

# CNCERT/CC

## 2007 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



## 关于CNCERT/CC 2007年网络安全工作报告

本文档所包含的信息代表 CNCERT/CC 对截至发布日期之前所讨论问题的当前观点。

本文档仅用于提供信息之目的。CNCERT/CC 对于本文档中的信息不做任何明示、暗示或法定的担保。CNCERT/CC 无法保证发布日期之后所提供的任何信息的准确性。

本文档版权为 CNCERT/CC 所有。非商业目的情况下，转载或引用其中的有关内容，包括数据及图表，请注明出处。

遵守所有适用的版权法是用户的责任。如未获得 CNCERT/CC 明确的书面许可，不得以任何形式将本档的任何部分或全部内容用于商业目的。

编者按：

感谢您阅读“CNCERT/CC 2007 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：[cn-cert@cert.org.cn](mailto:cn-cert@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	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	11
5 互联网业务流量监测情况	13
6 木马与僵尸网络监测情况	15
6.1 木马监测情况	15
6.2 僵尸网络监测情况	16
7 被篡改网站监测情况	18
7.1 我国网站被篡改情况	19
7.2 我国政府网站被篡改情况	19
7.3 攻击我国网站的主要黑客情况	20
8 网络仿冒（网络钓鱼）情况	21
9 恶意代码捕获及分析情况	21
10 网络安全信息服务情况	23
10.1 安全信息通报	23
10.2 网站信息发布	23
11 我国网络安全应急组织发展情况	23
11.1 我国网络安全应急组织列表	23
11.2 CNCERT/CC应急服务支撑单位列表	25
12 CNCERT/CC组织的重要活动	27
13 国际合作与交流	30
14 结束语	31
15 术语解释	32

# 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](mailto: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

2007年,我国公共互联网网络整体上运行基本正常,但从CNCERT/CC接收和监测的各类网络安全事件情况可以看出,网络信息系统存在的安全漏洞和隐患层出不穷,利益驱使下的地下黑客产业继续发展,网络攻击的种类和数量成倍增长,终端用户和互联网企业是主要的受害者,基础网络和重要信息系统面临着严峻的安全威胁。2007年各种网络安全事件与2006年相比都有显著增加。CNCERT/CC接收的网络仿冒事件和网页恶意代码事件成倍增长,分别超出去年总数的近1.4倍和2.6倍,监测发现我国大陆被篡改网站数量比去年增加了1.5倍。

2007年,在地下黑色产业链的推动下,网络犯罪行为趋利性表现更加明显,追求经济利益依然是主要目标。黑客往往利用仿冒网站、伪造邮件、盗号木马、后门病毒等,并结合社会工程学,窃取大量用户数据牟取暴利,包括网游账号、网银账号和密码、网银数字证书等。木马、病毒等恶意程序的制作、传播、用户信息窃取、第三方平台销赃、洗钱等各环节的流水作业构成了完善的地下黑色产业链条,为各种网络犯罪行为带来了利益驱动,加之黑客攻击手法更具隐蔽性,使得对这些网络犯罪行为的取证、追查和打击都非常困难。

信息系统软件的安全漏洞仍然是互联网安全的关键问题,但层出不穷的应用软件安全漏洞的危害性已经与操作系统的安全漏洞平分秋色。我国普遍使用的微软操作系统的安全漏洞仍然是黑客攻击的首选目标,但近些年不断发展和广泛应用的各种应用程序(如IE浏览器、暴风影音多媒体播放器、VMware虚拟机和各种P2P下载软件)中存在的安全漏洞也被越来越多的披露出来,相关的漏洞机理、概念验证(POC)代码等可被用来开发攻击程序的信息也很容易通过公开的搜索引擎收集,甚至网上已经公开出现售卖软件漏洞的现象。因此,安全漏洞问题变得越来越复杂和严重。

据CNCERT/CC监测发现,2007年我国大陆地区被植入木马的主机IP数量增长惊人,是去年的22倍,木马已成为互联网的最大危害。地下黑色产业链的成熟,为木马的大量生产和广泛传播提供了十分便利的条件,木马在互联网上的泛滥导致大量个人隐私信息和重要数据的失窃,给个人带来严重的名誉和经济损失;此外,木马还越来越多地被用来窃取国家秘密和工作秘密,给国家和企业带来无法估量的损失,我国大陆被植入木马计算机的控制源中,大多数位于我国台湾地区,这一现象已经引起有关部门的关注。

僵尸网络仍然是网络攻击的基本手段和资源平台。2007年CNCERT/CC抽样监测发现感染僵尸程序的境内外主机数达623万个,其中我国大陆有362万个IP地址的主机被植入僵尸程序,并有1万多个境外控制服务器对我国大陆地区的主机进行控制。僵尸网络主要被利用发起拒绝服务(DDoS)攻击、发送垃圾邮件、传播恶意代码,以及窃取受感染主机中的敏感信息,而由僵尸网络发出的大流量、分布式DDOS攻击是目前公认的世界难题,不仅严重影响互联网企业的运作,而且严重威胁着我国互联网基础设施的运行安全。

2007年我国的互联网域名注册和使用数量飞速增长,达到1,193万个,年增长率达到190.4%<sup>1</sup>,与此同时,域名已经成为黑客利用的主要工具。利用域名,攻击者可以灵活、隐蔽地实施大规模网页挂马、僵尸网络控制、网络仿冒等恶意活动。Fast-Flux等动态域名解析技术的出现,导致根据IP来对攻击行为的追查和阻断更加困难;2007年还出现了利用域名解析服务程序存在的安全漏洞,对公共域名解析服务器进行域名劫持的安全事件,在大量用户毫不知情的情况下将其引诱到钓鱼网站或含有恶意代码的网站,这类事件危害性非常大。所以,加强对域名的管理和域名解析系统的安全防护非常重要。

我国网站的安全问题十分严峻,大量网站被黑客入侵和篡改,甚至被植入木马攻击程序,

---

<sup>1</sup>注:该数据来自中国互联网络信息中心(CNNIC)2008年1月第21次《中国互联网络发展状况统计报告》。

成为黑客的得力工具。利用网站操作系统的漏洞和 WEB 服务程序的 SQL 注入漏洞等，黑客能够得到 Web 服务器的控制权限，轻则篡改网页内容，重则窃取重要内部数据，更为严重的则是在网页中植入恶意代码（俗称“网页挂马”），使得更多网站访问者受到侵害。网页挂马是黑客最喜欢的木马散播方式。随着 Web2.0 应用的推广，相关安全问题逐渐凸显，针对该类交互式网站的攻击事件在不断增多。

尽管网络安全问题令人们对互联网越来越担忧，但令人感受鼓舞的是，网络安全问题已经得到国家领导层和各相政府部门、行业机构的重视。在国务院的直接领导下，我国的国家网络安全应急体系建设取得进一步发展；信息产业部进一步完善了公共互联网应急预案，并加强了包括 CNCERT/CC 和各互联网运营商的工作体系的建设；各重要信息系统主管部门纷纷加强了网络安全管理力度和能力建设；CNCERT/CC、互联网协会等行业机构也积极组织业界开展了一系列专项研究和联合行动。总之，网络安全保障已经成为各相关部门的工作重点之一，我国互联网的安全态势将有所改变。

### 3 网络安全事件接收与处理情况

为了能够了解和应对互联网安全威胁，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 CNCERT/CC 接收非扫描类网络安全事件报告 4390 件<sup>2</sup>（已合并了通过不同方式报告的同一天网安全事件）。每月接收非扫描类事件具体数量如图 1 所示。其中，8 月和 12 月接收的网络安全事件报告较多。



图 1 2007 年非扫描类网络安全事件月度统计

<sup>2</sup> 自 2007 年开始，CNCERT/CC 在统计网络安全事件报告时，仅统计其他组织或者个人向 CNCERT/CC 报告的非扫描类事件报告数量，不包含 CNCERT/CC 监测发现的事件。同时，将漏洞报告也作为一种事件报告进行统计。此统计方式的变更会造成事件报告数量与 2006 年相比的大幅度下降，特此说明。

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的统计情况如图 2所示。与 2006 年相比，主要类型的安全事件数量均近成倍增加，网络仿冒事件数量由 563 件增加至 1326 件，增长率近 1.4 倍；垃圾邮件事件数量由 587 件增加至 1197 件，增长率达 1 倍；网页恶意代码事件数量由 320 件增加至 1151 件，增长率近 2.6 倍。

2007年网络安全事件类型分布

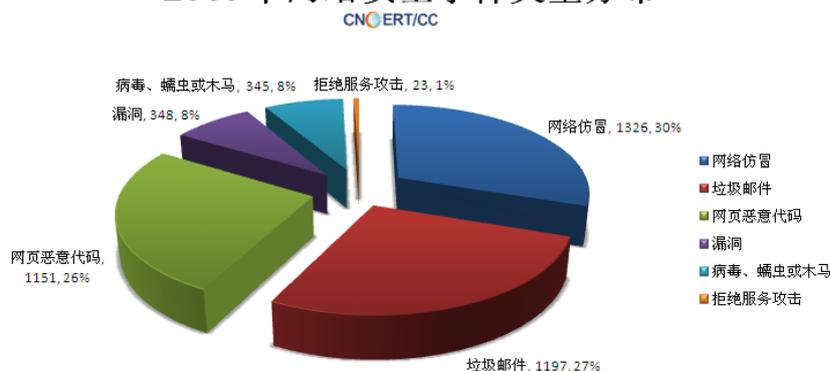


图 2 2007 年网络安全事件类型分布

### 3.2 事件处理情况

2007 年CNCERT/CC共成功处理各类网络安全事件 1057 件，事件类型主要有网络仿冒、网页恶意代码、网页篡改、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，涉及国外商业机构的网络仿冒类事件，以及国内政府机构和重要信息系统部门的网页篡改类事件的数量最多。

2007年CNCERT/CC处理网络安全事件数量



图 3 2007 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 年各省分中心参与事件处理数目如图 4所示，其中新疆、北京、上海、广东和辽宁处理事件数量居前 5 位。

## CNCERT/CC各省分中心2007年参与事件处理数目对比

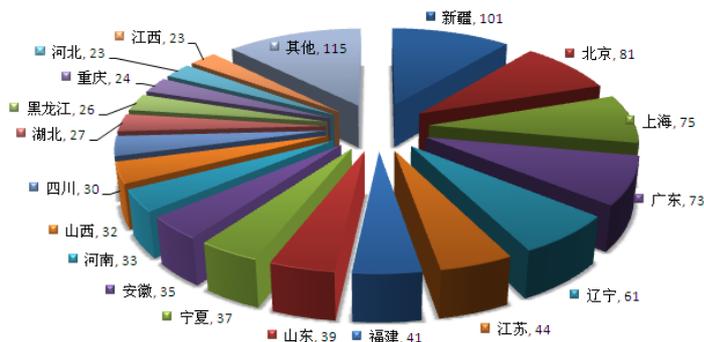


图 4 CNCERT/CC 各省分中心 2007 年参与事件处理数目对比

### 3.3 事件处理部分案例介绍

#### 3.3.1 恶意代码事件处理

##### “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。通过当地运营商的协助，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于 1 月 20 日重装了系统，故有关网页也被删除。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。

##### 处理反 google 病毒

2007 年 8 月出现一种反 google 的病毒，感染该病毒的用户在打开 Google.cn 或者 Google.com 时，会看到提示：“Google 退出中国,请用百度进行搜索”。这是由于被感染主机的 hosts 文件被恶意修改，导致用户对 google 网站的访问被引向含有大量恶意代码的恶意服务器，该主机对应域名为 591ani.cn。对此，CNCERT/CC 一方面联系有关域名注册商，得到了对方的积极支持和快速响应，按照国家有关规定关闭了 591ani.cn 域名；另一方面通过 CNCERT/CC 浙江分中心联系恶意服务器的用户并删除了恶意代码程序。

#### 3.3.2 分布式拒绝服务攻击事件

##### 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。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。

### 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。

## 3.3.3 域名相关安全事件

### 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](http://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。

### caomapi.com 恶意域名处理

2007 年 7 月，CNCERT/CC 发现互联网中有多个网站（如：[www.aqshw.cn](http://www.aqshw.cn)，[www.m85853.com.cn](http://www.m85853.com.cn)，[www.m85853.cn](http://www.m85853.cn)，[www.hao123hao123.cn](http://www.hao123hao123.cn)）正在散播恶意代码，并且这些恶意代码都将窃取到的数据发送到 [ppp.caomapi.com](http://ppp.caomapi.com)。CNCERT/CC 一方面立即协调四川、上海、广东等分中心清除散播恶意代码网站所对应主机上的恶意代码；另一方面由于 [caomapi.com](http://caomapi.com) 域名多次将所对应 IP 进行更换，而 [ppp.caomapi.com](http://ppp.caomapi.com) 域名注册人所登记的信息及联系方式都是虚假信息，故 CNCERT/CC 与域名注册单位取得联系，得到了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。

### 处理 3322.org 中大量散播恶意代码的二级域名

8 月 17 日，CNCERT/CC 收到国外应急组织的报告，称 [3322.org](http://3322.org) 的大量二级域名站点正在散播恶意代码。经验证核实，CNCERT/CC 确认其中 133 个 [3322.org](http://3322.org) 的二级域名都确实含有散播恶意代码的链接。事实上，由于 [3322.org](http://3322.org) 的域名注册单位提供免费二级域名解析服务，所以非常容易被黑客利用从事恶意活动。对此，CNCERT/CC 立即联系 [3322.org](http://3322.org) 的域名注册单位进行处理，8 月 20 日有关恶意链接地址全部被删除。

## 某公司网站的域名劫持事件

11月3日，CNCERT/CC 接到应急服务支撑单位报告，发现某著名公司网站中包含恶意软件，用户在登录时主机会被暗中植入多个木马程序。经调查发现，虽然该域名是该公司所用，但所解析出的网站 IP 地址却对应一台黑客控制主机，该黑客通过对域名服务器的攻击达到这一目的。CNCERT/CC 立即启动相关技术平台的监测，发现黑客攻击导致存在解析错误问题的 DNS 服务器已有近 20 台，涉及多个省份，受影响用户范围十分广泛。CNCERT/CC 立即通知相关运营商紧急排查和恢复各 DNS 服务器，目前已基本排除了影响。

此案例表明，黑客利用 DNS 服务软件——Bind 的漏洞实施的攻击手法可以实现对任意域名的大范围劫持。该攻击行为具有很强的隐蔽性，用户防范难度很大，一旦被恐怖分子或敌对势力利用，必将给我国互联网网络信息安全带来严重的后果。

事后，CNCERT/CC 向各运营商发出安全建议，建议将 DNS 服务器软件立即升级到最新版本，提高黑客攻击难度，同时加强对 DNS 服务器的运维保障，及时发现和处置域名劫持事件。

### 3.3.4 网页恶意代码和网络仿冒事件

#### 某国内著名网站被嵌入恶意代码

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”（即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结果，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。

#### 我国主机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，而且与一个用户取得了直接联系，但用户配合并不积极。在 CNCERT/CC 的努力解释和协调下，两个用户终于在十几天采取了消除安全问题的措施。

在此事件中，被黑客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。该事件反映出近期网络仿冒的新趋势，即黑客每次建立一个新的仿冒网站时都注册新的域名，并通过该域名来实现重定向。通过这种办法，新的仿冒网站可以暂时逃过采用黑名单机制的反仿冒网站系统的过滤，因为从发出欺骗邮件到仿冒网站被添加到黑名单需要一些时间。黑客的新策略导致了仿冒网站域名的爆炸式增长，为了便于操作，黑客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。

### 3.3.5 其他典型事件处理情况

#### 处理 TCP5168 端口异常流量事件

8月23日，CNCERT/CC 监测发现 TCP 5168 端口流量出现可疑快速增长，同时国际上多个合作伙伴也通报了同一情况。CNCERT/CC 立即针对该事件进行相关部署，一方面对 TCP 5168 端口的流量进行重点监测，另一方面与国内外网络安全机构保持联系，关注事态进展。

经初步判断，该端口流量增长与 22 日公布的趋势科技企业级反病毒产品中存在的缓冲区溢出漏洞有关。虽然趋势科技已经发布了相关升级补丁，但由于升级操作存在滞后性，不排除攻击者企图利用该漏洞实施扩散恶意代码等大规模攻击的可能。监测数据显示，从 8 月 23 日 2 时起到 27 日 13 时 5168 端口流量最高增长幅度与历史监测数据相比超过 10 倍，但平均占用网络带宽不足 100M 字节，流量在 23 日 12 时达到高峰后未再出现持续攀升现象，对网络整体的影响不明显，24 日 01 时起流量开始大幅下降。同时综合各方反馈情况来看，本次出现的流量增长很可能是黑客操纵大量“肉鸡”进行漏洞的恶意扫描引起，尚未发现恶意代码传播迹象，也未捕获到可疑恶意代码样本。CNCERT/CC 于 24 日在 CNCERT/CC 官方网站发布了安全公告，提醒相关用户及时升级补丁，并通知运营商加强网络监测，开展漏洞检查处理。同时，继续与国内外相关机构保持联系，关注事件进展。

总体来看，此次事件并未造成严重影响，但不排除出现蠕虫扩散的可能。该事件说明黑客利用最新漏洞来实施“零日攻击”的能力在加强，攻击目标已经从 Windows 操作系统扩展到主流应用软件，对我们网络安全保障提出了更高的挑战。

#### 成功摧毁一个活跃僵尸网络

10 月份，CNCERT/CC 监测到一个大规模僵尸网络的活动非常频繁，包括进行大范围的扫描和向大量国内外网站发起针对 PHP 漏洞的攻击。经分析，该僵尸网络控制服务器位于我国江西省。10 月 16 日，在 CNCERT/CC 江西分中心的密切配合下，迅速联系到该僵尸网络控制服务器的用户。用户获知后，立即对该服务器进行了全面检查，发现其在 10 月 11 日遭到了黑客攻击，并已经被黑客完全控制，随后用户立即采取紧急措施，并针对该服务器采取了安全加固措施。从 CNCERT/CC 的监测数据来看，10 月 16 日 17 时 58 分之后，该僵尸网络已停止活动。

## 4 信息系统安全漏洞公告及处理情况

近年安全漏洞数量不断增加，仍是信息系统的主要安全隐患。据美国 CERT/CC 统计<sup>3</sup>，该组织 2007 年全年收到信息系统安全漏洞报告 7236 个。自 1995 年以来，漏洞报告总数已达 38016 个，具体统计结果如图 5 所示。

<sup>3</sup> 数据来源：[http://www.cert.org/stats/vulnerability\\_remediation.html](http://www.cert.org/stats/vulnerability_remediation.html)

## 安全漏洞数量年度统计

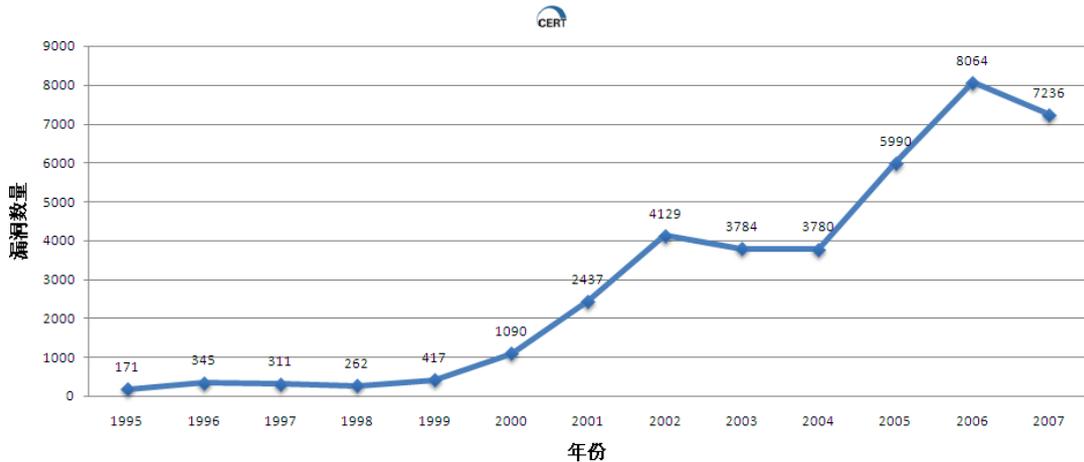


图 5 安全漏洞数量年度统计

2007 年微软公司正式公布了 69 个<sup>4</sup>具有编号的安全漏洞。其中，除 Windows 操作系统漏洞外，安全漏洞更多的集中出现在了 IE 浏览器和 MS Office 等应用软件上。

CNCERT/CC 对于漏洞发布一直予以高度重视，2007 年共整理发布与我国用户密切相关的漏洞公告 104 个。下面列举几个 2007 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（MS07-017）

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

<sup>4</sup> 数据来源：<http://www.microsoft.com/china/technet/security/current.mspx>

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。

#### Cisco IOS 在 IPv6 路由包头处理、安全复制协议、下一跳解析协议、语音服务中存在的四个漏洞

CNCERT/CC 在 8 月 9 日向运营商通告了 Cisco IOS 存在的四个漏洞，分别是“使用 IPv6 路由包头的 Cisco IOS 信息泄漏”、“Cisco IOS 安全复制授权绕过漏洞”、“Cisco IOS 下一跳解析协议漏洞”、“Cisco IOS 和 Cisco Unified Communications Manager 中的语音漏洞”。这些漏洞危害严重，利用处理伪造 IPv6 路由包头时存在的漏洞，可以导致 IPv6 目的地址缓存区的数据泄漏，或者运行 Cisco IOS 的设备宕机；利用安全复制授权绕过漏洞，黑客可读写 Cisco 设备的文件系统中的任意文件，甚至系统配置文件；利用后两个漏洞可对 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 紧急通知各运营商采取应急措施，及早排除利用这些安全漏洞发起网络攻击的安全隐患。

## 5 互联网业务流量监测情况

分析互联网流量中的业务种类及其所占流量比例变化，一方面能够为互联网的运营管理提供参考，另一方面也有利于把握主流的互联网业务并关注其中的安全问题。

根据 CNCERT/CC 在 2007 年对互联网业务流量（字节数）抽样统计，利用 TCP 协议的网络应用中，Web 浏览、P2P 下载、电子邮件和即时聊天工具占用带宽最多。Web 浏览是互联网用户的主要网上行为，而利用 80 端口漏洞对 Web 网站的攻击使得防火墙等传统防护手段难以奏效。电子邮件协议 SMTP 使用 TCP 25 号端口，同时该端口还充斥着大量的蠕虫和垃圾邮件流量。eMule、迅雷、Bitcomet 等 P2P 软件是目前最流行的下载工具，大量的 P2P 报文不仅影响到了其他互联网业务质量，而且成为传播病毒、蠕虫、间谍软件等恶意代码的载体，并存在泄露个人或敏感信息的问题。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也是安全防护的重点。

TCP 协议流量端口前十位如图 6 和表 1 所示：

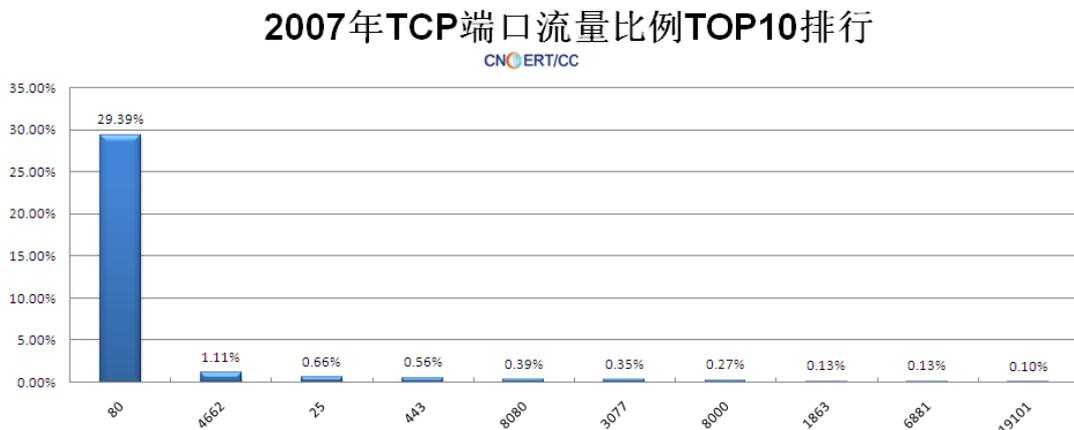


图 6 2007 年 TCP 协议流量端口排名前十位

TCP 端口	TCP 流量排名	百分比	主要的业务种类
80	1	29.39%	网页服务端口
4662	2	1.11%	eMule 下载工具默认端口
25	3	0.66%	SMTP 默认端口
443	4	0.56%	网页服务端口
8080	5	0.39%	网页服务端口
3077	6	0.35%	迅雷下载工具默认端口
8000	7	0.27%	QQ 通讯端口
1863	8	0.13%	MSN Messenger 协议登陆服务端口
6881	9	0.13%	P2P 下载软件端口
19101	10	0.10%	clubbox 服务开放端口

表 1 2007 年 TCP 协议流量端口排名前十位

UDP 协议中最占用带宽的网络应用是 P2P 下载软件(如迅雷和 eMule), 其次是 Windows 信使服务软件。使用 UDP 协议的 DNS 服务占总流量的 1.3%。

UDP 协议流量端口前十位如图 7 和表 2 所示。

### 2007年UDP端口流量比例TOP10排行

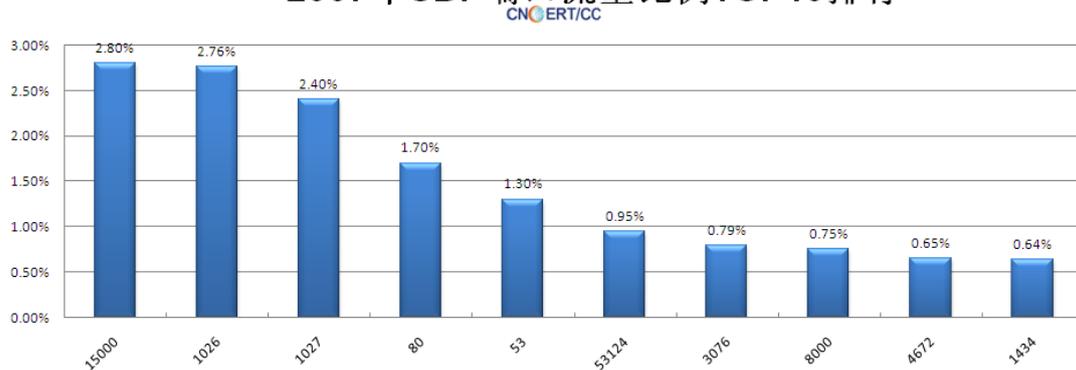


图 7 2007 年 UDP 协议流量端口排名前十位

UDP 端口	UDP 流量排名	百分比	主要的业务种类
15000	1	2.80%	迅雷下载工具默认端口
1026	2	2.76%	MS Messenger 端口
1027	3	2.40%	MS Messenger 端口
80	4	1.70%	网页服务端口
53	5	1.30%	DNS 服务端口
53124	6	0.95%	未知
3076	7	0.79%	迅雷下载工具默认端口
8000	8	0.75%	QQ 通讯端口
4672	9	0.65%	eMule 下载工具默认端口
1434	10	0.64%	MSSQL 服务端口

表 2 2007 年 UDP 协议流量端口排名前十位

## 6 木马与僵尸网络监测情况

木马和僵尸网络是目前非常有效的远程监听和秘密控制手段，也是目前黑客盈利的重要工具。鉴于木马和僵尸网络的潜伏性与其行为的不可预料性特征，对我国互联网安全构成了严重威胁，尤其是在失窃密方面对国家安全造成严重危害，CNCERT/CC 对此两类事件一直密切关注，并进行重点监测。

### 6.1 木马监测情况

CNCERT/CC 在 2007 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 433429 个，被控制端 IP 地址总数为 2861621 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，CNCERT/CC 对常见的木马程序活动状况进行抽样监测，发现我国大陆地区 995154个<sup>5</sup>IP 地址的主机被植入木马，与2006年（44717个IP地址）相比增加迅猛。我国大陆地区被木马程序控制的计算机IP地址分布情况如图 8所示，木马被控制端最多的地区分别为广东、江苏、浙江、山东、河北和北京。

2007年被境外通过木马程序控制的中国大陆主机  
对应IP按地区分布 CNCERT/CC

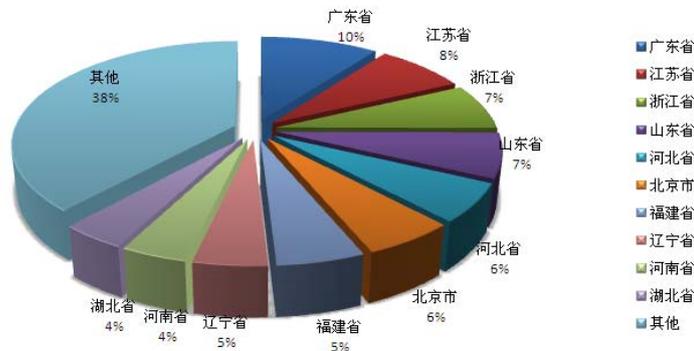


图 8 2007 年中国大陆地区被木马控制的计算机 IP 分布图

#### 6.1.2 非中国大陆地区木马控制端分布统计

CNCERT/CC监测发现大陆地区以外111063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 9所示，其中位于中国台湾的木马控制端占多数，其次依次为美国、韩国、中国香港和日本。

<sup>5</sup> 由于IP定位库更新，2007 年全年与上半年对我国大陆地区被植入木马的IP地址数量统计情况略有出入。

## 2007年利用木马程序控制中国大陆主机的境外IP按国家和地区分布

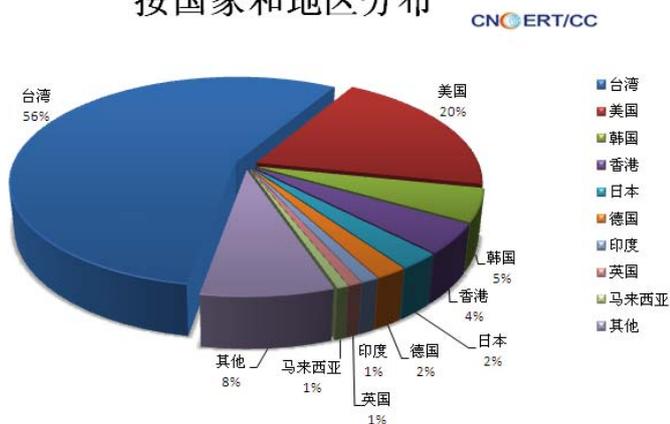


图 9 2007 年通过木马控制我国计算机的境外 IP 分布图

### 6.1.3 木马网络规模分布

随着黑客技术的发展，黑客对木马的控制也呈现集中化趋势，构成大小不一的木马网络（即控制端和被控端组成的网络）。CNCERT/CC通过对不同规模的木马网络的监测发现，大部分木马网络属于小型化，规模小于等于1000的木马网络占绝大多数，如图 10所示。同时，也存在较大规模（大于5000）的木马网络，并且其活动十分频繁。

#### 2007年木马网络规模分布图

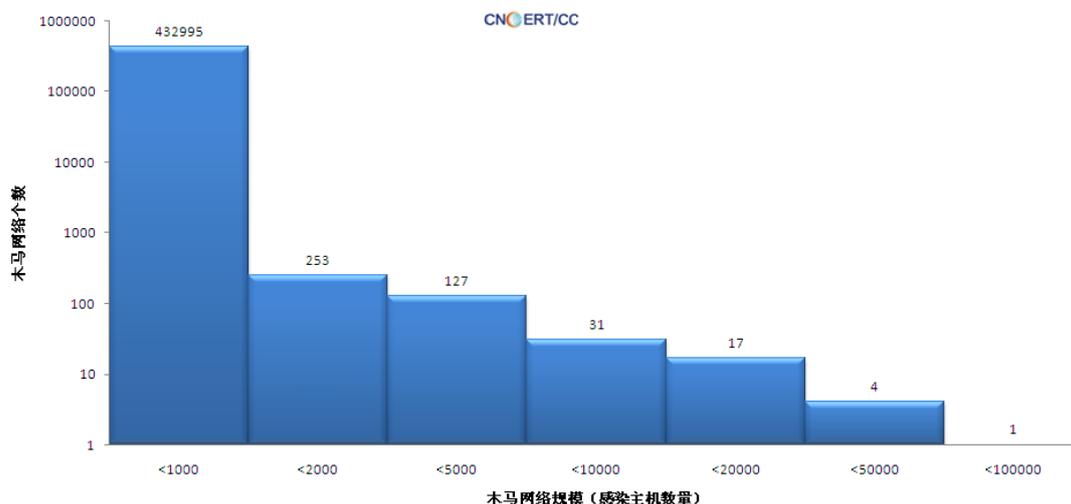


图 10 木马网络规模分布

## 6.2 僵尸网络监测情况

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 年抽样监测发现我国大陆有 3624665 个 IP 地址的主机被植入僵尸程序。

2007 年 CNCERT/CC 共发现各种僵尸网络被用来发动拒绝服务攻击 10988 次、发送垃圾邮件 112 次、实施信息窃取操作 3949 次。

从 CNCERT/CC 现有监测的情况和国际知名网络安全公司的有关报告可以看出，我国已成为感染僵尸程序的计算机数量最多的国家，但这些计算机多数是被其他国家或地区所控制。这同我国互联网用户的安全防范意识和防护能力较低密切相关。

## 6.2.1 僵尸网络控制服务器分布

2007 年，CNCERT/CC 共发现在 17063 个控制服务器中，有 10399 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 11 所示，其中位于美国的占 32%、中国台湾占 13%、韩国占 7%。

2007年中国大陆地区外僵尸网络控制服务器分布

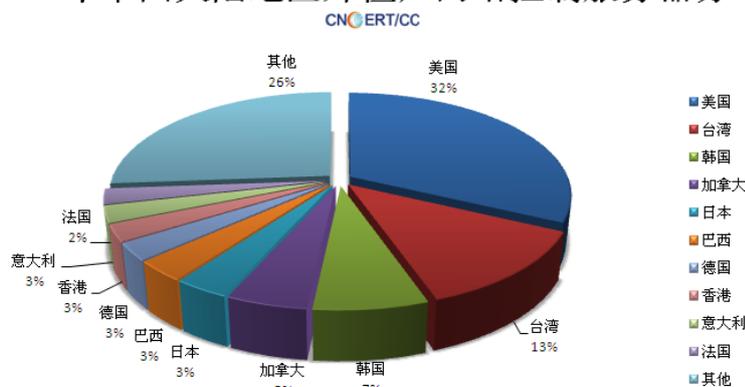


图 11 2007 年中国大陆地区外僵尸网络控制服务器分布图

## 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，CNCERT/CC 的分布式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 12 所示。其中，僵尸网络最常用的控制端口分别是 6667、1863 和 7000 等。

## 僵尸网络控制服务器使用端口分布

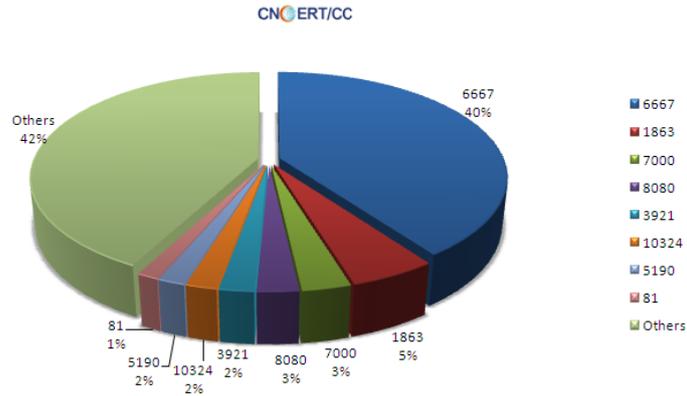


图 12 2007 年僵尸网络控制服务器使用端口分布图

### 6.2.3 僵尸网络规模分布

僵尸网络的规模总体上呈现小型化、局部化和专业化特征。1千以内规模的僵尸网络居多。大规模的僵尸网络仍然存在，有19个僵尸网络操控的计算机（即“肉鸡”）数量超过10万台。2007年监测到的僵尸网络规模数量分布如图 13所示。

#### 2007年僵尸网络规模分布图

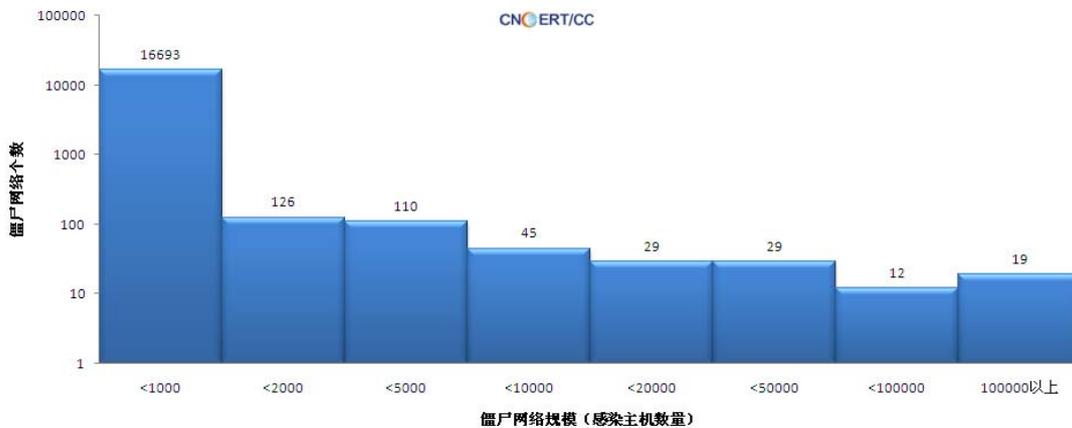


图 13 2007 年僵尸网络规模分布图

## 7 被篡改网站监测情况

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

CNCERT/CC监测到发现中国大陆被篡改网站的数量近年来增长迅猛。2007年，CNCERT/CC监测到中国大陆被篡改网站总数累积达61228个，比去年增加了1.5倍。近年来中国大陆网页被篡改情况年度统计如图14所示。

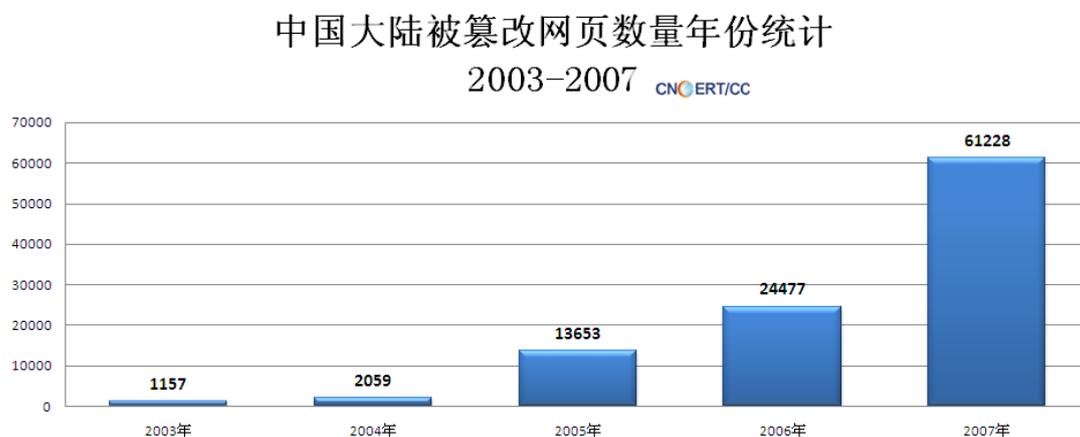


图 14 中国大陆网页被篡改情况年份统计(2003-2007)

2007年我国被篡改网站数量按月统计情况如图15所示。



图 15 2007年被篡改网站数量统计

## 7.2 我国政府网站被篡改情况

2007年，中国大陆政府网站被篡改数量达3407个。某些政府网站被篡改后长期无人过问，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。2007年中国大陆政府网站被篡改各月累计达4234个。其中，10月、11月和8月被篡改网站数量居多。2007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16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7%，与往年相比（2006年为16%），该比例有所下降，但明显高于我国.cn域名下的政府网站所占的3.5%比例<sup>6</sup>，被篡改的gov.cn网站的数量每年在大幅增加，说明gov.cn网站的安全性仍需提高。

中国大陆被篡改的网站中政府网站所占比例月度统计



图 16 2007 年中国大陆被篡改的网站中政府网站所占比例月度统计

### 7.3 攻击我国网站的主要黑客情况

了解黑客的行为模式，及时掌握他们的动向，对于整体把握网络安全态势、针对性的增加网络防护力量、配合有关部门打击网络犯罪具有积极的意义。

根据 CNCERT/CC 统计，2007 年在对我国网站实施篡改攻击的黑客中，排名前十位的攻击者如下表所示。

排名	攻击者	攻击网站数量	占被篡改网站总数的比例
1	sinaritx	1731	2.8%
2	1923turk	1417	2.3%
3	the freedom	1156	1.9%
4	aLpTurkTegin	1052	1.7%
5	Mor0Ccan Islam Defenders Team	864	1.4%
6	iskorpitx	761	1.2%
7	寒水芊芊	754	1.2%
8	黑侠	681	1.1%
9	电脑迷	669	1.1%
10	lucifercihan	525	0.9%

表 3 2007 年对我国网站实施篡改攻击的前十位黑客

根据 CNCERT/CC 掌握的资料来看，有些攻击者年龄较小，但已具备了较高的黑客入侵技术。这些攻击者中既有个人，也有带宗教色彩的团队。在对我国网站实施篡改攻击的前十位黑客中，除“寒水芊芊”、“黑侠”和“电脑迷”为中国黑客外，其他攻击者均是来自

<sup>6</sup>注：该数据来自中国互联网络信息中心（CNNIC）2008 年 1 月第 21 次《中国互联网络发展状况统计报告》。

土耳其的黑客团队，具有强烈的宗教和反欧美反以色列意识。

## 8 网络仿冒（网络钓鱼）情况

2007年CNCERT/CC共接到网络仿冒事件报告1326件，具体成功处理了394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4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)	259
eBay(美国网上交易站点)	255
RSA Cyota(美国网络安全公司)	128
Castlecops(美国网络安全机构)	143
Mark Mornitor(美国网络安全公司)	74

表4 2007年向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

为了加强对恶意代码的监测处理能力，CNCERT/CC在全国部署了分布式蜜网系统。通过对该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，每日平均捕获样本3408次，图17给出了每日的样本捕获趋势。

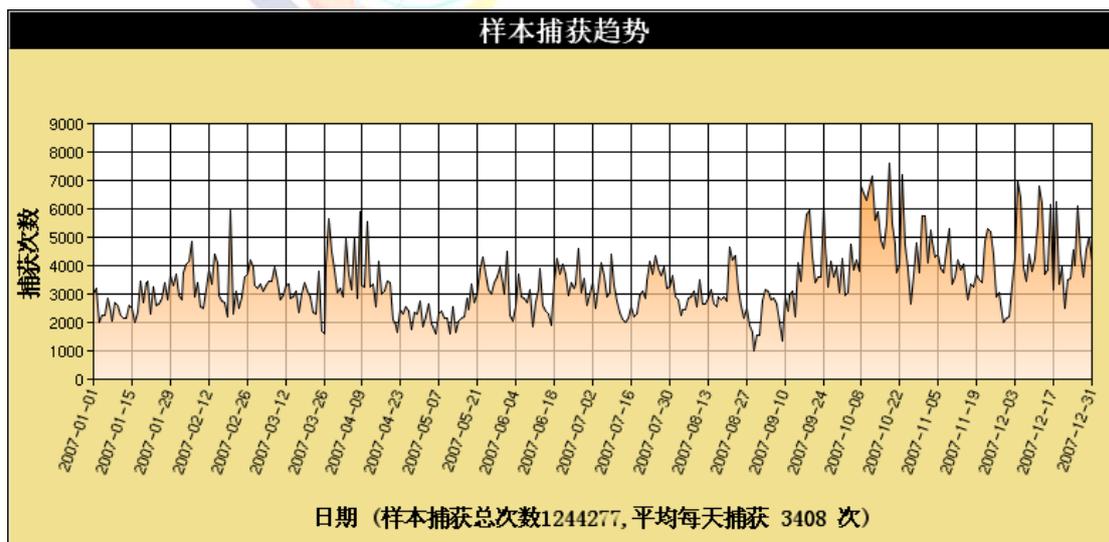


图17 分布式蜜网样本捕获趋势图

蜜网采用被动式监测方式，一个恶意代码可能会被捕捉到多次。图18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 496 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。

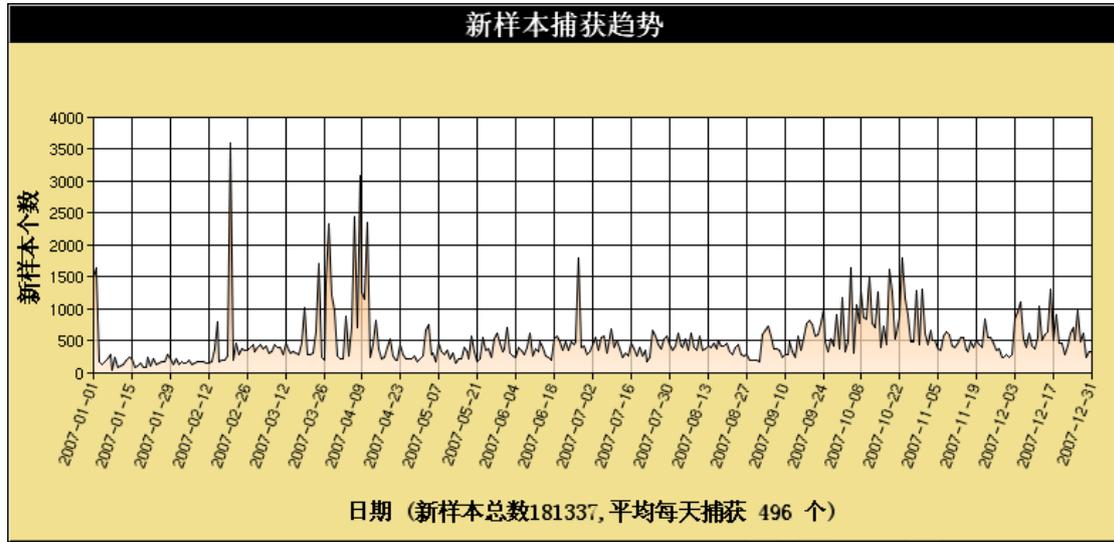


图 18 分布式蜜网新样本捕获趋势图

2007 年蜜网共捕获 181337 个恶意代码样本，位于前十位的恶意代码如表 5 所示：

排名	恶意代码名称	总捕获次数
1	Backdoor.Win32.VanBot.ax	82852
2	Net-Worm.Win32.Allapple.b	79196
3	Backdoor.Win32.PoeBot.c	69636
4	Net-Worm.Win32.Allapple.e	33712
5	Virus.Win32.Virut.b	33485
6	Backdoor.Win32.SdBot.aad	23998
7	Virus.Win32.Virut.a	21084
8	Backdoor.Win32.Rbot.bni	19348
9	Backdoor.Win32.Rbot.gen	18017
10	Backdoor.Win32.SdBot.xd	16891

表 5 分布式蜜网捕获次数前十名的恶意代码

以上恶意代码以后门木马和网络蠕虫病毒为主，主要是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。VanBot、PoeBot（派波）、SDBot、Rbot（瑞波）等僵尸程序均具有很高的危害性。

## 10 网络安全信息服务情况

CNCERT/CC 提供的网络安全信息服务主要包括漏洞公告、安全建议、统计报告等，除了通过网站向公众提供外，CNCERT/CC 同时利用邮件、专题报告等形式向基础信息网络、重要信息系统运营部门提供定向的信息服务。

### 10.1 安全信息通报

CNCERT/CC 将自主发现的以及从国际应急组织渠道获取的重要网络安全信息及时通报给有关部门。2007 年，CNCERT/CC 共向有关部门通报网络安全信息 162 次，其中，报告重大漏洞 5 次。今后 CNCERT/CC 将进一步与有关部门和运营商建立并规范信息共享机制，及时、有效的通告各种安全信息，提高重要信息系统和基础信息网络的网络安全防护能力。

### 10.2 网站信息发布

CNCERT/CC 网站是 CNCERT/CC 对公众提供网络安全信息服务的重要窗口。2007 年，CNCERT/CC 通过网站发布了 359 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 19。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。

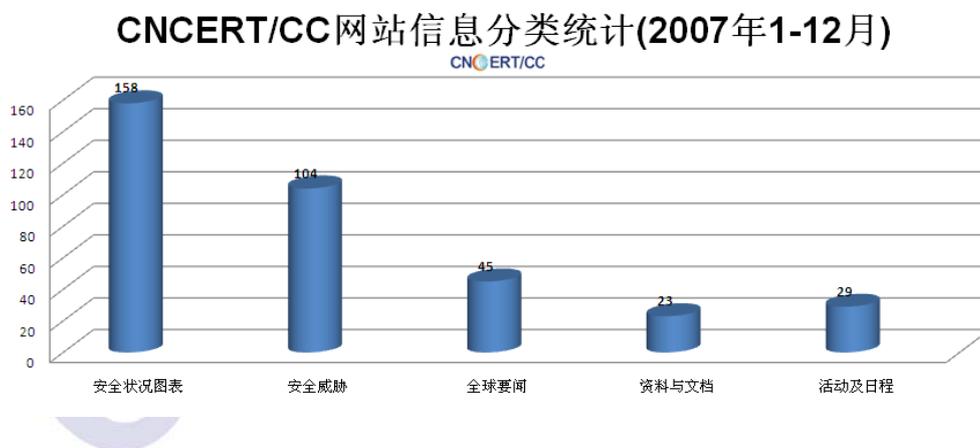


图 19 2007 年 CNCERT/CC 网站信息分类统计

## 11 我国网络安全应急组织发展情况

### 11.1 我国网络安全应急组织列表

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

计算机网应急响应组（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12月，我国目前有网络安全应急组织60家。除国家计算机网络应急技术处理协调中心外，其他社会化、商业化的应急组织见表5所示<sup>7</sup>。其中，在中国应急组织社区登记的应急组织共计33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*	<a href="#">30Wish</a>
西安安智科技有限公司*	<a href="#">ANGELLTECH</a>
哈尔滨安天信息技术有限责任公司*	<a href="#">Antiy Labs</a>
北京冠群金辰软件有限公司*	<a href="#">CA-Jinchen</a>
中国教育和科研计算机网应急响应组*	<a href="#">CCERT</a>
成都微软技术中心*	<a href="#">CDMTC</a>
中国移动网络与信息安全应急小组*	<a href="#">CMCERT/CC</a>
深圳市安络科技有限公司*	<a href="#">CNNS</a>
中国科技网网络安全应急小组*	<a href="#">CSTCERT</a>
中国联通天津分公司*	<a href="#">CUCC-TJ</a>
山东中创软件商用中间件有限公司*	<a href="#">CVICSE</a>
河南山谷创新网络科技有限公司*	<a href="#">Chinavvy</a>
福建富士通信息软件有限公司*	<a href="#">FFCS</a>
随锐科技*	<a href="#">G-AVR</a>
广西大学信息网络中心*	<a href="#">GXUNC</a>
贵阳华旺科技有限公司*	GYHW
合肥工业大学网络安全与应急响应组*	<a href="#">HFUTCERT</a>
北京万网新兴网络技术有限公司*	<a href="#">HiChina</a>
北京江民新科技术有限公司*	<a href="#">JIANGMIN</a>
北京安氏领信科技发展有限公司*	<a href="#">LinkTrust</a>
国家计算机网络入侵防范中心*	<a href="#">NCNIPC</a>
东软计算机安全事件应急小组*	<a href="#">NCSIRT</a>
中联绿盟信息技术(北京)有限公司*	<a href="#">NSFOCUS</a>
上海中科网威信息技术有限公司*	<a href="#">Netpower</a>
山东科技大学中国核心网络安全小组*	<a href="#">SDUST-CKNSG</a>
山东新潮信息技术有限公司*	<a href="#">SDXC</a>

<sup>7</sup>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。

神州通信有限公司*	<a href="#">SNZO</a>
华为电信网络与业务安全实验室*	<a href="#">TNSSL</a>
连云港港湾科技有限公司技术支持中心*	<a href="#">TSC-HT</a>
天融信安全运营中心*	<a href="#">TopSec SOC</a>
启明星辰应急响应小组*	<a href="#">VCERT</a>
武汉大学省级应急服务支撑中心*	<a href="#">WHUPCERT</a>
CERNET 华东（北）地区应急响应组	<a href="#">NJCERT</a>
北京大学网络安全紧急响应组	<a href="#">PKUCERT</a>
<a href="#">成都电子机械高等专科学校</a>	
<a href="#">新疆大学校园网应急响应组</a>	
<a href="#">CERNET山西省主节点应急响应组</a>	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	<a href="#">BUPTCERT</a>
CERNET 西南地区应急响应组	<a href="#">CDCERT</a>
广州华南理工大学网络中心	<a href="#">GZCERT</a>
<a href="#">河南教育科研计算机网应急响应小组</a>	
<a href="#">湖南主节点及中南大学应急响应小组</a>	
CERNET 华中地区应急响应组	
江西省节点应急响应组	JXCERT
<a href="#">四川轻化工学院网管中心</a>	
<a href="#">吉林大学网络中心应急响应组</a>	
川北医学院	
<a href="#">CERNET贵州主节点</a>	
山西财经大学网络中心	
<a href="#">宁夏大学网络中心</a>	
青海师范大学网络中心	QH-CCERT
CERNET 华南地区紧急响应组	<a href="#">GZCERT</a>
大连理工大学校园网紧急响应组	<a href="#">DLCERT</a>
上海交通大学计算机紧急响应组	<a href="#">SJTUCERT</a>
CERNET 山东网络中心紧急响应组	<a href="#">SDCERT</a>
东北农业大学校园网安全响应组	<a href="#">NEAUCERT</a>
复旦大学校园网紧急响应组	<a href="#">FDU-CERT</a>

表 6 我国社会化、商业化的网络安全应急组织名称

## 11.2 CNCERT/CC 应急服务支撑单位列表

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，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。

以下是CNCERT/CC支撑单位列表：

■ **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  
中国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  
上海二零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 CNCERT/CC 组织的重要活动

### 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重要事件应急处理，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，执法部门应加大执法打击力度

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，构建和谐网络”。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 成功召开计算机恶意程序治理法律环境高层研讨会**

8 月 28 日，2007 安全中国—计算机恶意程序治理法律环境高层研讨会在北京国际艺苑皇冠假日酒店隆重召开。信息产业部、公安部、国务院法制办、国务院信息化办公室等八个政府部门的代表和来自 20 家专业机构和互联网企业的代表出席了此次研讨会。会议现场，与会人员就中国目前的网络安全形势以及对网络木马等恶意程序的法律治理环境问题进行了深入的探讨和剖析，网络安全立法得到进一步推动。

本次研讨会由国家计算机网络应急技术处理协调中心（CNCERT/CC）和《检察日报》联合主办，由腾讯计算机信息技术有限公司、北京金山软件有限公司承办，得到了政府、行业、法律、媒体等各届人士的支持与关注。

会上，来自政府部门的代表和来自互联网企业的代表分别从法律和技术角度层面，围绕网络恶意行为定义、网络犯罪的判定、调查取证和处罚开展了热烈讨论。与会代表一致认为：

一、应进一步加强治理恶意软件的普及宣传工作、共同提高互联网用户的信息安全意识和防范手段。

二、应进一步加强政府主管部门与互联网企业、用户之间在网络安全立法执法工作上的联系和交流，共同推动国家在有关治理恶意软件的立法、执法等方面的工作。

三、网络安全专业机构和各互联网企业应加强研究与合作，积极为国家立法机构提供技术和信息上的支持，并配合司法机关加大对恶意互联网程序的打击。

### **“关于应对利用域名从事网络攻击处置机制研讨会”成功召开**

随着互联网的蓬勃发展，我国互联网域名数量飞速增长，然而域名作为用户与网络应用间的桥梁和纽带，也越来越多地被黑客利用从事大规模地恶意代码散播、网络仿冒、僵尸网络控制等多种恶意活动。为了有效处置此类利用域名从事网络攻击的安全事件，更好的保护互联网健康发展，切实做好十七大网络安全保障工作，2007 年 9 月 12 日，信息产业部电信管理局组织召开了“关于应对利用域名从事网络攻击处置机制研讨会”，该会议由 CNCERT/CC 承办，参加单位还包括 CNNIC 及 21 家国内主要域名注册服务机构。

会议通报并讨论了网络攻击事件中的域名被利用情况，认为快速处置被网络攻击所利用的域名对于维护公共互联网的安全十分必要，一致赞同在信息产业部领导下，根据《中国互联网域名管理办法》（中华人民共和国信息产业部令第 30 号）和国家相关法律法规，对被网络攻击所利用的域名建立快速、有效的处理机制。本次会议讨论并通过了“应对利用域名从事网络攻击处置机制（试行）”。

## 13 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。

### CNCERT/CC 走访东盟四国 共建网络安全

2007 年 7 月 10 日至 22 日, CNCERT/CC 在信息产业部外事司的统一安排下, 派代表团走访了越南、老挝、缅甸、柬埔寨四个东盟国家的网络安全应急处理主管部门。在本次走访中, CNCERT/CC 向这四国介绍了我国的应急体系发展历史和现状, 以及 CNCERT/CC 的职责和工作模式; 听取了四国对其互联网发展状况和网络安全工作的现状、问题以及实际需求的情况; 与各国讨论了具体的合作内容和计划。各国均表示将学习 CNCERT/CC 的先进经验和运作模式建立或建设本国的国家级应急响应组织, 并希望与 CNCERT/CC 进一步加强合作。

通过本次走访, CNCERT/CC 根据四国在网络安全方面的实际需求, 确定了与四国不同的合作重点。由于越南的互联网发展迅速, 对网络安全应急处理工作有迫切需求, 而且越南 VNCERT 已经开展了大量工作, 所以 CNCERT/CC 拟与越南 VNCERT 开展信息共享、网络安全事件处理、应急演练、培训等方面的深入合作; 而由于柬埔寨、缅甸和老挝的互联网较为落后, 网络安全事件的数量和危害相对都较小, 柬埔寨 CamCERT 和缅甸 mmCERT 都还在能力建设阶段, 老挝尚没有建立 CERT 组织, 所以与这三个国家则主要是继续在培训方面提供支持。

本次走访将成为 CNCERT/CC 与越南、老挝、缅甸、柬埔寨四个东盟国家合作的一个新的起点, 对推动“中国—东盟网络与信息安全应急处理协作框架”的制定, 配合信息产业部进一步落实 2005 年 5 月《中国—东盟建立面向共同发展的信息通信领域伙伴关系北京宣言》中的相关工作起到积极的作用。

### 亚太应急演练 APCERT 成功阻断网络攻击

2007年11月21日亚太计算机网络应急组织联盟（APCERT）成功完成了其一年一度的应急演练。今年的演练背景是2008年的北京奥运会，通过以阻断奥运会期间的网络攻击为目的，来检验APCERT成员组织在亚太地区面对网络威胁的应急处理能力。今年也是CNCERT/CC第四次参加亚太区的应急演练。

今年演练的重点在于，最大程度地减少网络攻击可能造成的影响，特别是大规模的恶意程序传播以及影响正常经济活动或政治稳定性的有针对性的攻击行为。本次演练跨越5个时区，从格林尼治标准时间23点至8点，这对各参与成员的事件响应与处理流程是个挑战。今年的演练方案是由马来西亚MyCERT、澳大利亚AusCERT与新加坡SingCERT三个组织联合设计并实施的。来自亚太12个国家和地区的13个CERT组织参与了演练，包括澳大利亚、文莱、中国、中国香港、印度、日本、马来西亚、新加坡、韩国、中国台湾、泰国和越南。

通过本次演练，不仅检验各个参与成员组织的通讯能力，特别是跨地区和时区的消息沟通与传递能力以及有效决策能力和快速行动能力，而且进一步加强了各参与成员组织的协调与合作。

## 14 结束语

2007年，我国互联网安全状况可以说是宏观上态势平稳，微观上暗流涌动。

宏观上态势平稳主要体现在两个方面，一是尽管基础网络始终面对着各种网络攻击的考验，但却没有因此而发生大规模的拥塞或中断事件；二是尽管一年来新出现的恶意代码数量达十几万种，且其中不乏“熊猫烧香”这样的恶性病毒，但是依托互联网运行的国家重要信息系统没有出现严重的瘫痪事件。而从微观上看，不论是从安全隐患上看还是从正在发生的安全事件上看，目前的形势不得不让人感到忧虑。首先，我国整个信息化应用已经进入快速发展期，应用软件的种类和数量大大增加，但是很多被广泛使用的软件，包括国内生产的软件，甚至国外正版软件却存在严重的安全漏洞，这些漏洞已经被黑客掌握和频繁利用；其次，我国网站的数量在不断攀升，但网站的安全性普遍较低，这不仅招致黑客的频繁入侵，还被植入网页恶意代码，造成大量用户在访问这些网站时遭受木马攻击，为个人、企业和国家的信息安全带来巨大损失；三是黑客群体进一步趋利化、产业化、组织化，网络黑恶势力在逐渐扩大，黑客攻击愈加猖獗，攻击目标更具针对性。

这种宏观和微观两种状况是矛盾的，但却又是并存的。究其原因，一是由于近年来我国整体互联网安全意识有所提高，从国家到企业和个人或多或少采取了一些安全防护措施，起到了一定的作用；二是互联网基础运营商和重要信息系统部门加大了对网络基础设施和安全保障能力的投入，基础网络和信息系统的健壮性和稳定性有明显提高；三是黑客目前通过攻击网络用户来赚取经济利益为主要目的，尚未明显地表现出把基础网络和重要信息系统等国家关键设施作为主要的攻击目标。

在三方面因素的综合作用下，我国互联网有惊无险地走过了2007年，但是当我们着眼2008年，甚至放眼将来的时候，就不由得感到形势的紧迫。

首先，2008年是奥运年，奥运会的网络安全问题是最大的考验。根据历史上的经验，为了“出名”，很多黑客都把奥运会作为挑战和攻击的对象，此外北京奥运会又可能面临个人、群体、组织乃至国家性的或带有某种政治目的的网络攻击，因此网络安全形势十分严峻。

同时，我国互联网安全保障水平较差和防范意识较低的现状已经被那些垂涎我国国家秘密、商业和技术秘密的窃密者利用，并将继续大肆利用。如何将网络安全防护和安全保密工作结合好，是摆在我们面前的关键问题。

再则，随着我国市场经济的深入发展和民众维权意识的提高，人民对影响日常学习、生

活、工作的互联网基础设施、重要信息系统，甚至日常互联网应用的稳定性和安全性要求不断提高，对政府维护网络安全打击网络犯罪的要求越来越迫切。

我们还看到，互联网技术还在加速发展，各种新业务模式、新业务种类、新应用软件不断出现在用户面前，随之而来的必然有各种各样的安全漏洞、黑客攻击，网络安全问题解决的如何，直接关系到公众的切身利益，关系着产业的持续、健康发展，关系着国家信息基础设施的稳定运行。

作为国家基础网络安全保障重要的技术支撑部门，CNCERT/CC 将在工业和信息化部 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，同时 CNCERT/CC 也真诚地希望能够与其他网络安全专业机构、行业部门开展密切合作，充分发挥集体的智慧和力量，全面提高公共互联网的安全保障能力。

## 15 术语解释

### 木马

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。木马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。

### 僵尸网络

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，是当前互联网安全的主要威胁之一。

### 恶意代码

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。

### 蜜罐和蜜网

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。