CNCERT/CC
2005 年网络安全工作报告

CNCERT/CC

国家计算机网络应急技术处理协调中心

CNCERT/CC

目　录

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）是从事网络安全应急协调处理的非盈利组织。CNCERT/CC 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。

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，并在 2005 年的 APCERT 指导委员会换届选举中，当选为 APCERT 第一任副主席。CNCERT/CC 有条件及时与国外应急小组和其他相关组织进行交流与合作，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安全技术，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：+86 10 8299 0999，8299 1000（英文）
传真：+86 10 8299 0375
PGP Key：http://www.cert.org.cn/cncert.asc

2. 网络安全监测与分析

网络安全监测是通过各种手段对网络安全信息进行搜集、分析与判断。CNCERT/CC 建设并运行的 863-917 网络安全监测平台是我国网络安全事件监测的核心平台，目前已经实现对网络安全事件 7x24 小时不间断监测，并及时汇总我国公共互联网络安全事件信息。CNCERT/CC 还与多家网络安全研究机构合作，及时获得网络安全事件动态信息和蠕虫、木马等恶意代码样本和特征，为在第一时间进行监测创造了有利条件。

2.1. 漏洞发布

根据国际权威应急组织 CERT/CC 统计[1]，2005 年全年收到漏洞报告 5990 个，平均每天超过 15 个。自 1995 年以来共计收到漏洞报告总数 22716 个，具体统计结果如图 2-1 所示。从统计情况来看漏洞数量比 2003 年和 2004 年有了很大程度的增加。

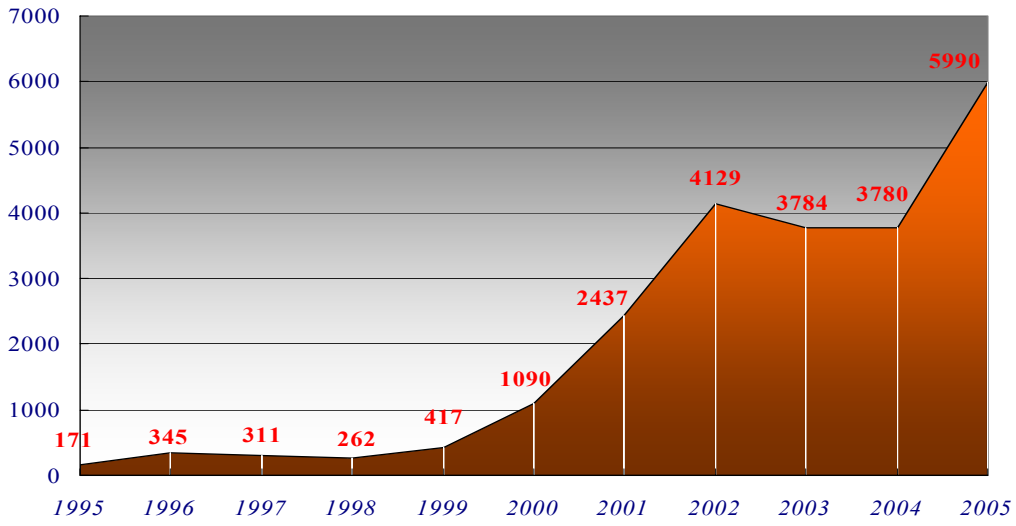


图 2-1

微软 2004 年正式公布了 34 个安全漏洞， 2005 年则公布了 48 个安全漏洞，是 2004 年的 1.4 倍。除操作系统和浏览器外，应用软件出现的安全漏洞也在不断增加。CNCERT/CC 2005 年共整理发布漏洞公告 75 个。

漏洞的大量存在是网络安全问题的总体形势趋于严峻的重要原因之一。

2.2. 蠕虫和木马监测

2005 年蠕虫、木马、间谍软件等恶意代码在网上的传播和活动仍然频繁。据 CNCERT/CC 技术支撑单位安天实验室统计，从 2005 年 1 月 1 日到 2005 年 12 月 31 日，接收到不同渠道的 278697 次样本上报，较前一年同期增长 2.2 倍，入库有效样本 150902 个，较前一年增长 1.8 倍，最终合并出 24275 个新病毒名称（含变种）。瑞星全球反病毒监测网的统计数据[2]（中国大陆部分）显示，2005 年截获的新病毒数量达到了 72836 个，比 2004 年增长了一倍还多。

1 数据来自于 CERT/CC 的网站，http://www.cert.org
2 数据来自于《中国大陆地区 2005 年电脑病毒疫情和安全趋势报告》，http://www.rising.com.cn

2005 年出现了几个利用系统漏洞进行传播的蠕虫，比如利用 MS05039 的.ZoTob（狙击波）家族，还有年末利用多个漏洞的 Dasher（黛蛇）家族，但都没有造成过大的影响。这与微软的 WinXP SP2 出现有一定关系，由于 WinXP SP2 的 DEP/NX 保护技术，使得许多常规的缓冲区溢出无法正常利用，所以即使许多用户没有打补丁，一些常规利用系统漏洞传播的蠕虫流传范围也大大缩小。

2005 年利用电子邮件手段传播的蠕虫整体呈下降趋势，而即时消息(主要是通过 QQ/MSN/ICQ)蠕虫迅速增多。出现的针对 Symbian 系统的手机蠕虫也值得关注。总体来看，2005 年的恶意代码呈现出五大趋势:

1、即时消息蠕虫(IM-Worm)迅速增多

利用 MSN/ICQ/QQ 等即时消息软件传播的蠕虫在 2005 年迅速增多，出现了 Summon、Kelver、Briopa 等利用 MSN 传播和 QQRRober、QQTran 等利用国产的 QQ 传播的蠕虫。这其中有几种较先进的即时消息蠕虫，比如可以随即跟好友聊天，可以将聊天语言设置为本地语言的即时消息蠕虫，即时消息蠕虫已经成为一种趋势。

2、群发邮件蠕虫（MassMail-Worm）逐渐减少

2004 年出现了 Mydoom, NetSky, Bagle 和 Zafi 等非常活跃的邮件蠕虫。2005 年，这类蠕虫（包括新出现的 Mytob）仍然活跃，占九成以上，但较 2004 年显著降低。原因包括多个方面：媒体广泛宣传，用户安全意识加强；杀毒软件改进了对受密码保护的邮件附件的处理技术，对邮件附件中可执行文件提前扫描；微软对 Outlook,Outlook Express 出现的漏洞及时打补丁。这些都使得邮件蠕虫走向衰退。但是今年存活率较高的 Mytob 家族却发展的较平稳，Mytob 家族不仅采用邮件传播这种单一的手法，而且运用 BOT 网络控制、漏洞扫描攻击等多种传播手法才得以存活。

3、手机病毒/蠕虫技术的进化

2004 出现的 Cabir 蠕虫感染 Symbian 手机操作系统，利用 Bluetooth 作为传播途径。2005 年，出现了更多的利用 Bluetooth 传播的手机蠕虫，这些蠕虫仍然瞄准 Symbian 系统，但传播手段趋于多样化。出现了利用彩信(MMS)传播的 Comwar 蠕虫和感染.sis 文件的 Lasco 病毒。需要说明，很多 Symbian 蠕虫都利用了公开源代码的 Cabir 蠕虫的代码。Lasco 虽然感染文件，但.sis 格式类似于.zip 或.rar 这类压缩文件，并且它利用 Bluetooth 作为传播手段，也可认为它是蠕虫。SymbOS.Pbstealer 家族已经出现了多个变种，手机病毒虽然还没有大规模流传，但进化速度迅速，朝着大规模感染、难以清除、欺骗性高的方向演进。

4、Rootkit 技术的应用呈增加趋势

蠕虫、Bot 甚至 Adware 都在使用 Rootkit 技术隐藏自身，提高生存能力。Rootkit 技术的普及和广泛应用将给用户清除恶意代码带来很大困难。今年 Net-Worm.Win32.Dasher 的控制端是第一个利用 Rookit 技术隐藏自身大范围传播的蠕虫家族。Rookit 技术的普及，不仅仅在蠕虫家族，在应用市场，包括 SONY 的 CD、symantec 的软件中，都曾利用了该技术，导致许多纠纷。Rootkit 技术使得计算机专业人员，也难以发现和清除这类恶意代码。这种隐蔽性的攻击将越来越难以发现和清除。

5、木马与 Spyware 数量迅速增加

蠕虫同比去年有减少趋势，而以窃取银行帐号、密码和个人信息，获得经济利益为目的的木马和间谍软件迅速增多，成为当前黑客手中的主要工具。2005 年，网络攻击比以往隐晦得多，许多攻击手法在地下流传，定向的木马攻击较为频繁，针对网络游戏、网络银行的木马、Spyware 种类繁多，变种繁多。

蠕虫和木马等恶意代码的不断发展进化，给网络和用户带来了更大的威胁。

2.3. 流量监测

CNCERT/CC 的 863-917 平台能够实时、准确、直观地显示各种网络业务流量信息，帮助判断当前的运行状况，发现流量异常现象。

4 月 11 日晚 10 时左右，我国某运营商发生了一起全国性的断网事故。图 2-2 是 863-917 平台在当时得到的一个数据情况：

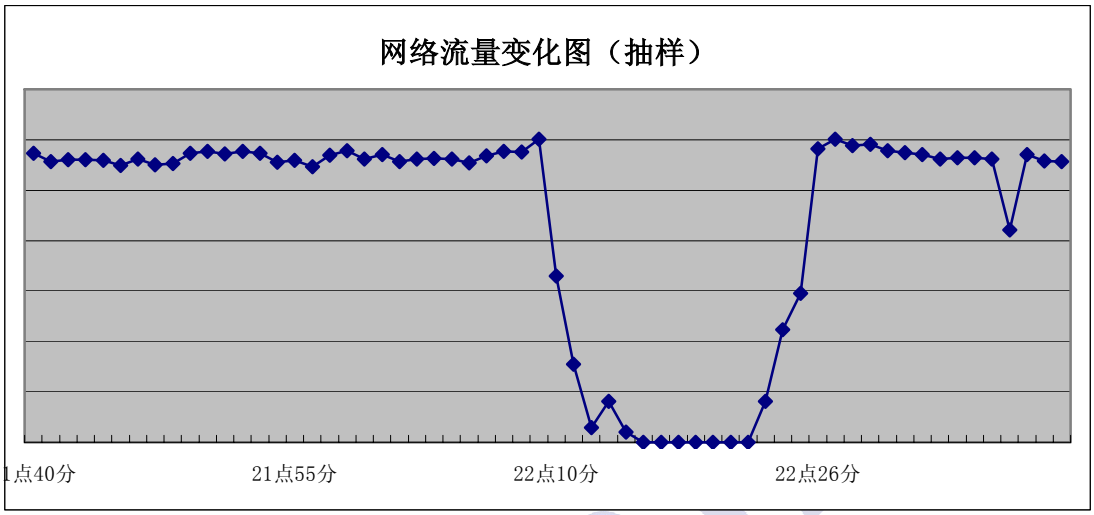


图 2-2

根据 CNCERT/CC 网络安全监测系统的流量数据进行抽样统计显示：当前最消耗带宽的网络应用应属 Web 浏览（37.82%）和利用 P2P 软件（15.43%）共享文件。电子邮件协议采用 TCP 25 号端口（6.00%），是现在应用的最广泛的协议之一。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。TCP 135/445 端口是最经常被攻击的端口，我们熟悉的冲击波类蠕虫就利用 135，震荡波利用 445。我们监测到的各种 bot，多数也在利用这两个端口进行扩散传播。各种应用对带宽的占用情况如图 2-3 所示。

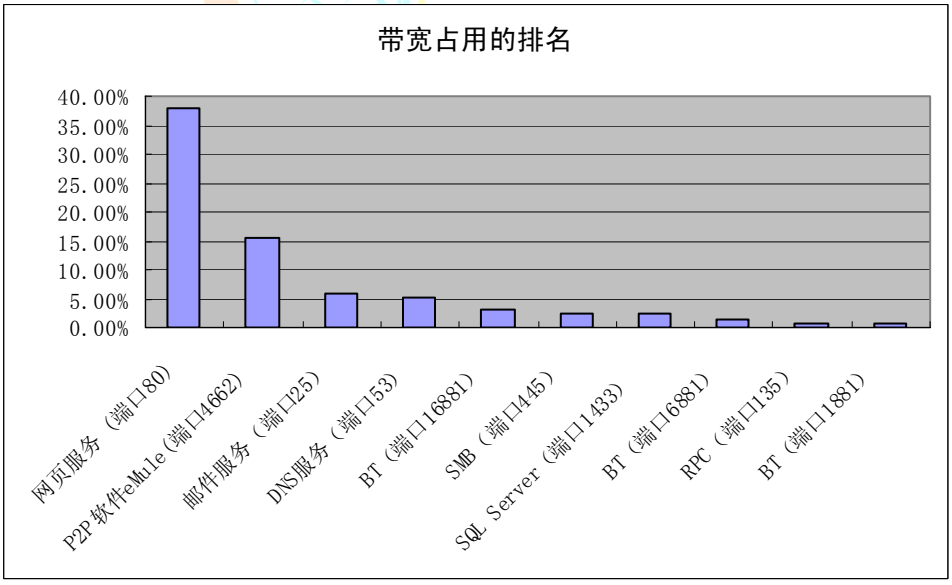


图 2-3

2005 年 4 月，CNCERT/CC 对某运营商中常用 P2P 软件占用的带宽做了抽样调查。结果表明：P2P 软件引起的总流量占 IP 协议总流量的 24.7%，超过 HTTP 协议占 IP 协议总流

量的21.7%和SMTP的1％。在P2P软件引起的TCP流量中，以eMule(19.7%)和Bittorrent(5.5%)为主;UDP流量中，除eMule(13%)和Bittorrent(2%)外，Gnutella类P2P软件引起了很大的流量（4％）。

1. 使用TCP协议的各类P2P软件引起的流量在TCP协议总流量中的比例

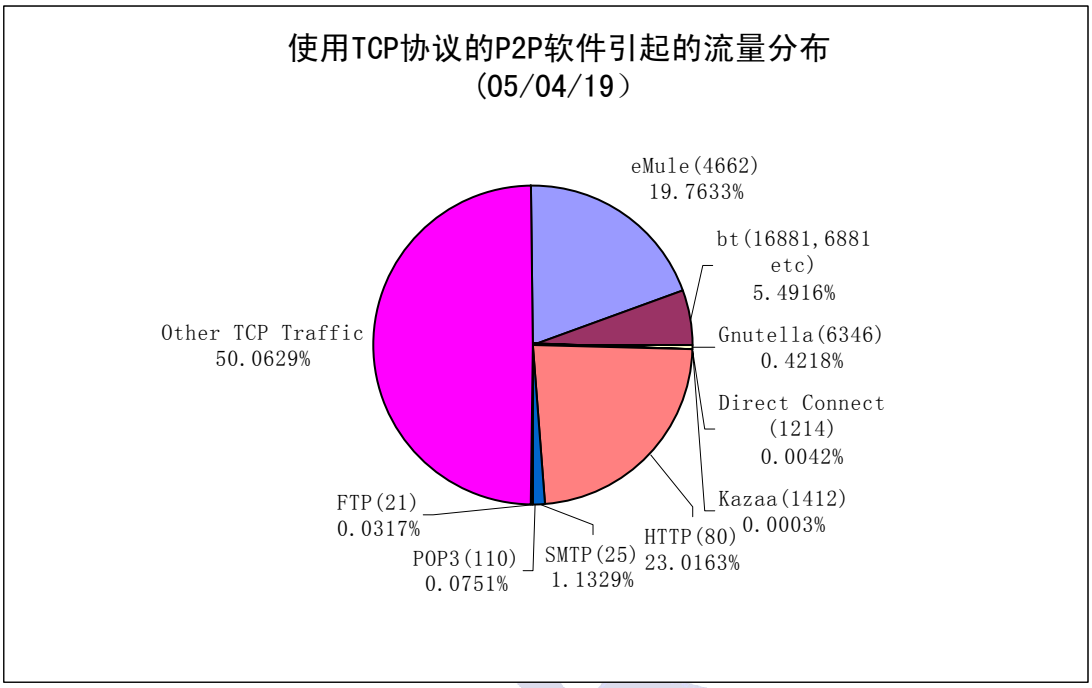


图 2-4

2. HTTP和emule流量－时间变化图

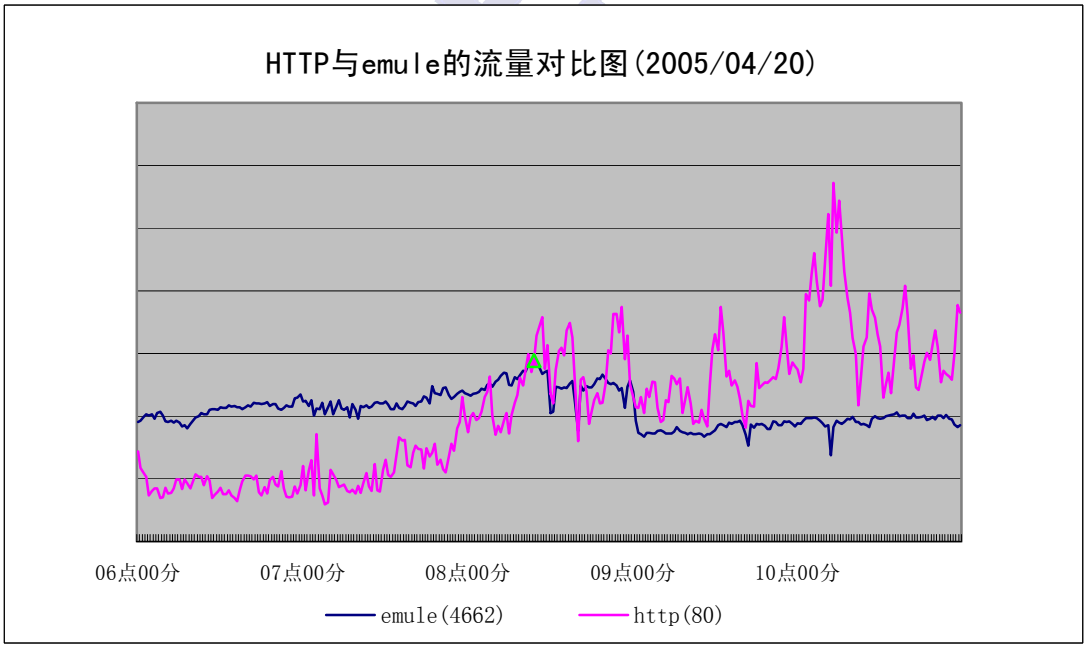


图 2-5

此外，还值得关注的是从05年4月开始，利用 UDP 1026/1027端口向PC直接发送垃圾信息的数量非常多，一度导致这两个端口所占流量已经远远超过电子邮件流量，仅次于Web服务和P2P软件引起的流量，后来经有关各方的积极处理，该垃圾信息流量得到了控制。

2.4. 木马事件

各类安全事件中，木马和后门事件的危害是最为严重的，因为此类事件隐蔽性非常强，是造成失泄密危害的重要原因。

2005 年，CNCERT/CC 对常见的 28 种木马程序的活动状况进行了抽样监测，发现我国大陆地区 2 万 2 千 5 百多个 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下图所示，最多的地区分别为广东省（21%）、上海（15%）和江苏(10%)。

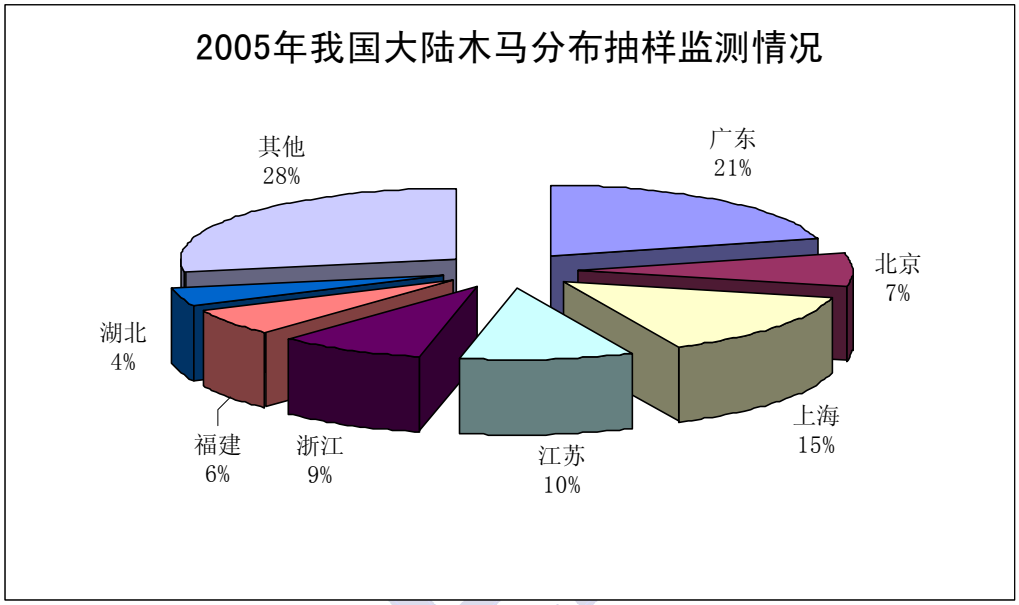


图 2-6

同时发现大陆地区以外 2 万 2 千 8 百多个主机地址和这些木马进行通信。按国家和地区分布如图 2-7 所示，最多的国家和地区分别为：美国（25%）、台湾省（18%）、香港特别行政区（18%）、日本（12%）。

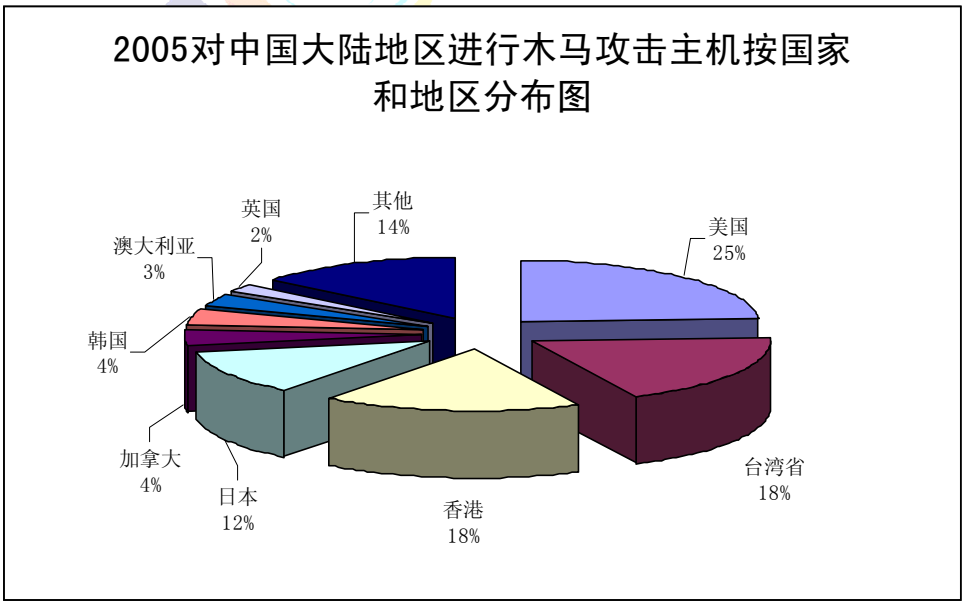


图 2-7

以上的数据只是对我国互联网上木马活动情况的初步统计，实际情况会更加严重和复

杂。随着我国互联网应用日益普及，日益增加的木马程序将造成计算机数据的失窃和被控，感染木马的计算机不仅面临严重的泄密威胁，更容易被黑客利用发起有组织的大规模攻击。而且木马类程序不断出现，用户很难发觉，因此造成的影响往往比较长久。CNCERT/CC 将进一步加强对木马的监测与分析，加大对木马类事件的处理力度，确保我国基础网络和重要信息系统的安全。

2.5. 间谍软件(Spyware)

间谍软件（Spyware）通常是一个独立的程序。Spyware 监视用户和系统活动、窃取用户敏感信息，包括用户名、密码、银行卡和信用卡信息等，然后将窃取到的信息以加密的方式发送给攻击者。从 2004 年至今，间谍软件（Spyware）的数量、种类和危害不断增加，引起了广泛重视。2005 年，大部分蠕虫、木马等恶意代码也都加入了 Spyware 功能，敏感信息失窃成为用户面临的主要威胁。

2005 年，CNCERT/CC 对常见的 30 余种 Spyware 的活动情况进行了抽样监测，发现我国大陆至少有 70 万台主机被植入了某种类型的 Spyware。这些 Spyware 向服务器汇报搜集到的信息；从服务器读取关键字、下载更新版本。这些控制 Spyware 活动的服务器绝大多数位于国外，其中最多的是美国（42 个）和韩国（26 个）。

2.6. 对 WEB 网站的恶意攻击

2005年，CNCERT/CC对常见的50种针对Web网站的攻击进行了抽样监测，发现境外22万台主机曾对我国发起攻击。其间，对我国大陆进行网站攻击最频繁的国家和地区为：美国（40%）、日本（11%）、台湾省（10%）和韩国（8%）。

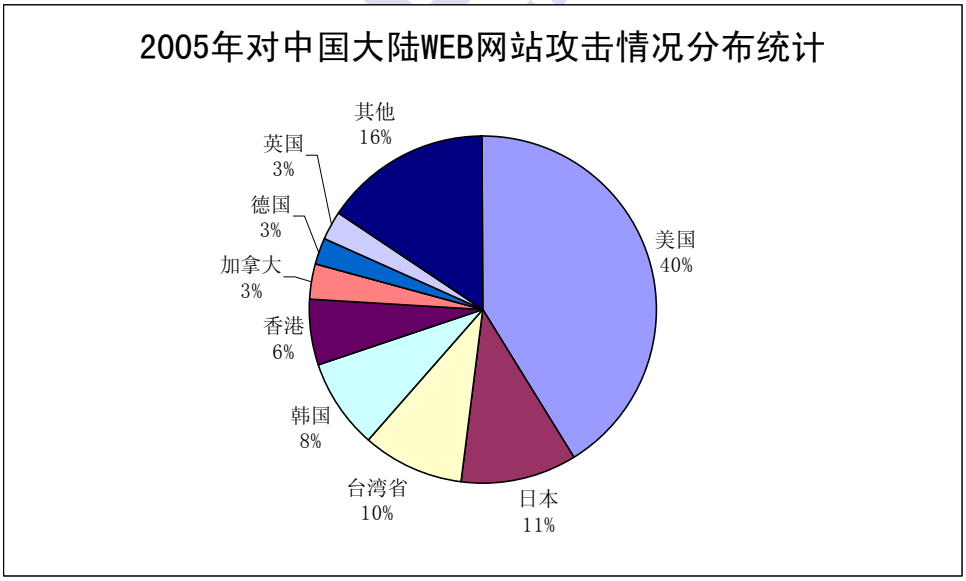


图 2-8

2. 7. “僵尸网络”（BOTNET）

僵尸网络（恶意的 Botnet）不同于特定的安全事件，它是攻击者手中的一个攻击平台。这个攻击平台由互联网上数百到数十万台计算机构成，这些计算机被黑客利用蠕虫等手段植入了僵尸程序并暗中操控。利用这样的攻击平台，攻击者可以实施各种各样的破坏行为，而

且使得这些破坏行为往往比传统的实施方式危害更大、防范更难，例如：攻击者利用这个平台，可以反过来创建新的僵尸网络、释放蠕虫、实施 DDos 攻击、发送垃圾邮件、窃取敏感信息、为网络仿冒提供宿主或中转环境等。

通过僵尸网络实施这些攻击行为，不仅简化了攻击步骤，提高了攻击效率，而且更易于隐藏攻击者的身份，甚至僵尸网络的控制者还可以从这些攻击中获得经济利益，例如发送垃圾邮件、窃取个人信息、通过 DDos 攻击进行敲诈等，这正是僵尸网络得以发展的重要推动力。

从技术角度来看，僵尸网络的编写者已经不局限于利用 IRC 协议进行控制。Agobot 的一个变种 PhatBot 就同时具有 P2P 和 IRC 两种通信和控制协议，基于 P2P 技术的僵尸网络在健壮性、安全性和隐蔽性等方面都有很大提高，给僵尸网络的发现和控制带来挑战。

2005 年出现了利用 rootkit 原理隐藏进程的 bot(rBot 变种)，以后很可能出现更多的利用 rootkit 技术的 bot，这符合 bot 的特点：不像传统蠕虫一样快速扫描，引起异常，而是强调隐蔽性。

从 2004 年开始至今，僵尸网络受到世界各地越来越多的重视，对僵尸网络的研究需要进一步加强。CNCERT/CC 对僵尸网络的研究主要是：僵尸网络的生命周期、控制者实际控制手段的研究、Bot 采用的安全措施研究、控制服务器判断可疑客户端的依据、开源 IRC 服务器的修改方法研究、僵尸网络的应用模式等方面。

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，发现的僵尸网络的规模从数百到数万不等。在 1 月－12 月期间，CNCERT/CC 共发现同时在线的节点数大于 5000 的僵尸网络有 143 个，其中最大的 Diablo 僵尸网络最多时有 157142 个客户端。这些僵尸网络不断扫描扩张、更新版本、下载间谍软件和木马、发动各种形式的拒绝服务攻击。

需要说明的是，8 月 15 日出现的 Zotob 蠕虫所创建的僵尸网络，实际上影响并不大。从北京时间 8 月 16 日到 8 月 23 日，CNCERT/CC 通过抽样监测发现感染 Zotob.a 和 Zotob.b 的主机分别为 128 个和 208 个。

僵尸网络的规模趋于小型化，1 千至 1 万规模的僵尸网络更受到攻击者青睐。

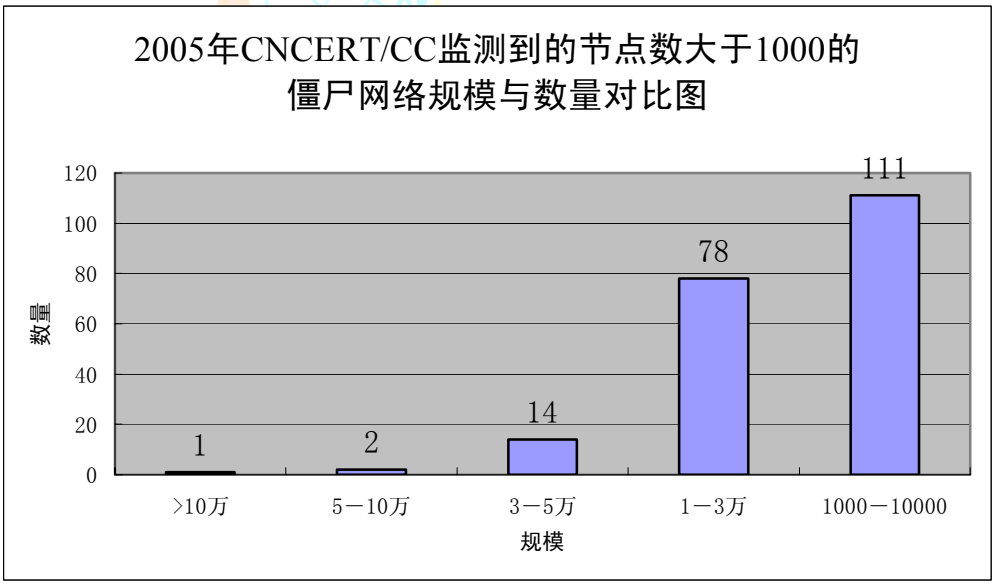


图 2-9

3. 网络安全事件处理情况

CNCERT/CC 是接收国内网络安全事件报告的重要机构，同时作为国际应急组织 FIRST 和亚太地区应急组织 APCERT 的成员，CNCERT/CC 负责接收国际网络安全事件报告。目前 CNCERT/CC 有专门接收事件报告的热线电话、电子邮件，CNCERT/CC 网站有专门的事件报告系统，网络用户可以在线填写网络安全事件报告表单，提交网络安全事件信息。CNCERT/CC 有专人对用户报告网络安全事件进行分析处理，遇重大网络安全事件还将向有关部门报告，进入紧急处理程序。2005 年 CNCERT/CC 进一步规范和细化了内部网络安全事件处理流程，加强对重要网络安全事件的跟踪和管理，分别制订和修订了针对各类网络安全事件的处理程序，全面提高了事件处理的质量。

3.1. 事件报告情况

3.1.1. 网络安全事件数量统计

2005 年，CNCERT/CC 共收到国内外通过应急热线、网站、电子邮件等报告的网络安全事件 12 万多件，平均每月 1 万多件，每月的具体事件报告数量见图 3-1。需要说明的是，在 2005 年收到的事件报告中约 93％为扫描类网络安全事件。除扫描外的国内外网络安全事件报告共 9112 件。

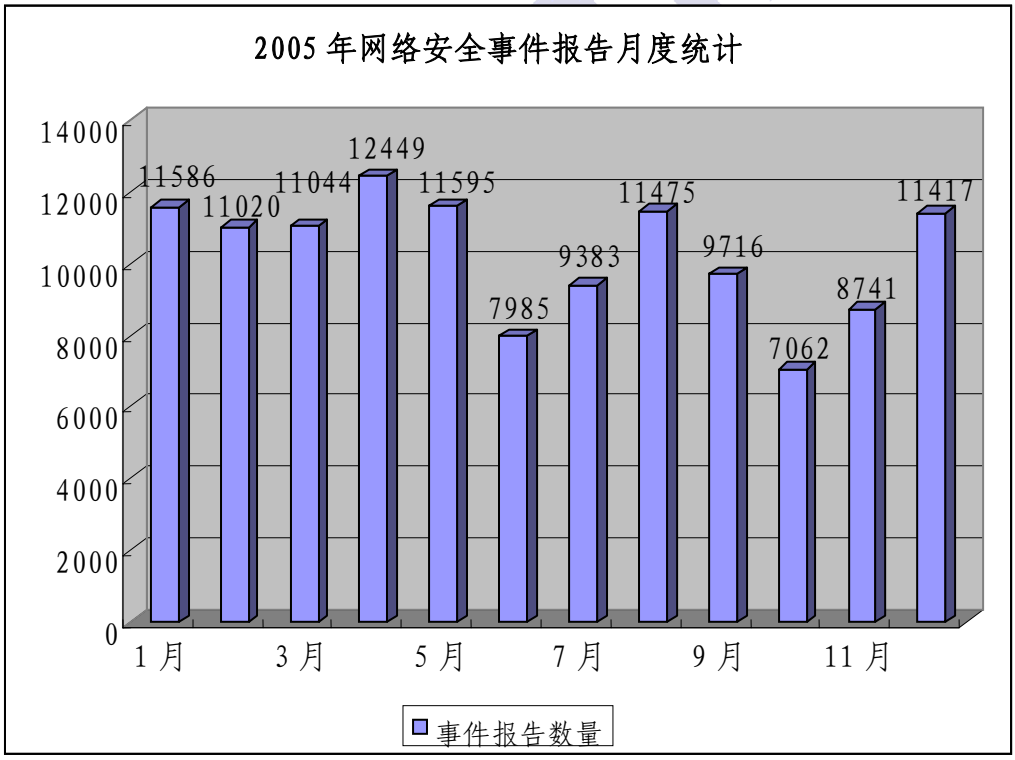


图 3-1

2005 年 CNCERT/CC 接收的无论是非扫描类还是扫描类事件报告，与 2004 年相比，数量都增长了一倍左右。与 2003 年相比，04 年和 05 年事件报告数量的增长更加明显。2003 年至 2005 年事件报告数量比较情况如图 3-2 所示。

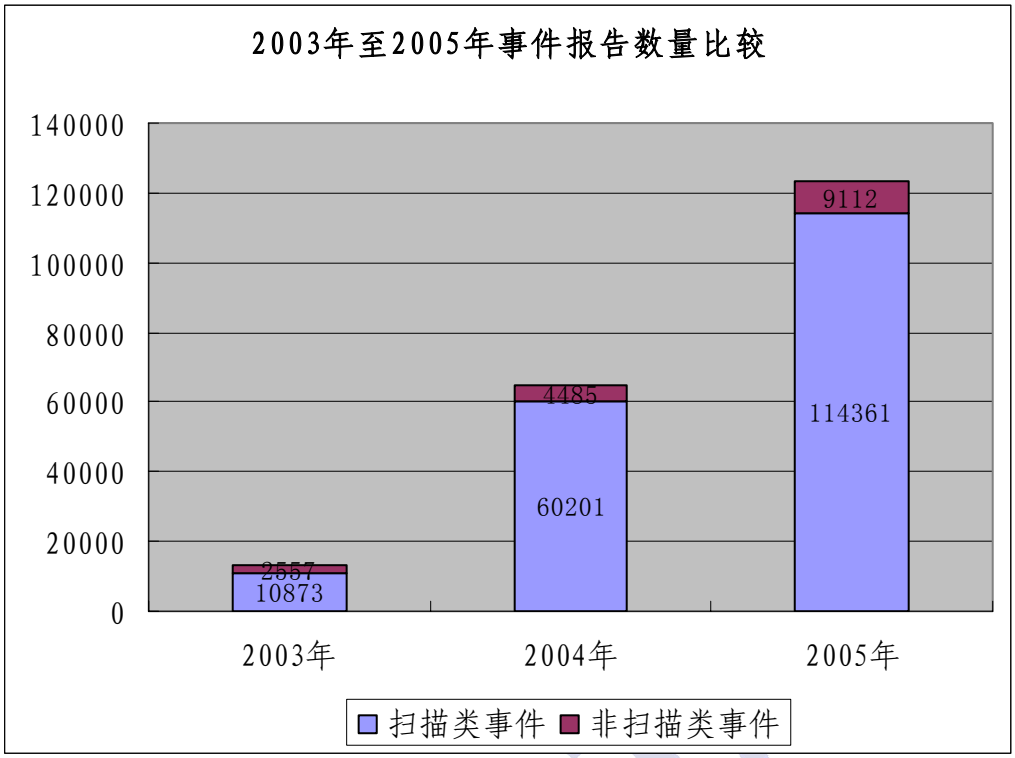


图 3-2

3.1.2. 网络安全事件分类统计

2005 年，CNCERT/CC 收到的 9112 件**非扫描类**网络安全事件报告按类型统计情况如图 3-3 所示，报告较多的是网页篡改（8130 件）、网络仿冒（475 件）和垃圾邮件（161 件）。

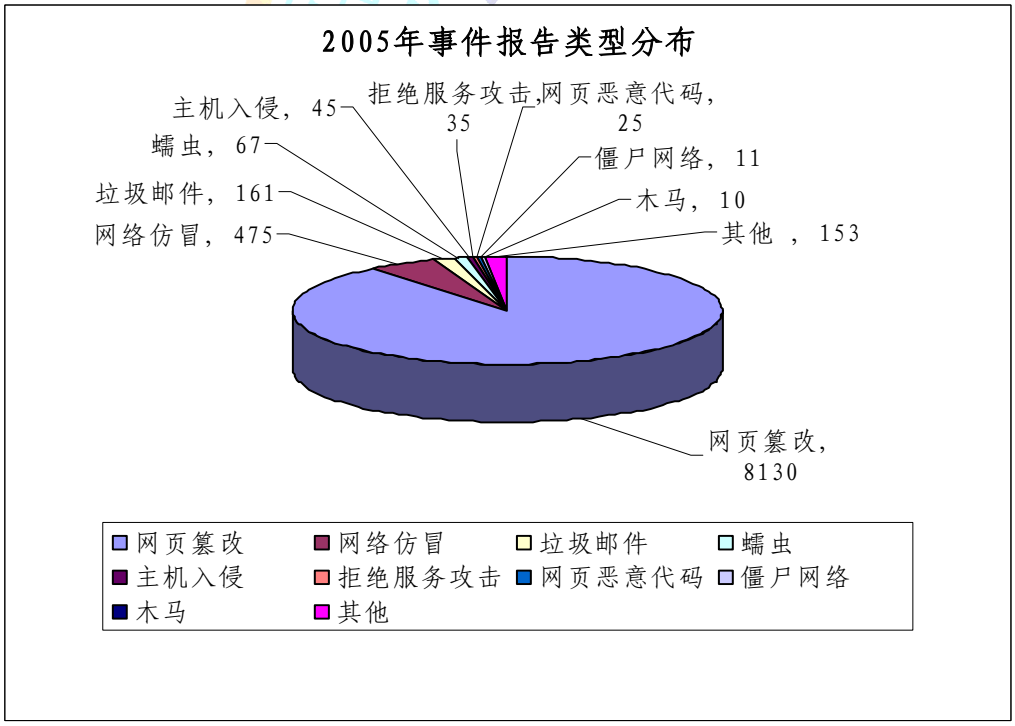


图 3-3

3.1.3. 国外网络安全事件报告

2005 年，CNCERT/CC 共收到来自国外的事件报告 464 件（除国外自动转发的扫描类事件以外），其中网络仿冒 456 件、木马 4 件、拒绝服务攻击 1 件、主机入侵 1 件、其他 2 件。

可以看到，在来自国外的事件报告中，绝大部分是网络仿冒的报告，它们共来自 40 多个国外的组织机构，其中 40%来自 eBay。

表 3-1 列出了报告网络仿冒事件数量最多（前十名）的组织机构，它们全部来自国外。

网络仿冒事件报告者 （前十个报告数量最多的组织机构）	数量
eBay	207
MarkMornitor（美国安全公司）	43
Brandimension（加拿大安全公司）	22
BFKCERT（德国 CERT）	17
VeriSign	17
AUSCERT（澳大利亚 CERT）	15
Inter identitiy（美国安全公司）	14
MasterCard（万事达卡）	13
HSBC（汇丰银行）	10
Royal Bank of Scotland（苏格兰皇家银行）	10
KrCERT（韩国 CERT）	7
Citigroup（花旗银行）	6

表 3-1

3.2. 事件处理情况

CNCERT/CC 协助用户进行事件处理，以便尽快消除网络安全事件对用户造成的各方面危害，帮助用户尽量减少损失。同时，按照国际惯例，在事件处理的过程中，帮助用户保存必要的证据，以便用户需要寻求司法协助时参考使用。

3.2.1. 参与事件处理数目按省份统计

2005 年，CNCERT/CC 共处理网络安全事件 400 余件，大部分事件是 CNCERT/CC 国家中心根据事件涉及主机所属地区，协调各省分中心进行处理的。各省分中心参与处理的事件数目对比情况见图 3-4，其中广东、上海、福建等地处理事件数量较多。

2005 年，CNCERT/CC 处理的主要事件类型包括网页篡改、网络仿冒、僵尸网络、主机入侵、拒绝服务攻击、恶意代码等。各类事件所占比例如图 3-5 所示，其中网页篡改（53%）和网络仿冒（31%）类事件所占比例较大。

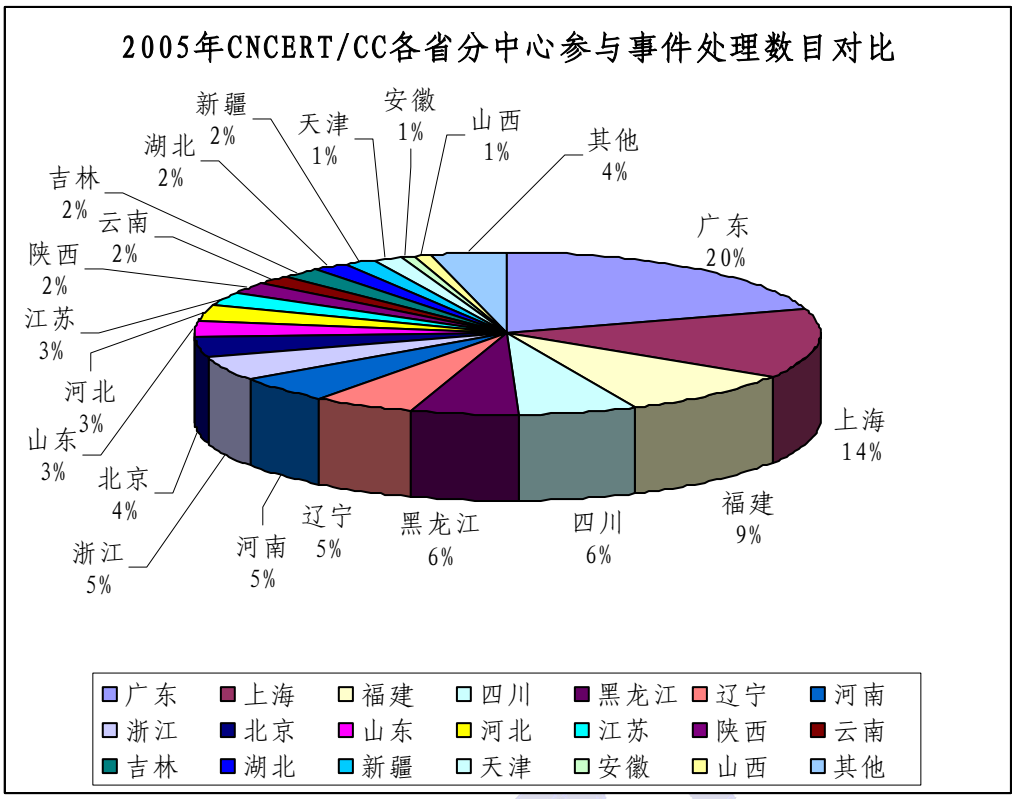

2005年CNCERT/CC各省分中心参与事件处理数目对比
新疆 2%
天津 1%
安徽 1%
山西 1%
其他 4%
湖北 2%
吉林 2%
云南 2%
陕西 2%
江苏 3%
河北 3%
山东 3%
北京 4%
浙江 5%
河南 5%
辽宁 5%
黑龙江 6%
四川 6%
福建 9%
上海 14%
广东 20%
广东 上海 福建 四川 黑龙江 辽宁 河南
浙江 北京 山东 河北 江苏 陕西 云南
吉林 湖北 新疆 天津 安徽 山西 其他

图 3-4

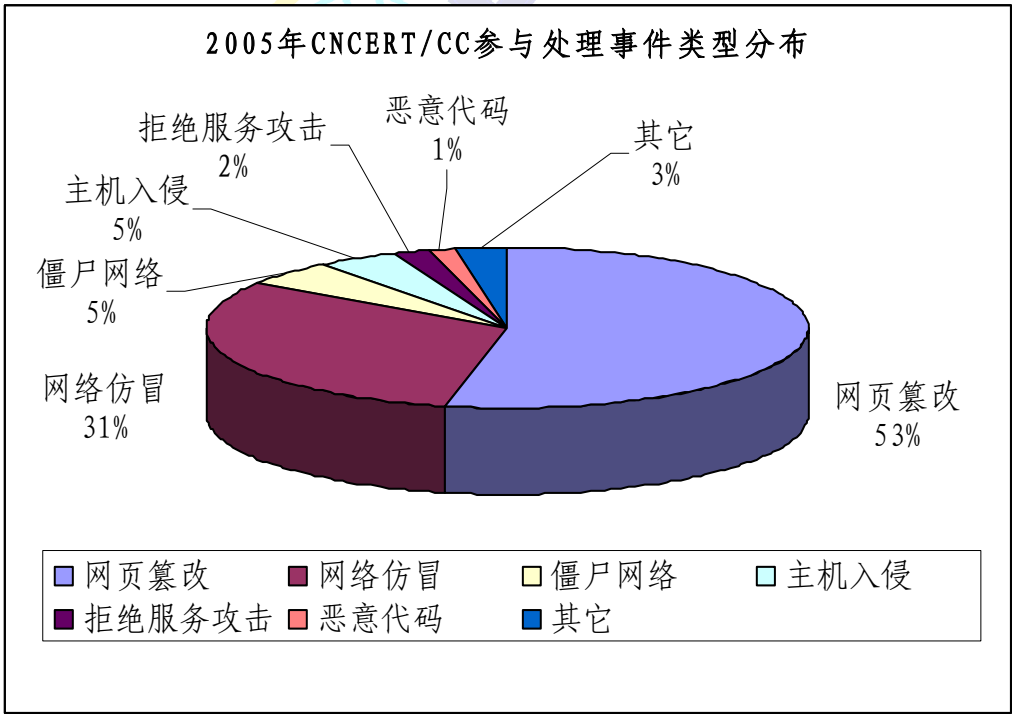

2005年CNCERT/CC参与处理事件类型分布
拒绝服务攻击 2%
恶意代码 1%
其它 3%
主机入侵 5%
僵尸网络 5%
网络仿冒 31%
网页篡改 53%
网页篡改 网络仿冒 僵尸网络 主机入侵
拒绝服务攻击 恶意代码 其它

图 3-5

3.3. 重点处理事件情况

3.3.1. UDP1026 和 1027 端口流量异常事件

2005 年 6 月，CNCERT/CC 通过 863-917 网络安全监测平台监测发现：我国公共互联网上 UDP1026 和 1027 端口对应的 UDP 协议流量急剧上升。6 月至 7 月 UDP1026 和 1027 端口流量合计在公共互联网的总流量中所占的比率达 11.49％。由于该端口不提供任何常见互联网服务，CNCERT/CC 判定这是一起严重占用公共互联网带宽的异常流量事件。

对此事件，CNCERT/CC 给予了高度关注，进行了持续跟踪监测分析，分析结果表明：此异常流量是由于有人利用专门发送“垃圾信息”的程序大量发送垃圾信息所导致的。垃圾信息的内容都相同，大意是：用户系统有危险，请访问某网站进行修复。经验证，该网站并未对访问用户进行恶意操作，仅提示用户下载一个正常的查杀间谍软件的工具。

由于发送“垃圾信息”的程序可能严重影响网络传输质量，CNCERT/CC 对发送垃圾信息的源头进行了调查，并陆续发现了位于某几个省内的多台机器在向大量 IP 发送此垃圾信息，于是立即协调 CNCERT/CC 当地分中心对这些主机进行了处理。

同时，为了抑制公共互联网的垃圾信息泛滥的上升趋势，CNCERT/CC 及时通过电子邮件将有关分析报告通报了相关运营商，建议其采取相应过滤措施，并通知用户采取打补定、升级系统的防范措施。某骨干运营商根据 CNCERT/CC 的建议采取了相应的措施后，控制了 3G 左右的流量，效果非常明显。

最终，在 9 月中旬，UDP1026 和 1027 端口流量大幅减少，恢复了正常水平。

3.3.2. 密切关注 8－15 期间的国内外黑客活动

香港某报于 8 月初称“中国红客”正计划在 8 月 15 日期间发动针对日本右翼网站的攻击活动，该攻击可能会利用部分韩国的主机进行。该报道在我国和日、韩媒体上被反复转载，引起了各国相关部门的注意。为此，CNCERT/CC 对黑客的活动保持密切关注，并通过日、韩两国的国家级应急组织——JPCERT/CC 和 KrCERT/CC 持续了解日、韩两国国内的黑客动向，但并未发现任何有组织的黑客活动迹象，最终的实际情况也表明的确没有发生媒体所说的黑客攻击事件。

3.3.3. Toxbot 僵尸网络事件

2005 年 10 月 17 日，CNCERT/CC 接到荷兰 SURFnet CERT 应急小组的事件报告，称有 29 万多个属于中国的 IP 被植入 W32/Toxbot 家族程序，这些 IP 成为一个巨型僵尸网络的成员。同时，CNCERT/CC 也注意到“informationweek”网站在 10 月 10 日报道：“荷兰警方日前宣布捣毁了一个巨型计算机僵尸网络（botnet）。目前，警方已经逮捕了 3 名涉嫌制造该僵尸网络的荷兰男子。荷兰警方称，被逮捕的 3 名嫌犯利用 Toxbot 木马程序感染用户的计算机，然后在染毒计算机上安装广告插件和间谍软件。”。CNCERT/CC 与 SURFnet CERT 联系后确认，其提供的属于中国的 29 万个 IP 正是报道中所提到的僵尸网络的成员。SURFnet CERT 称此僵尸网络的规模非常之大，受控计算机数目达到 120 万台左右。

由于此事件涉及中国主机的数目较多，可能产生严重危害，CNCERT/CC 迅速采取如下应对措施：

1、追踪僵尸程序样本，通过分析实验研究其检测、清除和防护方法。根据荷方提供的地址，迅速定位到某受控主机并成功提取出僵尸程序，在多家技术支撑单位的支持下，及时分析出该僵尸网络的运行信息，研究出检测、清除和预防方法。

2、通过 863-917 平台监测僵尸网络发展趋势。监测结果表明，该僵尸网络的规模在监测时已经大幅度减少。

3、协调有关单位共同采取保护措施，清除僵尸程序。首先按照与重点保障部门的合作流程将涉及该部门的受害主机通知对方，然后将其余涉及主机 IP 分发给所属运营单位，请其向受害网络用户告知该事件的危害性和处理办法，并提醒用户采取必要的安全加固措施。同时，通过 CNCERT/CC 网站和互联网网络安全工作委员会成员宣传此事的危害和解决办法。

3.3.4. 黛蛇蠕虫事件

临近岁末国内互联网上出现了一次大规模的蠕虫事件，2005 年 12 月 15 日，CNCERT/CC 截获了一个可利用 MS Windows 操作系统最新高危漏洞——微软 MS05-051 传播的名为“黛蛇”（Dasher.B）的蠕虫。该蠕虫主要针对 Windows 2000 操作系统、部分 Windows XP 系统和部分 WindowsServer2003 操作系统，通过攻击 TCP/1025 端口获得远程执行命令的权限；此外，该蠕虫还可以针对微软 MS04-045、MS04-039 漏洞和利用 SQL 溢出工具进行攻击。Dasher.B 蠕虫运行后，会扫描并试图利用漏洞来攻击目标主机，目标主机的地址是根据该蠕虫自身携带的地址列表随机生成的，多数为中国用户。该蠕虫攻击目标主机成功后，会操纵目标主机自动连接到某控制服务器（位于湖南长沙）请求黑客指令，然后按照该黑客指令从某个 ftp 服务器（由控制服务器动态指定）下载并运行一个键盘记录软件和 Dasher 蠕虫文件包，从而完成传染过程。

众多迹象表明，该蠕虫事件是一次有计划的，专门针对中国互联网用户的攻击，经过对蠕虫的整个传染过程分析，如果该蠕虫大规模感染扩散成功将造成以下几种危害：

1、用户数据有被窃取的可能，如果被感染的是重要信息系统用户，还会存在信息失泄密的危险；

2、伴随大量的扫描，会影响网络性能；

3、键盘记录程序还会自动连接一个网站（位于广东汕头）下载 SDBot 僵尸程序，形成一个巨大的僵尸网络。

CNCERT/CC 协调 CNCERT/CC 分中心切断了蠕虫传播路径，并在第一时间在网站上发布了蠕虫预警公告，同时通报了相关运营单位进行统一处理，根据自身情况采取必要措施，协助用户清除蠕虫，防止蠕虫继续传播。

3.3.5. 西太平洋银行－万事达卡网络仿冒事件

2005 年 10 月 25 日，CNCERT/CC 接到 IBM 应急小组投诉，称中国境内某一主机运行了澳大利亚西太平洋(West Pacific)银行的仿冒网站。CNCERT/CC 立即协调相关分中心进行核实、定位，并按照 IBM 应急小组提供的路径，通过远程技术分析发现了其投诉的仿冒西太平洋银行网页的内容和部分用户的信息，CNCERT/CC 按照网页仿冒事件处理流程立即对仿冒网页和有关信息进行了删除处理。

在远程分析过程中，CNCERT/CC 还在该主机上意外发现了其仿冒其他银行网页的痕迹，并最终排查到一个包含有 11 个用户信息的文本文件，信息内容具体全面，包括有用户地址、姓名、信用卡号、ATM 机密码号、生日、地址交易保障号等。

CNCERT/CC 立即联络国际上数家知名的银行，根据国际反欺诈工作组(APWG)成员提供的银行卡号的特点与分类，查得该 1 1 个被盗的用户帐号都属于万事达卡，并归还了相应的帐号及相关信息，帮助用户和银行挽回了损失。

3.3.6. 其他网络仿冒事件

2005 年 CNCERT/CC 共接到网络仿冒类事件报告 400 多件，其中完成处理 145 件。这些网络仿冒类事件绝大部分是国际应急组织和安全小组报告并要求协助处理的，被仿冒的网站大都是国外的著名金融机构，也有少量仿冒国内工商银行和淘宝网的事件报告。2005 年每月网络仿冒事件报告数量情况见图 3-6。

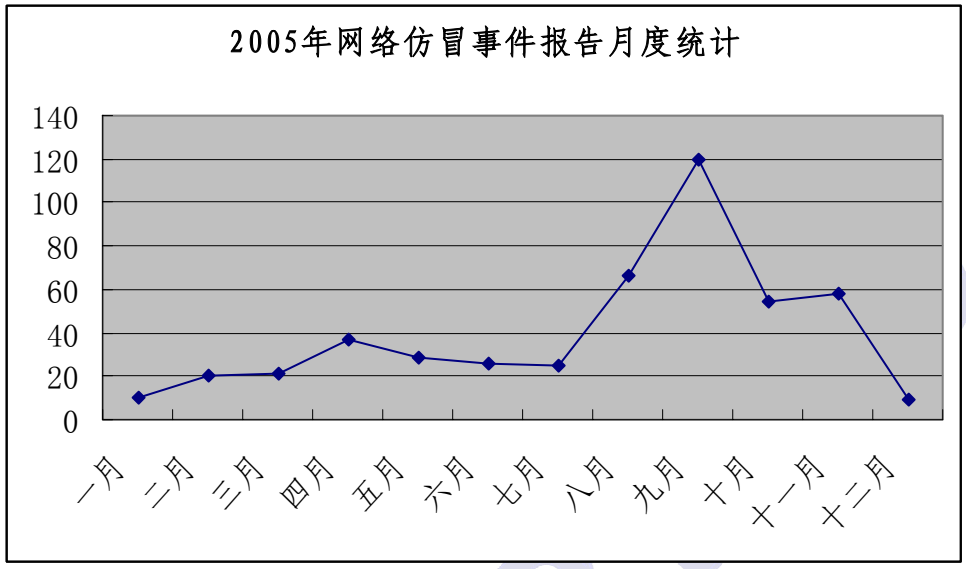


图 3-6

网络仿冒行为通常会选择其他国家地区的计算机来建立仿冒网页，以逃避本国司法和执法部门的调查和处罚。目前，很多境外黑客利用其所入侵并控制的我国境内的主机来建立仿冒网页。CNCERT/CC 对网络仿冒的处理大都是由 CNCERT/CC 各省分中心具体承担，其过程一般是定位仿冒主机，然后联系该主机用户并介绍有关情况，协助用户及时清除仿冒网页或进一步清除黑客植入的后门，建议用户加强网络安全防范工作等。从事件处理情况看，很多被黑客利用的主机处于无人维护的状态，在没有安装补丁、防病毒软件、防火墙的情况下连接互联网，给黑客留下可乘之机。尽管许多用户对网络仿冒事件的处理提供了积极的帮助，但仍然有一些用户对网络仿冒的危害没有充分认识，只是简单删除了主机内的仿冒网页或格式化硬盘，没有做必要的漏洞和木马清除等防范工作，结果出现同一主机被多次利用的情况。

由于 CNCERT/CC 在网络仿冒事件处置方面积极进行处理，在相关国际会议和国际反网络仿冒工作组 (APWG)里，引起许多国家 CERT 组织以及有关公司和机构的关注，纷纷加大了和 CNCERT/CC 的合作力度。

随着我国网上银行、网上购物等电子商务的普及，我国面临的网络仿冒事件威胁必将逐渐增大，也引起了国内执法、银行、金融等部门足够重视。我国国内需要建立类似 APWG 的机制，发挥国内各部门各机构的优势，加强与有关国际组织的合作交流，以更好的应对威胁网络仿冒的威胁。

3.3.7. 拒绝服务攻击

2005 年，拒绝服务攻击事件(DoS)仍频繁发生，CNCERT/CC 也接到多起拒绝服务攻击事件的报告。攻击者主要是针对知名的互联网业务站点和重要的应用服务器，导致一些业务不能正常进行，给被攻击者带来业务收入、客户资源、企业形象等各方面的损失。

2004 年 11 月 CNCERT/CC 接到了一起严重的分布式拒绝服务攻击（DDoS）事件报告，对该事件的处理一直持续到 2005 年 1 月。在该事件中，用户遭到长时间持续不断的 DDoS

攻击，攻击流量一度超过 1000M，攻击类型超过了 11 种，用户的经营行为几乎无法进行，直接经济损失超过上百万元。CNCERT/CC 通过协调多个分中心和运营商进行了处理，并配合公安部门进行调查和取证。结果显示黑客是通过所控制的一个大型僵尸网络发起的攻击，目的是通过影响受害者的网站业务来达到商业竞争优势。

2005 年 4 月深圳市某人才交流服务网站因受到来历不明的 DDOS 攻击，导致该网站无法正常访问，损失相当严重，遂向 CNCERT/CC 广东分中心报告。CNCERT/CC 广东分中心技术人员分析后，认为该网站受到了 SYN-Flood 攻击，并在攻击再次发生时，在 CNCERT/CC 国家中心、相关运营商各方的通力配合下，逐级排查，最终确定攻击流量来自国外，采取措施之后使网站恢复正常访问。

2005 年 8 月我国某域名注册和虚拟主机服务提供商遭受 SYN Flood DDOS 攻击，CNCERT/CC 在接到该事件报告后，立即协调有关分中心和运营商开展了积极有效的追查攻击源工作，并最终在较短时间内追查和排除了其中一个最具危害性的攻击源，这使得该公司业务很快恢复了正常。

由于目前互联网上广泛使用的 IPv4 协议存在的缺陷，彻底杜绝 DoS 是非常困难的，因此 CNCERT/CC 主要通过不断加强技术能力和协调能力来重点处理规模大、影响严重的 DoS 事件，并积极推动与公安部门的合作，对恶意攻击者诉诸法律。

3.3.8. 网页篡改

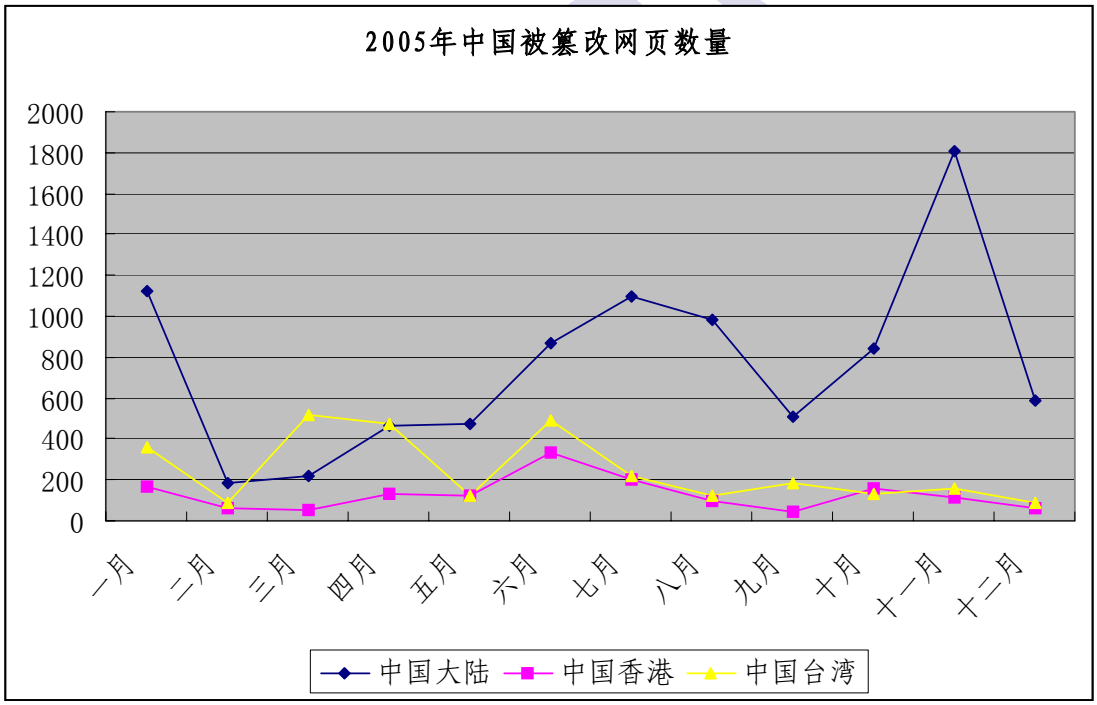


图 3-7

2005 年 CNCERT/CC 每日对我国网站被篡改情况保持跟踪监测，并及时通知我国大陆地区网站所在省的分中心协助解决，尽力帮助被篡改网站快速恢复。2005 年，监测到的我国被篡改网站总数达到 13653 个，其中协调分中心帮助用户进行处理的有 250 件。

2005 年我国被篡改网站数量按月统计情况如图 3-7 所示。

其中，我国大陆地区政府网站被篡改数量共计达 2027 个，其月度情况统计如图 3-8 所示：

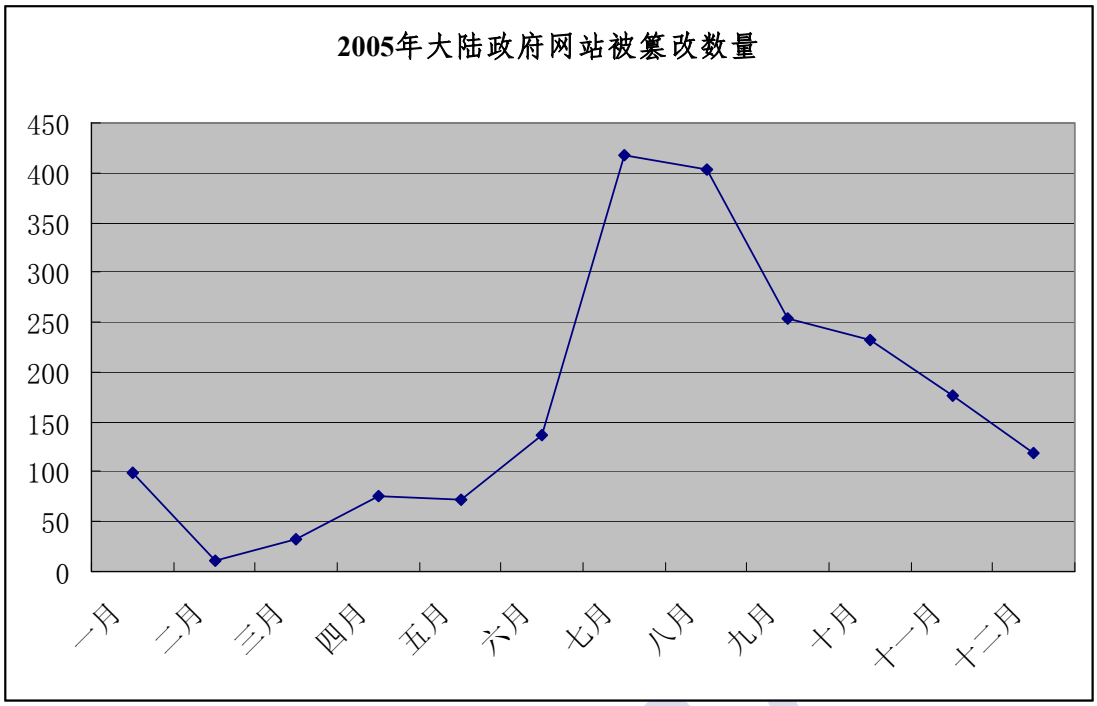


图 3-8

总体上看，在我国大陆被篡改的网站中，有 22%是政府网站，明显大于我国.cn 域名下的政府网站所占的 2.2％比例[注：该数据来自 CNNIC2006 年 1 月中国互联网发展状况统计报告]，从而说明我国政府网站容易遭受黑客攻击，其安全性亟待提高。

4. 网络安全信息服务

网络安全事件影响日益广泛，网络安全保障的难度越来越大，仅仅靠少数的网络安全应急组织和服务机构远远不够，需要提高全社会网络安全意识和应对网络安全事件的能力。CNCERT/CC 网络安全信息服务是面向国内各行各业和广大网民，提供全面、及时、有效、权威、实用的网络安全信息，使网络安全管理人员和用户及时了解最新网络安全宏观状况、漏洞补丁、应急技术、安全工具等方面的信息，目标是全面提高全社会对网络安全事件的预防和应对能力。

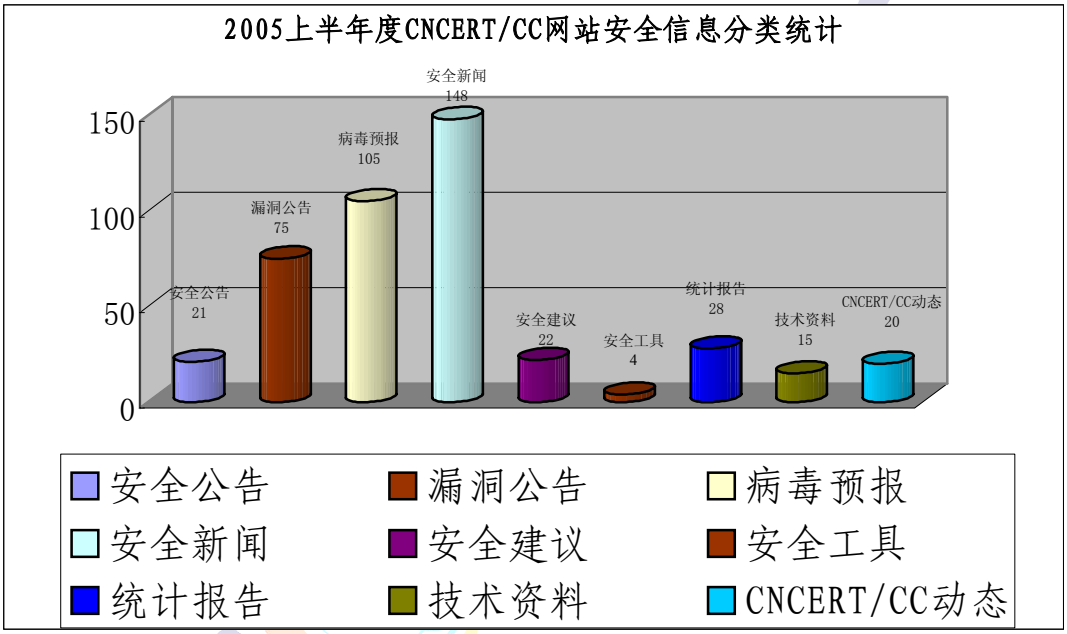
4.1. 安全信息通报

CNCERT/CC 将网络安全平台所发现的及从国际应急组织渠道获取的与有关部门信息系统有关的安全事件及时通报给有关部门。2005 年 CNCERT/CC 加大了这方面的工作力度。全年共向有关部门发出网络安全预警信息 5 次，共涉及 IP 地址二百多个；为国内骨干网运营商等提供了所有 CNCERT/CC 的安全公告信息，并投入力量针对性和骨干网关键设备相关的漏洞进行了分析研究，例如，在去年底发现一起大规模僵尸网络后，1 月份，通过各地分中心将属于各主要运营商的感染僵尸程序的 IP 地址通报各地运营商，并协助其进行了处置。这些安全预警和安全事件信息对重要部门和运营商及时做好防范，及早发现安全隐患起到了积极作用。4 月份，对 Cisco 的安全公告中公布的 “Crafted ICMP Messages Can Cause Denial of Service” 漏洞，CNCERT/CC 立即组织力量进行了研究，提出了应对措施，及时将漏洞和应对措施通知了给各运营单位。6 月份，对通过监测发现 UDP1026/1027 端口流量异常的事件，

持续跟踪监测分析，并通报了各个运营单位进行了过滤处理，最终在 9 月中旬恢复了正常水平； 12 月份，将黛蛇蠕虫(dasher.b worm)情况，通报了各个运营单位，协调各个单位统一进行处理，制止了蠕虫的大规模爆发；目前，CNCERT/CC 将规范与有关部门和运营商的信息共享机制，并继续推动此项工作。

4.2. CNCERT/CC 网站

CNCERT/CC 网站已成为对外提供网络安全信息服务的重要窗口。2005 年通过网站发布了近 440 条消息，其中包括安全公告、漏洞公告、病毒预报、安全报告、安全新闻、安全建议、安全工具、统计报告等栏目。特别是在 2005 年中国计算机网络安全应急年会之后,CNCERT/CC 将年会资料报告和年度总结报告免费公布到 CNCERT/CC 网站，已成为国内外安全组织和网站纷纷参考或转载的权威信息来源。



4.3. 电子邮件

相对于以网站形式提供信息服务的开放性，CNCERT/CC 还通过电子邮件的形式为一些用户群体提供定向的信息服务，目的是在第一时间将 CNCERT/CC 发布的各类信息送达用户。目前 CNCERT/CC 的用户群（邮件订户）包括各省分中心、运营商 CERT 组织、服务试点单位、技术支撑单位、APCERT、FIRST，以及 2005 年新增加的中国互联网协会网络与信息安全工作委员会、TRANSIT 培训班学员、东盟培训班学员等。

5. 网络安全会议与培训

5.1. 2005 中国计算机网络安全应急年会（CNCERT/CC ’05）在桂林召开

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 2005 中国计算机网络安全应急年会（CNCERT/CC ’05）于 2005 年 3 月 24 日至 25 日在广西桂林成功召开。本次会议得到了信息产业部、国务院信息办、公安部、国家网络与信息安全协调小组办公室、相关国际组织等有关机构的大力支持，共有来自于相关部委办、CNCERT/CC 各省

分中心、国际网络安全应急论坛组织（FIRST）、欧洲计算机网络研究和教育协会（TERENA）、亚太地区应急处理联盟（以下简称 APCERT）指导委员会成员单位（澳大利亚 AusCERT、日本 JPCERT/CC、韩国 KrCERT/CC、中国香港 HKCERT/CC）、东盟 7 个国家、我国互联网运营商应急小组、科研院所、国内安全企业、新闻媒体代表共计 300 余人出席了本次会议。会议以“构建主动、开放、有效的网络安全应急体系”为主题，旨在以整体协同的基础上为产业与应用各方建立新的网络安全观，进一步推动网络安全问题得到系统有效的解决。大会引起了国内媒体的广泛关注，10 家媒体的记者到会采访了本次会议，并在会议开幕的当天对会议情况进行了报道，国内很多知名网站也都在第一时间报道了本次会议。

在此次会议上， CNCERT/CC 还与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）。这一网上社区将致力于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，以便于应急组织之间的交流与合作，并且为广大网络用户单位和个人在寻求应急组织的帮助时提供方便。

截至 12 月底，共有 16 家应急组织在中国 CERT 社区注册，这些应急组织是：哈尔滨安天信息技术有限责任公司、北京冠群金辰软件有限公司、成都微软技术中心、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）、中国科技网网络安全应急小组（CSTCERT）、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、广西大学信息网络中心、北京万网新兴网络技术有限公司（中国万网）、北京江民新科技术有限公司、国家计算机网络入侵防范中心、东软计算机安全事件应急小组（NCSIRT）、山东科技大学中国核心网络安全小组（SDUST-CKNSG）、天融信安全运营中心（TopSec SOC）、启明星辰应急响应小组（VCERT）。

5.2. TRANSITS 国际高级训练营首度在中国举办

为进一步壮大我国网络安全应急组织的力量，在国际网络安全应急论坛组织（FIRST）和欧洲计算机网络研究教育协会（TERENA）两大国际权威应急组织联盟的支持与授权下，国家计算机网络应急技术处理协调中心（CNCERT/CC）引入了由 FIRST 与 TERENA 合作推出的国际高级计算机网络安全应急专家培训，于 2005 年 3 月 22 日至 23 日在中国桂林 CNCERT/CC '05 年会前期举办。此次培训由 FIRST 与 TERENA 委派的 6 名国际专业讲师前来授课，学员包括来自中国各科研院所、CNCERT/CC 及其各省分中心、互联网运营商应急小组、国内安全企业、东盟各相关国家等共 90 多名。TRANSITS 课程从 CSIRT 组织、CSIRT 运营、技术、法律、漏洞处理等五大方面对学员展开培训。本次培训的目的主要是通过解决计算机安全事件响应组（CSIRT）技术专家缺乏的问题，来推动 CSIRT 的建立和加强现有的 CSIRT。

到目前为止，TRANSITS 已经在欧洲地区举办了 5 期网络安全事件处理小组专家的培训，本次在中国桂林举办的 TRANSITS 培训是旨在亚太地区推广网络安全事件处理及响应能力的首次培训。

5.3. CNCERT/CC 成功承办了中国-东盟国家计算机应急组织能力建设与地区合作研讨班

应信息产业部外事司关于中国东盟信息通信培训项目建议书的要求，2005 年 9 月 5 日至 9 月 12 日，由北京邮电大学国际电信开发培训中心与 CNCERT/CC 联合承办的中国-东盟国家计算机应急组织能力建设与地区合作研讨班在北京成功举办。

来自柬埔寨、缅甸、越南、老挝、新加坡、泰国 6 个东盟地区不同国家的共 14 名学员参加了本次研讨班。其中,10 名学员是东盟国家邮电部和信息通信部门的官员,2 名是国家信息委员会的官员,其余 2 名是大学的经理。

培训期间，CNCERT/CC 派讲师分别就网络安全趋势与应急组织（CERT）的发展、 国家级应急组织的建立与管理、国家网络安全预警能力建设综述、主要网络安全事件的应对措施等几大类培训内容对学员进行了授课。同时，还针对本国互联网发展面临的安全问题，互联网安全管理和应急处理方面的政策、机构、规划，本国应急组织建设情况等内容与学员进行了深入的交流与探讨，以帮助学员掌握相关的网络安全技术与实际应用能力，建立国家应急组织，防范各类安全事件的发生。

同时,为了让学员能更深入的了解中国的网络安全技术及发展经验，CNCERT/CC 与北京邮电大学国际电信开发培训中心还安排学员们参观了相关的网络安全厂商、电信设备厂商及运营商。

5.4. CNCERT/CC 主办的“健康网中行网络安全知识电视竞赛”首次播出

2005 年 9 月 17 日,由 CNCERT/CC 主办的“健康网中行网络安全知识电视竞赛”在北京电视台 BTV-3《知识就是力量》栏目首次播出，并于 12 月份在中国教育电视台向全国播出。本次竞赛集知识性、趣味性及技术性为一身，将网络安全方面的专业知识以一种通俗化、大众化的形式传递给了广大电视观众。

如何让我们的网络安全更加有保障，如何让人们对网络的安全有正确的认识，并借此提高全社会的网络安全防范和保护意识，是 CNCERT/CC 组织本次竞赛的主要目的。

CNCERT/CC 自 2005 年年初开始策划、七月份着手进行筹备此次知识竞赛，在中国通信学会通信安全委员会、中国互联网协会网络与信息安全工作委员会、北京网中行网络技术有限公司及北京电视台的大力支持下，圆满完成了本次网络安全电视知识竞赛的全部工作。

为了使本次竞赛题目尽可能覆盖全面，CNCERT/CC 向中国互联网协会网络与信息安全工作委员会的成员单位征集了题目，最终的竞赛题库出自以下 14 个单位，分别为 CNCERT/CC、网中行、安络、上海交大、江民、金山、绿盟、启明星辰、安天、国家计算机网络入侵防范中心、山东省信息总公司、瑞星、国家计算机病毒应急处理中心和东软。参赛队伍分别由 CNCERT/CC 所在的 13 个省（自治区、直辖市）分中心进行组队，来自北京、上海、重庆、黑龙江、吉林、辽宁、山西、河南、江西、浙江、广东、广西、海南的 13 支代表队参加了本次竞赛，每个参赛队共三名队员，分别来自 CNCERT/CC 分中心、本地运营商和网络安全机构。北京代表队获得了本次竞赛的冠军。

5.5. CNCERT/CC 承办 2005 年互联网网络安全应急演练

为深入贯彻落实《信息产业部互联网网络安全应急预案》，受信产部应急工作办的委托，12 月 20 日下午 CNCERT/CC 承办了由部应急工作办、CNCERT/CC、中国电信、中国网通、中国联通、中国移动、中国铁通五大骨干网运营商参加的 2005 年互联网网络安全应急演练。观摩演练的领导有信息产业部奚国华副部长、国信办、中编办、国家发展和改革委员会、财政部、公安部、商务部、中科院、国家奖励办、北京市奥组委以及骨干网运营商、信息产业部相关司局、各省通信管理局、国家计算机网络应急技术处理协调中心和分中心的领导和同志。本次演练不仅检验了应急预案的科学性和可操作性，也是对应急队伍的一次很好锻炼。

6. 国际合作与交流

6.1. APCERT2005 年年会在日本召开 CNCERT/CC 当选 APCERT 副主席

2005 年 2 月 22 日至 24 日，APCERT 2005 年年会在日本京都召开。CNCERT/CC 参加了本次大会，并在 APCERT 指导委员会换届选举中，当选为 APCERT 第一任副主席。本次会议有来自 14 个经济体的 16 个应急组织参加，主要回顾了 APCERT 成立两年来的发展历程和取得的成绩；举行了指导委员会主席、副主席、秘书选举；审议新成员的入会申请；讨论经济体应急联络点（POC）机制及 APCERT 未来的工作重点；专题讨论 2004 年造成严重影响的网络仿冒事件有关情况。

经换届改选后的新一届 APCERT 指导委员会主席为 AusCERT、副主席为 CNCERT/CC、秘书为 JPCERT/CC。同时，上述三组成员均当选为新一届 APCERT 指导委员会委员，其他当选委员有韩国 KrCERT/CC、香港地区 HKCERT、新加坡 SingCERT 和马来西亚 MyCERT。来自菲律宾的 GCSIRT 和文莱的 BruCERT 在本次会议上被正式接纳为 APCERT 一般会员（General Member）。

大会还决定积极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 未来的工作重点，包括积极加入 APEC 电信工作组等。本次会议为 APCERT 进一步发展奠定了良好基础，必将大大推进亚太地区的网络安全应急处理工作。

6.2. CNCERT/CC 参加第 31 届 APEC 电信工作组会议

2005 年 4 月 3 日至 8 日，CNCERT/CC 随中国代表团参加了在泰国曼谷召开的第 31 届 APEC 电信工作组会议。在本次会议上，CNCERT/CC 一方面作为中国代表团成员参与各项涉及网络与信息安全方面议题的讨论，另一方面作为 APCERT 的副主席成员，应邀在电子安全工作组大会上做了“亚太地区网络安全问题发展趋势”的报告，从民间应急组织（CERT）的角度介绍了目前亚太地区在网络安全和应急处理上面临的最新问题和对策。CNCERT/CC 在报告中提到，2004 年以来互联网上威胁网络基础设施安全的事件越来越少，没有一起安全事件造成互联网的大面积瘫痪，这说明互联网本身的运行安全得到了加强，但是，威胁网络终端用户和具体网络应用的安全事件却越来越多，这一方面说明整个互联网使用者的安全意识还亟待加强，另一方面也对负责网络安全的各个部门提出了新的课题。

此外，来自美国和日本的应急组织专家分别做了有关间谍软件方面的技术报告，提出各个国家和地区要对间谍软件的危害性给予充分认识。

CNCERT/CC 和美国、日本应急组织的报告得到与会代表的充分重视，澳大利亚代表团提出在下一次电信工作组会议上设立有关间谍软件方面的研讨会，该建议得到了大会的支持。本次大会还就垃圾邮件、PKI、网络安全文化、互联网容灾等多个方面进行了讨论。

6.3. CNCERT/CC 参加第二届中日韩网络与信息安全研讨会

2005 年 6 月 9 日，CNCERT/CC 派代表随信息产业部参加了在日本东京举行的第二届中日韩网络与信息安全研讨会。来自中国信息产业部、日本总务省（Ministry of Internal Affairs and Communications）、韩国信息通信部（Ministry of information and Communication）的代表和各国信息通信安全机构的专家，共 21 人参加了本次会议。各国代表分别介绍了本国在网络与信息安全方面的机构建设、政策制定、网络安全应急处理与信息共享及反垃圾邮件等方面的工作，并就相关问题开展了深入探讨。

CNCERT/CC 在会上做了题为“网络安全趋势与合作方向”的报告，介绍了网络安全的最新发展趋势和中日韩三国在网络安全应急处理方面的合作需求，该报告受到了与会代表的极大关注和积极响应。

6.4. CNCERT/CC 应邀参加亚欧会议网络安全研讨会

2005 年 6 月 23 日至 24 日，由韩国信息通信部(Ministry of Information and Communication, Republic of Korea）主办，韩国信息安全局 KISA（Korea Information Security Agency）承办的亚欧会议网络安全研讨会在韩国汉城举行。应主办方邀请，CNCERT/CC 派技术专家参加了此次会议。来自 38 个亚欧会议国家的政府部门代表和技术专家也参加了此次研讨会。

此次会议是经第五届亚欧首脑会议批准，由“亚欧会议加强网络安全倡议”确定的。“亚欧会议加强网络安全倡议”是第五届亚欧首脑会议（2004 年 12 月，越南河内）通过的重要后续行动新倡议，我国是该倡议共提国。该倡议包括建立信息交流等合作机制，研究预防和处理网络恐怖主义、垃圾邮件的措施，制定网络安全标准，举办高级别会议为各国制定相关政策提出建议等内容。

两天的会议由建立协作的应急响应框架（Establishing a Cooperative Response Framework）、推广安全文化（Promoting a Culture of Security）、发展遏制网络攻击的能力（Building Capabilities to Mitigate Emerging Cyber Attacks）及全体讨论（Plenary Discussion）四个部分组成。

通过此次会议，CNCERT/CC 与亚欧会议各成员国交流了在应对网络安全威胁方面的经验，了解了亚欧会议各成员国在网络安全方面的有益经验和方法，进一步开拓了合作渠道，增进了 CNCERT/CC 与国外应急组织的了解，为进一步开展合作打下了一定基础。

6.5. CNCERT/CC 组团参加第十七届 FIRST 会议

2005 年 6 月 24 日至 7 月 2 日，CNCERT/CC 组团参加了在新加坡举行的第十七届 FIRST 大会，代表团成员分别来自信息产业部电信管理局、CNCERT/CC、中国移动和中国联通等单位的应急组织。参加本次大会的代表有 325 人，来自 5 大洲的 38 个经济体，涉及 90 个 FIRST 成员。

本次会议内容丰富，包括有国家基础信息设施保护、大规模网络监测、集中式网络安全事件日志收集和分析、无线入侵监测系统、无线网络安全、漏洞分析研究、网络欺诈、间谍软件等多个专题。

CNCERT/CC 代表在会上作了题为“CNCERT/CC2004 年反网络欺诈活动回顾”的报告，同时，通过本次会议，CNCERT/CC 和与会代表进行了广泛的交流，与更多国家和地区的应急组织建立了更加直接的联系，并对国际应急组织的新特点和发展趋势有了更深入的了解，主要表现在以下几个方面：

1、应急组织继续不断增多，出现更多政府和国家级应急组织

FIRST 在过去一年里，又增加了 21 个正式成员，其中包括欧洲、美洲很多的政府或国家级应急组织。

越来越多的政府和国家级应急组织的出现，说明更多的国家认识到了国家级应急组织对于应对公共网络安全的威胁以及保护国家关键基础信息设施的作用和价值，这也使 FIRST 目前对犯罪取证、与执法机构的合作、国家关键基础设施保护等问题开始有了更多的讨论。

2、区域性应急合作组织日趋活跃

欧洲的应急合作组织 TF-CSIRT、亚太地区的 APCERT 在本次会议上都比较活跃，从各方面的情况来看，国际上区域性应急合作组织正在变得日益活跃，国际组织间的更广泛的合

作也将成为趋势。

3、应急组织间信息交换和互动进入实质性阶段

许多应急组织都在积极推动安全事件信息的交换和共享，以推动区域和全球的安全事件协作。美国、德国等应急组织在推动应急组织间的信息共享方面都取得了实质性的进展，同时，日本和韩国的应急组织之间也已经开始了日常的数据交换。

在会议期间 APCERT 还召开了指导委员会会议，确定了 APCERT 2006 年年度会议将在中国召开。另外，CNCERT/CC 提出的在 APCERT 成员中加强技术和数据交流、开展亚太区域网络安全状况调查等议案得到了广泛支持，APCERT 将陆续开展这些工作。

此外，会议前期 CNCERT/CC 组织部分参会代表参加了欧洲 TF-CSIRT 的应急组织培训计划 TERENA 的讲师培训，由于 APCERT 已经和 TF-CSIRT 签订了合作备忘录，CNCERT/CC 将在本区域应急组织培训等方面发挥更大作用。

6.6. CNCERT/CC 参加信息社会世界高峰会议网络安全研讨会

2005 年 6 月 28 日至 7 月 1 日，CNCERT/CC 应邀参加了由国际电信联盟(ITU)主办的信息社会世界高峰会议网络安全研讨会（ITU WSIS Thematic Meeting for Cybersecurity）。来自网络安全相关的成员国的政策制定部门、管理部门、国际和政府间组织、隐私保护组织以及通信服务提供商、信息通信技术公司、学术组织、民间组织等共 150 多名代表参加了此次会议。

此次会议是根据 2003 年 12 月 12 日信息社会世界高峰会议第一阶段通过的原则宣言和行动计划的有关决议要求组织的，并作为 2005 年 11 月 16 至 18 日信息社会世界高峰会议突尼斯阶段会议的准备工作。

CNCERT/CC 在会上做了题为“建立国家级应急响应能力”的报告，介绍了我国网络安全应急体系和应急平台建设的经验，该报告受到了与会代表的极大关注和响应。

通过此次会议，CNCERT/CC 进一步了解了国外在反垃圾邮件和网络安全立法、技术监测、标准和国际合作方面的经验，并与国外的 CSIRT 组织进行了广泛的交流。

6.7. CNCERT/CC 参加第 32 届 APEC 电信工作组会议

2005 年 9 月 5 日至 9 日,第 32 届 APEC 电信工作组会议在韩国汉城召开，来自 APEC 成员组织和经济合作发展组织(Organization for Economic Co-operation and Development 英文简称 OECD）的近 200 名代表出席了本次会议。

CNCERT/CC 随信息产业部一同出席了本次会议，并重点参加了“APEC 和 OECD 联合工作会议”、“电子安全工作组会议”和“商务促进指导委员会会议”、“APEC 电信工作组全会”等与网络安全相关的会议，并在 APEC 和 OECD 联合工作会议（APEC/OECD Joint Workshop）“促进发展全球有效应急响应能力”分主题会议上，做了题为“CNCERT/CC 跨国合作实践及经验”的报告。

会上，各经济体围绕计算机及网络安全的技术、法律、政策、教育等多个议题展开了充分的讨论。可见,网络安全问题已经成为全球各经济体普遍关注的热点问题，特别是网络安全新技术、新动态更是受到了各经济体的密切关注。同时 ,各国 CERT 应急响应能力建设和国际协作也越来越受到国际社会的重视。

6.8. CNCERT/CC 参加亚太联合网络安全应急演练

国家计算机网络应急技术处理协调中心（CNCERT/CC）于 2005 年 12 月 21 日上午参加

了由亚太网络安全应急联盟（APCERT）举行的旨在检验各成员应急响应和协作配合能力的2005 亚太联合网络安全应急演练。

此次演练是由中日韩三国的 APCERT 成员第二次牵头组织的跨地区联合演练，参加今年联合演练的成员增加到 10 个，分别来自澳大利亚、中国大陆、中国香港、中国台湾、日本、韩国、马来西亚、菲律宾、新加坡等 9 个经济体。

该演练以一个假设的跨地区大规模僵尸网络事件为处理对象，该僵尸网络发动了针对韩国多个重要网站的攻击，在接到韩国(KrCERT)的报警后，APCERT 各成员在各自国家和地区迅速采取措施阻止并摧毁了该僵尸网络。僵尸网络是由大量被黑客通过专门程序——僵尸程序控制的计算机组成的“地下网络军队”，它被黑客远程控制来发起各种攻击，如分布式拒绝服务攻击（DDOS）等。

此次成功的演练充分检验了 APCERT 成员的联络机制和应对互联网攻击的响应流程，也表明了 APCERT 成员能够通过发挥各自经济体的作用来积极协助其他成员处理涉及本经济体的攻击事件。

同时，CNCERT/CC 认为，本次演练也更进一步说明了建立国家级和地区级的应急组织间的可信合作关系和处理流程，是应对目前日益严重的跨地区安全事件的最有效、最重要的途经之一。我国目前已经形成了国内的公共互联网应急体系，而 CNCERT/CC 与 APCERT 的合作则架设了一个连接国际应急体系的可信桥梁。CNCERT/CC 将对本次演练进行认真总结，进一步改进与国际、国内同行的合作方式和工作流程，提高我国的应急能力和协调能力，从而更好地为保障我国互联网安全服务，为带动 APCERT 推动亚太地区的互联网安全贡献力量。

7. 结束语

总体来看，2005 年没有发生造成严重后果的大规模网络安全事件，利用系统漏洞进行传播的蠕虫已经不再是安全事件中的独家主角，而以僵尸网络、间谍软件、身份窃取为代表的各类恶意代码则逐渐成为最大威胁，同时，拒绝服务攻击、网络仿冒、垃圾邮件等安全事件仍然猖獗；此外，2005 年也发生多起与政治纪念日和时政相关的网络攻击活动，因此 2005 年的安全事件在保持整体数量上显著上升的同时，也呈现出技术复杂化，动机趋利化、政治化的特点。

根据中国互联网信息中心 2006 年 1 月 17 日公布的《中国互联网络发展状况统计报告》显示，截至 2005 年 12 月 31 日，我国上网用户总数为 1.11 亿人，上网计算机达到 4950 万台，网络用户和网络主机的数量仍然在持续增长，与此同时，电子政务、电子商务、网络游戏、网络博客等互联网业务正在快速扩展，新的操作系统、新应用软件不断投入使用，这些都导致大量人为主观疏忽和网络系统客观漏洞的存在。而黑客攻击动机已经从单纯的追求“荣耀感”向获取多方面实际利益和表达政治情绪的方向转移，黑客技术的发展也将重点放在网上木马、间谍程序、恶意网站、网络仿冒、僵尸网络等方面，因此，网络安全问题变得更加错综复杂，涉及范围将不断扩大。

由于黑客发动攻击的目的的转变，2006 年发生大规模的网络安全事件的可能性比较小，以僵尸网络、间谍软件、身份窃取为代表的恶意代码，以及网络仿冒、网址嫁接／劫持类安全事件将会继续增加，对新流行的网络应用的安全事件将会发生，这些问题将导致事件数量整体仍呈上升趋势。

2006 年利用系统漏洞进行传播的蠕虫仍将不会是主角，但是漏洞的利用周期将继续缩短。蠕虫全面 0day 化将成为事实，扫描型蠕虫的对整体网络压力影响力继续减少，蠕虫逐步走慢速扫描、可靠扩散的道路；

僵尸网络（botnet）将进一步获得发展，大规模僵尸网络数量将减少，小规模的僵尸网络数量将会增加，被感染的僵尸节点数量增长将趋缓，僵尸网络使用的通讯协议将从 IRC 协议发展到多协议并存的状态，将会出现僵尸网络采用自定义的通讯协议的情况，自定义协议将形成具有加密、认证、压缩能力的完整体系；

新网络攻击初显端倪，网络钓鱼（phishing）会演变出新的形势，网址嫁接（pharming）与网址劫持（hijack）事件将不断增多。间谍软件（包括广告件、色情件等等）将继续发展，越来越多的走向半合法化的灰色地带，手机上的间谍软件将会出现。基于 symbian 的手机病毒将进一步增多，但 Linux 和 WinCE 平台是否会出现大量病毒值得观望。随着 VoIP 业务的逐渐普及，Voicespam 出现的可能性增大。出于竞争等经济目的，VoIP 网关被攻击的可能性也逐渐增大；

无线网应用日益广泛，由无线协议本身导致的安全事件将有所增加。

骨干网网络设备本身的漏洞依然存在，发生由于骨干网络设备故障引起的网络中断等安全事件还是存在可能。

总之，在我国互联网产业继续快速发展的同时，网络安全形势将注定趋于复杂和严重。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。

编者按：

谢谢您阅读“CNCERT/CC2005 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，来信地址为：cncert@cert.org.cn。

版权声明：

“CNCERT/CC2005 年网络安全工作报告”版权为 CNCERT/CC 所有。转载或引用其中的有关内容，包括数据及图表，请注明出处。