

CNCERT/CC

2006 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 2006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 2006 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。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	5
3.1 事件接收情况	6
3.2 事件处理情况	7
3.3 事件处理案例介绍	8
4 信息系统安全漏洞公告情况	10
4.1 CNCERT/CC 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	16
7 被篡改网站监测分析	17
7.1 我国网站被篡改情况	18
7.2 我国大陆地区政府网站被篡改情况	19
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 网络安全信息服务	22
10.1 安全信息通报	23
10.2 CNCERT/CC 网站信息发布	23
10.3 电子邮件列表信息发布	23
10.4 2005 年全国网络安全状况调查情况	24
11 网络安全应急组织发展情况	25
11.1 国际部分	25
11.2 国内部分	25
12 国际合作与交流	26
13 结束语	26

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，并于 2006 年再度当选副主席。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

2006 年,我国公共互联网继续快速发展,用户数量已超过 1.37 亿,各种互联网新业务如雨后春笋般涌现,电子政务、电子商务得到进一步推广,互联网的社会基础设施功能表现得越来越明显。与此同时,互联网作为一个运行系统和社会公共环境,其所面对的和所隐藏的安全威胁也越来越复杂,越来越严重。

CNCERT/CC 在 2006 年接收和自主发现的网络安全事件与去年同期相比有了大幅度的增加,其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、涉及国内外商业机构的网络仿冒类事件和针对互联网企业的拒绝服务攻击类事件的影响最为严重,僵尸网络和木马的威胁依然非常严重,攻击者谋求非法利益的目的更加明确,行为更加嚣张,黑客地下产业链基本形成。

信息系统安全漏洞是各种安全威胁的主要根源之一。2006 年 CNCERT/CC 共整理发布和我国用户密切相关的漏洞公告 87 个,同比 2005 年增长了 16%;其中的部分漏洞严重威胁互联网的运行安全,更多的漏洞则对广大互联网用户的系统造成严重威胁。2006 年与安全漏洞关系密切的零日攻击现象在互联网上显著增多。“零日攻击”是指漏洞公布当天就出现相应的攻击手段,例如 2006 年出现的“魔波蠕虫”(利用 MS06-040 漏洞)以及利用微软 word 漏洞(MS06-011 漏洞)木马攻击等。

此外,恶意代码成为黑客入侵用户主机、构建僵尸网络,进而窃取用户重要信息并控制受害计算机发动大规模攻击的重要手段。2006 年,仅 CNCERT/CC 每天通过分布式蜜网所捕获的新的漏洞攻击型恶意代码数量就达到 96 个,平均每天捕获次数高达 3069 次。除此以外,互联网上还充斥着大量通过网页、邮件、聊天攻击、P2P 传播的恶意代码,令人防不胜防。

从 CNCERT/CC 掌握的情况来看,我国互联网用户和信息系统遭受攻击情况不容乐观。

在木马方面,CNCERT/CC 抽样监测发现我国大陆地区约 4.5 万个 IP 地址(以下无特殊说明均包含动态 IP)的主机被植入木马,与去年同期相比增长一倍。同时还发现境外约 2.7 万个木马攻击源,主要位于美国、韩国和中国台湾。

在僵尸网络方面,CNCERT/CC 抽样监测发现我国大陆地区约有 1 千多万个 IP 地址的主机被植入僵尸程序;境外约 1.6 万个 IP 对我国境内的僵尸主机实施控制,主要仍位于美国、韩国和中国台湾。

在网页被篡改方面,CNCERT/CC 监测到中国大陆被篡改网站总数达到 24477 个,与去年同期相比增长接近一倍,其中 .gov 网站被篡改数量为 3831 个,占整个大陆地区被篡改网站的 16%。政府网站被频繁入侵,不仅极大影响了政府形象,也体现出我国在电子政务发展中遇到严重的安全隐患。

总体来看,我国的公共互联网网络安全状况令人堪忧,在利益的驱动下网络安全事件更加频繁、隐蔽和复杂,需要政府、产业界、运营商、网络用户等各方给以高度重视并加强合作,采取切实有效的措施加以应对。

3 网络安全事件接收与处理情况

CNCERT/CC 通过热线电话、传真、Email、网站等方式接收公众的网络安全事件报告。在收到事件报告后,CNCERT/CC 协调各省分中心对于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进行及时、有效处理。网络安全事件的接收与处理数量反映了我国互联网网络安全的宏观状况,同时也体现出我国计算机网络应急处理的能力。

3.1 事件接收情况

2006 年 CNCERT/CC 接收 26476 件非扫描类网络安全事件报告（其中包括从 2006 年 8 月启用的自主研发的篡改网页监测系统发现的数据），与 2005 年相比增长了两倍左右。2003 年至 2006 年，CNCERT/CC 接收非扫描类事件报告数量比较如图 1 所示。

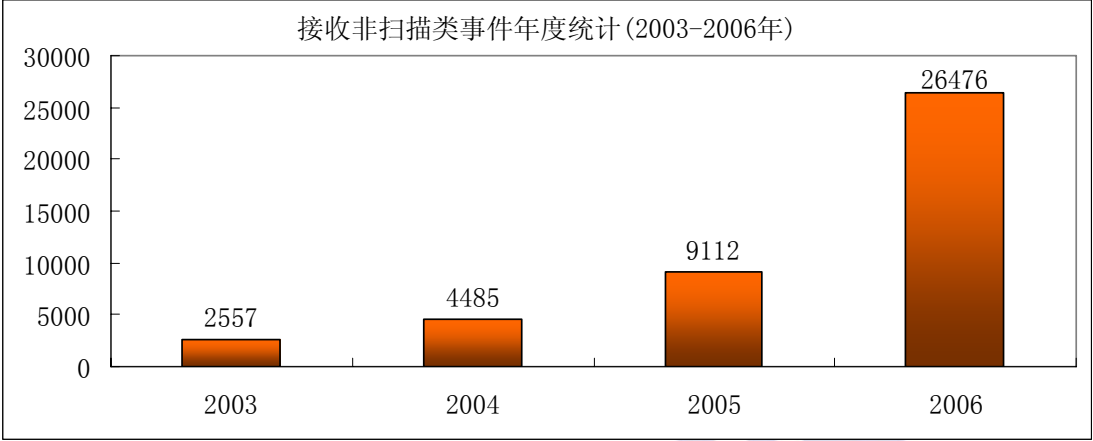


图 1 接收非扫描类事件年度统计(2003-2006 年)

按所报告的事件类型统计，报告较多的是网页篡改、垃圾邮件、网络仿冒和网页恶意代码事件。与 2005 年相比，网络仿冒事件的数量由 475 件增加至 563 件，网页恶意代码事件由 25 件增加至 320 件，垃圾邮件事件由 161 件增加至 587 件。其中网页恶意代码类事件报告同比激增 12.8 倍，垃圾邮件事件报告也有明显增加。

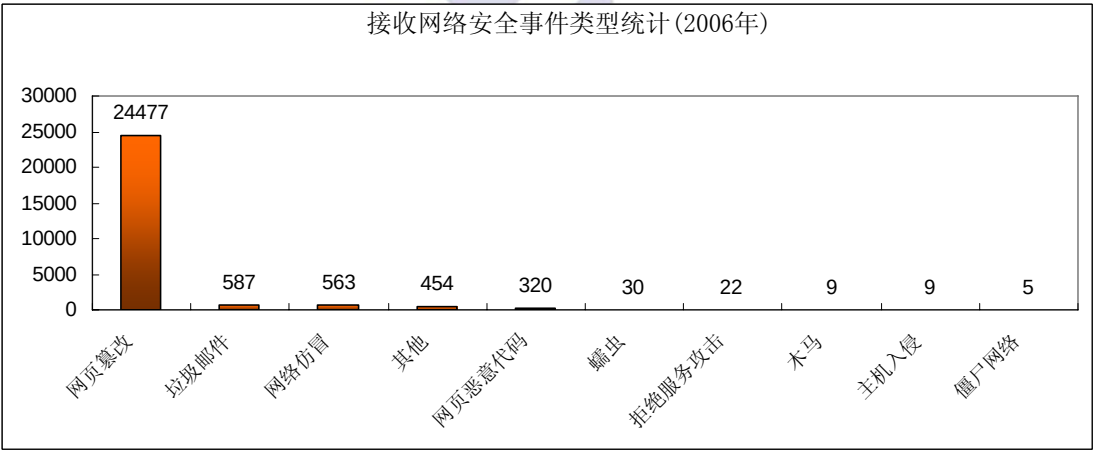


图 2 接收网络安全事件类型统计(2006 年)

2006 年每月的具体事件报告数量如图 3 所示。需要说明的是，2006 年 8 月份开始，CNCERT/CC 启用被篡改网页监测系统，并扩大了收集网页篡改报告的数据来源。从图 3 可以看到，自添加了被篡改网页自主监测手段后，每月的事件报告数量有了明显的上升。

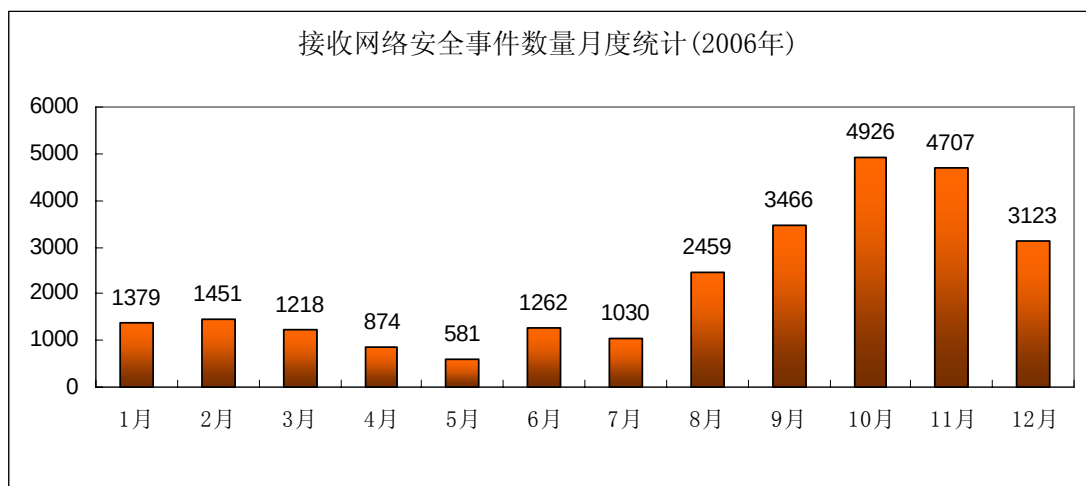


图3 接收网络安全事件数量月度统计(2006年)

3.2 事件处理情况

2006年CNCERT/CC共成功处理网络安全事件613件,主要事件类型包括网页篡改、网络仿冒、恶意代码网站、拒绝服务攻击等,各类事件处理数量如图4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。

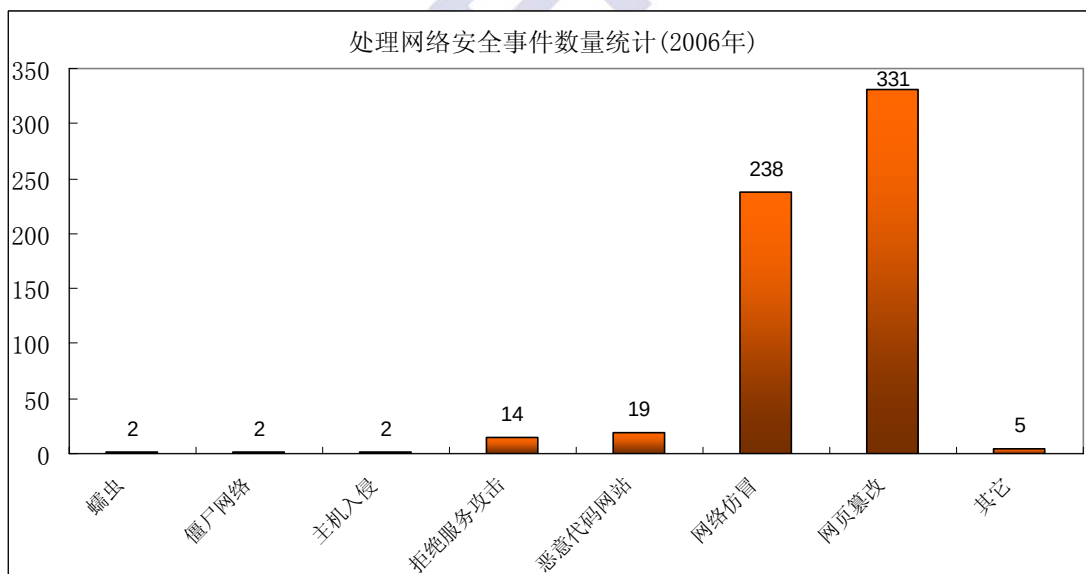


图4 处理网络安全事件数量统计(2006年)

CNCERT/CC在我国大陆各省设有分中心,大多数安全事件都是由CNCERT/CC国家中心(总部)指挥协调各分中心进行处理的。2006年各省分中心参与事件处理的次数如下图所示,其中广东、北京、上海、福建、辽宁处理事件数量居前5位。

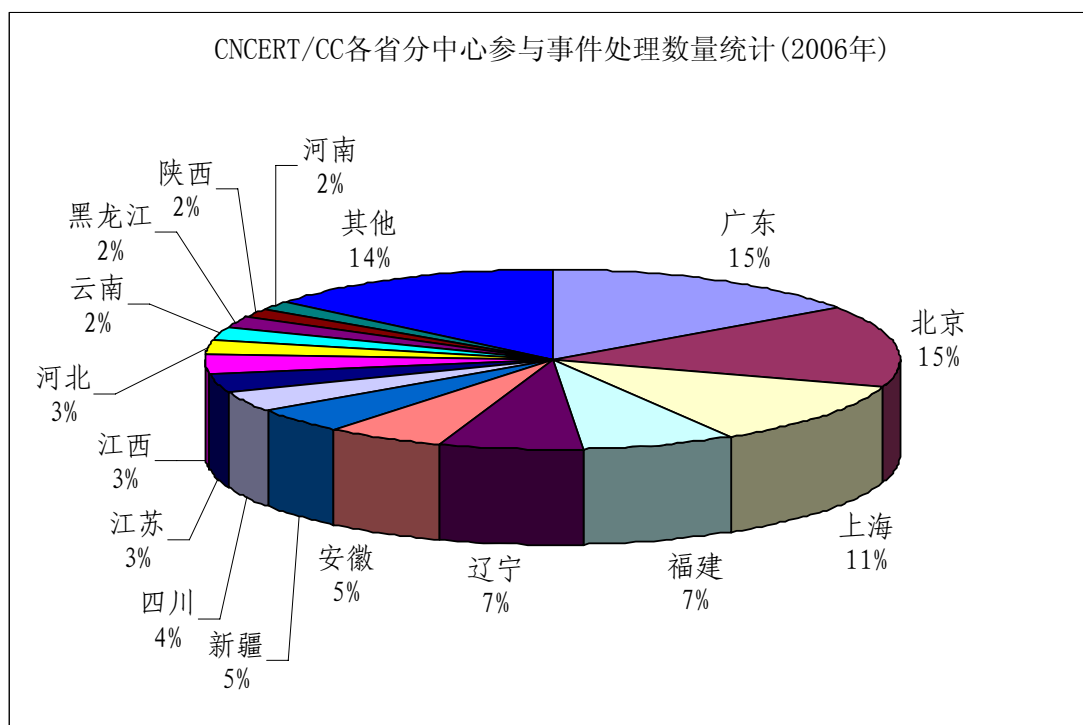


图 5 CNCERT/CC 各省分中心参与事件处理数量统计(2006 年)

3.3 事件处理部分案例介绍

3.3.1 “魔波”蠕虫处理

2006 年 8 月 8 日，微软公司发布了例行安全公告。CNCERT/CC 从国际渠道获知针对公告中的 MS06-040 漏洞（远程服务的溢出攻击漏洞）的攻击代码已经出现。8 月 14 日，CNCERT/CC 成功捕获到针对该漏洞进行自动传播的蠕虫（“魔波”）样本，经深入分析发现，该蠕虫可攻击所有存在漏洞的 Windows 系统。蠕虫入侵以后，会在受害主机上释放一个僵尸程序，并驱使受害主机连接到特定的 IRC 服务器接收黑客控制，从而构成一个大规模的僵尸网络。从僵尸程序内置的命令来看，黑客可以用其发起拒绝服务攻击，扫描或文件下载等行为。14 日当天，CNCERT/CC 也接到用户报告，称怀疑遭受蠕虫的攻击，影响较严重。

根据掌握的信息，CNCERT/CC 认为攻击者可能利用国内大量用户未及时安装 MS06-040 漏洞补丁的间隙，制造更多的蠕虫或蠕虫变种在网上传播，会对我国互联网造成严重危害，于是立即启动了大规模网络安全事件处理流程。

CNCERT/CC 一方面迅速切断了位于我国大陆境内的僵尸网络控制服务器，阻止黑客对受害主机的控制；另一方面对该蠕虫的扩散和感染情况进行监测。截至 8 月 18 日，CNCERT/CC 共掌握感染“魔波”蠕虫的 IP 地址 105 万个，其中中国大陆境内为 12.5 万个，除向我国相关部门通报情况并积极配合处置外，CNCERT/CC 还向 APCERT 成员以及英国、阿根廷、巴西、西班牙、加拿大、德国、墨西哥、波兰、俄国、法国、意大利、智利、奥地利等受影响较重的 13 个国家的 CERT 组织通报了各方感染主机的详细信息，促进该事件在全球范围内的协同处理。9 月中旬，该事件的处理基本结束。

本次事件处理是我国应急组织第一次在全球性事件处理中发挥主导作用,由于事件处理的及时有效,因此得到了各应急组织的好评,树立了中国作为负责任的互联网大国的良好形象。

3.3.2 拒绝服务攻击事件

2006 年拒绝服务攻击事件频繁发生,并表现出规模大、目标确定、经济目的突出的特点。针对这种情况,CNCERT/CC 加大了对于拒绝服务攻击事件的处理力度,全年共处理拒绝服务攻击事件 14 起。

帮助江苏扬州一公司结束了持续两年遭受分布式拒绝服务攻击的局面

5 月 17 日,CNCERT/CC 接到报告,称江苏省扬州某公司持续两年遭到分布式拒绝服务(DDOS)攻击,最近的攻击致使该公司整个网络运营业务完全中断,损失严重。CNCERT/CC 协同分中心和服务试点单位立即对攻击源进行了定位、远程取证和技术分析,为江苏省扬州市公安部门提供资料,协助公安部门将涉案黑客缉拿归案。

帮助某网站查找分布式拒绝服务攻击源

12 月 8 日,CNCERT/CC 接到事件报告,称北京某高新企业网站遭受分布式拒绝服务攻击,攻击造成整个 IDC 机房内几百台服务器的网络通信受阻。CNCERT/CC 协同多个分中心对 5 个攻击流量最大的攻击源进行定位,在运营商的配合下对攻击源进行了远程取证和技术分析,并向公安部门提供了有力线索。

协调处理辽宁锦州某运营商遭分布式拒绝服务攻击事件

12 月 15 日,CNCERT/CC 接到事件报告,称辽宁锦州某运营商遭分布式拒绝服务攻击,来自陕西省的两个 IP 地址发送大量数据包到辽宁锦州的路由器。CNCERT/CC 陕西分中心立即协调运营商处理,攻击于当日中止。

3.3.3 其它典型事件处理介绍

与韩国应急组织协调处理我国网民盗用韩国居民身份证号码事件

2 月 21 日,韩国应急组织向 CNCERT/CC 反映,数万个中国网站发布或转载了韩国居民身份证号码,大量中国网民盗用这些号码用来注册韩国的网络游戏和其他网站,该事件严重威胁个人隐私,已成为韩国国内当时最受关注的话题之一。CNCERT/CC 对此事进行了认真调查分析,将所掌握的情况及时向有关部门报告,并提出了相关建议,同时与韩方保持密切沟通,了解其国内的局势发展和可能出现的针对我国的大规模网络攻击迹象。由于双方的及时沟通和相互理解,该事件得到了有效的控制,没有带来更严重的外交纠纷。

协助科技网处理某科技集团一研究所的 Rbot 僵尸网络事件

4 月 24 日,中国科技网应急组织向 CNCERT/CC 发来协助请求,报告某国家科技集团研究所发生了严重的网络安全事件。CNCERT/CC 立即启动了相关的处理流程,前往现场进行技术调查,发现并提取恶意程序样本;对样本进行了全面分析后,确认该样本为僵尸程序 Rbot 的新变种。随后,CNCERT/CC 向科技网发函通报了分析情况和处理建议,使得该事件

得以成功解决。

帮助我国某大型公司处理一起非法入侵事件

12月27日，CNCERT/CC 接到国家某大型企业的事件报告，称该公司的计算机系统近期被四次非法入侵，入侵者删除了大量域账户和很多重要文件，严重影响了信息系统的安全运行和企业的正常生产。CNCERT/CC 迅速前往用户现场进行详细分析，判断出该事件是企业内部人员所为，并向该企业提供了涉嫌人员的相关定位信息，该企业根据此线索成功处理了该事件，还特意向 CNCERT/CC 致函感谢。

4 信息系统安全漏洞公告情况

据美国 CERT/CC 统计¹，该组织 2006 年全年收到信息系统安全漏洞报告 8064 个，平均每天超过 22 个，与 2005 年同期相比增长了 34.6%。自 1995 年以来，漏洞报告总数达到 30780 个，具体统计结果如图 6 所示。

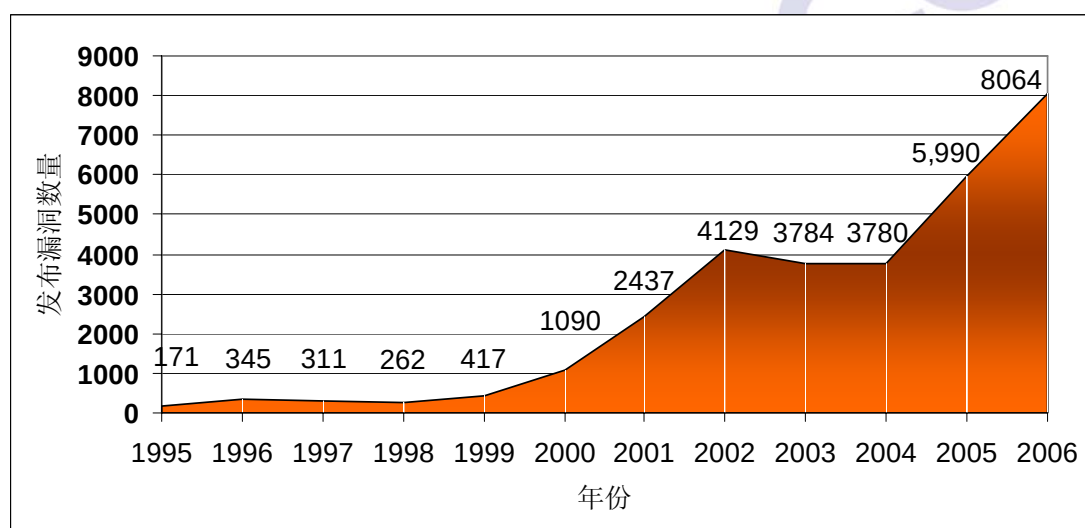


图 6 网络安全漏洞数量统计

2006 年除 windows 漏洞和 IE 浏览器漏洞外，微软公司 Office 软件的安全漏洞也在不断增加。微软公司在 2005 年正式公布了 55 个具有编号的安全漏洞，2006 年则公布了 78 个²，同比增长 41.8%。漏洞的大量出现和不断快速增加是网络安全总体形势趋于严峻的重要原因之一。

4.1 CNCERT/CC 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，在第一时间将相关的漏洞信息通告给运营商、重要信息系统管理部门和用户，从而有效降低了漏洞对于我国互联网的影响。2006 年 CNCERT/CC 共整理发布和我国用户密切相关的漏洞公告 87 个，2005 年同期发布漏洞公告 75 个，同比增长 16%。下面列举几个 2006 年 CNCERT/CC 重点处理的漏洞。

¹ 数据来源：<http://www.cert.org>

² <http://www.microsoft.com/china/technet/security/current.mspx>

CNCERT/CC 发现 Windows 系统 IPSec 漏洞

2006 年 7 月, CNCERT/CC 发现微软 Windows 2000 操作系统的 IPSec 策略管理存在环境竞争漏洞, 该漏洞可能导致用户配置的原有 IPSec 策略失效, 导致原本加密的用户数据在用户不知情的情况下以明文传输, 从而带来信息泄露的风险。针对此漏洞, CNCERT/CC 通知微软公司, 并报送了国家主管部门, 提醒互联网运营单位注意。

微软 Word 缓冲区溢出漏洞 (MS06-027)

5 月底, CNCERT/CC 获知微软 Word 存在一个缓冲区溢出漏洞, 用户一旦打开一个利用此漏洞的 Word 文档可能诱发攻击。考虑到我国的 Word 用户众多, CNCERT/CC 高度重视此漏洞的情况, 及时在网站上发布了公告, 并跟踪利用该漏洞的后门, 对攻击程序进行了分析和监测。

Juniper 路由器存在的严重安全漏洞

CNCERT/CC 于 6 月 23 日通过国际渠道获知, 全球最大的网络设备厂商之一——Juniper 的路由器被发现存在严重安全漏洞, 当路由器用于 IPv6 网络, 并持续接收特定结构的 IPv6 数据包时, 系统将因内存溢出而崩溃。攻击者通过远程攻击即可造成使用该路由器的 IPv6 网络瘫痪。因为我国互联网中有很多 Juniper 路由器, CNCERT/CC 及时向各互联网运营单位发出了安全预警, 各运营商均做出快速响应, 及时升级了相关网络设备。

Oracle 六月份关键补丁涉及的系列产品漏洞

Oracle 六月份关键补丁涉及的产品漏洞主要影响对象是使用大型数据库系统的企业和部门, 考虑到 Oracle 数据库在我国的广泛使用, CNCERT/CC 及时向有关部门报告了漏洞信息, 并在网站上发布了安全公告, 建议用户下载 Oracle 发布的安全补丁并立即升级数据库系统。

微软 OFFICE 的远程代码执行漏洞 (MS06-048)

微软 OFFICE 的远程代码执行漏洞 (MS06-048) 存在于其 OFFICE 办公套件的 PowerPoint 中, 该软件在我国应用非常广泛。CNCERT/CC 在微软发布针对该漏洞的补丁程序之前, 获知此漏洞, 并判断在尚没有补丁的情况下, 广大使用 PowerPoint 用户的系统将面临严重威胁, 为此, CNCERT/CC 于 7 月 24 日及时向有关部门做了报告, 并在网站上发布了安全公告, 提醒用户谨慎处理来源不明的 PowerPoint 文件。

5 互联网业务流量监测分析

随着互联网的迅速发展, 各种新兴互联网应用技术不断出现并得以广泛使用, 这使得互联网流量中的业务种类及其所占流量比例也发生明显变化。对流量的分析不仅能对互联网运营的科学化管理提供重要参考, 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 对互联网业务流量的抽样统计, 在 TCP 协议中, 前三类最占带宽的网络应用是 Web 浏览、P2P 下载和电子邮件。

各种 P2P 下载软件 (例如 eMule、BitTorrent、迅雷等) 占用了大量网络带宽, 说明其拥有大量用户群, 如果其中存在安全漏洞并被黑客掌握, 必将带来严重后果。事实上, 2006 年日本曾发生因一种热门 P2P 下载软件存在严重漏洞而导致的重要机密泄漏事件。因此我国应对此引起必要的重视。

TCP 25 号端口承载着电子邮件协议，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。

各种业务流量的具体情况如图 7 所示：

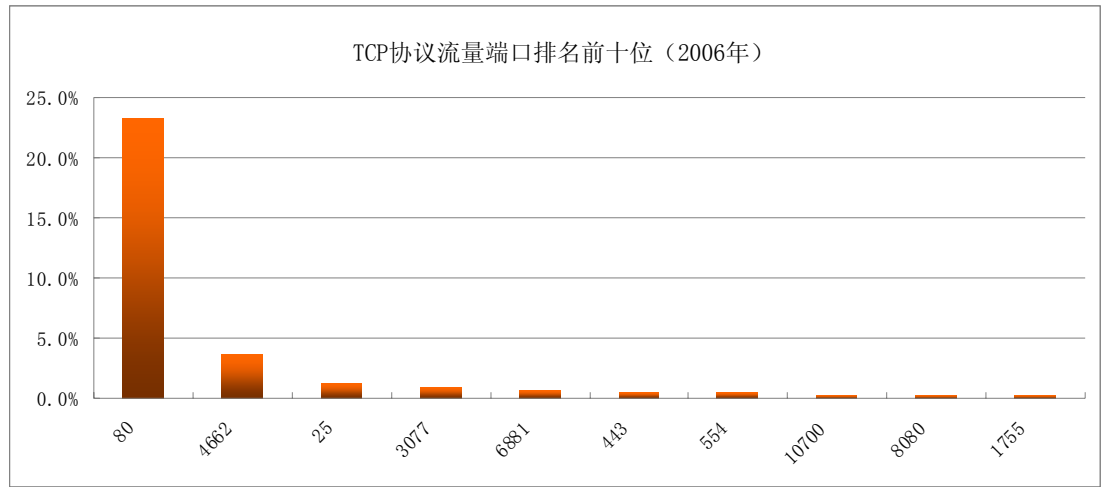


图 7 TCP 协议流量端口排名前十位（2006 年）

TCP 端口	TCP 流量排名	百分比	主要的业务种类
80	1	23.3%	网页服务
4662	2	3.6%	eMule 下载
25	3	1.2%	Email 服务
3077	4	0.9%	迅雷下载
6881	5	0.6%	BitTorrent 下载
443	6	0.5%	网页服务
554	7	0.5%	RTSP 实时流协议
10700	8	0.3%	eMule 下载
8080	9	0.2%	网页服务
1755	10	0.2%	MMS 微软媒体服务

表 1 TCP 协议流量端口排名前十位（2006 年）

在 UDP 协议中，主要的应用是 DNS 服务，它在 UDP 包数统计中排名第一，在 UDP 端口流量中排名第三，占 UDP 总流量的 2.2%。DNS 是互联网正常运行的基本和必要服务，因此需要重点的保护；与此同时，黑客也越来越多地开始利用动态域名等服务来操控僵尸网络，躲避追踪和处置，因此对 DNS 服务的监测和管理需要进一步加强。

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 eMule、常用于视频点播的实时流协议也占用较多带宽。具体情况如图 8 所示。

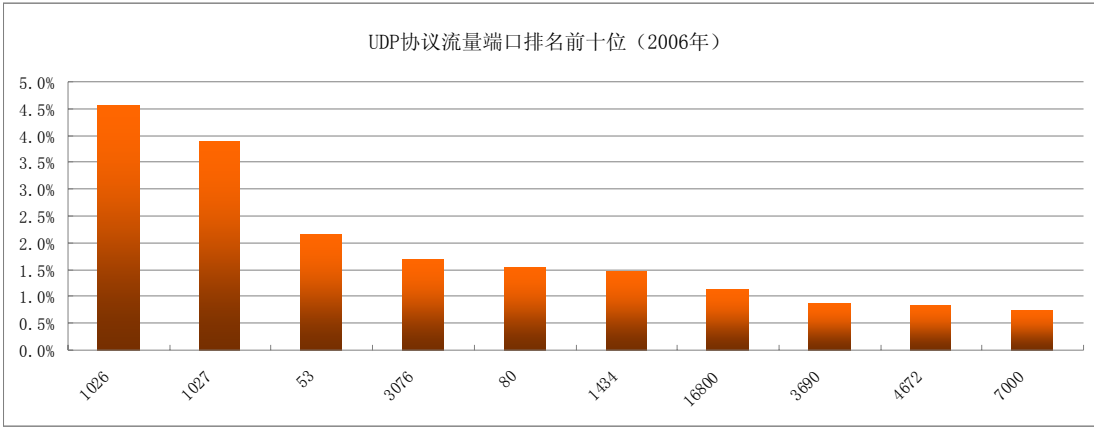


图 8 UDP 协议流量端口排名前十位（2006 年）

UDP 端口	UDP 流量排名	百分比	主要的业务种类
1026	1	4.6%	MS Messenger 服务
1027	2	3.9%	MS Messenger 服务
53	3	2.2%	DNS 服务端口
3076	4	1.7%	迅雷下载
80	5	1.5%	网页服务
1434	6	1.5%	MSSQL 服务
16800	7	1.1%	Tvants 电视蚂蚁
3690	8	0.9%	svnserve 服务
4672	9	0.9%	eMule 下载
7000	10	0.7%	酷狗下载

表 2 UDP 协议流量端口排名前十位（2006 年）

此外，鉴于互联网 IP 电话业务发展迅速，在 2006 年上半年，CNCERT/CC 对于 SIP 协议的使用情况进行了抽样监测，统计结果表明在实际应用中，有约 60% 的 SIP 协议使用默认的 UDP 5060 端口。从国内分布来看，SIP 服务器主要分布在上海、广东、北京、江苏、福建等地，其中上海最多——占 25%，其次是广东——占 18%。从国家和地区分布来看，SIP 服务器主要在美国、中国台湾、中国香港，其中美国最多——占 46%，其次是中国台湾和中国香港，分别占 19% 和 11%。

6 木马与僵尸网络监测分析

各类安全事件中，木马和僵尸网络类事件隐蔽性非常强且危害严重，会危及用户的个人隐私、敏感信息，同时也是造成泄密事件、垃圾邮件事件和大规模 DDoS 攻击发生的一个重要原因，CNCERT/CC 对于木马与僵尸网络的活动情况给予充分关注，长期利用 863-917 网络安全监测平台进行抽样监测，并不断增加技术手段来加大发现力度。

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。

6.1.1 中国大陆地区被木马控制的计算机分布统计

2006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44717个IP 地址的主机被植入木马，与去年同期相比增长一倍。我国大陆地区木马活动分布情况如图9所示，木马被控制端最多的地区分别为广东省（18%）、北京（15%）、福建（8%）和浙江(8%)。

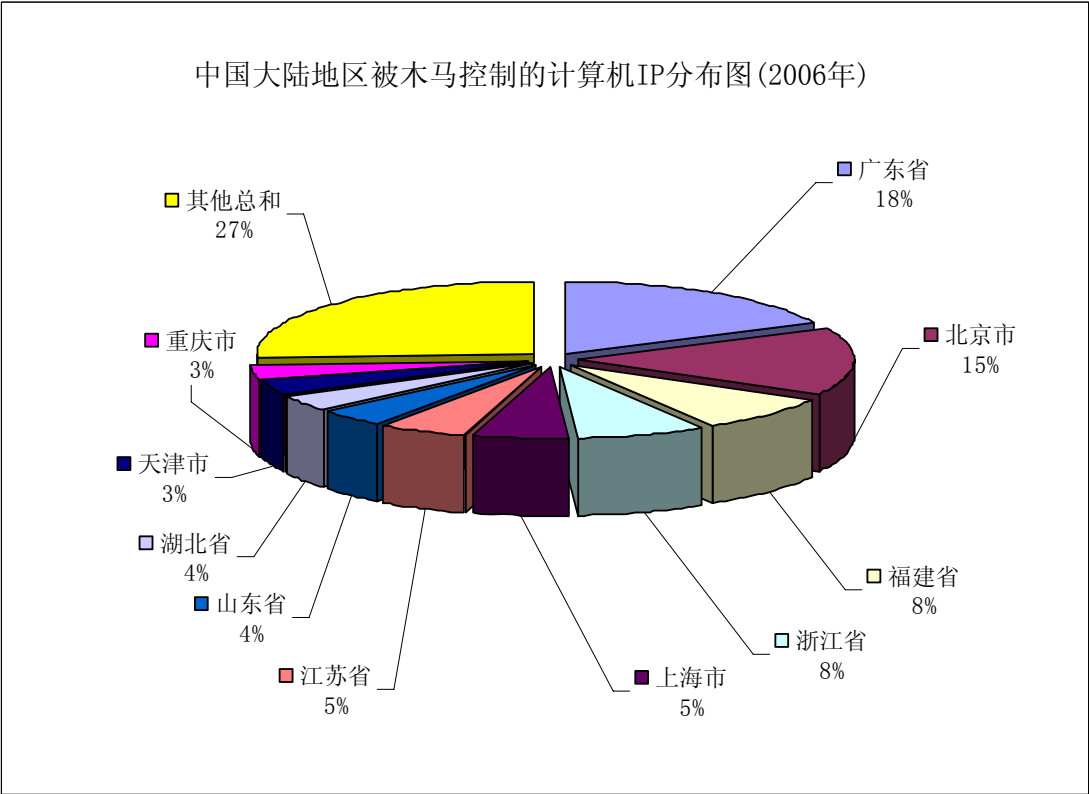


图 9 中国大陆地区被木马控制的计算机 IP 分布图(2006 年)

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27560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10所示，其中位于美国（25%）、韩国（12%）、中国台湾（9%）、日本（8%）和中国香港(7%)的木马控制端数量居前五位。

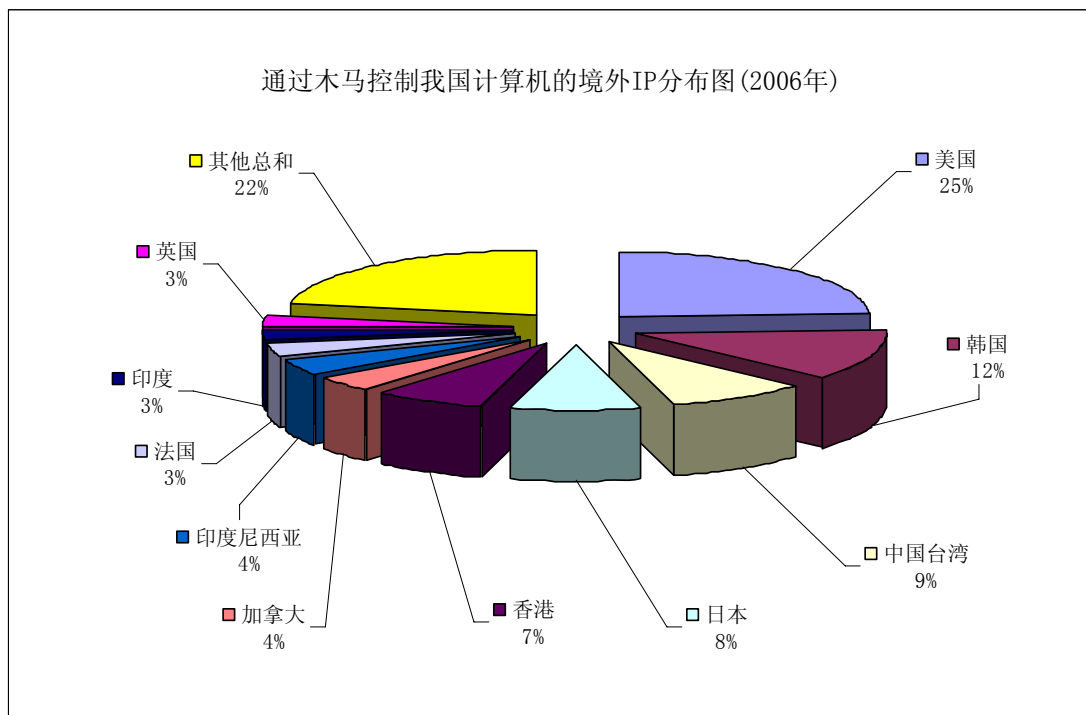


图 10 通过木马控制我国计算机的境外 IP 分布图(2006 年)

6.1.3 木马规模分布

CNCERT/CC通过对6千多个不同规模的木马网络（即控制端和被控端组成的网络）进行以天为周期的观测。平均每天发现350个控制端对木马网络实施控制。其中大部分木马网络属于小型化，规模小于等于10的木马网络所占比例为80%，规模小于等于50的木马网络所占比例则达到90%。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。

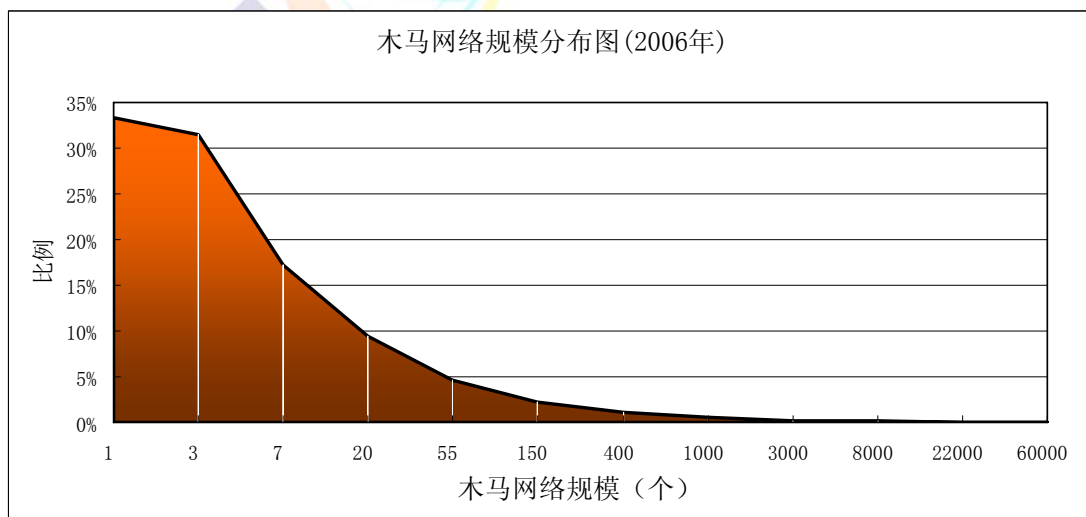


图 11 木马网络规模分布图(2006 年)

6.2 僵尸网络数据分析

僵尸网络通常由互联网上数百到数万甚至上百万台计算机构成,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。利用僵尸网络,攻击者可以释放蠕虫、实施分布式拒绝服务攻击、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,同时还能够利用其创建新的僵尸网络。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,2006 年抽样监测发现我国大陆约有 1 千多万个 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

2006 年,CNCERT/CC 共发现 1 万 6 千多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 12 所示,其中位于美国的占 33%、韩国占 10%、中国台湾占 9%。

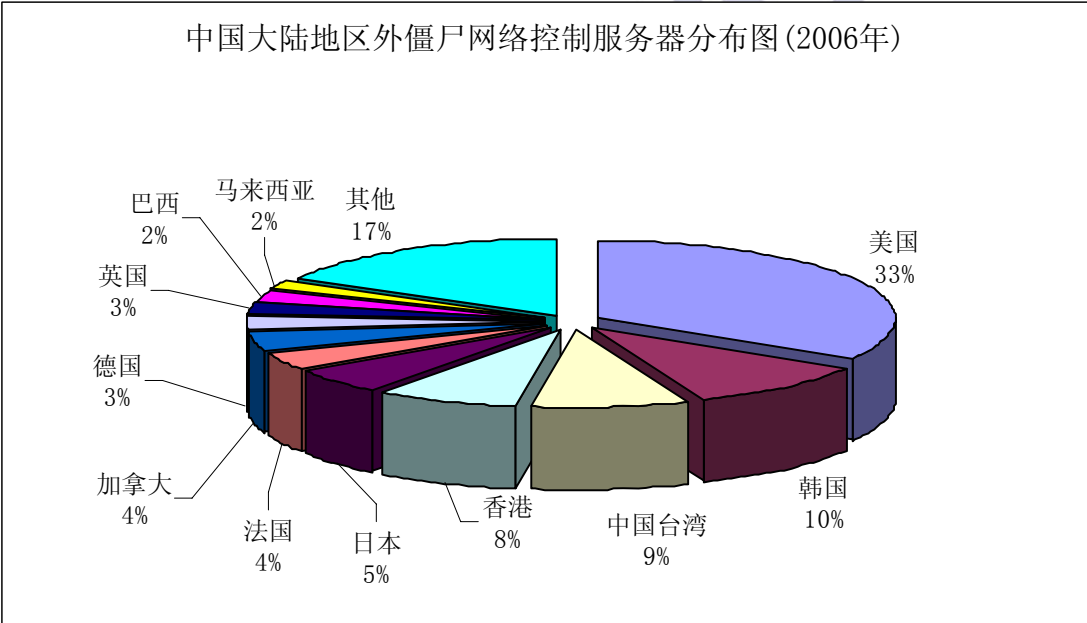


图 12 中国大陆地区外僵尸网络控制服务器分布图(2006 年)

6.2.2 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更受到攻击者青睐。2006 年监测到僵尸网络各种规模所占比例分布如图13所示。

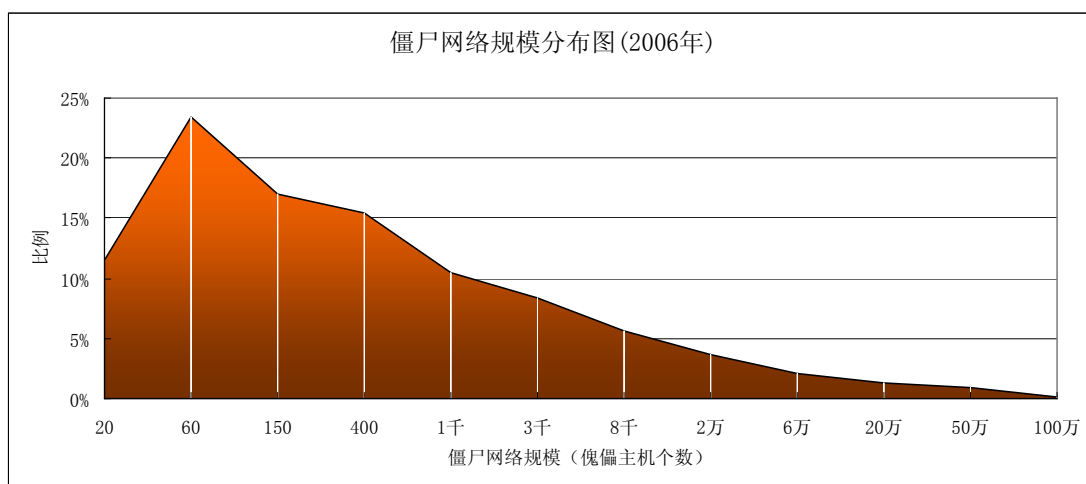


图 13 僵尸网络规模分布图(2006 年)

6.2.3 僵尸网络使用的控制端口分布

在基于IRC协议的僵尸网络中，使用IRC协议默认端口6667的僵尸网络仅占总数的24%，因此，端口过滤并不能很好地阻止黑客对企业/单位内部受害主机的控制。使用IRC协议的僵尸网络控制端口分布如图14所示。

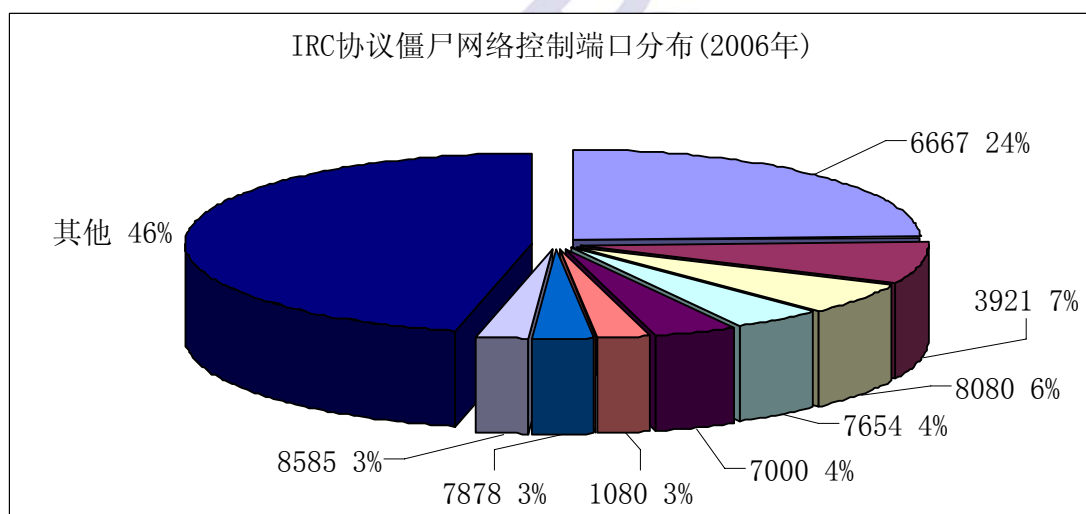


图 14 IRC 协议僵尸网络控制端口分布(2006 年)

7 被篡改网站监测分析

CNCERT/CC 从 2003 年开始关注我国大陆网站被篡改情况。2006 年继续保持每日对中国大陆地区网站被篡改情况跟踪监测，并增加了自主监测手段，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，尽力确保被篡改网站快速恢复。

7.1 我国网站被篡改情况

2006 年全年 CNCERT/CC 监测到中国大陆被篡改网站总数达到 24477 个，与前三年监测情况相比总数有了明显增多，与去年同期相比增长接近一倍，年度情况统计如图 15 所示。

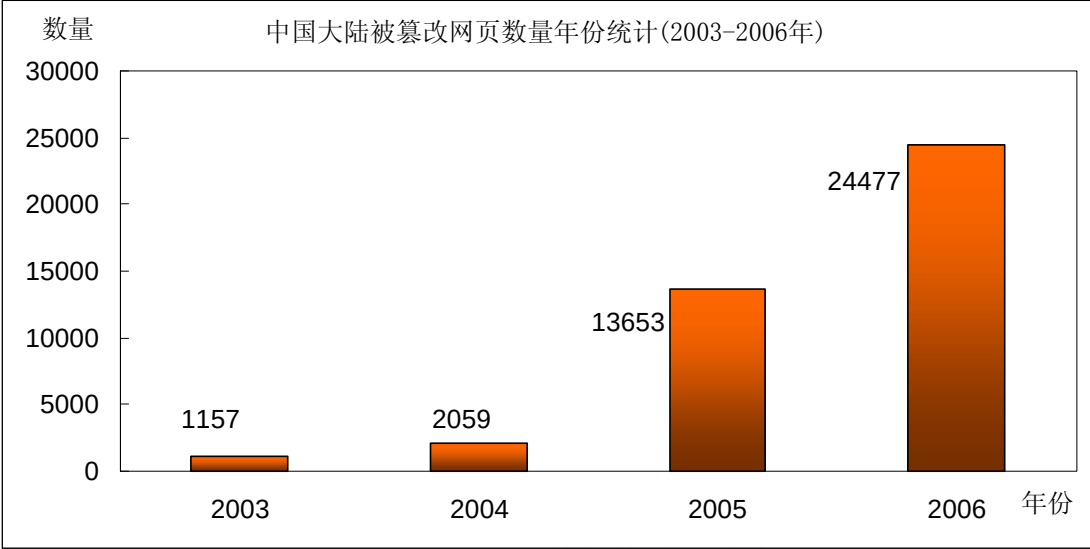


图 15 中国大陆被篡改网页数量年份统计(2003-2006 年)

7.1.1 2006 年被篡改网站月份统计

2006 年 1 月至 12 月期间，中国大陆被篡改网站的数量处于波动上升的趋势。前 6 个月每月数据量保持 1000 个左右波动，在 8 月份加入自主监测手段后，CNCERT/CC 发现的中国大陆被篡改网站数量大幅上升，按月统计情况如图 16 所示。

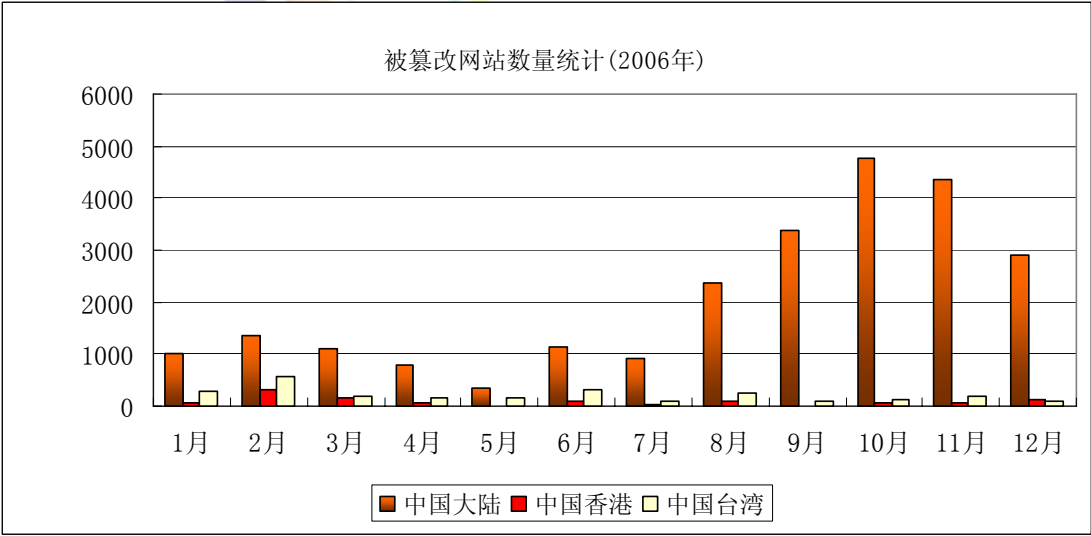


图 16 被篡改网站数量统计(2006 年)

7.2 我国大陆地区政府网站被篡改情况

2006 年，中国大陆政府网站被篡改数量共计 3831 个，与前三年监测情况相比有了显著上升，去年同比增加 89%，四年来年度情况统计如图 17 所示。

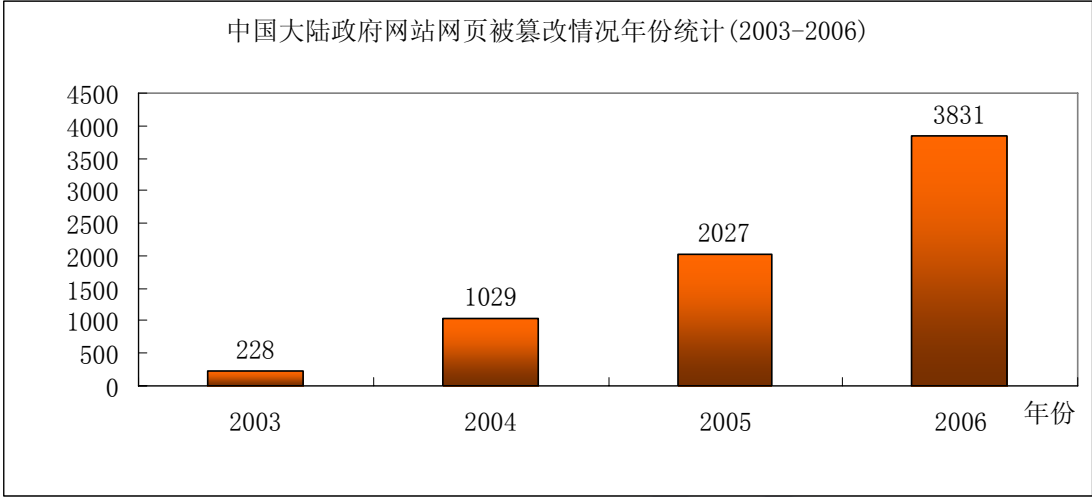


图 17 中国大陆政府网站网页被篡改情况年份统计(2003-2006)

从政府网站被篡改情况的走势图来看，2006 年 1 月到 7 月期间被篡改政府网站所占比重很大，8 月份启用自主监测系统之后，发现的被篡改网站总量大幅上升，因此被篡改政府网站的比重有所降低，但每月仍约占 10%左右。2006 年全年来看，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 16%，可见政府网站的安全性十分脆弱。

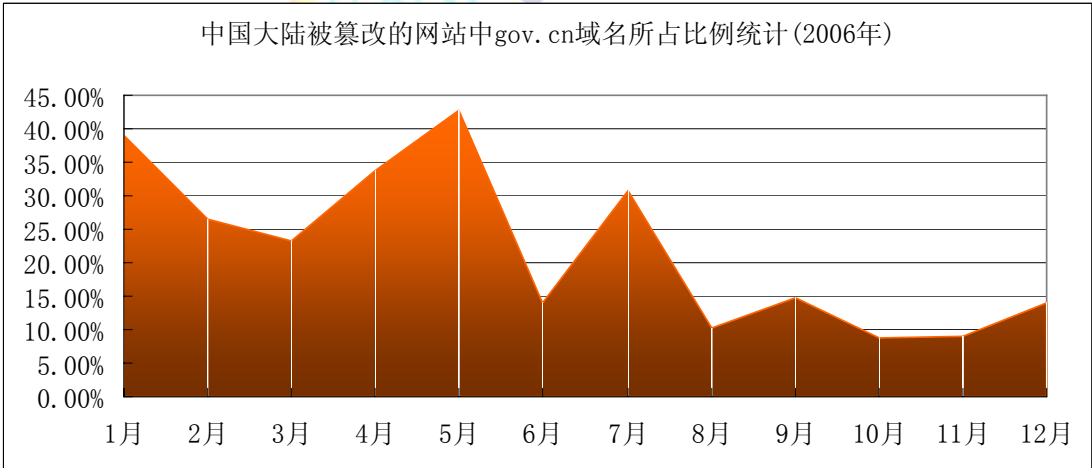


图 18 中国大陆被篡改的网站中 gov.cn 域名所占比例统计(2006 年)

从被篡改的 gov.cn 域名网站数量上看，1 月至 12 月期间，中国大陆政府网站被篡改的数量处于波动上升的趋势。

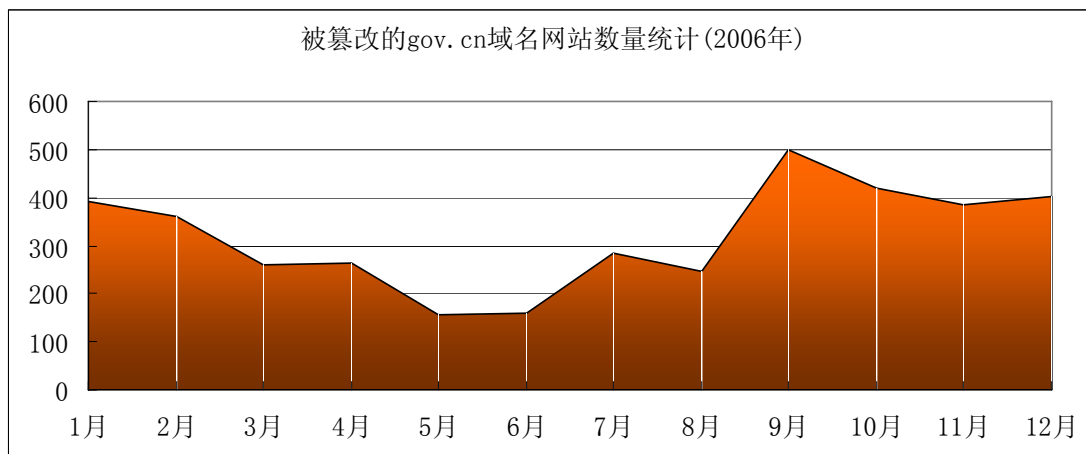


图 19 被篡改的 gov.cn 域名网站数量统计(2006 年)

政府网站容易被篡改的主要原因是安全性差，网站建设与保护措施建设不同步，平时缺乏必要的维护，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

根据 APWG (Anti-Phishing Working Group, 反网络仿冒工作组) 组织的统计数字³, 2006 年 1 月至 11 月, 利用我国大陆主机建立仿冒网页的数目占全球的 14.36%, 居全球第二位。2006 年 CNCERT/CC 共接到网络仿冒事件报告 563 件, 具体成功处理了 238 件。这些网络仿冒类事件全部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。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
eBay (美国网上交易站点)	207
Verisign (美国网络安全公司)	141
Brandimensions (加拿大网络安全公司)	46
HSBC (汇丰银行)	22
MM Ops Center (美国网络安全公司)	22

表 3 向 CNCERT/CC 报告网络仿冒事件前 5 名统计

此外, CNCERT/CC 对涉及我国政府和重要信息系统部门的网络仿冒事件尤为关注。2006 年出现多起我国政府和重要信息系统网站被植入仿冒网站的事件, 例如 2006 年 4 月, 国外多家媒体以“中国的银行网站被利用作 Phishing”为题, 报道了中国某银行网站被植入仿冒 Paypal 网站的事件; 2006 年 5 月 27 日, 北京市某区政府服务器被植入香港汇丰银行的仿冒网站; 2006 年 6 月 19 日, 大连市某区政府网站邮件服务器被植入电子港湾(eBay)的仿冒网站。针对我国部分政府和重要信息系统运营单位主机被入侵后进行网络仿冒的情况, 我

³ <http://www.antiphishing.org>

中心向有关主管部门作了专题报告,并提出若干加强政府和重要信息系统部门网站安全的建议。

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。

为了加强对恶意代码的监测处理能力,CNCERT/CC 陆续在北京、上海、重庆、吉林、四川、广东等 15 个省份完成了分布式蜜网试验系统的部署,并于 2006 年 6 月 19 日开始试运行。

蜜罐是蜜网(即蜜罐网)的基本组成部分,是一个专门构造的、可控的、具有多种安全漏洞的网络“陷阱”主机,通过监测蜜罐被扫描、攻击和攻陷的过程,可以掌握各种攻击活动。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。

CNCERT/CC 通过对于分布式蜜网捕获恶意代码样本的分析,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。自蜜网运行以来,每日平均捕获样本 3069 次,图 20 给出了每日的样本捕获趋势。

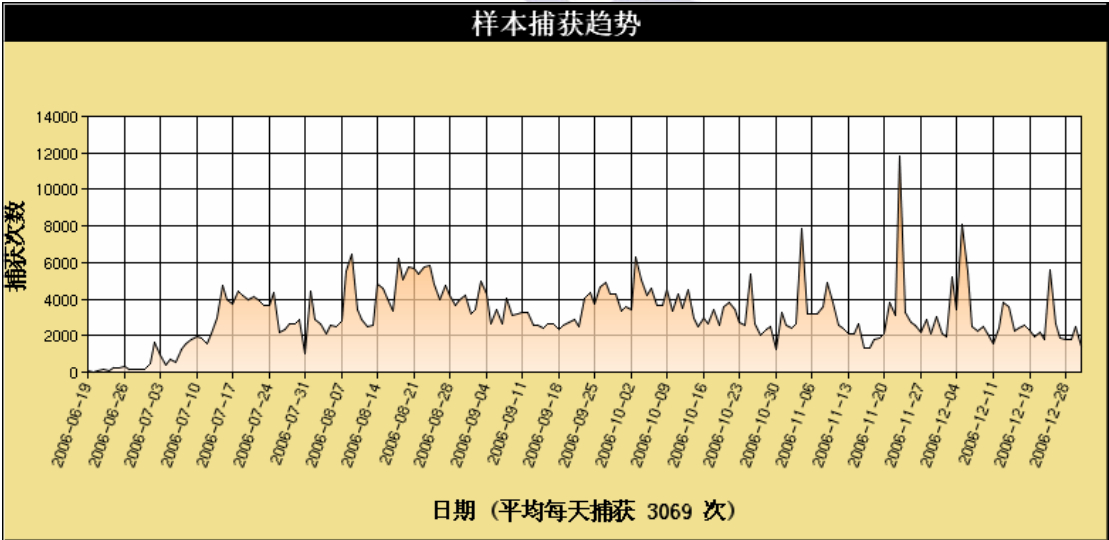


图 20 分布式蜜网样本捕获趋势图

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 96 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。

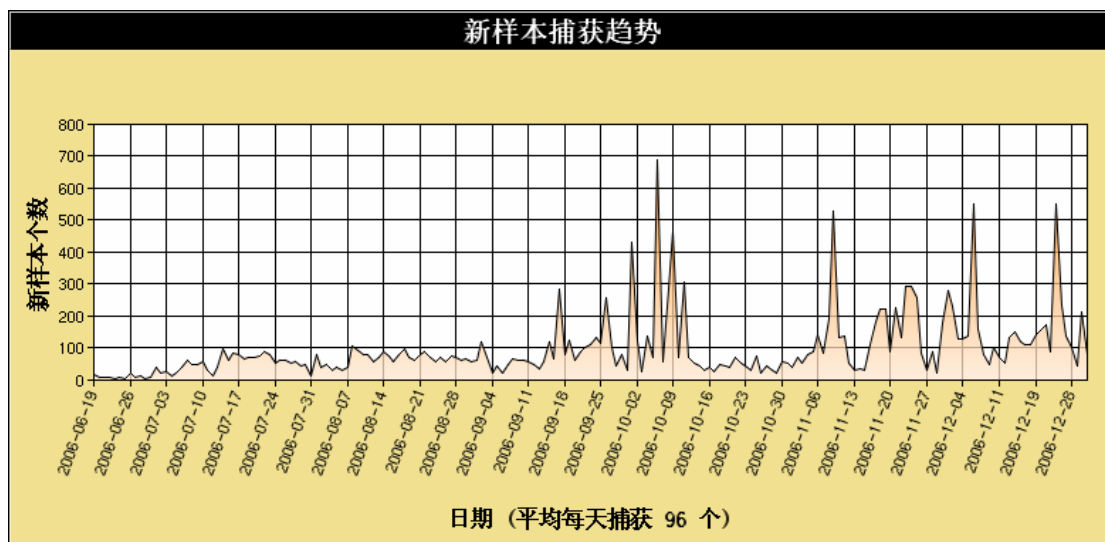


图 21 分布式蜜网新样本捕获趋势图

2006 年 6 月 19 日至 12 月 31 日期间，蜜网共捕获 18912 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.Rbot.aem	38790
2	Virus.Win32.Virut.b	38617
3	Backdoor.Win32.PoeBot.c	36104
4	Backdoor.Win32.Rbot.bci	35657
5	Backdoor.Win32.SdBot.aad	31268
6	Backdoor.Win32.Rbot.gen	27246
7	Virus.Win32.Virut.a	17287
8	Backdoor.Win32.IRCBot.ul	14517
9	Backdoor.Win32.SdBot.xd	14242
10	Trojan-PSW.Win32.Nilage.zh	10018

表 4 分布式蜜网捕获次数前十名的恶意代码

Win32.Rbot（瑞波）及其变种是蜜网捕获次数最多的恶意代码，在前十名中分别列 1、4、6 位。该恶意代码能够利用微软 MS02-061、MS03-007、MS03-026、MS04-011 四个漏洞，并可通过猜测弱口令和利用其它的恶意程序生成的后门进行传播，它感染计算机后留下后门并通过 IRC 协议进行远程控制形成僵尸网络，具有较高的危害性。

此外，列第 3 位的 PoeBot（派波）、列第 5、9 位的 SdBot（赛波）和列第 8 位的 IRCBot 也都是利用微软的漏洞进行传播，并在感染的机器上留下后门程序，后门程序主动连接控制服务器并最终形成僵尸网络。黑客能够利用僵尸网络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、攻击和散发垃圾邮件或进行网络欺诈活动。

10 网络安全信息服务

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。2006 年，CNCERT/CC 共向有关部门通报网络安全信息 14 次，其中，报告重大漏洞 7 次，报告重要事件情况 7 次，通报与重要部门信息系统有关的安全事件涉及 IP 地址一百多个。

2006 年 3 月，CNCERT/CC 对瑞波变种 (Backdoor/Rbot.auv) 蠕虫所形成的僵尸网络情况进行监测，并将有关情况通报了相关部门。4 月份，通过监测发现北京地区某运营商 UDP1026/1027 端口流量异常的事件，并及时通报了相关运营单位进行了处理，通过处理很快网络流量恢复了正常水平。8 月份，在 MocBot 蠕虫的处理过程中，CNCERT/CC 就 154 个重要 IP 地址受感染的情况通知了国内相关部门，并将其他国内感染用户 IP 地址通报了所属运营商的应急组织。今后，CNCERT/CC 将进一步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。

10.2 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。2006 年，CNCERT/CC 通过网站发布了近 240 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 22。2006 年中国计算机网络安全应急年会之后，CNCERT/CC 还将年会资料发布到在网站上。目前，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。

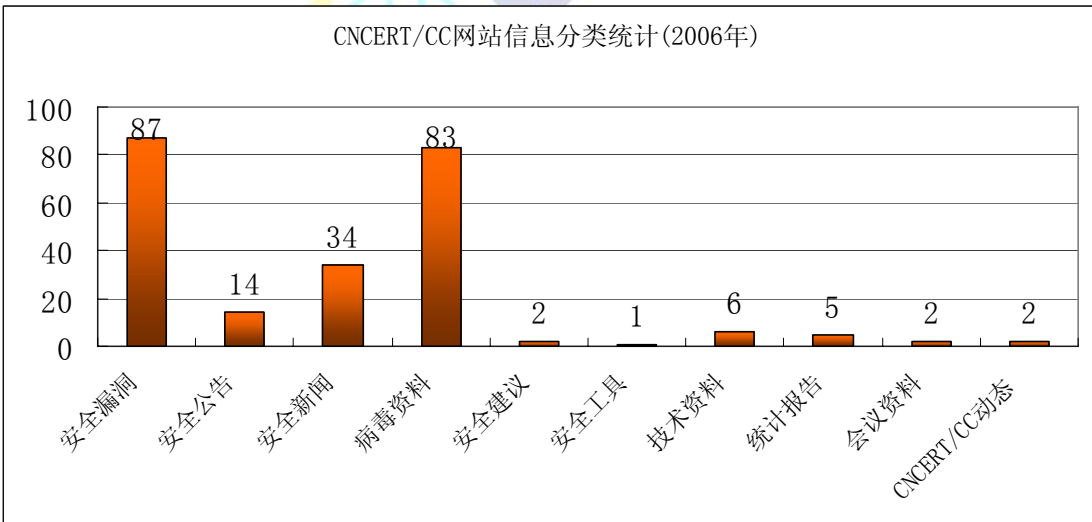


图 22 CNCERT/CC 网站信息分类统计(2006 年)

10.3 电子邮件列表信息发布

除采用网站形式公开提供信息服务外，CNCERT/CC 还通过电子邮件的形式为特定用户群体提供定向的信息服务，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、应急服务试点单位、技术支撑单位、中国互联网协会网络与信息安全工作委员会、APCERT、FIRST、TRANSIT 培训班学员、东盟培训班学员等。同时，2006 年 CNCERT/CC 向中国互联网协会网络与信息安全工作委员会等单位发布网络安全月报共 12 期。

10.4 2005 年全国网络安全状况调查情况

2005 年 12 月 8 日至 2006 年 3 月 15 日，CNCERT/CC 组织进行了“2005 年全国网络安全状况调查”活动，并将所形成的调查报告向相关部委定向发布。本次调查样本取自我国二十三个城市，调查对象涉及十四个行业的网络或信息系统负责人。

调查发现，目前我国各地区、各行业使用互联网或计算机网络系统的比例越来越大，网络安全问题逐渐成为影响业务运行、制约生产力发展的重要因素之一。

目前，我国多数单位的业务网络能够较好地遵循与互联网物理隔离的原则，因此，内部业务网在较大程度上避免了外部的攻击威胁；但随着我国信息化建设的进一步发展，金融、保险、税务、交通等与生活息息相关的业务活动将越来越依赖互联网进行，因此，采取物理隔绝以外的其他网络安全技术措施成为保障这些系统正常运行的重要手段；防火墙和防病毒软件是目前应用最为广泛的安全产品，但也是最为传统、最为基本的技术措施，日益增长的网络应用业务需要更多更新的安全技术保障，例如电子签名、生物特征识别、授权技术等，但这些技术在我国还远没有得到广泛应用。

随着国家层面对网络安全工作的重视，各行业对自身信息系统的安全保障工作也在逐步加深，制定了各自的业务系统应急保障预案，相应的规章制度建设、标准制订、技术保障措施等都得到了一定程度的完善。与此同时，各单位对网络安全人才的要求也越来越高，这与目前我国专业网络安全技术人员匮乏的现状之间的矛盾日益突出。网络安全虽然得到了更多的重视，但是各单位在网络安全上的投入上仍然比较缺乏，这不仅体现在安全产品的部署上，也体现在员工培训、安全评估次数、安全意识教育等多个方面。从根本上讲，加强网络安全工作的重要前提是大力提高各单位管理层对网络安全的重视程度。

对于安全事件出现的次数和造成的损失，从被访单位的反馈来看并不十分严重，这主要是由于大多数关键业务并非完全依赖于计算机网络，不过这一调查结果的客观准确性也受到现在的很多攻击隐蔽性很强、对软件系统故障的损失一直缺乏准确的估算方法等因素的影响。即便如此，被访单位还是对网络攻击的威胁有相当的担忧，首当其冲的是恶意代码，其次是对基础网络及信息系统本身的攻击和破坏，这将是今后一段时间网络安全行业所需解决的主要问题。

在本次调查中发现，用户对第三方提供的网络安全服务——例如安全评估、安全检查、事件处理等的接受程度相对于技术产品来说要低许多，这说明我国目前的网络安全服务市场还未真正形成，其原因一方面是由于相应的服务标准、监管体制、服务质量等方面还不成熟，另一方面也是由于用户“重产品轻服务”的惯性思维依然存在。这一调查结果表明，我国用户对网络安全保障的理解还存在较大的偏差和误解，急需通过各种培训培养正确的网络安全意识。

通过调查发现，2005 年我国虽然未遭受由网络安全问题导致的巨大损失，但并不意味着我国的网络安全形势非常乐观，各行业对网络安全工作的重视程度不够、防护措施单一、经费投入不足等现象是影响我国网络安全工作的主要因素，随着各行业对网络信息系统的依赖越来越大，网络安全将面临日益严重的威胁。

11 网络安全应急组织发展情况

11.1 国际部分

FIRST(事件响应与安全组织论坛)

FIRST 作为全球最大的计算机安全应急组织联盟,也是网络安全专业领域中唯一的全球性组织,2006 年取得了较大的发展,其成员数量达到了 191 个。CNCERT/CC 于 2002 年成为 FIRST 正式成员时,其成员数量仅 110 个。目前, FIRST 成员中有 5 个来自中国,包括大陆的 CNCERT/CC、大陆的 CMCERT/CC(中国移动)、香港的 HKCERT、台湾的 TWNCERT 和 TWCERT/CC。其中, CMCERT/CC 是 06 年新加入的成员。

2006 年, FIRST 有关的重要事件包括:

5 月 5-10 日, FIRST、TERENA 与阿联酋 ETISALAT-CERT 共同举办了在中东地区的首次 TRANSITS 培训。FIRST、TERENA 曾与 CNCERT/CC 于 05 年举办了在中国的首次 TRANSITS 培训。

6 月 25-30 日, FIRST 年度大会在美国巴的摩尔召开。新成立的卡塔尔 CERT 的加盟被称象征着中东地区的互联网应急响应向前迈进了一大步。会议同期还召开了 G8 会议,邀请了执法部门与 CERT 共同商讨反网络犯罪的问题。

9 月 22 日, FIRST 成立了四个新的 SIG(特别兴趣小组),包括滥用处理、恶意软件分析、执法机构与 CERT 的合作以及网络监测,目的是通过细分领域深入讨论安全问题。

9 月 25-27 日, FIRST 于韩国首尔召开技术研讨会, CNCERT 代表团参加了会议。

10 月 7-12 日, FIRST 于巴西里约热内卢召开技术研讨会。

APCERT(亚太地区计算机网络应急响应组织)

APCERT 作为亚太地区最有影响力的应急响应合作组织,迄今吸引了亚太地区 14 个经济体的 19 个应急组织成员,并在不断扩展壮大。其中,来自中国的成员包括大陆的 CNCERT/CC 与 CCERT、香港的 HKCERT 以及台湾的 TWCERT/CC 和 TWNCERT。2006 年,又有三个新组织加入 APCERT,分别是新加坡 BP DSIRT 和 NUSCERT(新加坡国立大学)以及印度 CERT-In。

2006 年, APCERT 的两项重要活动分别是 APCERT 年会和 APCERT 应急演练。其中,由 CNCERT/CC 主办的 APCERT 年会于 3 月底在中国北京召开,这是 APCERT 确定独立举行年会后的第一次会议,有 50 余名各国代表参加。除 APCERT 成员组织外,还有来自 FIRST、APEC-TEL、ENISA(欧洲网络与信息安全署)、OAS(泛美合作组织)、TF-CSIRT(欧洲科研网应急组织联盟)、ASEAN(东盟)和美国 CERT/CC 的代表参加。

2006 年 12 月,包括 CNCERT/CC 在内的 15 个应急组织参与 APCERT 应急演练。

ENISA(欧洲网络与信息安全署)

ENISA 是欧盟新成立的政府合作机构。2006 年, ENISA CSIRT 发布了一套 CERT 指南,从业务管理、流程管理和技术等各个方面描述了如何建立一个 CERT 组织。

11.2 国内部分

中国 CERT 社区

中国 CERT 社区(<http://community.cert.org.cn/>)是由 CNCERT/CC 和中国互联网协会网络与信息安全工作委员会共同发起成立的一个网上社区,致力于收集汇总来自不同行业、不

同地区 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。自 2005 年初成立以来, 已有 20 个 CERT 组织加入。其中, 覆盖全国地区的 CERT 组织有:

CCERT

CCERT 的全称是中国教育和科研计算机网紧急响应组, 也是 CERNET 网络安全应急响应体系的总称, 包括 CERNET 内部各级网络中心的安全事件响应组织或安全管理相关部门。CCERT 与 CNCERT/CC 一样, 均是 APCERT 的发起成员, 并相互配合参与了 APCERT、FIRST 的多次活动。

CMCER/CC

中国移动网络与信息安全应急小组 (简称 CMCERT/CC) 成立于 2002 年 9 月, 负责协调和处理中国移动的通信网、各业务系统及各支撑系统的安全应急事件。2006 年, 经 CNCERT/CC 与 HKCERT 的推荐, CMCERT/CC 成功加入 FIRST。

12 国际合作与交流

2006 年, CNCERT/CC 参与的国际合作与交流主要体现在三次大型活动, 分别是主办 2006 APCERT 年会、主办中国-东盟网络安全应急处理研讨会和参加 APCERT 应急演练。

2006 年 3 月 27-29 日, 由 CNCERT 主办的 APCERT 年会在北京友谊宾馆召开。本次年会为期两天半, 包括三个封闭会议和两个开放会议。其中, 开放会议组织了 12 场讲座。在年会的换届选举中, CNCERT 再次当选 7 个指导委员会委员之一, 并再次当选 APCERT 副主席单位, 这是各成员组织对于 CNCERT/CC 在亚太地区互联网网络安全方面发挥重要作用的肯定。本次年会参与代表 50 余人, 是历年来最多的一次, 涉及 17 个国家和地区。CNCERT/CC 专业的组织和热情的服务给各国与会人员留下了深刻印象。

2006 年 12 月 18-22 日, 中国-东盟网络安全应急处理研讨会于北京港澳中心瑞士酒店召开。本次研讨会是在信息产业部的指导下由 CNCERT/CC 具体承办, 会议旨在通过面对面的交流, 探讨中国与东盟各国间建立网络安全应急处理联络与协调机制的可行性, 为未来双方网络与信息安全应急处理协作框架的建立奠定基础。东盟各国的与会代表主要来自各国主管信息产业或科技的部委以及国家级 CERT。在一周的会议期间, 中国及东盟各国的与会代表们围绕五大主题进行了充分的交流和讨论, 内容涉及各国互联网的发展状况和主要问题、各国政府开展互联网安全管理的思路与方法、各 CERT 组织与政府、产业的合作、各 CERT 组织的能力建设与国际合作, 以及最为重要的主题——中国-东盟应急处理协作框架。最终, 会议取得了令人满意的成果, 与会各国代表不仅呈献了三十多场专题报告, 同时, 还联合确定了“中国-东盟网络与信息安全合作建议书”。

2006 年 12 月 19 日, CNCERT/CC 继 04、05 年之后连续第三年参加了 APCERT 应急演练。本次演练将应急处理的对象定位在被嵌入恶意代码的网站, 这种方式已经成为黑客大规模传播恶意代码, 控制大量计算机的重要手段之一。来自 13 个国家和地区 (澳大利亚、文莱、中国大陆、中国香港、中国台湾、日本、韩国、新西兰、马来西亚、新加坡、泰国和越南) 的 15 个应急组织参与了本次演练, 本次演练还首次邀请了部分 APEC 经济体成员的 CERT 组织参加。

13 结束语

根据中国互联网信息中心(CNNIC)2007 年 1 月 23 日公布的《中国互联网络发展状况统

计报告》⁴显示，截至 2006 年底，我国上网用户总数为 1.37 亿人，占全国人口的 10.5%，与去年同期相比，中国网民人数增加了 2600 万人，是历年来网民增长最多的一年，增长率为 23.4%。CN 域名总数超过 180 万，与 2005 年同期相比，增长幅度达到 64.4%。宽带上网的网民达到 10400 万人，占网民总数的 75.9%。

中国互联网目前已经进入宽带时期，网络用户和网络资源持续增长，同时我国互联网产业已初具规模并快速发展。但是，互联网的开放性和应用系统的复杂性带来的安全风险也随之增多，各种网络漏洞的大量存在并不断攀升仍是网络安全的最大隐患；网络攻击行为日趋复杂，各种方法相互融合后的定向性和专业性攻击使网络安全防御更加困难。

根据 2006 年 CNCERT/CC 的监测分析结果，预计 2007 年随着微软 Windows XP SP2 的广泛使用和 Windows Vista 的逐渐推广，利用微软系统漏洞进行传播的蠕虫对网络的压力逐步减少；但针对终端系统漏洞的“零日攻击”和利用网络攻击获取经济利益成为趋势。其中以僵尸网络、间谍软件为代表的恶意代码，以敲诈勒索为目的的分布式拒绝服务攻击、以网络仿冒、网址嫁接、网络劫持等方式进行的在线身份窃取类事件将会继续增加，针对 P2P、及时通信等新型网络应用的安全攻击将会迅速发展，网站被篡改事件将持续在高位徘徊，这些问题将导致网络安全事件数量整体仍呈上升趋势。

针对目前漏洞多发的状况和“零日攻击”的趋势，CNCERT/CC 建议用户注意操作系统、重要应用以及安全防护系统的及时更新，并打开系统的防火墙功能，在主机层面阻止网络攻击的发生。CNCERT/CC 建议企业和政府机构在组织内实施最低权限原则，阻止恶意软件的安装和运行，通过做好内部网络的安全防护和服务器的加固维护工作，减少网页篡改事件和网络仿冒事件的发生。

CNCERT/CC 将在信息产业部的领导下，在互联网安全应急预案框架内，提高网络安全事件的发现能力，持续推动网络安全事件处理流程的规范化，加强与应急组织、网络运营商、网络服务提供商（ISP/ICP/IDC/域名注册商等）以及其他有关部门的联系与合作，从而形成快速、有效的网络安全事件应急响应机制，全面提升对于公共互联网的安全保障能力。

⁴ 数据来源：<http://www.cnnic.com.cn>