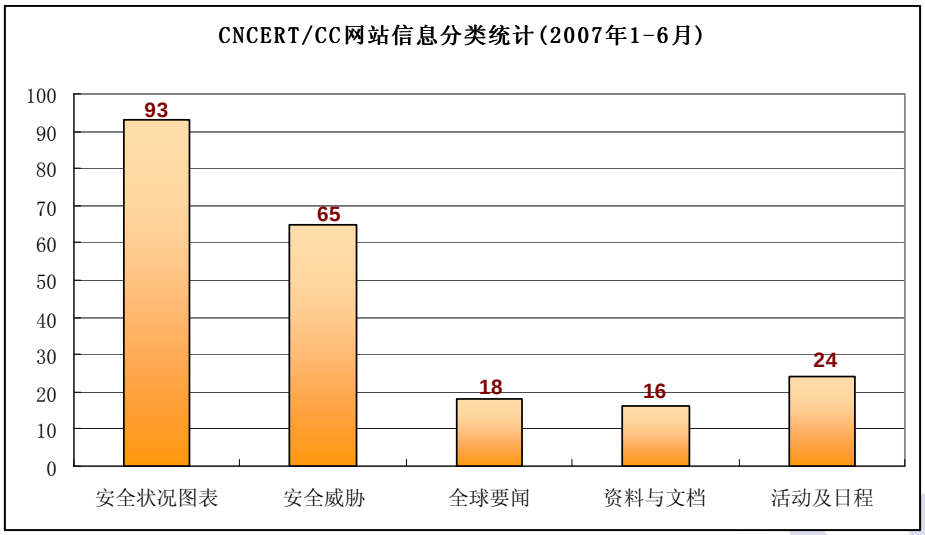



图 16　2007 年上半年 CNCERT/CC 网站信息分类统计

# 11 网络安全应急组织发展情况

## 11.1　国内应急组织发展情况

针对错综复杂的网络安全问题，为保障互联网和重要信息系统的正常运作，有效防范和应对各类网络安全事件，提高网络安全防护能力，我国通过建设专业化的网络安全应急组织，构建完善的网络应急体系，建立了快速高效的网络安全事件应急处理机制。中国教育和科研计算机网紧急响应组（CCERT）是我国最早的应急组织，成立于 1999 年，是依托于中国教育和科研计算机网的一个非盈利、非政府的民间组织。国家支持的国家计算网络应急技术协调中心（CNCERT/CC）成立后，标志着应急组织的作用得到了国家层面的重视和支持。此后，我国应急组织得到了迅速发展，初步形成了以 CNCERT/CC 为核心，各分中心为延伸、以骨干网络运营单位应急组织为主体、以有社会安全防范机构、公司为支撑、以大学、科研院所为后援的应急体系。

为团结国内所有应急组织，发挥各自优势，共同保障国内互联网的安全， 2005 年 3 月，CNCERT/CC 和中国互联网协会计算机网络与信息安全工作委员会共同发起成立了中国 CERT 社区（http://community.cert.org.cn）。目的是通过网上社区，收集汇总来自不同行业、不同地区的 CERT 组织的基本信息和联络方式，形成中国 CERT 组织的门户网站。

据不完全统计，截止 2007 年 7 月，我国目前有应急组织 57 家，见表 5 所示[2]。其中，在中国应急组织社区登记的应急组织共计 30 家。

| 网络安全应急组织中文名称 | 名称简写 |
|---|---|
| 上海三零卫士信息安全有限公司* | 30Wish |
| 西安安智科技有限公司* | ANGELLTECH |
| 哈尔滨安天信息技术有限责任公司* | Antiy Labs |

[2]注：该表内容主要来自 CNCERT 和 CCERT 网站，带“*”号的表示该应急组织已在中国 CERT 社区登记，其他组织以 CCERT 网站（http://www.ccert.edu.cn/）发布的成员单位为准。

| | |
|---|---|
| 北京冠群金辰软件有限公司* | CA-Jinchen |
| 成都微软技术中心* | CDMTC |
| 中国移动网络与信息安全应急小组* | CMCERT/CC |
| 国家计算机网络应急技术处理协调中心* | CNCERT/CC |
| 深圳市安络科技有限公司* | CNNS |
| 中国科技网网络安全应急小组* | CSTCERT |
| 中国联通天津分公司* | CUCC-TJ |
| 山东中创软件商用中间件有限公司* | CVICSE |
| 河南山谷创新网络科技有限公司* | Chinavvv |
| 福建富士通信息软件有限公司* | FFCS |
| 广西大学信息网络中心* | GXUNC |
| 贵阳华旺科技有限公司* | GYHW |
| 合肥工业大学网络安全与紧急响应组* | HFUTCERT |
| 北京万网新兴网络技术有限公司* | HiChina |
| 北京江民新科技术有限公司* | JIANGMIN |
| 北京安氏领信科技发展有限公司* | LinkTrust |
| 国家计算机网络入侵防范中心* | NCNIPC |
| 东软计算机安全事件应急小组* | NCSIRT |
| 中联绿盟信息技术(北京)有限公司* | NSFOCUS |
| 山东科技大学中国核心网络安全小组* | SDUST-CKNSG |
| 山东新潮信息技术有限公司* | SDXC |
| 神州通信有限公司* | SNZO |
| 华为电信网络与业务安全实验室* | TNSSL |
| 连云港港湾科技有限公司技术支持中心* | TSC-HT |
| 天融信安全运营中心* | TopSec SOC |
| 启明星辰应急响应小组* | VCERT |
| 中国教育和科研计算机网紧急响应组* | CCERT |
| CERNET 华东（北）地区应急响应组 | NJCERT |
| 北京大学网络安全紧急响应组 | PKUCERT |
| 成都电子机械高等专科学校 | |
| 新疆大学校园网应急响应组 | |
| CERNET 山西省主节点应急响应组 | SXCERT |
| 攀枝花学院病毒应急响应处理小组 | |
| CERNET 河北省主节点响应组 | |
| 华北地区北邮主节点应急响应组 | BUPTCERT |
| CERNET 西南地区应急响应组 | CDCERT |
| 广州华南理工大学网络中心 | GZCERT |
| 河南教育科研计算机网应急响应小组 | |
| 湖南主节点及中南大学应急响应小组 | |
| CERNET 华中地区应急响应组 | |
| 江西省节点应急响应组 | JXCERT |
| 四川轻化工学院网管中心 | |
| 吉林大学网络中心应急响应组 | |

| | |
|---|---|
| 川北医学院 | |
| CERNET 贵州主节点 | |
| 山西财经大学网络中心 | |
| 宁夏大学网络中心 | |
| 青海师范大学网络中心 | QH-CCERT |
| CERNET 华南地区紧急响应组 | GZCERT |
| 大连理工大学校园网紧急响应组 | DLCERT |
| 上海交通大学计算机紧急响应组 | SJTUCERT |
| CERNET 山东网络中心紧急响应组 | SDCERT |
| 东北农业大学校园网安全响应组 | NEAUCERT |
| 复旦大学校园网紧急响应组 | FDU-CERT |

表 5　我国网络安全应急组织名称

## 11.2 CNCERT/CC 组织的相关重要活动

**CNCERT/CC 举办分布式拒绝服务攻击(DDoS)事件专题研讨会**

自 2006 年 12 月份以来，利用分布式拒绝服务(以下简称 DDoS)攻击的网络敲诈活动愈演愈烈，对正常的网络应用、服务和经济活动造成了严重影响，也随时会威胁到基础网络和重要信息系统的正常运行，引起了社会各界的强烈关注。2007 年 1 月 12 日 CNCERT/CC 和中国互联网协会网络安全工作委员会在北京召开了 DDoS 事件专题研讨会，邀请了来自政府、协会、学术、业界和用户等各方专家代表共近 50 名，以推动公共互联网的和谐发展，为电子商务等新网络经济提供良好的网络发展环境。

会议通过报告和研讨的形式进行了充分交流，会议内容归纳起来主要集中在以下四个方面：

一、拒绝服务攻击已经形成产业链，且对我国互联网行业及依靠互联网的应用行业造成了巨大危害

自 2006 年 12 月份以来，针对一些中小型互联网企业，包括 DNS 服务器和域名转发服务器的攻击数量明显增多，攻击流量也明显增大，超过 1G 的攻击流量频频出现，CNCERT/CC 掌握的数据表明，最高时攻击流量达到了 12G。

目前的互联网黑色产业链“互联网地下经济”已经颇具规模，形成了较完整的价值链，而且，黑客实施攻击的犯罪成本非常低，攻击工具可以在网上以非常低的成本获得，大大降低了攻击者实施攻击的技术门槛，相反的是，处理 DDoS 攻击、追踪攻击的代价却很高。由于网络的互联性和无边界性，溯源的过程涉及到的技术、管理、法律、执法等多方问题目前都不能妥善解决，使得溯源难度极大，其成本也远远大于攻击成本。

DDoS 攻击带来的威胁已经越来越大。除严重影响以至中断用户的应用外，据用户反映，在医药行业和游戏行业利用 DDoS 的相互攻击现象已经非常普遍，甚至形成了只有交“保护费”才能免遭攻击的局面，这大大提高了企业运营的门槛，对新经济发展造成严重的阻碍。目前，华东华南地区已有越来越多年产值达数千万的中小企业走上信息化道路，依靠网络开展业务，由于缺乏积极有效的方法应对 DDoS 攻击，使得攻击发生后的影响范围也不断扩大，不仅影响网络托管服务商，而且网络运营商的骨干链路流量也开始受到影响，如果任其发展，势必严重危害到互联互通的问题。

由于黑客并不对政府、涉及国计民生的网站及单位进行 DDoS 攻击，而是选择中小企业，或者利用某些行业的混乱局面进行讹诈，而这些行业尤其是中小企业，在遭受 DDoS 攻击后，

依靠自身力量通常难以防范，因此，用户希望政府采取积极有效措施维护并保障互联网安全，维护健康有序的互联网商业环境，保障互联网行业及其应用的正常发展。

二、应对拒绝服务攻击的防护技术手段欠缺，有待研发新产品，建设针对性技术手段

目前的网络产品及安全产品，只能解决终端用户上恶意攻击流量的部分问题，这是远远不够的。要想有效应对 DDoS 攻击问题，就必须不仅仅是从终端到网络，还包括从技术到管理，从被动到主动，解决多方面的问题。

此外，参会专家认为，从技术角度，针对伪造攻击 IP 地址，厂商应在开发产品中尝试些新的方法，例如，不保存连接信息来避免资源滥用；而对真 IP 地址，由于追溯成本非常高，可以考虑建立一种成本相对较低的手段，这需要运营商积极发挥应有作用，而不是简单的将用户网站路由设为“黑洞路由”，使恶意流量无法访问；针对攻击源头，则可以通过研究蜜网技术发现攻击者，以及分析网上广泛散播的攻击工具特征来识别特定攻击并实现有针对性的防护。

三、社会各界需要加大应对拒绝服务攻击的协调力度

防范拒绝服务攻击，除预先采取防护性技术措施外，应急处置环节也非常重要。国家公共应急体系，应是分层次的，高层是由政府部门主导，实现对基础信息网络和重要信息系统的保护和安全事件应急处理，而低层主要保障公民和法人的切身利益，由于直接关系到广大网民的利益，必须充分调动社会力量才能共同完成。

CNCERT/CC 作为国家级的网络应急处理协调中心，关注和处理的重点只能是国家层面的，面对广泛的针对中小企业的攻击，目前，在人力资源和技术资源上投入有限，必须发挥各个方面的作用，形成有效的应急协调机制，其中，政府、运营商、应急组织、用户、厂商等都应发挥相应作用。因此，CNCERT/CC 将积极发挥自身的协调作用，并把对此类网络安全事件的处理能力通过各方力量有效的辐射出去，是 CNCERT/CC 今后工作的一个重要方面。

四、政府部门应加强管理，执法部门进行专项执法打击

与会专家、代表建议，从政府政策角度，应对 DDoS 的措施包括继续推动源路由认证措施，实现源路由过滤；在公共互联网范围内制定并推广 DDoS 处理规范，界定运营商、应急组织、用户等环节的角色和定位。此外，应当加大对攻击者的打击力度。刑法 285 条为打击对国家政府网站的攻击提供了有效依据，执法部门可以通过严办几起典型案例，来清理整顿目前的公共互联网环境。

通过本次研讨会，使得各界专家和代表加深了对拒绝服务攻击现状及危害的认识，了解到技术、管理、应急等方面的应对措施和方法，更认识到应对拒绝服务攻击必须各方联合，共同采取措施，才能有效的应对拒绝服务攻击。

**2007 中国计算机网络安全应急年会暨中国互联网协会网络安全工作年会在无锡顺利召开**

由国家计算机网络应急技术处理协调中心（以下简称 CNCERT/CC）主办的 2007 中国计算机网络安全应急年会暨中国互联网协会网络安全工作年会于 2007 年 4 月 5 日至 7 日在江苏无锡顺利召开。本次会议得到了国务院信息化工作办公室、信息产业部、国家网络与信息安全信息通报中心、第 29 届奥林匹克运动会组织委员会以及国内外相关单位的大力支持，共有来自于相关部委、重要信息系统部门、CNCERT/CC 各省分中心、我国互联网运营商应急小组、科研院所、国内安全企业、新闻媒体代表约 200 人出席了本次会议。

本次会议的主题是“服务信息社会，共建和谐网络”。 与会的各界领导、业内专家和学者围绕这一主题，从电子政务安全、奥运安全、网上金融安全、公共互联网安全等四个方面展开了广泛的交流与探讨，对推动我国网络安全工作的发展和公共互联网应急体系的建设起到了积极的作用。

考虑到2008年奥运会即将在北京召开，CNCERT/CC特别邀请到2000悉尼奥运会、2004雅典奥运会和2006都灵冬奥会网络安全保障工作的参与者做了报告，并与北京奥组委技术部的领导和专家就奥运安全保障工作进行了交流探讨。本次会议对北京奥组委做好08奥运会的网络安全工作提供了非常有意义的参考，进一步加强了对 CNCERT/CC 在重大时期对重要信息系统提供安全保障能力的认识，对推动双方的深入合作起到了积极作用。

会议期间，还召开了中国互联网协会网络安全工作第三次年会，20 多名委员参加了会议，共同总结了06年的工作成果，并提出了07年的工作计划。

连续第四届举办的中国计算机网络安全应急年会，不仅吸引了高质量的参会者，而且吸引了有关媒体的关注。包括中央电视台新闻频道在内的近十家业界知名媒体参访了本次会议，他们通过大众媒体、专业网站及杂志对年会进行了报道和肯定，对提高整个社会和广大用户的网络安全意识起到了积极的意义。

**CNCERT/CC 成功举办应急服务支撑单位改选评审会**

为拓宽国家计算机网络应急技术处理协调中心（简称CNCERT/CC）掌握宏观网络安全状况和网络安全事件的信息渠道，增强 CNCERT/CC 对互联网重大、突发性事件的处理能力，强化以 CNCERT/CC 为核心的应急技术处理支撑体系建设，促进面向公共互联网应急处理服务的规范化和本地化，CNCERT/CC 于2007年初启动了“第二届CNCERT/CC应急服务支撑单位改选”工作。

2007年6月21日至22日，“国家计算机网络应急技术处理协调中心应急服务支撑单位改选评审会”在吉林省延吉市成功举办，标志着CNERT/CC应急服务支撑单位改选工作圆满结束。本次评审会得到了国务院主管部门、信息产业部、电信运营商和重要信息系统单位的大力支持和帮助。来自国信办、信产部电信管理局、中国网通、中国移动、中国联通、国家电网和 CNCERT/CC 的相关领导专家组成了评审委员会。评审专家从运营状况、服务规范和服务能力等方面出发，结合 CNCERT/CC 应急服务支撑工作需要，对参选企业进行了科学严谨的评估和审核。

经过历时近两天的企业答辩和专家评审，共评选出了8家“CNCERT/CC国家级应急服务支撑单位”和26家“CNCERT/CC省级应急服务支撑单位”，为进一步提高我国公共互联网应急处理能力、构建和谐网络提供了技术和资源保障。

2004年CNCERT/CC首次面向社会公开选拔了一批国家级、省级公共互联网应急服务试点单位，三年来的试点实践证明：应急服务支撑单位已成为我国公共互联网应急体系的重要组成部分，本次应急服务支撑单位改选是应急服务试点工作的继承和发展。“CNCERT/CC应急服务支撑单位改选评审会”的成功举办，标志着作为国家网络安全应急保障体系重要组成部分的 CNCERT/CC 应急服务支撑体系获得了政府、业界的认可，同时也是对广大信息安全服务企业实力的一次集中检阅，对促进网络应急服务行业的规范化、市场化，推动我国公共互联网应急服务事业的发展具有积极意义。

**国家级应急服务支撑单位:**

北京启明星辰信息技术有限公司
沈阳东软软件股份有限公司
北京神州绿盟科技有限公司
北京天融信科技有限公司
北京瑞星科技股份有限公司
浪潮集团有限公司

北京安氏领信科技发展有限公司
上海中科网威信息技术有限公司

**省级应急服务支撑单位:**

福建富士通信息软件有限公司
甘肃万维信息技术有限责任公司
深圳任子行网络技术有限公司
北京启明星辰信息技术有限公司深圳分公司
广东科达信息技术有限公司
河南山谷创新网络科技有限公司
哈尔滨安天信息技术有限公司
武汉虹旭信息技术有限责任公司
北京启明星辰信息技术有限公司沈阳分公司
山东新潮信息技术有限公司
太原理工天成科技股份有限公司
西安安智科技有限公司
上海三零卫士信息安全有限公司
上海谐润网络信息技术有限公司
成都思维世纪科技有限责任公司
四川电信有限公司
杭州思福迪信息技术有限公司
武汉大学
贵州华信众联科技发展有限公司
贵州华旺科技有限公司
江苏南大苏福特软件股份有限公司
南京联创网络科技有限公司
北京江南博仁科技有限公司
北京江民新科技术有限公司
北京万网志成科技股份有限公司
世纪互联数据中心有限公司

# 12 国际合作与交流

**APCERT2007 年会在马来西亚召开 CNCERT/CC 续任 APCERT 副主席**

2007 年 2 月 7 日至 9 日，APCERT 2007 年度工作会议在马来西亚召开。CNCERT/CC 参加了本次大会，并在换届选举中，连任 APCERT 副主席。会议主要进行了指导委员会、主席、副主席、秘书处的换届选举；回顾了 APCERT 各经济体成员在 2006 年的工作开展情况；并同其它业界公司和有关组织开展了技术交流；讨论制定了下一步工作开展计划。

经换届改选后的新一届 APCERT 指导委员会主席为 MyCERT （马来西亚）、副主席为 CNCERT/CC、秘书处为 JPCERT/CC（日本）。同时，AusCERT（澳大利亚）、JPCERT/CC、MyCERT 在新一届 APCERT 指导委员会委员改选中当选。

会议讨论了目前的主要网络安全形势和问题。垃圾邮件、网络钓鱼、DDoS 攻击、网页篡改/恶意网页等事件最为频繁；僵尸网络是攻击者开展上述大多数恶意活动的利器，因此有效对抗僵尸网络是解决上述安全问题的关键；网页篡改/恶意网页则是攻击者散播恶意代码的一个重要途径，检测并清除恶意网页对于阻断攻击的途径十分必要。网络攻击显示出更强的针对性和目的性，社会工程学日益被广泛利用，但防护者对漏洞信息及其它相关数据却缺乏有效管理和安全共享机制。会议同时探讨了相关技术手段建设情况，包括僵尸网络追踪技术、恶意网页发现技术、漏洞评估技术，以便为今后有效应对上述问题提供必要支撑能力。

大会决定继续推进经济体应急联络点（POC）工作机制，确保重点紧急事件的顺利处理；并确定了 APCERT 今年的工作重点，包括开展数据共享、应急演练和培训工作，不断加强成员之间以及 APCERT 组织与其它国际组织机构的有效协作。本次会议将进一步推进亚太地区的网络安全应急处理工作的顺利开展。

# 13 结束语

虽然 2007 年上半年整体安全态势平稳，但各类安全事件数量较之以往均有明显增幅。随着网络用户和网络资源的大量增加，以及各种系统漏洞的大量存在和不断发现，使得网络安全问题变得更加错综复杂。加之网络攻击行为日趋复杂，各种方法相互融合，使得网络安全防御更加困难。

根据 2007 年上半年的监测与分析，预计 2007 年下半年发生大规模网络安全事件的可能性比较小。Windows Vista 系统的日益推广将减少利用微软操作系统漏洞进行蠕虫传播的可能性。然而针对 Web 浏览器和网络应用的漏洞，尤其是 P2P 下载软件、即时聊天工具等新型网络应用的安全攻击将会增多。以敲诈勒索、僵尸网络、间谍软件为代表的恶意代码，以及网络仿冒、网址嫁接、网络劫持等在线身份窃取类安全事件将会不断增加，网站被篡改事件数量递增的趋势仍将持续。总之，以获利为主要目的的攻击行为将长期存在，小规模的僵尸网络将成为主流攻击手段持续发展，这些问题会导致网络安全事件数量整体呈上升趋势。

网络安全问题的影响不断扩大，且很难在短期内得到全面解决。对重要信息系统，除应加大网络安全投入外，应重视网络安全应急组织建设，以更好的防范网络安全事件，规范有效地应对网络安全事件，提高用户网络安全意识，保障重要信息系统的正常安全运行。对于政府和中小企业而言，必须注意加强其信息系统安全建设和日常维护工作，全面提升安全防护能力，重点防范网页篡改和分布式拒绝服务 DDoS 类攻击。同时，加强网络的内部管理，避免由于内部员工上网行为的不当而造成的系统被入侵、资料泄密及网络阻塞等。对普通用户而言，需要做好对恶意软件的防护措施，及时升级杀毒软件和防火墙，开启必要功能，并及时下载、安装计算机系统的安全漏洞补丁程序，以免遭受攻击。同时，谨慎处理来路不明的网络链接和邮件附件。

作为国家基础网络安全保障重要的技术支撑部门，CNCERT/CC 将在信息产业部的领导下，继续围绕提高能力和扩大服务两大核心任务，重点提高事件监测和发现能力，加强事件分析和事件管理，积极拓展和发挥应急体系的作用，全面提高公共互联网的安全保障能力。