

中国互联网网络安全报告

(2008 年上半年)

国家计算机网络应急技术处理协调中心



关于中国互联网网络安全报告(2008年上半年)

本文档所包含的信息代表国家计算机网络应急技术处理协调中心(中文简称国家互联网应急中心;英文简称 CNCERT/CC 或 CNCERT)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。国家互联网应急中心(CNCERT)对于本文档中的信息不做任何明示、暗示或法定的担保。国家互联网应急中心(CNCERT)无法保证发布日期之后所提供的任何信息的准确性。

本文档版权为国家互联网应急中心(CNCERT)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。如未获得国家互联网应急中心(CNCERT)明确的书面许可,不得以任何形式将本文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“中国互联网网络安全报告(2008 年上半年)”,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

1	关于国家计算机网络应急技术处理协调中心.....	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.....	9
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.....	10
6	木马与僵尸网络监测分析.....	12
6.1	木马数据分析.....	13
6.2	僵尸网络数据分析.....	14
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
7.3	对我国网站实施篡改攻击的主要黑客情况.....	18
8	网络仿冒事件情况分析.....	20
9	恶意代码捕获及分析情况.....	21
10	国家互联网应急中心(CNCERT)网站信息发布	23
11	网络安全应急组织发展情况.....	23
11.1	国内应急组织发展情况.....	23
11.2	国家互联网应急中心(CNCERT)组织的相关重要活动	25
12	国际合作与交流.....	27
13	结束语.....	28

1 关于国家计算机网络应急技术处理协调中心

国家计算机网络应急技术处理协调中心(中文简称国家互联网应急中心; 英文简称 CNCERT/CC 或 CNCERT)是在工业和信息化部的直接领导下, 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。

国家互联网应急中心(CNCERT)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。国家互联网应急中心(CNCERT)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。国家互联网应急中心(CNCERT)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。

国家互联网应急中心(CNCERT)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。

国家互联网应急中心(CNCERT)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

2008 年上半年,我国互联网基础设施和重要信息系统整体上运行基本正常,没有出现造成严重影响或后果的大规模网络安全事件。但是,网络攻击的频次、种类和复杂性均比去年大幅增加,遭入侵和受控计算机数量巨大,潜在威胁和攻击力继续增长,信息数据安全问题日益突出,网络安全形势依旧严峻。

国家互联网应急中心(CNCERT)接收和自主监测的各种网络安全事件数量与 2007 年上半年同期相比有较为显著的增加。其中,垃圾邮件事件和网页恶意代码事件增长较快,网页恶意代码同比增长近一倍;网页篡改事件和网络仿冒事件也有大幅增长,同比增长分别是 23.7%和 38%,其中涉及国内政府机构和重要信息系统部门的网页篡改事件、涉及国内外商业机构的网络仿冒事件是 2008 年上半年事件监测和处置的重点。

网页篡改事件特别是我国大陆地区政府网页被篡改事件呈现大幅增长趋势。统计显示,2008 年上半年我国大陆地区被篡改的.gov.cn 网站数量比 2007 年上半年增加 41%,共计 2242 个,占被篡改网站总数的比例达到 7%,而 gov.cn 域名仅占.cn 域名总数的 2.3%,这说明.gov.cn 网站遭受黑客攻击的可能性相对较高。2008 年 5 月 1 日,我国颁布施行《政府信息公开条例》,该《条例》的推行对政府信息化建设提出了新的要求,同时也对电子政务信息系统的网络安全提出更高的要求。由于政府网站整体安全水平较低,往往是黑客攻击的重要目标,因此,作为政府对外形象的窗口、发布权威信息和与公众开放交流的平台,电子政务信息系统的网络安全管理是一个需要各级部门高度重视的问题。

我国大陆地区感染木马和僵尸网络的主机数量巨大。国家互联网应急中心(CNCERT)的监测数据显示,2008 年前 5 个月监测到的感染木马和僵尸网络的主机数量缓慢波动上涨,但在 6 月份出现跳跃式增长。这一现象跟国家互联网应急中心(CNCERT)加强监测力度和扩大监测范围有关,但更令人担忧的原因则是攻击者似乎在北京奥运会前夕加紧活动,图谋通过网络攻击干扰数字奥运的顺利举行。

造成木马和僵尸网络产生和扩散的一大途径是恶意代码的肆虐传播。2008 年上半年,国家互联网应急中心(CNCERT)通过技术平台共捕获约 90 万个恶意代码,比去年同期增长 62.5%;其中新的恶意代码样本 8.9 万个,与去年同期基本相近;通过国内外合作渠道接收到恶意代码样本 49.6 万个。综合各种来源数据并从中去掉重复的恶意代码样本,上半年实际新增样本数达 52.9 万个。数据合作方包括了国内外主要的反病毒厂商,CERT 组织和安全机构,从众多反病毒产品的角度看,与网络游戏相关的恶意代码,恶意代码下载器及灰鸽子家族系列的恶意程序最为突出,对终端用户的威胁也更大。恶意代码的整治是保障网络安全的关键和难点。

信息系统软件的安全漏洞仍是各种安全威胁的主要根源,但层出不穷的应用软件安全漏洞的威胁也越来越大。2008 年上半年,国家互联网应急中心(CNCERT)针对影响较大的共 40 个安全漏洞通过网站发布了漏洞公告,其中部分漏洞直接威胁到互联网基础设施的运行安全,更多的漏洞则严重威胁广大互联网用户的信息系统,如:Realplay 播放器漏洞、联众世界漏洞、暴风影音漏洞等。同时,针对漏洞出现的攻击程序、代码也呈现出目的性强、时效性高的趋势。

综合分析以上情况,当前网络安全形势严峻的原因主要有以下几个:一是由于近年来中国互联网持续快速发展,我国网民数量、宽带用户数量、.cn 域名数量都已经跃居全球第一位,而我国网络安全基础设施建设、民众的网络安全意识培养还跟不上互联网发展的步伐,

庞大的用户群、信息系统群加之粗放式网络安全管理埋下了安全隐患；二是随着技术的不断提高，攻击工具日益专业化、易用化，攻击方法也越来越复杂、隐蔽，防护难度较大；三是互联网业务与现实社会中诸如货币、交易、讯息交互等活动不断融合，为网络世界的虚拟要素附加了实际价值，越来越多的承载这类业务的信息系统成为黑客攻击的目标。

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，国家互联网应急中心(CNCERT)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，国家互联网应急中心(CNCERT)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处理应急事件的能力。

3.1 事件接收情况

2008 年上半年国家互联网应急中心(CNCERT)共接收 3291 件非扫描类网络安全事件报告，其中每月接收的非扫描类事件报告的具体数量如图 1 所示。

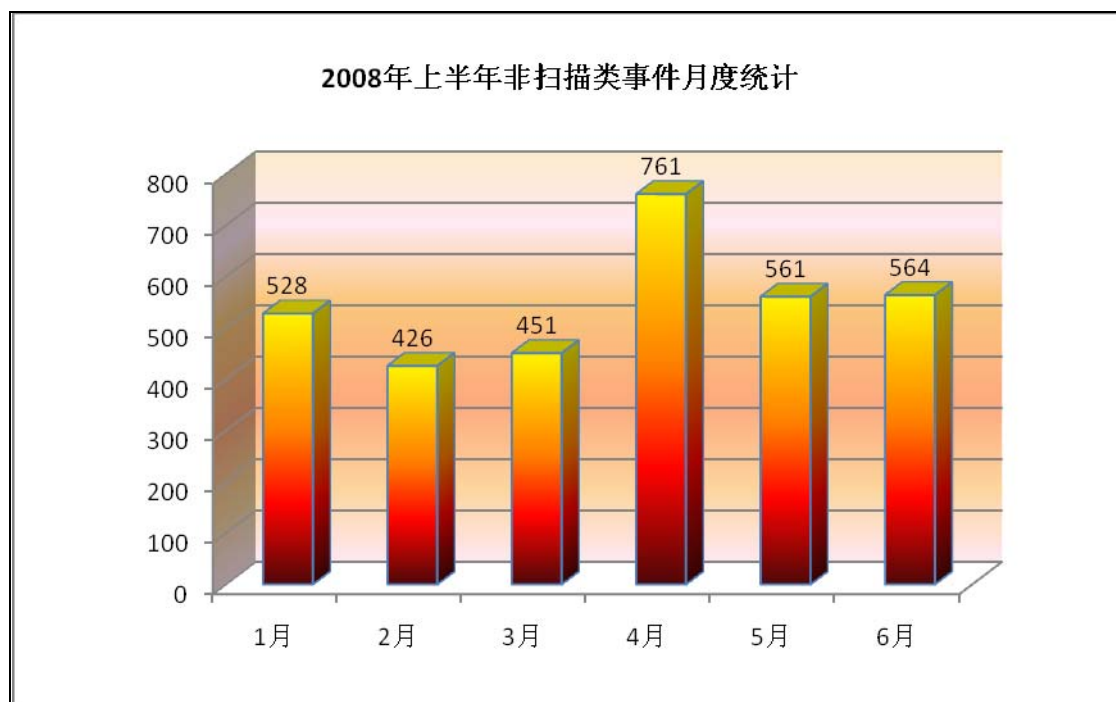


图 1 2008 年上半年非扫描类事件月度统计

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），结果如下：垃圾邮件事件数量最多，共 1218 件，占接收事件总数的 37.01%，同比增长 169%，网页恶意代码事件同比增长 95%；网络仿冒事件的数量达 890 件，占 27.04%，同比增长 38%；漏洞事件为 249 件，占 7.57%；病毒、蠕虫或木马事件达 222 件，占 6.75%；拒绝服务攻击事件为 9 件，比去年同期(13 件)略有下降，占不到

1%。总体情况看来，2008 年上半年所接收的网络安全事件总数与去年同期相比大量增加，而垃圾邮件事件、网页恶意代码事件、网络仿冒事件尤为突出，呈现大幅增长。

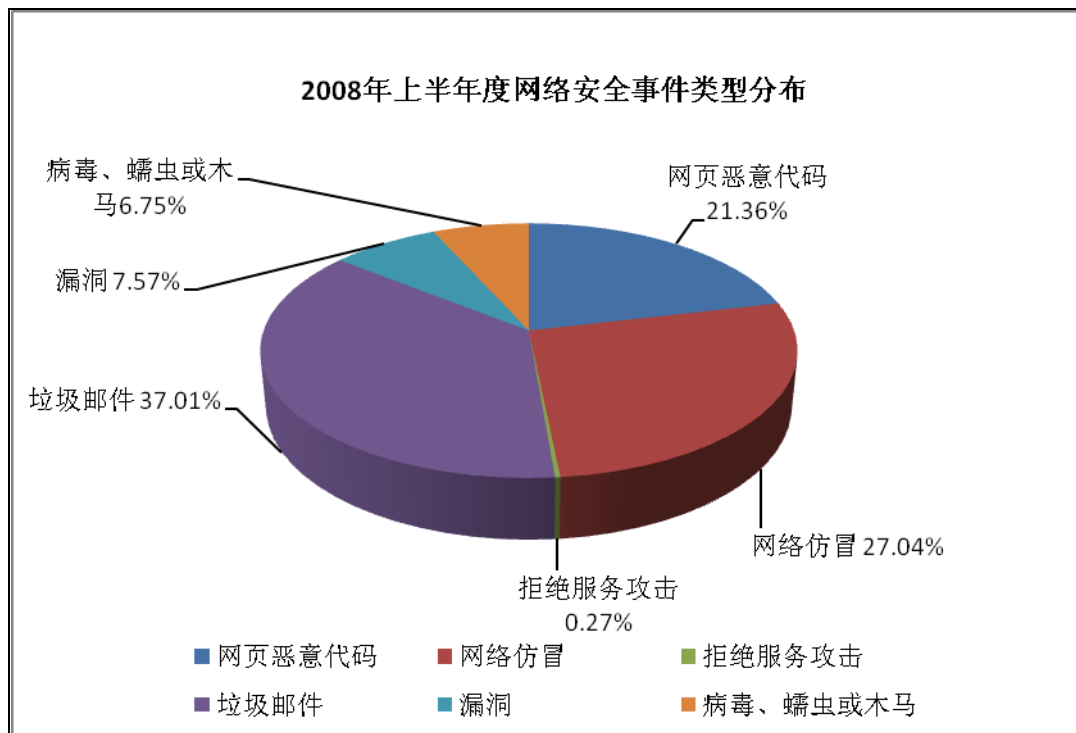


图 2 2008 年上半年网络安全事件类型分布

3.2 事件处理情况

2008 年上半年国家互联网应急中心(CNCERT)共成功处理各类网络安全事件 653 件，事件类型¹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。在国家互联网应急中心(CNCERT)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内外商业机构的网络仿冒类事件数量最多。

¹ 国家互联网应急中心处理的事件中包含自主监测到的事件。

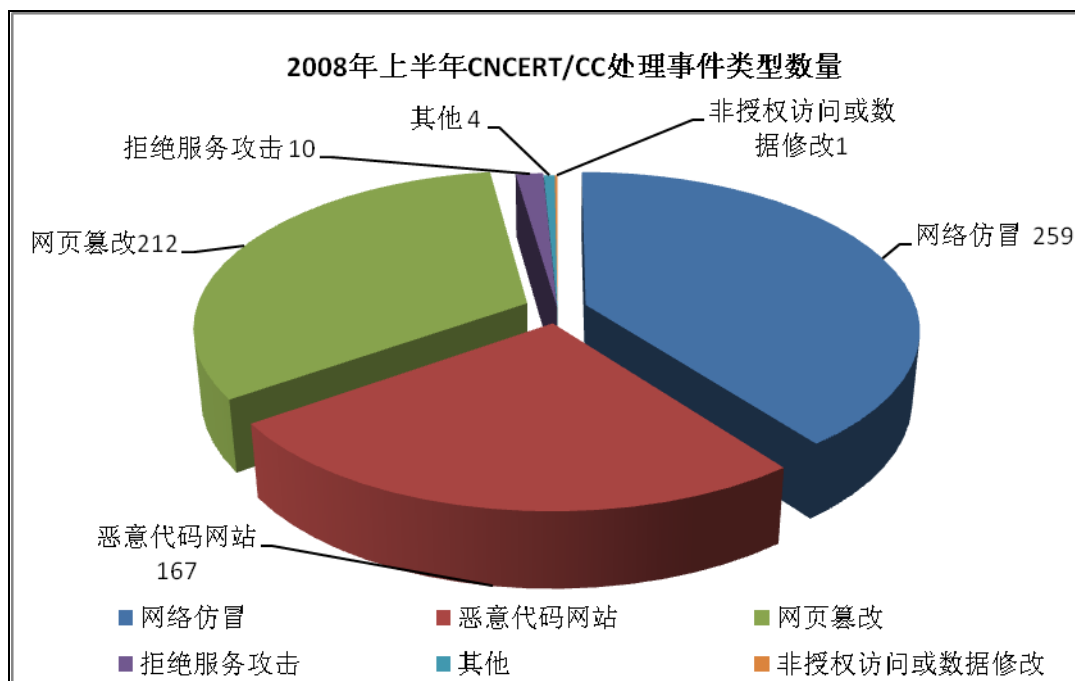


图 3 2008 年上半年国家互联网应急中心(CNCERT)处理网络安全事件数量统计

国家互联网应急中心(CNCERT)一般是通过国家中心（总部）协调其在大陆各省所设分中心来处理安全事件。2008 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，其中辽宁、北京、海南、宁夏和广东处理事件数量居前 5 位。

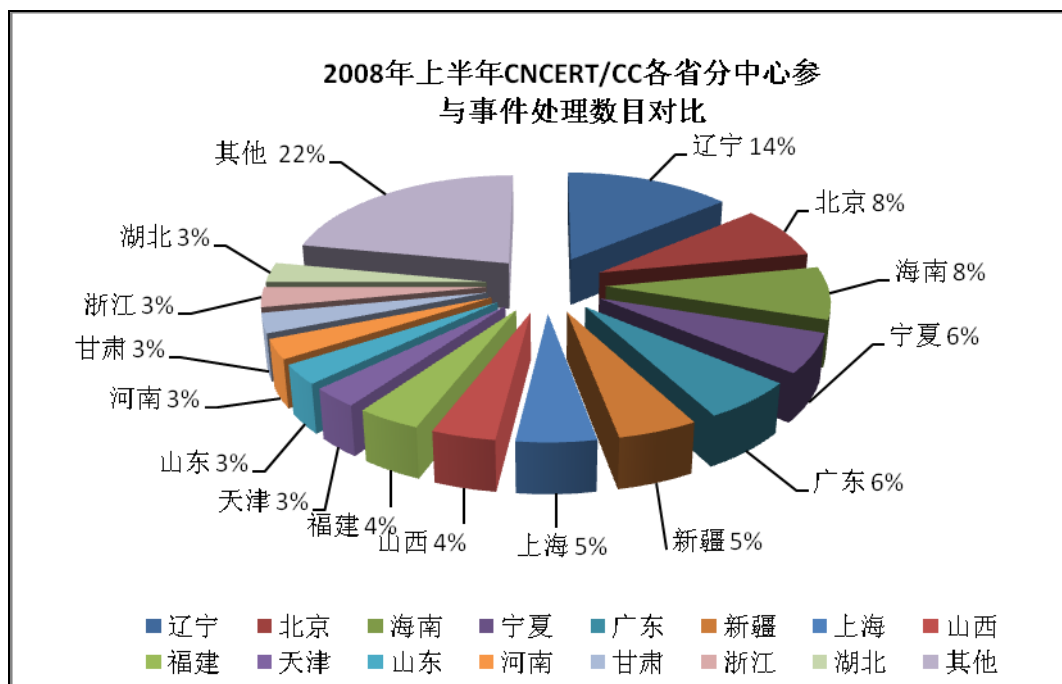


图 4 国家互联网应急中心(CNCERT)各省分中心 2008 年上半年参与事件处理数目对比

3.3 事件处理部分案例介绍

3.3.1 我国某部委互联网基础信息资源网站受攻击事件

国家互联网应急中心(CNCERT)于 2008 年 1 月 3 日监测发现,我国某部委互联网基础信息资源网站受到较大规模的攻击,攻击源来自不同的 C 类网段,分布于广东、江苏、吉林等地。国家互联网应急中心(CNCERT)协调广东、江苏、吉林等分中心,对攻击源进行排查,最终确定了此次攻击发动的多个源头。国家互联网应急中心(CNCERT)迅速向相关运营商通报了事件情况,并通知相关安全责任人对攻击流量进行过滤,及时有效地缓解了该信息系统受到的攻击压力。

国家互联网应急中心(CNCERT)还协调各分中心与各省运营商进行联系,对攻击源头主机进行调查取证,并依照相关处理流程和办法对涉嫌攻击的 IP、主机进行了处理。2008 年 1 月 7 日,完成全部主机的处置工作,经监测,受害信息系统流量与安全状况未见异常。

3.3.2 “机器狗”病毒事件处理

2008 年 3 月 10 日,国家互联网应急中心(CNCERT)捕获到一些恶意代码样本,经研判,这些样本的某些特征与“机器狗”病毒特征相符。该病毒可以给用户的电脑下载大量的木马、病毒、恶意软件、插件等。一旦“中招”,用户的电脑便随时可能感染任何木马、病毒,这些木马病毒会疯狂地盗用用户的隐私资料(如帐号密码、私密文件等),也会破坏操作系统,使用户的机器无法正常运行。该病毒还可以通过内部网络传播、下载 U 盘病毒和 ARP 攻击病毒,能引发整个网络的电脑全部自动重启。

通过对感染该病毒样本的主机 IP 进行排查,发现此病毒触发的 IP 在国内分布呈局部化、分散化的特点,国内感染主机分布于广东、河南、广西、黑龙江、海南等省份。感染病毒的 IP 基本上同属于一个 C 类网段,连接地址都是非常近似的,并有不断扩张的趋势。

国家互联网应急中心(CNCERT)及时启动事件处理流程,将感染“机器狗”病毒的 IP 地址段下发到各分中心,协调各分中心对感染恶意代码的计算机进行排查,并进行逆向分析,得到木马控制端用户及主机的详细信息。通过对上述主机的定位与分析,国家互联网应急中心(CNCERT)协调天津、重庆、江苏、海南、吉林各分中心及当地运营商及时进行调查取证,掌握了相关证据后对涉及传播恶意代码的主机及域名进行了处理,并及时通知感染此病毒的互联网用户对主机进行杀毒、加固等清理工作。2008 年 4 月 1 日,通过监测对比发现,病毒感染的势态已经得到有效遏制。

3.3.3 国内某政府网站被挂马事件

2008 年 4 月 29 日,国家互联网应急中心(CNCERT)通过监测发现,某省某部门网站首页被挂载木马。由于该部门属于国家重要的行政部门,其网站首页挂马会对政府形象及公共安全造成较大影响。国家互联网应急中心(CNCERT)协调该省分中心,立即与该省相关部门取得了联系,将事件有关信息及时做了通报,分析了事件的危害及其可能造成的影响,指出了事件应对的方法,建议有关部门尽快采取措施,消除不良影响。相关责任单位接到通知后,已经采取措施,清除了木马。2008 年 5 月 4 日,经验证,挂马网页链接已恢复正常。

事件处理期间,国家互联网应急中心(CNCERT)及分中心与该省相关部门联系沟通密切,协作配合顺畅,保证了事件得到及时有效地处置。对此,有关单位表示了诚挚的感谢,并希望今后加强与国家互联网应急中心(CNCERT)的合作。

4 信息系统安全漏洞公告及处理情况

国家互联网应急中心(CNCERT)对于漏洞发布予以高度重视,2008 年上半年共整理发布与我国用户密切相关的漏洞公告 40 个,其中对大规模 SQL Injection 事件的处理收效显著,具体情况如下:

2008 年 4 月中旬以来,我国互联网上大量网站遭到 SQL 注入攻击,包括许多政府机构、企事业单位、教育部门等的众多公共网站。国家互联网应急中心(CNCERT)初步研判为黑客采用了某种自动化的 SQL 注入攻击工具,对成千上万存在 SQL 注入漏洞的网站进行攻击,并嵌入恶意代码链接将受害网站的访问用户暗中引向恶意站点,导致用户面临针对多个漏洞(如: Realplay 播放器漏洞、联众世界漏洞、暴风影音漏洞、MS06-014 漏洞)的恶意代码攻击,一旦攻击成功,用户计算机就将被植入恶意代码而受到黑客的完全控制。

国家互联网应急中心(CNCERT)在网站上及时发布关于此次事件的态势信息,并对互联网用户提出一些有效可行的应对措施: (1) 公布监测到的恶意站点列表; (2) 建议网站管理员立即检查并修补网站的 SQL 注入漏洞,如: 被入侵的网站的网页源文件中会看到类似“<script src=http://恶意网站域名/...></script>”的代码,管理员可通过在源文件中查找包括这些恶意网站的方式来简单判断是否已经被攻击; (3)同时,建议广大互联网用户通过修改本地 HOSTS 文件或个人防火墙配置,将恶意站点列入黑名单,阻止本机对这些网址的访问。

通过监测对比,对于其中在我国注册的域名,国家互联网应急中心(CNCERT)协调域名注册商对大部分域名进行了暂停域名解析服务的处理。截止 2008 年 5 月底,共处理了 25 个恶意站点域名,从源头上有效地打击了黑客的据点,成功阻止了 SQL 注入攻击事件在互联网上的大规模扩散。

5 互联网业务流量监测分析

根据国家互联网应急中心(CNCERT)在 2008 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、BitComet、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,占用大量网络带宽。因此,我国需重视此类软件的安全问题。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。

TCP 协议端口流量前十位如图 5 所示:

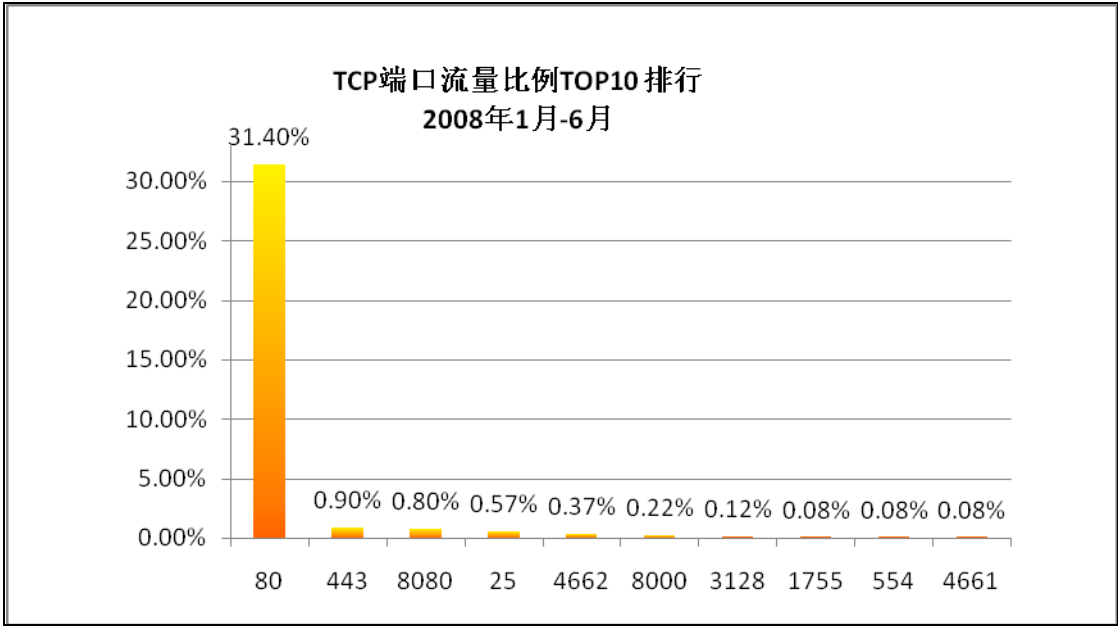


图 5 2008 年上半年 TCP 协议流量端口排名前十位

TCP 端口	TCP 流量排名	百分比	主要的业务种类
80	1	31.40%	网页服务
443	2	0.90%	网页服务
8080	3	0.80%	网页服务
25	4	0.57%	SMTP 默认端口
4662	5	0.37%	P2P 下载软件端口
8000	6	0.22%	QQ 通讯端口
3128	7	0.12%	网页服务
1755	8	0.08%	微软媒体服务
554	9	0.08%	微软媒体服务
4661	10	0.08%	P2P 下载软件端口

表 1 2008 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各类 P2P 软件下载端口，迅雷、eMule、BT 等 P2P 软件占用较大带宽。使用 UDP 协议的 DNS 服务，也占有较大流量，占 UDP 端口总流量的 1.34%。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，密切关注各大厂商发布的 DNS 漏洞，做好系统更新、升级、加固的工作。

UDP 协议端口流量前十位如图 6 所示。

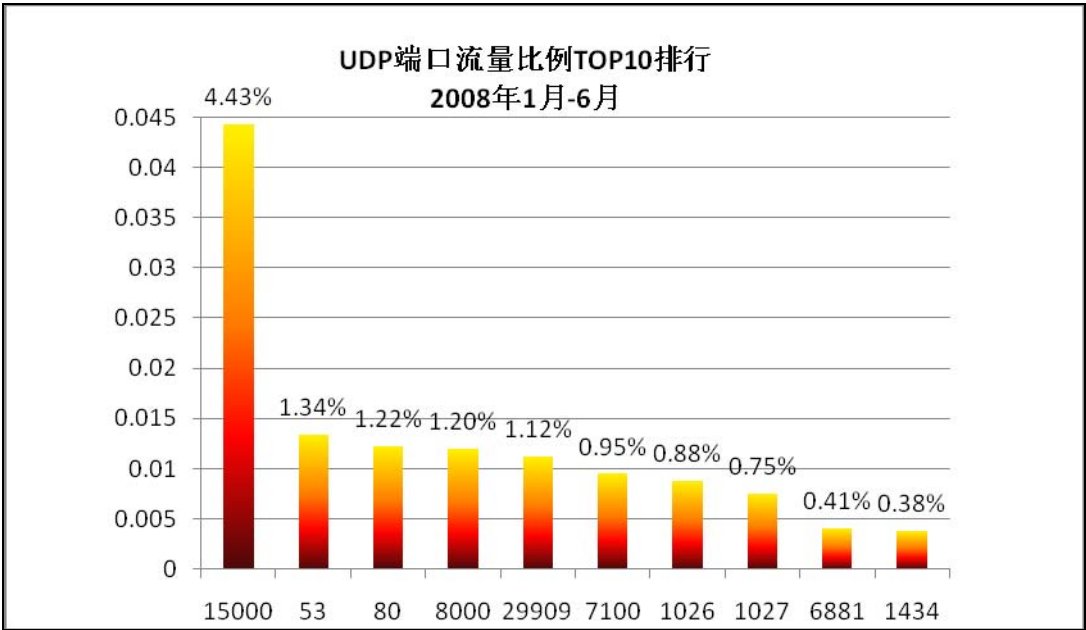


图 6 2008 年上半年 UDP 协议流量端口排名前十位

UDP 端口	UDP 流量排名	百分比	主要的业务种类
15000	1	4.43%	P2P 下载软件端口
53	2	1.34%	DNS 服务端口
80	3	1.22%	网页服务
8000	4	1.20%	QQ 通讯端口
29909	5	1.12%	未知端口
7100	6	0.95%	网络游戏通讯端口
1026	7	0.88%	MS Messenger 端口
1027	8	0.75%	MS Messenger 端口
6881	9	0.41%	P2P 下载软件端口
1434	10	0.38%	SQL Server Resolution 服务端口

表 2 2008 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，因此国家互联网应急中心(CNCERT)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。国家互联网应急中心(CNCERT)在 2008 年上半年抽样监测到，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 280068 个，被控制端 IP 地址总数为 1485868 个。

6.1.1 中国大陆地区被木马控制的计算机分布统计

2008年上半年，国家互联网应急中心(CNCERT)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302526个IP地址的主机被植入木马。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河北省（10%）、北京市(10%)、山东省（9%）、江苏省（9%）和广东省（9%）。

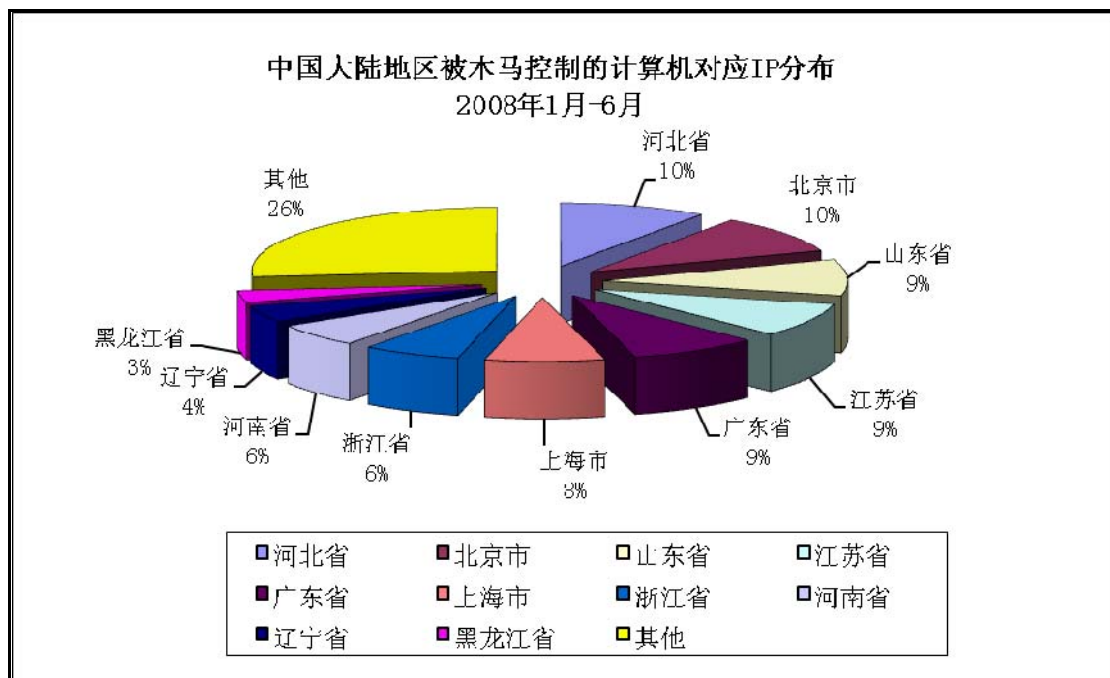


图 7 2008 年上半年中国大陆地区被木马控制的计算机 IP 分布图

6.1.2 中国大陆地区外木马控制端分布统计

国家互联网应急中心(CNCERT)监测发现大陆地区外98230个主机地址参与控制我国大陆被植入木马的计算机，与去年同期相比增长26.4%。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（65%）、美国（8%）、中国香港（5%）、韩国（3%）和越南（2%）的木马控制端数量居前五位。

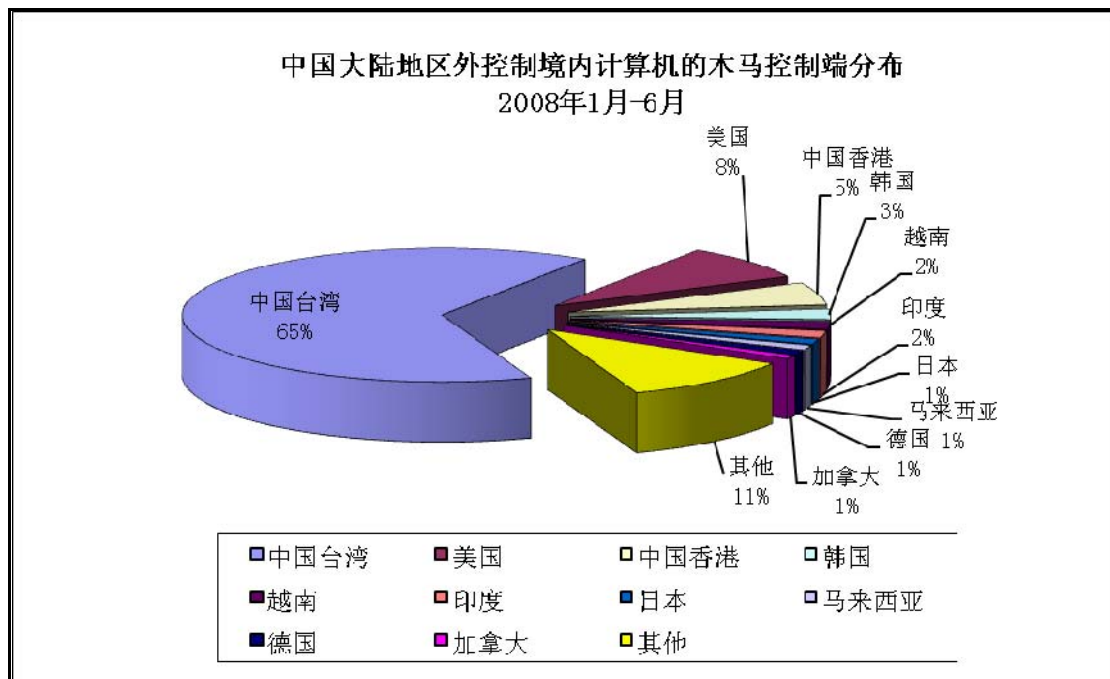


图 8 2008 年上半年通过木马控制我国计算机的境外 IP 分布图

6.2 僵尸网络数据分析

国家互联网应急中心(CNCERT)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，2008 年上半年抽样监测发现境内外约有 2 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

2008 年上半年，国家互联网应急中心(CNCERT) 共发现 2270 个境外控制服务器对我国大陆地区的主机进行控制，按国家和地区分布如图 9 所示，前五位的地区分别是：美国占 33%、韩国占 12%、加拿大占 6%、英国占 6%以及法国占 4%。

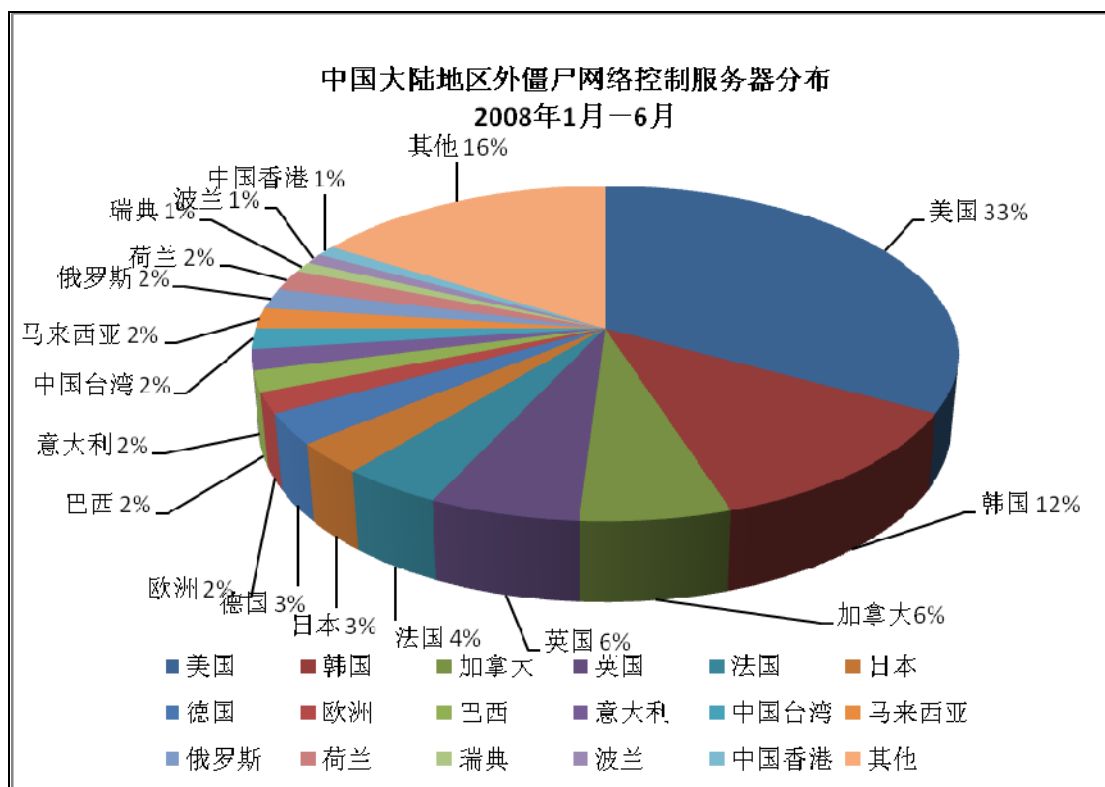


图 9 2008 年上半年中国大陆地区外僵尸网络控制服务器分布图

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。2008 年上半年，国家互联网应急中心(CNCERT)通过技术手段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。

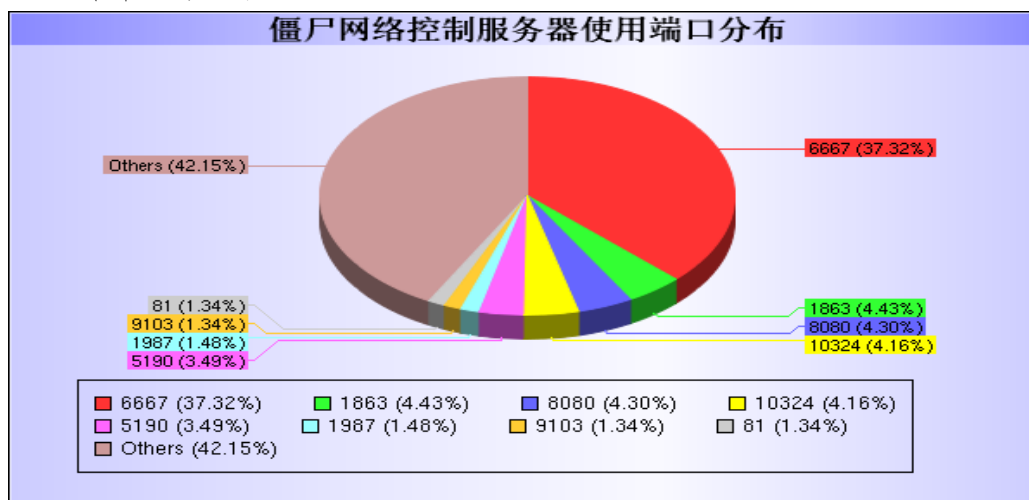


图 10 2008 年上半年僵尸网络控制服务器使用端口分布图

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。傀儡主机数量在1千以内规模的僵尸网络居多。2008年上半年监测到的僵尸网络规模数量分布如

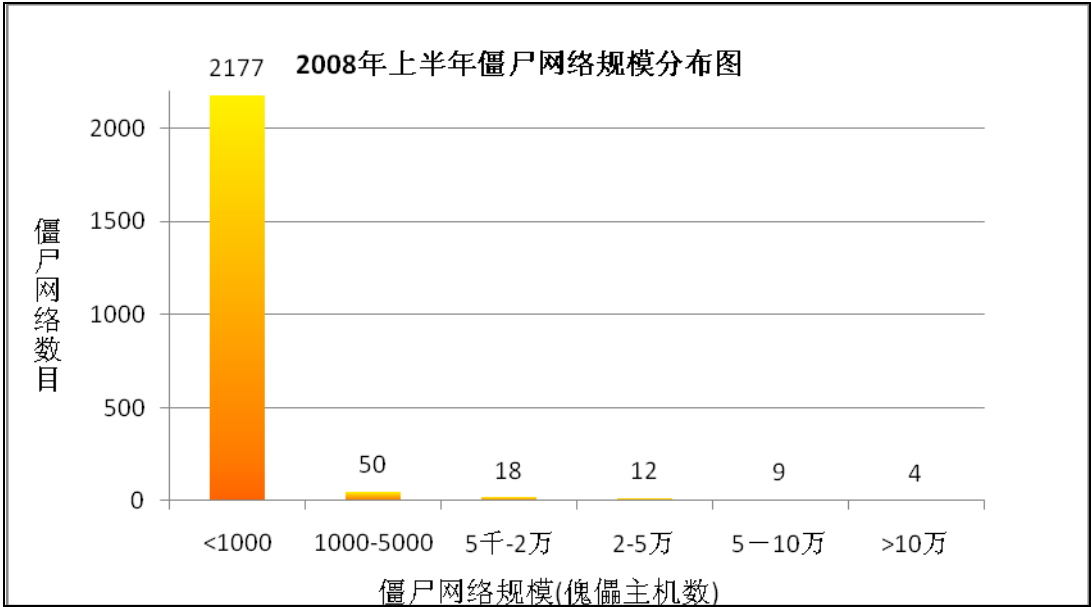


图 11所示。

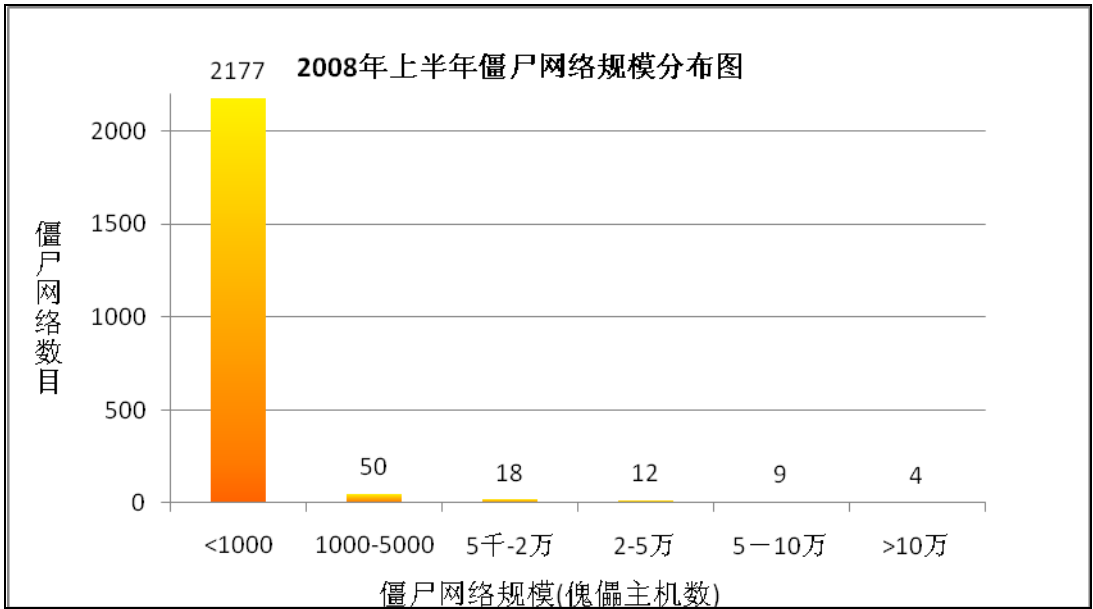


图 11 2008 年上半年僵尸网络规模分布图

7 被篡改网站监测分析

从 2003 年国家互联网应急中心(CNCERT)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

2008 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。国家互联网应急中心(CNCERT)监测到中国大陆被篡改网站总数达到 35113 个，同比增加了 23.7%。按月统计情况如图 12 所示。

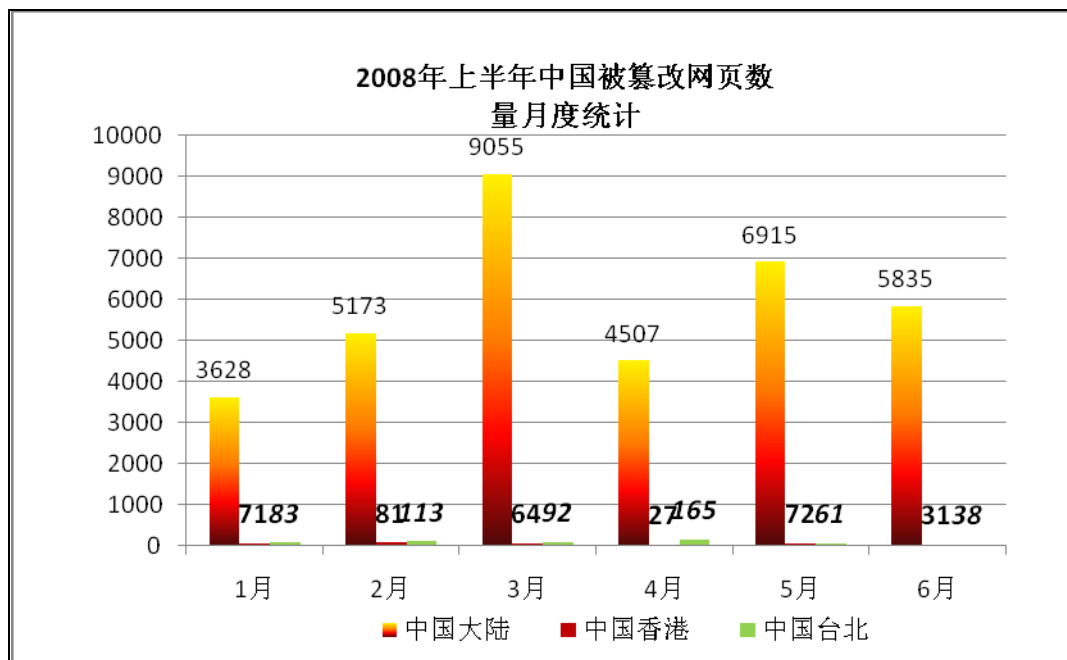


图 12 2008 年上半年中国被篡改网站数量

7.2 我国大陆地区政府网站被篡改情况

2008 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 2242 个。与去年上半年同期监测情况相比，增加了 41%。2008 年上半年中国大陆被篡改的网站中政府网站的数量及其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 域名网站约占整个大陆地区被篡改网站的 7%，而 gov.cn 域名网站仅占.cn 域名的 2.3%²，因此政府网站仍然是黑客攻击的重要目标。

²该数据来自中国互联网络信息中心（CNNIC）2008 年 7 月第 22 次《中国互联网络发展状况统计报告》。

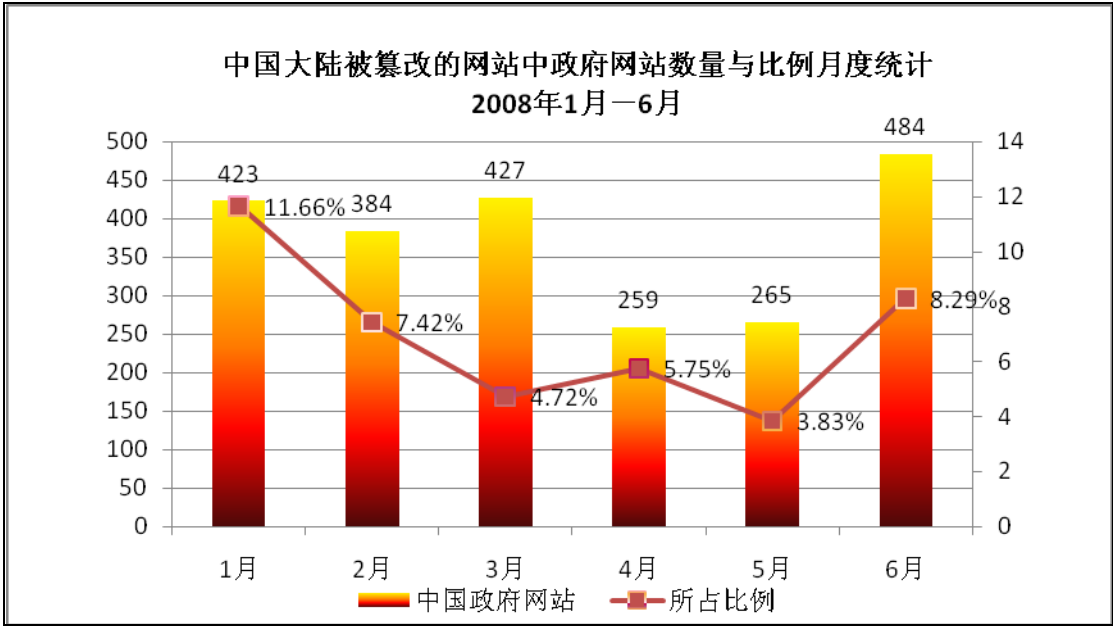


图 13 2008 年上半年中国大陆被篡改的网站中政府网站的数量及其所占比例

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。

7.3 对我国网站实施篡改攻击的主要黑客情况

2008 年上半年，国内外黑客（组织）对我国网站攻击频繁，平均每天就有数百起的网站被黑以及网页被篡改事件发生。2008 年 1 月至 6 月我国大陆地区网站被篡改数量如图 12 分布，可以看到，3 月和 5 月网站被攻击事件发生最为频繁，被篡改网站数量分别为 9055 个和 6915 个。

在对我国网站实施攻击的黑客（组织）中，统计各月篡改攻击排名前 5 名的情况如表 3 所示，可以看到，reDMin、sinaritx、roselare 等较为活跃。

月份	攻击者	篡改网站数量	攻击者所在国家和地区
2008 年 1 月	lucifercihan	316	土耳其
	iskorpitx	242	土耳其
	波哥 VS 布冯	191	中国湖南
	逍遥游	142	中国湖南
	reDMin	83	土耳其
2008 年 2 月	lucifercihan	698	土耳其
	ZoRRoKiN	362	土耳其

	sinaritx	304	土耳其
	reDMin	247	土耳其
	iskorpitx	132	土耳其
2008 年 3 月	reDMin	2191	土耳其
	sinaritx	1121	土耳其
	roselare	752	土耳其
	lucifercihan	507	土耳其
	网络小子	313	中国湖北
2008 年 4 月	sinaritx	303	土耳其
	搁浅	281	中国广东
	roselare	208	土耳其
	黑枫无泪	196	中国浙江
	reDMin	135	土耳其
2008 年 5 月	霸业永峰	1152	中国
	Mistakes@[D.R.T]	403	中国广东
	roselare	348	土耳其
	幽魂	326	中国
	d3triment@l	245	土耳其
2008 年 6 月	roselare	624	土耳其
	GUARD_FB	434	土耳其
	reDMin	405	土耳其
	sinaritx	294	土耳其
	aLpTurkTegin	290	土耳其

表 3 按月统计篡改网站的黑客前 5 名

按半年统计，排名前 10 位的如表 4 所示，结合月度统计分析，可以看到黑客（组织）活动既有持续性又有一定的间歇性；最活跃的网页篡改黑客（组织）主要来自土耳其。

攻击者	篡改网站数量	攻击者所在国家和地区
reDMin	3148	土耳其
Sinaritx	2225	土耳其
Roselare	2013	土耳其
lucifercihan	1536	土耳其
霸业永峰	1381	中国
aLpTurkTegin	735	土耳其
网络小子	687	中国湖北
ZoRRoKiN	625	土耳其
GUARD_FB	619	土耳其
波哥 VS 布冯	582	中国湖南

表 4 2008 年上半年对我国网站进行篡改攻击的黑客排名

8 网络仿冒事件情况分析

2008 年上半年国家互联网应急中心(CNCERT)共接到网络仿冒事件报告 645 件，成功处理了 237 件。被仿冒的网站大都是国外的著名金融交易机构。表 5 列出了被仿冒次数居前 5 名的网站，表 6 列出了向国家互联网应急中心(CNCERT)报告网络仿冒事件数量居前 5 名的组织机构。

被仿冒网站	数量
eBay (美国网上交易站点)	120
hsbc (汇丰银行)	118
Paypal (美国网上支付站点)	82
wachovia (美联银行)	19
yahoo (美国门户网站)	14

表 5 被仿冒网站前 5 名

网络仿冒事件报告者	数量
eBay(美国网上交易站点)	147
Hsbc(汇丰银行)	113
cyf-kr.edu.pl(CYFRONET AGH 信息中心)	86
RSA(RSA 信息安全公司)	39
fiducia.de(德国信息安全组织)	38

表 6 向国家互联网应急中心(CNCERT)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，国家互联网应急中心(CNCERT)从 2006 年开始陆续在全国部署 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。

2008 年 1 月到 6 月，共捕获恶意代码样本总数 899607 次，平均每天捕获 4942 次，图 14 给出了每日的样本捕获趋势。

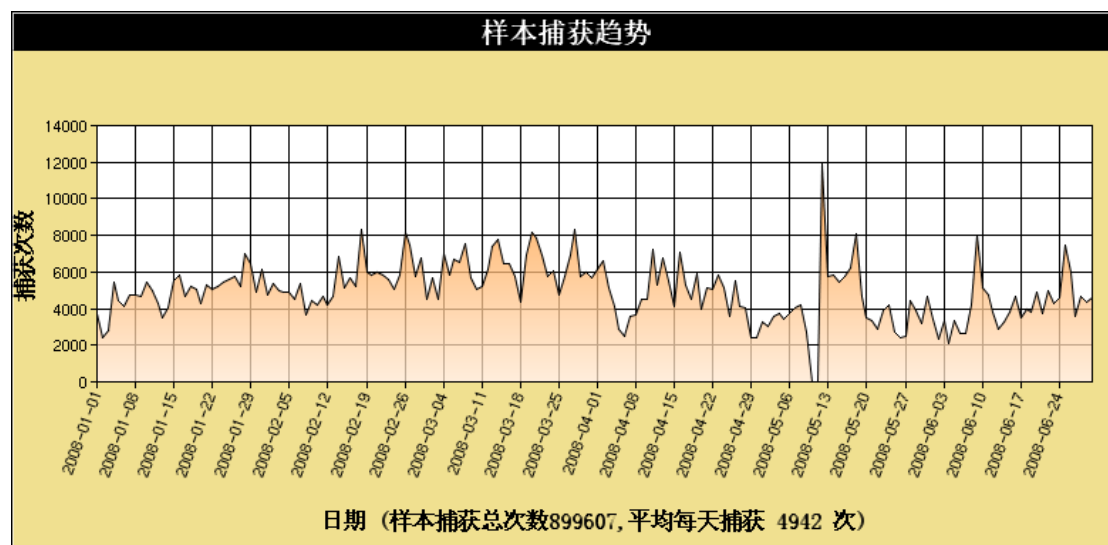


图 14 分布式蜜网样本捕获趋势图

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。2008 年 1 月到 6 月，共捕获不重复的恶意代码新样本总数 88580 个，平均每天捕获 489 个，图 15 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。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。

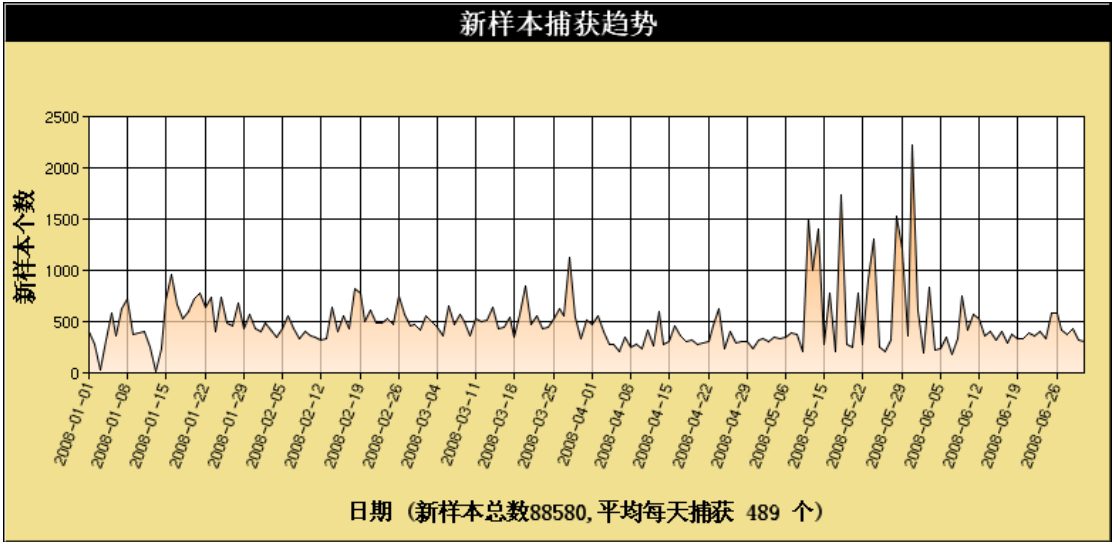


图 15 分布式蜜网新样本捕获趋势图

2008 年 1 月 1 日至 6 月 30 日期间，蜜网捕获的恶意代码样本中捕获次数位于前十位的恶意代码如表 7 所示：

排名	恶意代码名称	总捕获次数
1	Virus.Win32.Virut.n	42873
2	Net-Worm.Win32.Allapple.b	30215
3	Porn-Dialer.Win32.InstantAccess.dan	24435
4	Trojan.Win32.Qhost.aei	20349
5	Backdoor.Win32.VanBot.ax	18793
6	Trojan-Downloader.VBS.Small.gg	18224
7	Backdoor.Win32.SdBot.cpl	16280
8	Net-Worm.Win32.Allapple.e	42873
9	Virus.Win32.Sality.z	30215
10	Backdoor.Win32.EggDrop.au	24435

表 7 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。

此外，国家互联网应急中心(CNCERT)通过国内、国际合作渠道接收恶意代码样本 495911 个，日均 2724 个，按月统计数据如表 8 所示：

月份	1 月	2 月	3 月	4 月	5 月	6 月
恶意代码数量	41731	29301	62390	71981	97145	193363

表 8 CNCERT/CC 通过合作渠道获得的恶意代码月度统计

10 国家互联网应急中心(CNCERT)网站信息发布

CNCERT/CC 网站是国家互联网应急中心(CNCERT)对外公开提供网络安全信息服务的重要窗口。2008 年 1 月至 6 月,国家互联网应急中心(CNCERT)通过网站发布了 148 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。

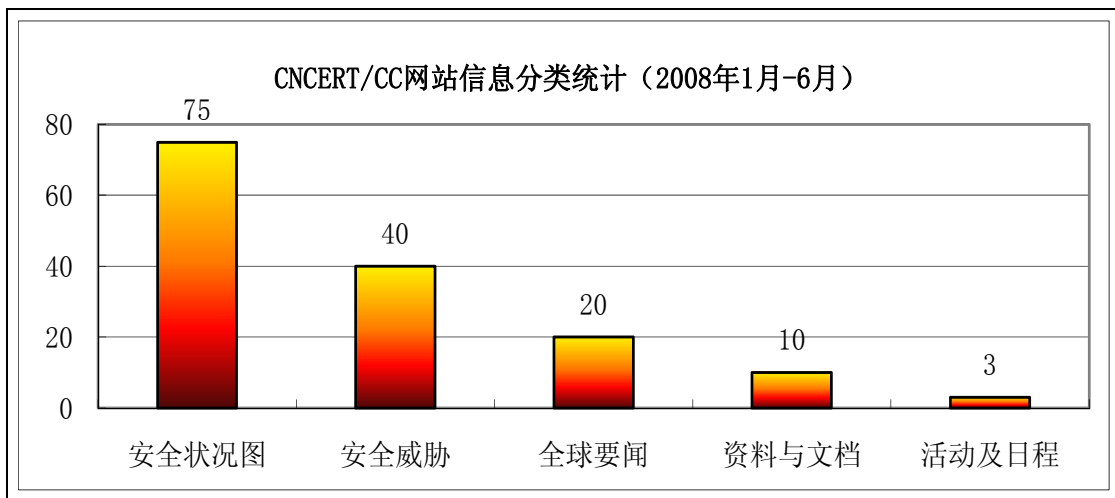


图 16 2008 年上半年国家互联网应急中心(CNCERT)网站信息分类统计

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处理协调中心(国家互联网应急中心(CNCERT))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,初步形成了以国家互联网应急中心(CNCERT)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,国家互联网应急中心(CNCERT)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 2008 年 7 月，我国目前有应急组织 59 家，如表 9 所示³。其中，在中国应急组织社区登记的应急组织共 32 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
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
北京万网志成科技有限公司(中国万网)*	HERT
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
上海中科网威信息技术有限公司*	Netpower
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
武汉大学省级应急服务支撑中心*	WHUPCERT
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	

³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。

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 9 我国网络安全应急组织名称

11.2 国家互联网应急中心(CNCERT)组织的相关重要活动

2008 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深圳顺利召开

2008 年 4 月 7 日~9 日,由国家计算机网络应急技术处理协调中心联合中国互联网协会网络与信息安全工作委员会主办的“2008 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”在深圳市西丽湖畔胜利召开。工业和信息化部奚国华副部长到会祝贺并作题为“加强网络安全、助力北京奥运”的主旨报告;中国工程院何德全院士和孙玉院士、国家互联网应急中心(CNCERT)王秀军主任、广东省通信管理局古伟中局长、工业和信息化部赵志国副局长、公安部十一局邓宏敏副局长,奥组委技术部贾胜文副部长、深圳市政府高国辉副秘书长、APCERT 古炜德副主席出席大会并做重要发言。来自国家网络安全管理部门,网络安全科研、产业机构,海关、税务、电信、金融等重要信息系统单位,国内网络安全应急组织以及东盟等十二个国家和地区的 300 余名代表参加了本次年会。

除全体大会外,本次年会共设有“电子政务安全”、“电子商务和金融安全”、“ISP&ICP 安全”、“网络安全信息技术”四个分论坛,与会领导、专家、学者围绕电子政务和电子商务安全、基础信息网络安全保障、培育健康有序的网络安全文化、网络安全应急的国际合作、重点城市的网络安全事件应急处置、安全漏洞的现状与发展趋势等诸多话题进行了广泛而深入的交流与探讨。

奚国华副部长在报告中指出：今年是全面贯彻落实十七大战略部署的第一年，也是奥运之年。在互联网蓬勃发展的形势下，努力构建健康、和谐的网络环境，做好奥运网络安全保障，保障信息化进程的健康推进是全社会共同的责任和义务。为进一步提高国家网络安全水平，奚副部长提出五点要求：一、深刻认识新形势下做好网络安全工作的重要性和紧迫性；二、全力以赴做好奥运网络安全保障工作；三、进一步完善网络应急处理协调机制；四、着力加强网络安全队伍建设和技术研究；五、进一步加强网络安全国际交流与合作。何德全院士在致辞中强调：网络安全应急是国家应急工作的重要组成部分，应适时总结已有工作成果，理清未来发展思路，使其得到切实有效地加强。孙玉院士所做题为“电信网络机理分类及安全属性分析”的专题报告，从电信基本原理出发阐述了电信网面临的安全威胁及解决办法。赵志国局长在“加强基础信息网络安全保护”的报告中，从行业主管部门的角度阐释了加强基础信息网络安全保护的必要性、重要性及有关政策。邓宏敏副局长、贾胜文副部长和古炜德副主席对大会的召开表示祝贺，并充分肯定了本次年会对打击网络犯罪、奥运网络安保和亚太网络应急体系建设的积极意义。

国家互联网应急中心(CNCERT)联合 ISCCC 举行国内信息安全服务资质认证评审

2008 年 6 月，国家互联网应急中心(CNCERT)联合中国信息安全认证中心（ISCCC），在国家互联网应急中心(CNCERT)去年评选的应急服务支撑单位基础上开展国家信息安全应急处理服务资质认证授权工作。2007 年 6 月，“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，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。本次国家信息安全应急处理服务资质认证授权工作的展开，有助于提高 CNCERT/CC 网络安全应急服务支撑体系的行业地位和影响力，并将已建立的应急服务支撑体系纳入到国家网络与信息安全服务认证体系中。将“CNCERT/CC 网络安全应急服务支撑单位”资质纳入国家信息安全认证认可体系进行统一管理，有利于推动国家互联网应急中心(CNCERT)网络安全应急服务支撑单位向国家资质转化，对进一步树立国家网络安全应急服务体系的权威性，推动网络安全应急服务行业的健康发展具有重要意义。

这次活动还表明，中国已开始对信息安全服务资质进行分级分类管理，这也是我国信息安全领域中的一项重要制度创新，它将为我国信息安全保障体系建设发挥重要作用。采用认证模式对信息安全服务资质进行管理适应政府行政体制改革的方向，符合 WTO 背景下的国际通行规则，更便于统一管理，更易实现我国设定的对信息安全服务资质的管理目标。

经过严格的评审，本次活动共评选出 6 家企业获得应急处理服务一级资质认证，16 家企业分获二级、三级资质认证。

以下单位获得应急服务一级资质认证：

北京启明星辰信息技术有限公司
北京天融信科技有限公司
北京神州绿盟科技有限公司
沈阳东软系统集成工程有限公司
北京安氏领信科技发展有限公司
浪潮集团有限公司

以下单位获得应急服务二级资质认证：

上海中科网威信息技术有限公司
成都思维世纪科技有限责任公司
哈尔滨安天科技股份有限公司
上海三零卫士信息安全有限公司

北京万网志成科技有限公司
广东科达信息技术有限公司
杭州思福迪信息技术有限公司
中国电信股份有限公司四川分公司
深圳市任子行网络技术有限公司
山东新潮信息技术有限公司
西安安智科技有限公司
上海谐润网络信息技术有限公司
太原理工天成电子信息技术有限公司
江苏南大苏富特软件股份有限公司
联创科技（南京）有限公司
以下单位获得应急服务三级资质认证：
北京江南博仁科技有限公司

12 国际合作与交流

APEC-TEL37 会议在东京召开 国家互联网应急中心(CNCERT)主持反僵尸网络研讨会

APEC-TEL37 次会议于 2008 年 3 月 23 日至 28 日在日本东京召开，国家互联网应急中心(CNCERT)派出 5 人与国内其他单位人员共 12 人参加了会议。国家互联网应急中心(CNCERT)参会人员作为安全工作组代表出席了全会和 SPSG 工作组会议。会议期间，由国家互联网应急中心(CNCERT)承办的僵尸网络应对技术研讨会在 SPSG 分会场成功召开。会议议题围绕“僵尸网络技术现状和发展趋势”、“反僵尸网络的技术对策”、“反僵尸网络的管理对策”以及“反僵尸网络工作的最佳实践”等展开。

会议讨论议题得到参会者广泛的关注和积极响应，对促进亚太地区政府和业界的交流合作、推动公众安全意识教育起到了积极作用；同时，宣传了我国在网络安全应急处理体系下，在政府和非政府层面致力于反僵尸网络工作付出的各项努力，扩大了我国在该方面的国际影响。本次专题研讨是我国首次在 APEC-TEL 会议上独立承办正式的研讨会，虽然没有成熟的经验可借鉴，国家互联网应急中心(CNCERT)竭尽全力做好各项前期准备、会场协调及后续总结报告等一系列工作，保证了会议的圆满举办。

国家互联网应急中心(CNCERT)于 2007 年 3 月在 APEC-TEL35 次会议上申请了“僵尸网络的治理策略和技术手段指南”项目，在本次会议上，国家互联网应急中心(CNCERT)对该项目的工作进展情况进行了汇报。僵尸网络问题引起了会议较为广泛的关注，各方对我们项目最终的输出成果寄予了较高的期待。在 SPSG 工作组会议上，各经济体还分别汇报了已承担项目的进展情况，会议同时对澳大利亚新申请的项目“提升网络安全意识教育”进行了研究，该申请取得了众多经济体的支持；国家互联网应急中心(CNCERT)同时指出了需要考虑在公众教育方面如何面对不同语言障碍的问题。会议还对新的热点问题进行了交流，包括：对网络基础设施的滥用，评估虚拟世界的安全性需求，海底光缆的相关问题探讨等。

国家互联网应急中心(CNCERT)接待匈牙利代表团来访 双方达成初步合作意向

2008 年 5 月 19 日至 20 日，匈牙利 CERT 代表团来访，对我国互联网网络安全情况和应急处置工作进行考察。5 月 19 日，国家互联网应急中心(CNCERT)在部应急指挥中心大楼举行会议，双方就目前关心的网络安全与应急处置问题进行了充分地交流。国家互联网应急中心(CNCERT)向匈方介绍了中国网络安全基本形势和应急体系框架、中国网络安全监测和

事件处置方面的工作以及中国互联网协会的反垃圾邮件工作等。匈方介绍了匈牙利 CERT 的发展历程、承担的职责、国内与国际合作情况以及提供的网络安全基础服务和按需提供的增值服务等内容。围绕“重要信息基础设施保护”、“公众安全意识教育开展”等议题，匈方重点介绍了其与银行业的合作模式、现状和远景，并重点介绍了由其建立并运行的专门负责安全意识教育的网站情况。通过交流，双方对工作中面临的挑战取得了一致认识，在今后增进信息和技术交流方面达成初步合作意向。双方还在开展日常的网络安全信息共享、网络安全软硬件能力建设等方面达成初步合作意向。对促进中国在国际上的网络安全协作领域，匈方表示愿意搭建中国与更多西方国家的桥梁，宣传中国网络安全领域的工作和付出的努力。匈方还邀请并愿意协助中国成为 Meridian 会议（CIIP 年会）的成员。

5 月 20 日，经国家互联网应急中心(CNCERT)协调，中国互联网信息中心(CNNIC)和中国万网分别接待了匈牙利代表团成员。CNNIC 专家向匈方介绍了其工作职责、中国的域名体系建设以及面临的安全威胁和防范措施等内容。中国万网作为国内最大的域名和虚拟主机服务提供商，介绍了其业务种类、面临的威胁以及与国家互联网应急中心(CNCERT)的合作情况。通过拓展交流，匈牙利代表团人员从多角度了解我国的互联网发展现状和网络安全的发展趋势，为增进了解、促进合作奠定基础。

第二十届 FIRST 大会在温哥华召开 国家互联网应急中心(CNCERT)作专题研究报告

6 月 21 日，国家互联网应急中心(CNCERT)派代表团参加在加拿大温哥华市举行的第二十届 FIRST 大会，会上国家互联网应急中心(CNCERT)与国际及其他国家 CERT 组织以及 ShadowServer 等民间安全组织深入交换了对当前互联网网络安全的意见，并达成多项数据与信息共享意向。会上国家互联网应急中心(CNCERT)的周勇林和王明华分别做了题为“CNCERT 蜜网技术”、“中国挂马网站研究”的专题报告，向与会代表介绍中国应急组织建设和发展的经验以及近些年来取得的成果，国家互联网应急中心(CNCERT)的报告受到国际社会的好评与认可，FIRST 同期刊登会议专题介绍国家互联网应急中心(CNCERT)的观点。

13 结束语

2008 年是奥运年，同时也是我国政治、经济、社会发展的关键一年。互联网在中国持续快速发展，截至 2008 年 6 月底，中国网民数量达到 2.53 亿，首次大幅度超过美国，跃居世界第一位；宽带网民数量达到 2.14 亿人，也跃居世界第一；中国的域名总数为 1485 万个，其中.cn 域名注册量已达 1190 万个，超越德国.de 域名，成为全球第一大国家顶级域名。互联网已成为重要的国家基础设施，在国民经济建设中发挥着日益重要的作用⁴。随着我国政府信息化基础建设的推进，信息公开程度的提升，网络和信息安全也已成为关系到国家安全、社会稳定的重要因素，社会各界都对网络安全提出了更高的要求，采取有效措施，建设安全、可靠、便捷的网络应用环境，维护国家网络信息安全，成为社会信息化进程中亟待解决的问题。

根据国家互联网应急中心(CNCERT)2008 年上半年监测的情况分析，上半年整体安全态势平稳，但垃圾邮件、网络仿冒、网页篡改等网络安全事件较以往均有明显增加，网络攻击带有的目的性、趋利性不断增强。木马、僵尸网络随着网络用户和网络资源的大量增加而极具扩散性，并且呈专业化、局部化和小型化的趋势。木马与僵尸网络的地下产业链继续扩大，

⁴该数据来自中国互联网络信息中心(CNNIC)2008 年 7 月第 22 次《中国互联网络发展状况统计报告》。

以获取利益为目的的僵尸网络、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，网页篡改事件和拒绝服务攻击事件数量递增的趋势仍将持续。IT 技术的不断革新，也伴随各种系统漏洞的大量存在和不断发现，而攻击手段与攻击时效也在不断提高，使得网络安全问题变得更加错综复杂，网络安全防御更加困难。

应对当前存在的网络安全问题，没有一劳永逸的解决方法。国家重要信息系统相关部门、政府机关、各企事业单位可以从以下方面着手做好网络安全工作：重视网络安全应急组织建设、重视与国内相关网络安全应急组织的交流协作；提升信息化管理水平，加强内部的网络安全管理；密切关注网络安全的态势与技术发展，做好信息系统的运行维护与安全防护工作；做好用户网络安全教育培训，提高用户安全意识。总之，做好网络安全保障工作，不仅要靠信息化基础硬件设施的投入，还需要着重打造网络安全的软环境。

作为国家基础网络安全保障的重要技术支撑部门，国家互联网应急中心(CNCERT)将在工业和信息化部领导下，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处理，积极拓展并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。