

2009 年中国互联网网络安全报告

(预览版)

国家互联网应急中心



关于 CNCERT

国家互联网应急中心（全称为国家计算机网络应急技术处理协调中心，英文简称为 CNCERT 或 CNCERT/CC）成立于 1999 年 9 月，是工业和信息化部领导下的国家级网络安全应急机构，致力于建设国家级的网络安全监测中心、预警中心和应急中心，以支撑政府主管部门履行网络安全相关的社会管理和公共服务职能，支持基础信息网络的安全防护和安全运行，支援重要信息系统的网络安全监测、预警和处置。

2003 年，CNCERT 在全国 31 个省成立分中心，完成了跨网络、跨系统、跨地域的公共互联网网络安全应急技术支撑体系建设，形成了全国性的互联网网络安全信息共享、技术协同能力。目前，CNCERT 作为国家公共互联网网络安全应急体系的核心技术协调机构，在协调国内网络安全应急组织（CERT）共同处理公共互联网网络安全事件方面发挥着重要作用。

CNCERT 的业务能力主要包括：

- **监测发现：**依托“863-917 网络安全监测系统”实现网络安全事件的监测发现。863-917 网络安全监测系统是一个全程全网、多层次、多渠道延伸的网络安全综合监测平台，目前已具备木马和僵尸网络监测、网页篡改监测、网页挂马监测、恶意代码捕获、流量异常监测、域名服务监测等能力。
- **通报预警：**依托对丰富数据资源的综合分析和多渠道的信息获取实现网络安全威胁的分析预警、网络安全事件的情况通报、宏观网络安全状况的态势分析等。此外，按照 2009 年工业和信息化部颁布实施的《互联网网络安全信息通报实施办法》承担通信行业互联网网络安全信息通报工作。
- **应急处置：**依托与运营商、域名注册商、安全服务厂商等相关部门的快速工作机制实现网络安全事件的应急处置。CNCERT 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 成员，负责接收国际网络安全事件报告，是中国处理网络安全事件的对外窗口。

CNCERT 的联系方式：

国家互联网应急中心 CNCERT

网址：<http://www.cert.org.cn/> 电子邮件：cncert@cert.org.cn

热线电话：+8610 82990999，82991000（英文） 传真：+8610 82990399

PGP Key：<http://www.cert.org.cn/cncert.asc>

目 录

一、 2009 年网络安全状况综述	4
(一) 全年网络安全总体状况	4
(二) 全年网络安全数据预览	9
二、 《2009 年中国互联网网络安全报告》章节目录	18
三、 术语解释	19

一、 2009 年网络安全状况综述

（一）全年网络安全总体状况

为全面掌握我国互联网网络安全状况，在工业和信息化部《互联网网络安全信息通报实施办法》的指导下，2009 年 CNCERT 协调和组织各地通信管理局、中国互联网协会、基础电信运营企业、域名注册管理和服务机构、非经营性互联单位、增值电信业务经营企业以及安全企业开展了通信行业网络安全信息通报工作。CNCERT 结合多年来开展网络安全工作的经验，在网络安全信息汇总、分析的实践中不断总结，制定了一套网络安全评价指标体系。依据 CNCERT 监测数据和通信行业报送的各类网络安全事件信息（如：计算机病毒和蠕虫、木马和僵尸网络、网页篡改和网页挂马、域名和路由劫持、高危漏洞等），CNCERT 应用该体系对每月的互联网安全指数进行评价，评价结果分为“优”、“良”、“中”、“差”、“危”五个级别。2009 年多数月份安全指数评价为“中”，一些月份（如：5 月、6 月）因出现重大网络安全事件、存在重大网络安全威胁或事件发生数量大幅上升等因素评价为“差”。全年各月未出现“优”、“良”、“危”的评价级别。

基于该体系的理论基础，CNCERT 将从基础网络运行安全、公共互联网安全、网络安全威胁以及网络安全感知等四个方面对 2009 年我国网络安全总体状况进行简要评述。

■ 基础网络运行安全

2009 年，全国基础网络运行状况整体平稳，但是全国范围或省级行政区域内发生了若干起造成较大或较大以上影响的网络安全事件，且较大及较大以上影响的事件发生次数较 2008 年呈增长态势。在互联网产业持续发展、互联网用户数量迅猛增长的形势下，上述事件的影响更为深远、传播效应更为明显。例如：5 月 19 日我国部分地区互联网网络故障事件、6 月 25 日中国电信广东省网流量异常事件、8 月中下旬国际互联网海底光缆连续中断事件等，不仅给普通互联网用户造成了较大或重大影响，还给相关部门和行业企业造成了不少的经济损失。

2009 年，互联网重要基础设施——域名系统面临着更为严峻的网络安全形势。一方面体现为 DNS 系统自身存在致命安全漏洞，如：7 月底被披露的“Bind 9”高危漏洞，影响波及全球数万台域名解析服务器，我国有数千台政府和重要信息系统部门、基础电信运营企业以及域名注册管理和服务机构的域名解析服务器

受到影响。另一方面，攻击域名解析服务器成为黑客的常用手段。除“5.19”事件外，在 CNCERT 接收到的多起国内域名注册服务机构报告的攻击事件中，较为严重的会导致相关机构服务完全瘫痪，造成其提供解析的数以十万计的网站域名无法正常访问。上述情况说明域名系统安全是基础网络运行安全中较为薄弱的环节，加强域名安全体系建设刻不容缓。

2009 年，针对境内互联网基础运行设施的攻击主要是拒绝服务攻击。拒绝服务攻击的目标一般情况下都是网络上的某一台服务器，但由于攻击流量巨大往往会引起被攻击目标所在的互联网区域网络基础设施负载过重，导致网络性能下降，影响到网络承载的其他业务。运营商及相关用户虽然采取了一些防范措施，如：流量清洗、防火墙过滤，但如果追查和清除攻击源的问题没有解决，仍不可避免地对相关业务的正常运行造成不同程度的影响。仅以 2009 年 10 月份辽宁、河北等地运营商的通报的情况看，拒绝服务攻击中一般流量¹攻击次数约占 86%，较大流量攻击次数约占 12%，大流量攻击次数约为 2%；上述攻击目标多指向 IDC 的服务器，其中较大或较大以上流量攻击通常会对 IDC 业务以及其承载互联网增值业务信息系统造成影响。防范拒绝服务攻击特别是分布式拒绝服务攻击（DDoS）是互联网企业安全运营亟需解决的一个难题。

■ 公共互联网安全

公共互联网安全事件主要指公共互联网用户遭遇的、发生在各类互联网应用服务上的安全事件。

2009 年公共互联网安全形势主要体现在以下几个方面：

木马和僵尸网络。木马和僵尸网络对用户网络信息安全构成最直接的威胁，其发展规模和趋势同时也反映了互联网黑色地下产业的活动状况。2009 年，CNCERT 监测到的境内被木马控制的主机 IP 共 26.2 万余个，较 2008 年大幅下降 53.6%；境外有 16.5 万个主机 IP 参与控制上述境内主机，较 2008 年下降 40.2%；境内被僵尸网络控制的主机 IP 共 83.7 万余个，较 2008 年下降 32.3%；境外有 1.9 万个主机 IP 参与控制上述境内主机，较 2008 年增长 257.8%。根据工业和信息化部颁布的《木马和僵尸网络监测与处置机制》，CNCERT 国家中心及各分中心协调运营商、域名机构持续开展了木马和僵尸网络的治理行动，及时监测发现、通报和处置主机感染情况。2009 年木马和僵尸网络境内受控主机数量的大幅下降，说明对木马和僵尸网络的治理取得了一定成效。但是，互联网黑色地下

¹参考中国联通辽宁省分公司提供的统计标准：一般流量、较大流量、大流量攻击是指流速分别为小于 5Gb、大于 5Gb 但小于 15Gb、大于 15Gb 的攻击。

产业规模庞大，仍然比较活跃，治理工作面临着更为艰巨的任务。

新型计算机病毒和蠕虫。计算机病毒和蠕虫对于用户主机最大的危害在于其大肆破坏用户操作系统以及存储在系统中的文件资料，人们记忆犹新的病毒和蠕虫有：“尼姆达”、“冲击波”、“震荡波”、“QQ 尾巴”、“熊猫烧香”等。2008 年底至 2009 年间，一种新型蠕虫——“飞客”（Conficker）蠕虫在全球互联网迅速传播。至 2009 年底，CNCERT 采用“sinkhole”方法²监测到全球感染“飞客”蠕虫的主机 IP 数量已超过 7000 万个，其中中国大陆地区是“重灾区”，每月感染主机 IP 数量约 1800 万个。感染“飞客”蠕虫的计算机不仅存在失泄密隐患，还是黑客发动网络攻击的“棋子”，黑客利用全世界数量庞大的感染主机可对互联网任意目标发动致命的攻击。类似“飞客”这样新型的蠕虫，如同木马和僵尸网络一样，是黑客争夺互联网主机资源控制权的利器，对互联网安全产生深远的影响。

网站安全。用户访问互联网的第一体验就是各种各样的 Web 网站，因此网站安全将严重影响用户的上网安全。CNCERT 重点监测我国网站被篡改和被挂马的情况。2009 年，中国大陆有 4.2 万个网站被黑客篡改，较 2008 年约下降五分之一。其中，被篡改的政府网站各月累计达 2765 个，较 2008 年下降约 22.3%。相较于政府网站占网站总数 1.1%的比例³，政府网站被篡改的比例相对较高。2009 年我国被篡改网站数量的下降在一定程度上说明网站整体安全性有所提升，但总的情况不容乐观。黑客攻击网站的另一种手法是利用网站漏洞挂载恶意代码（通常是木马类程序，即网页挂马），使得大量访问该网站的用户主机被黑客所控制或丢失敏感信息。2009 年网页挂马仍然是黑客地下产业链的重要一环，各类操作系统和应用软件安全漏洞的披露以及网络热点事件、搜索热词的出现，都是黑客进行网页挂马的“契机”。CNCERT 在 2009 年下半年加大了对网页挂马的监测和打击力度，在通信行业通报工作成员单位特别是安全厂商的支撑下，开展了活跃恶意域名的治理行动。此外，国内域名机构在下半年加强了域名管理的工作，使得黑客注册境内域名用作放马服务器⁴的机会成本增加。2009 年下半年特别是 10 月份以后，国内被挂马的网站数量有明显的下降⁵。

网络仿冒。随着电子商务的发展以及互联网消费的普及，网络仿冒成为网络欺诈的常见方式。大型电子商务网站、大型金融机构网站、第三方在线支付站点、

² “sinkhole”英文意思为通往地下沟渠的排水洞；在“飞客”蠕虫的监测中，主要用于牵引感染主机 IP 的访问流量，获得感染主机 IP 详细信息；

³ 数据出自 CNNIC 发布的《第 25 次中国互联网络发展状况统计报告》；

⁴ 放马服务器是指最终提供木马下载的服务器。网页挂马往往经过多次跳转后将用户引向放马服务器；

⁵ 相关数据参考了互联网网络安全信息通报工作成员单位——知道创宇、华为、奇虎 360、金山、启明星辰、安天、东软、绿盟、瑞星、天融信、联想网御、安氏、浪潮、网御神州等安全厂商报送的每月月报数据。

大型社区交友网站是网络仿冒的主要对象，黑客伪造与源站点高度相似的网站页面诱使用户登陆，套取账户信息以及其他个人私密信息，进而造成用户直接经济损失。2009 年，CNCERT 接收的网络仿冒事件数量共 1200 件，位列各类接收事件的第三位，约占总量的 5.5%。

■ 网络安全威胁

2009 年，信息系统安全漏洞仍是互联网企业和普通用户面临的主要安全威胁。网络设备、操作系统、服务器系统、数据库软件、应用软件甚至是安全产品的高危漏洞越来越多，带来严重的安全隐患。2009 年，CNCERT 在官方网站（<http://www.cert.org.cn>）上整理和发布与我国用户密切相关的漏洞公告 133 个，与去年相比增加 32%。其中一些重要的安全漏洞主要有：微软操作系统视频功能组件高危漏洞、微软 Office 组件高危漏洞、微软 IE 浏览器 0day 漏洞、域名系统软件 Bind 9 高危漏洞等。

信息系统安全漏洞特别是高危漏洞常被黑客利用来发动网络攻击。

例如，2009 年 7 月底披露的域名系统软件 Bind 9 高危漏洞。其利用方式非常简单，攻击者仅需发送一个特定构造的攻击包就能使存在漏洞的权威域名服务器崩溃，进而影响由服务器提供解析的数以万计的网站域名；7 月 31 日起，CNCERT 对互联网上 13 万余台域名服务器进行跟踪检测，检测到有 4 万余台采用 BIND，这当中又有约 10% 共计 4000 余台为我国境内的域名服务器。截至 9 月 17 日，互联网上采用 BIND 9 的域名服务器中仍有 90% 以上受到漏洞不同程度的影响。

又如，2009 年 7 月初披露的微软操作系统视频功能组件高危漏洞。根据 CNCERT 监测数据以及各互联网信息通报工作单位报送的信息，在漏洞披露后的一段时间内，黑客大肆利用漏洞进行网页挂马活动，侵害了众多网站和用户。黑客借此可以控制大量互联网主机，不仅可以窃取用户私密信息，更为危险的是可以构建大规模的僵尸网络，进而用来发送巨量垃圾邮件或发动其他更危险的网络攻击。

■ 网络安全感知

根据 CNCERT 对互联网业务流量的抽样监测结果，2009 年互联网用户主要的网络应用有：Web 浏览、软件下载、即时聊天、网络多媒体。因此，涉及相关应用的网络安全事件和问题是用户感知的重点。

例如：在“5.19”事件中，多省市互联网用户第一时间感知的就是主要门户网站无法登陆。事后，广大互联网用户对事件造成的严重影响以及所谓的“暴风门”议论纷纷。在“6.25”事件中，因腾讯公司应用服务器受广东省电信运营企业网络故障影响，多省市用户向 CNCERT 报告了 QQ 无法登陆的情况。此外，受“5.19”事件影响，一些社区论坛中出现了“全中国 DNS 受攻击”的猜测。在 8 月中下旬因海底地震造成的国际互联网海底电缆中断事件中，由于 MSN 服务异常，互联网用户大量在社区论坛中讨论、猜测可能原因。

随着网络安全事件的频繁发生以及用户的网络安全意识的逐步提高，用户对网络安全问题的感知也越来越强烈。2009 年，CNCERT 通过电子邮件、热线电话、网站提交、传真等多种方式共接收到 21927 件网络安全事件报告⁶，与 2008 年相比出现大幅增加，其中垃圾邮件事件、网页篡改事件、网页挂马事件的报告数量增长尤为突出。对于关系用户自身安全的重要事件信息，CNCERT 及时发布行业通报或网站公告。

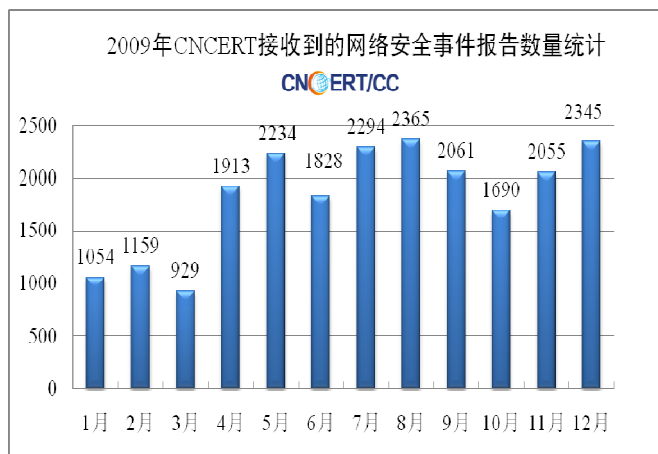
例如：2009 年 4 月，国内感染“飞客”蠕虫的主机 IP 数量急剧增加，CNCERT 连续篇发布监测专题报告，并将涉及政府和重要信息系统部门的感染主机 IP 通报相关部门进行处置；6 月高考前夕，CNCERT 监测到国内二十余所高校被密集挂马，及时发布了提醒考生和家长注意访问高校网站安全的公告；8 月 11 日，CNCERT 监测发现国内三个大型门户网站被同时挂马，影响众多互联网用户，CNCERT 迅速在官方网站发布重要安全公告并协调处置；10 月，CNCERT 接到用户举报，互联网有很多假冒央视“非常 6+1 栏目”网站的钓鱼网站，并通过飞信传播。CNCERT 安全公告提醒用户小心以防上当，同时协调域名机构清除了假冒站点。

值得注意的是，2009 年新闻媒体（包括网络媒体）对网络安全事件的跟踪和报道在一定程度上增强了用户对网络安全事件的感知程度。由此带来的积极影响有两方面，一是普及网络安全基本常识，提高了用户的网络安全意识；另一方面则发挥了新闻媒体的宣传监督作用。例如：央视“3.15”晚会曝光黑客制作、销售、传播木马牟取暴利的利益链条；“新闻 30 分栏目”报道 QQ 盗号案件揭开互联网黑色地下产业链的黑幕等。

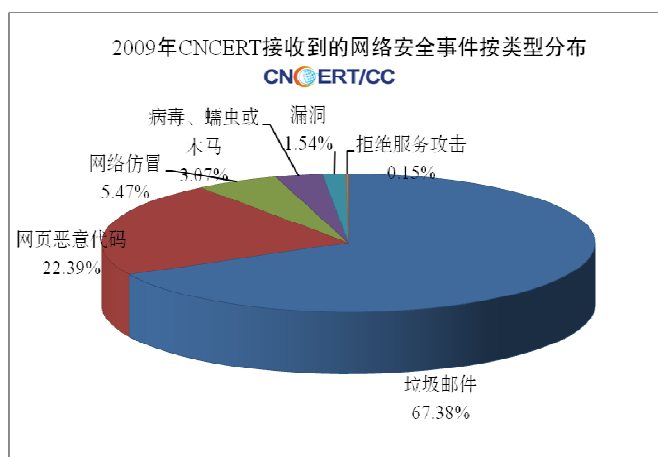
⁶ 不含扫描类事件，也合并了通过不同方式报告的同一网络安全事件。自 2004 年以来，CNCERT 通过电子邮件、热线电话、网站提交、传真等公开渠道接收国内外网络安全事件报告。虽然接收到有扫描类事件投诉，但不计数。列入计数的事件主要以造成实际影响或后果的事件类型为主。

（二）全年网络安全数据预览

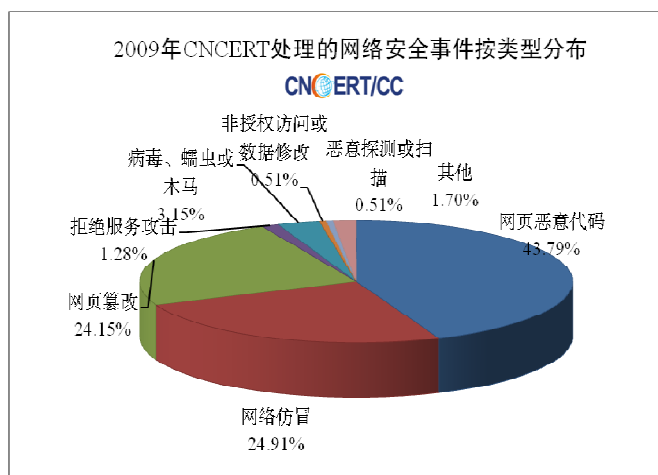
■ 网络安全事件接收与处理情况



2009 年 CNCERT 共接收 21927 件网络安全事件报告, 其中来自境外的报告事件占绝大多数, 为 21681 件。

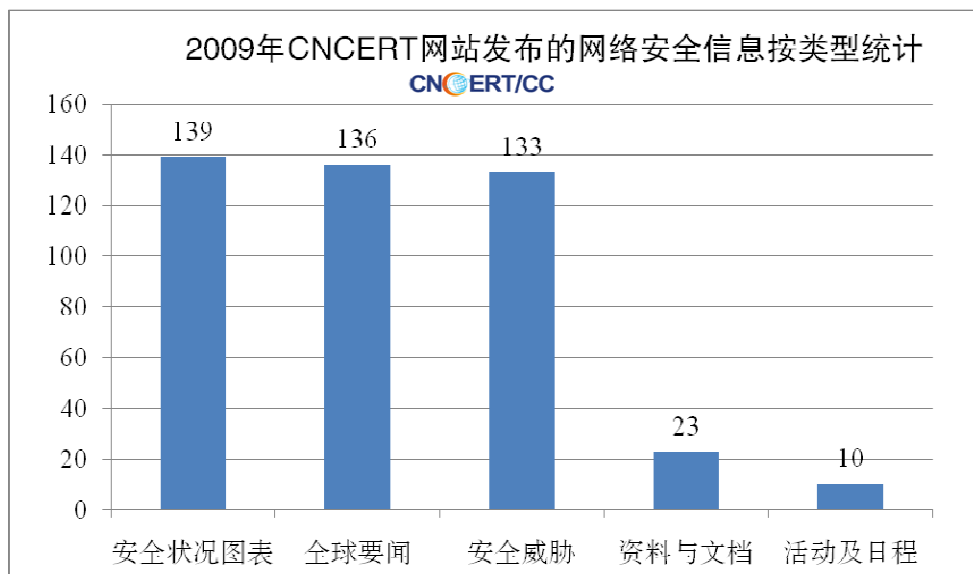


2009 年 CNCERT 接收到的网络安全事件报告中, 垃圾邮件、网页恶意代码(网页挂马)和网络仿冒事件居前三位。



2009 年 CNCERT 国家中心和各分中心对接收到网络安全事件进行核实、归类、合并后共处理事件 1176 件; 网页恶意代码、网络仿冒和网页篡改是事件处理的重点, 占事件处理总数的 93%。

■ 网络安全信息公告发布情况

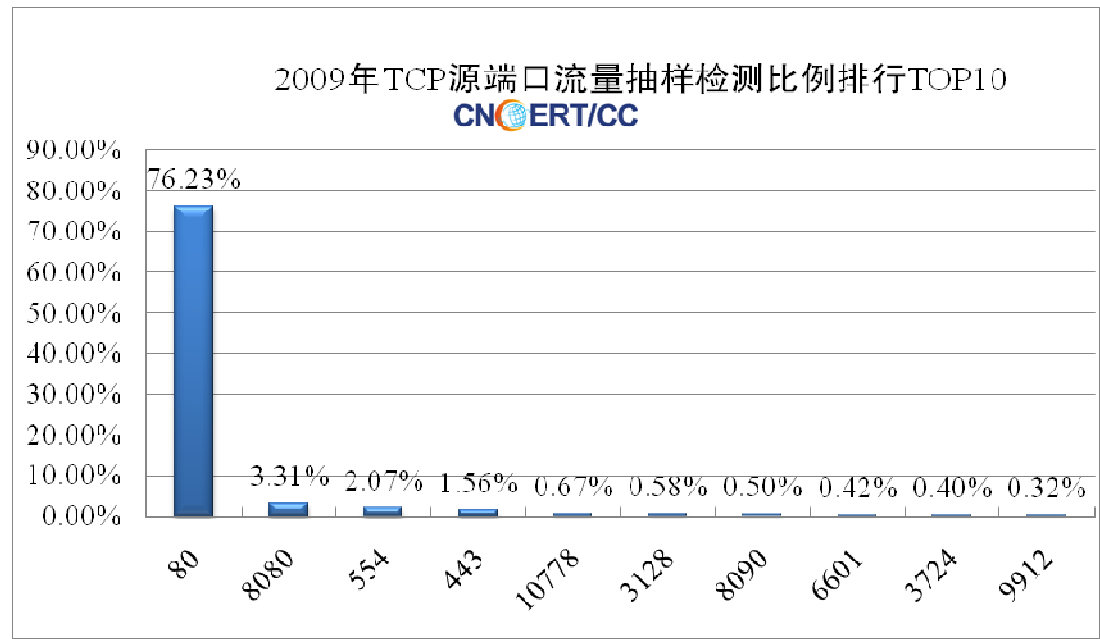


2009年CNCERT官方网站(www.cert.org.cn)共整理发布各类网络安全信息共441条,其中发布了133条与政府和重要信息系统部门、企事业单位以及互联网普通用户息息相关的**安全威胁公告(含安全漏洞)**，涉及操作系统、服务器软件系统、常用浏览器等，其中不乏微软操作系统视频功能组件高危漏洞、域名系统软件 Bind 9 高危漏洞等危害严重的漏洞；此外，还包括公布国内一些著名网站被密集挂马、高考前夕高校网站被大量挂马的公告信息。

CNCERT对上述安全漏洞和安全威胁信息持续进行跟踪，积极协调基础电信运营企业、域名注册和服务机构以及应急服务支撑单位进行处置。

■ 互联网业务流量监测情况⁷

TCP 端口流量抽样检测比例排行 TOP10

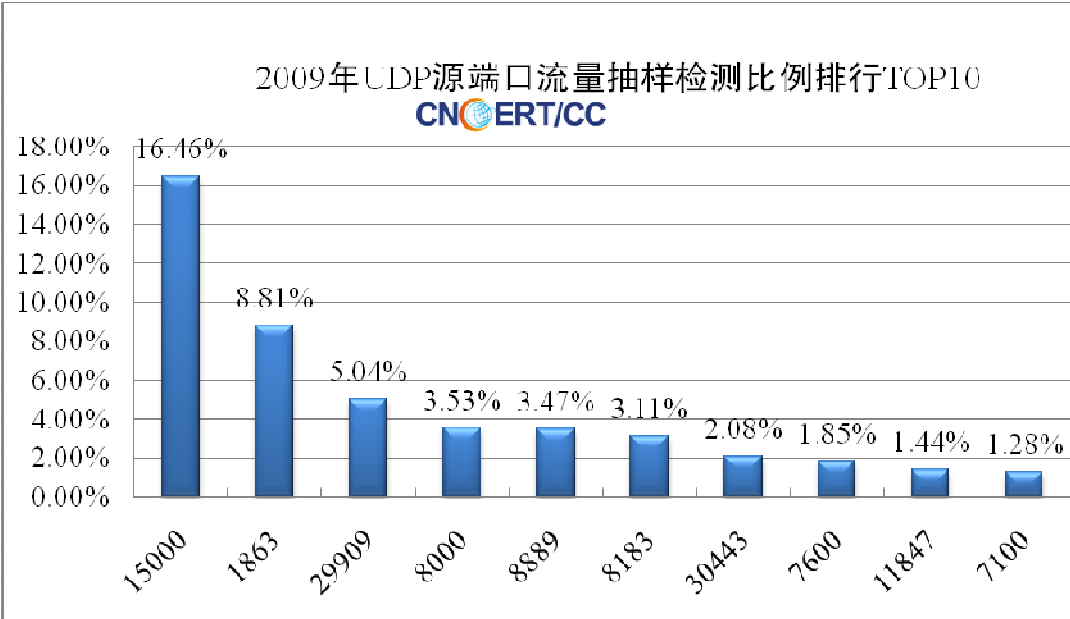


排名	TCP 端口	百分比	主要的业务种类
1	80	76.23%	网页服务端口
2	8080	3.31%	网页服务端口
3	554	2.07%	RTSP 协议端口
4	443	1.56%	网页服务端口
5	10778	0.67%	未知服务端口
6	3128	0.58%	代理服务器端口
7	8090	0.50%	代理服务器端口
8	6601	0.42%	未知服务端口
9	3724	0.40%	网络游戏端口
10	9912	0.32%	未知服务端口
--	其他端口	14.28%	

使用 TCP 协议的端口中，占用带宽最多的网络应用端口是：网页浏览、代理服务器和网络多媒体。

⁷ 本节所列 TCP 和 UDP 端口流量 TOP 10 采用的是源端口统计的方法，即在 Netflow 五元组中以源端口（SRC_PORT）字段作字节统计。另外，比例计算为：该源端口流量字节数/TOP 1024 源端口流量总字节数。

UDP 端口流量抽样检测比例排行 TOP10

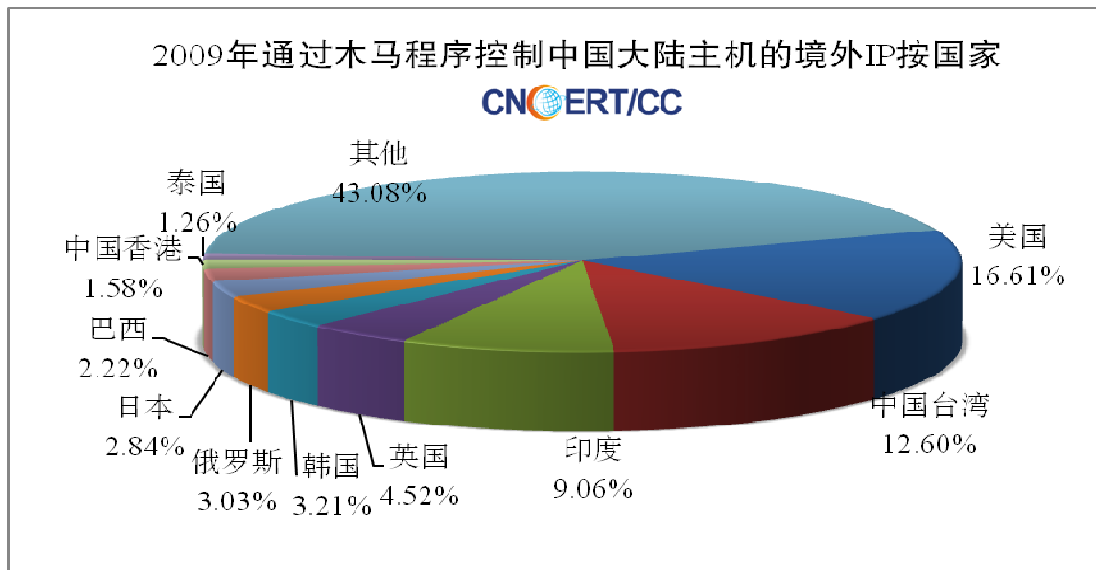
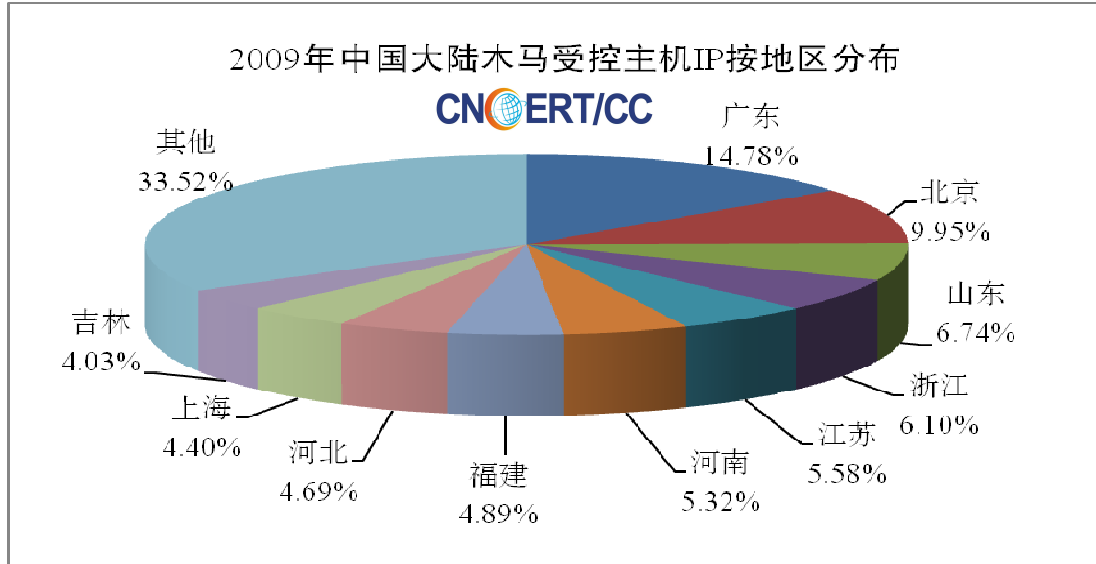


排名	UDP 端口	百分比	主要的业务种类
1	15000	16.46%	迅雷下载工具端口
2	1863	8.81%	MSN 服务端口
3	29909	5.04%	腾讯 TT 旋风下载端口
4	8000	3.53%	QQ 通讯端口
5	8889	3.47%	P2P 下载软件端口
6	8183	3.11%	P2P 下载软件端口
7	30443	2.08%	未知服务端口
8	7600	1.85%	未知服务端口
9	11847	1.44%	迅雷下载工具端口
10	7100	1.28%	网络游戏端口
--	其他端口	52.93%	-

使用 UDP 协议的端口中，占用带宽最多的网络应用是：P2P 下载、即时聊天和网络多媒体。

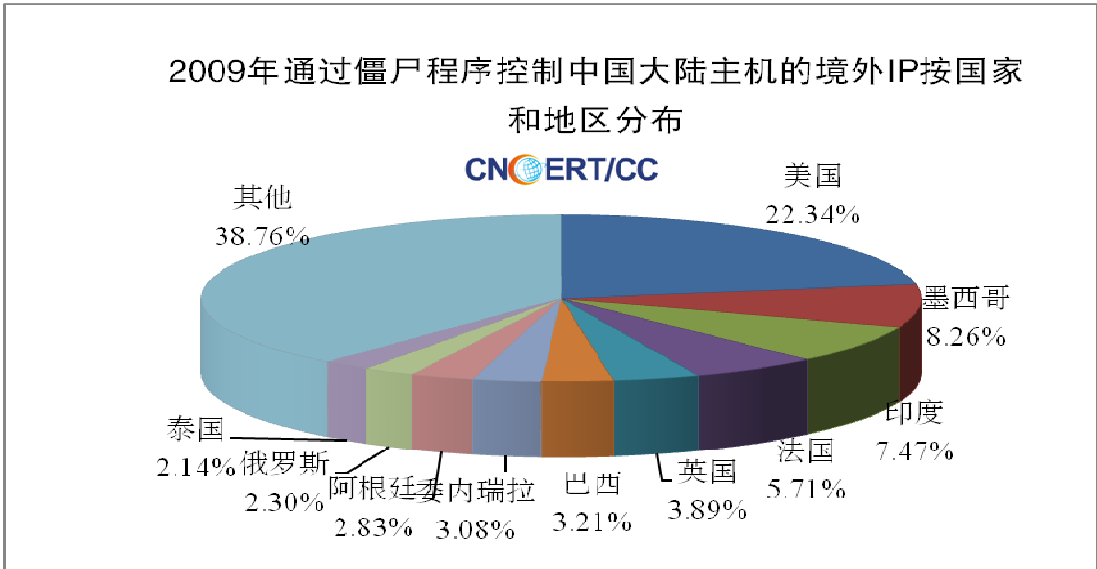
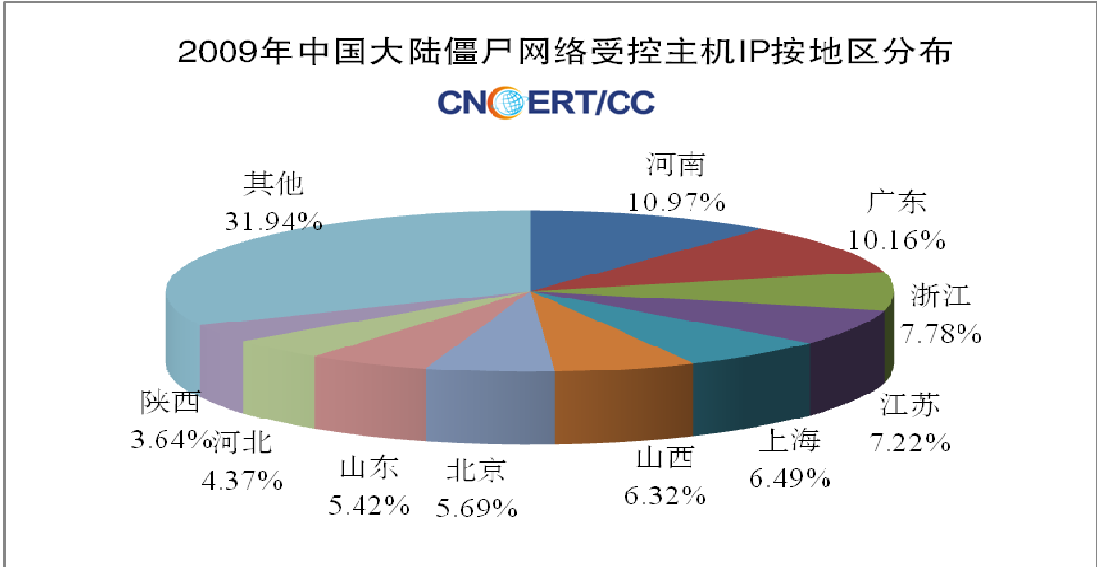
■ 木马和僵尸网络监测情况

木马监测情况



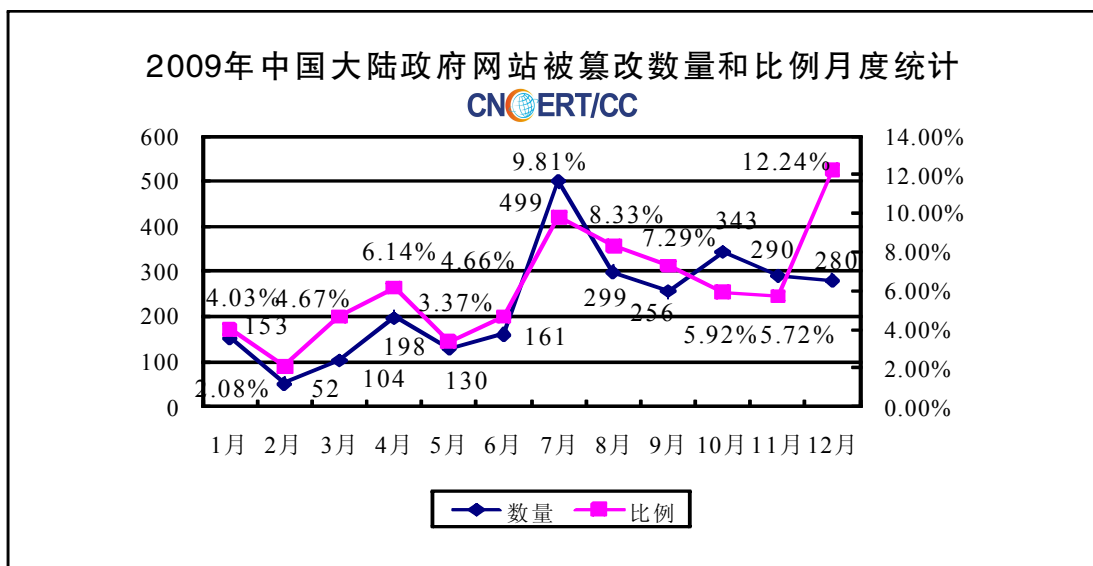
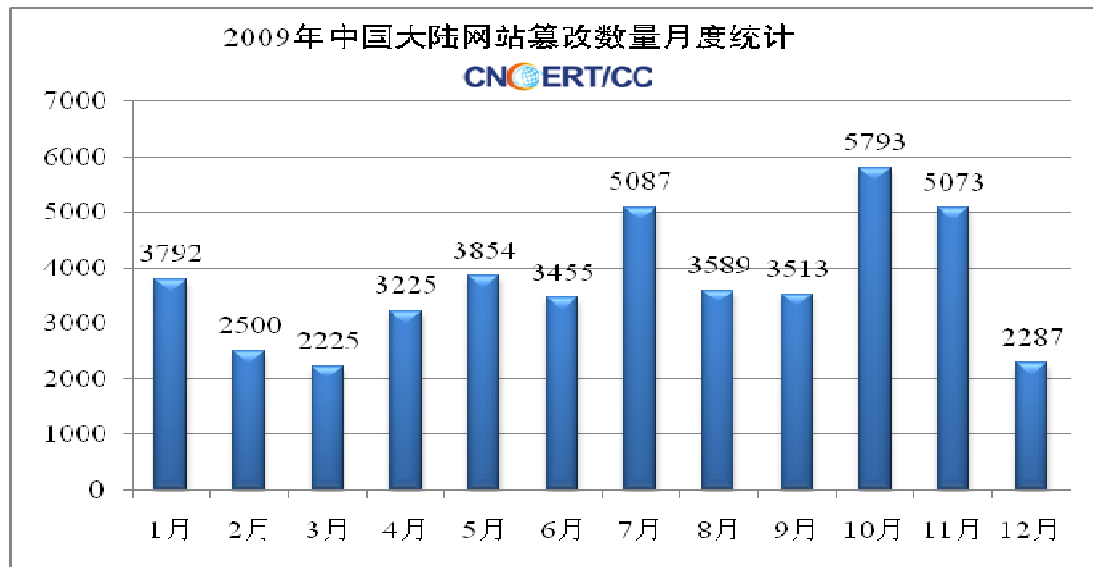
2009年，CNCERT监测到的境内被木马控制的主机IP共26.2万余个，较2008年大幅下降53.6%；境外有16.5万个主机IP参与控制上述境内主机，较2008年下降40.2%，数量排名前五位的国家和地区分别是：美国、中国台湾、印度、英国和韩国。

僵尸网络监测情况



2009年,CNCERT监测到的境内被僵尸网络控制的主机IP共83.7万余个,较2008年下降32.3%;境外有1.9万个主机IP参与控制上述境内主机,较2008年增长257.8%,数量排名前五位的国家和地区分别是:美国、墨西哥、印度、法国和英国。

■ 被篡改网站监测情况⁸



2009年，CNCERT 监测中国大陆有 4.2 万个网站被黑客篡改，其中，被篡改的政府网站各月累计达 2765 个；相较于政府网站占网站总数 1.1% 的比例 [注：该数据来自 CNNIC2010 年 1 月中国互联网络发展状况统计报告]，政府网站被篡改的比例相对较高。

⁸ 4.2 万个是在对 2009 年各月累计数量进行修正后得到，在上图所示的月度统计中，仍按原有各月累计数量进行描述。

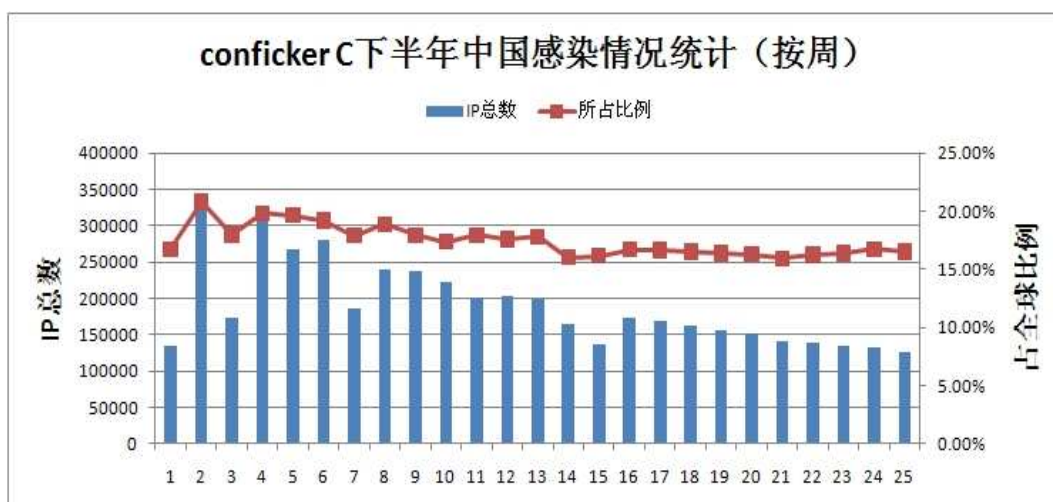
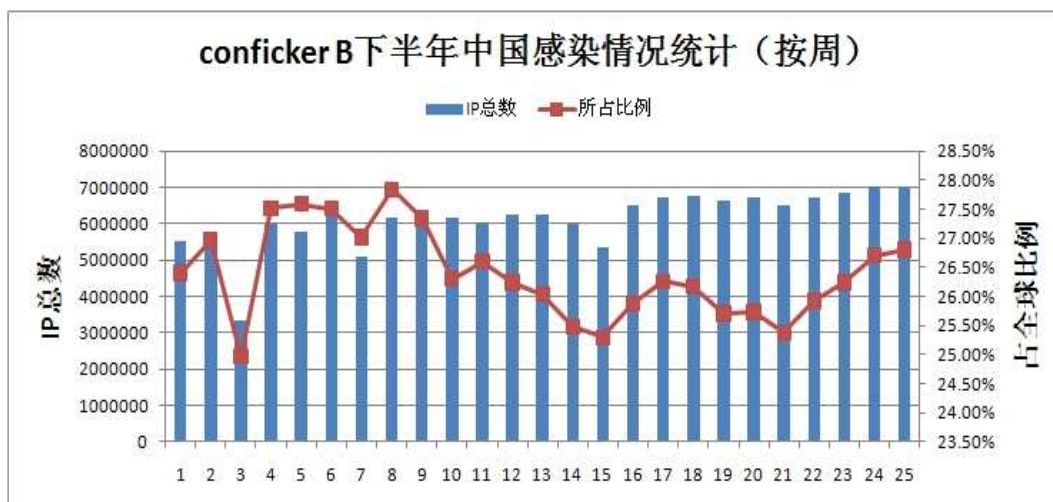
■ 网络仿冒事件处置情况

2009 年, CNCERT 共接到国内外机构报告的网络仿冒事件报告 1200 件。被仿冒的大都是著名金融机构、商业公司的网站。

2009 年向 CNCERT 报告网络仿冒事件报告者 TOP 10	
网络仿冒事件报告者	数量
ebay/paypal(美国电子商务站点)	269
auscert.org.au(澳大利亚 CERT)	130
HSBC(中国香港汇丰银行)	95
markmonitor.com(美国互联网安全服务公司)	95
s21sec.com(西班牙互联网安全服务公司)	69
cyf-kr.edu.pl(波兰 AGH 科技大学)	67
Cyveillance.com(美国互联网安全服务公司)	52
rsa.com(美国 EMC 公司安全事业部)	50
melbourneitdb.com(美国域名注册商)	31
brandprotect.com(美国互联网安全服务公司)	27

2009 年 CNCERT 接收到的被仿冒网站按事件次数 TOP 10	
被仿冒网站	次数
ebay/paypal(美国网上交易站点)	298
HSBC(中国香港汇丰银行)	97
BBVA(毕尔巴鄂比斯开银行)	54
BANCO BRADESCO S.A.(巴西布拉德斯科银行)	29
commonwealth bank of Australia(澳大利亚联邦银行)	28
facebook(国外交友网站)	24
citibank(美国花旗银行)	22
Westpac Banking Corporation(澳大利亚西太平洋银行)	21
Internal Revenue Service(美国国家税务局)	18
Twitter(国外交友网站)	17

■ “飞客”蠕虫（Conficker）监测情况



2008 年底飞客蠕虫开始在全球互联网蔓延并出现多个变种。其中，.B 和.C 变种传播范围较广。

《2009 年中国互联网网络安全报告》章节目录

CNCERT《2009 年中国互联网网络安全报告》将于 2010 年 5 月份由电子工业出版社出版发行，敬请关注。《2009 年中国互联网网络安全报告》章节目录如下：

《2009 年中国互联网网络安全报告》章节目录

- 1 2009 年网络安全状况综述
 - 1.1 总体状况
 - 1.2 数据导读
- 2 “您用互联网做什么？”——互联网业务流量监测分析
- 3 “您被攻击过吗？”——网络安全事件接收与处理
 - 3.1 事件接收和处理情况
 - 3.2 事件处理部分案例介绍
- 4 “您的计算机安全吗？”——网络安全漏洞公告与处置
- 5 “您的计算机被控制了吗？”——木马和僵尸网络监测情况
 - 5.1 木马数据分析
 - 5.2 僵尸网络数据分析
- 6 “您的计算机被感染了吗？”——恶意代码捕获情况
- 7 “您访问的网站安全吗？”——网站安全监测情况
 - 6.1 网站被篡改情况分析
 - 6.2 网站被挂马情况分析
- 8 “您遇到过网络钓鱼吗？”——网络仿冒事件情况
- 9 “欢迎您向我们举报。”——网络安全信息通报情况
- 10 “欢迎您分享我们的分析报告。”——网络安全专题研究
 - 10.1 2009 年重大网络安全事件评述
 - 10.2 2009 年国内网络安全监管动态
 - 10.3 2009 年国外网络安全监管动态
 - 10.4 2009 年“飞客”蠕虫监测分析报告
 - 10.5 2009 年木马和僵尸网络治理行动
- 11 “邀请您加入我们，共同应对安全威胁。”——国内网络安全组织与活动
 - 11.1 国内应急组织发展情况
 - 11.2 国内应急服务支撑单位
 - 11.3 国内网络安全重要活动
- 12 “我们一直是全球网络安全的重要力量。”——国际网络安全交流与合作
- 13 2010 年网络安全挑战与工作展望
- 14 网络安全术语解释
- 15 参考文献

三、 网络安全术语解释

- 信息系统

信息系统是指由计算机硬件、软件、网络和通信设备等组成的以处理信息和数据为目的的系统。

- 漏洞

漏洞是指信息系统中的软件、硬件或通信协议中存在缺陷或不适当的配置，从而可使攻击者在未授权的情况下访问或破坏系统，导致信息系统面临安全风险。

- 恶意代码

恶意代码是指在未经授权的情况下，在信息系统中安装、执行以达到不正当目的的程序。恶意代码分类说明如下：

1. 特洛伊木马（Trojan Horse）

特洛伊木马（简称木马）是以盗取用户个人信息，甚至是远程控制用户计算机为主要目的的恶意代码。由于它像间谍一样潜入用户的电脑，与战争中的“木马”战术十分相似，因而得名木马。按照功能，木马程序可进一步分为：盗号木马⁹、网银木马¹⁰、窃密木马¹¹、远程控制木马¹²、流量劫持木马¹³和其它木马六类。

2. 僵尸程序（Bot）

僵尸程序是用于构建僵尸网络以形成大规模攻击平台的恶意代码。僵尸网络是被黑客集中控制的计算机群，其核心特点是黑客能够通过一对多的命令与控制信道操纵感染僵尸程序的主机执行相同的恶意行为，如可同时对某目标网站进行分布式拒绝服务攻击，或发送大量的垃圾邮件等。按照使用的通信协议，僵尸程序可进一步分为：IRC 僵尸程序、HTTP 僵尸程序、P2P 僵尸程序和其它僵尸程序四类。

3. 蠕虫（Worm）

蠕虫是指能自我复制和广泛传播，以占用系统和网络资源为主要目的的恶意

⁹ 盗号木马：用于窃取用户电子邮箱、网络游戏等账号的木马。

¹⁰ 网银木马：用于窃取用户网银、证券等账号的木马。

¹¹ 窃密木马：用于窃取用户主机中敏感文件或数据的木马。

¹² 远程控制木马：以不正当手段获得主机管理员权限，并能够通过网络操控用户主机的木马。

¹³ 流量劫持木马：用于劫持用户网络浏览的流量到攻击者指定站点的木马。

代码。按照传播途径，蠕虫可进一步分为：邮件蠕虫、即时消息蠕虫、U 盘蠕虫、漏洞利用蠕虫和其它蠕虫五类。

4. 病毒（Virus）

病毒是通过感染计算机文件进行传播，以破坏或篡改用户数据，影响信息系统正常运行为主要目的恶意代码。

5. 其它

上述分类未包含的其它恶意代码。

随着黑客地下产业链的发展，互联网上出现的一些恶意代码还具有上述分类中的多重功能属性和技术特点，并不断发展。对此，我们将按照恶意代码的主要用途参照上述定义进行归类。

- 拒绝服务攻击

拒绝服务攻击是向某一目标信息系统发送密集的攻击包，或执行特定攻击操作，以期致使目标系统停止提供服务。

- 网页篡改

网页篡改是恶意破坏或更改网页内容，使网站无法正常工作或出现黑客插入的非正常网页内容。

- 网页仿冒

网页仿冒是通过构造与某一目标网站高度相似的页面（俗称钓鱼网站），并通常以垃圾邮件、即时聊天、手机短信或网页虚假广告等方式发送声称来自于被仿冒机构的欺骗性消息，诱骗用户访问钓鱼网站，以获取用户个人秘密信息（如银行帐号和帐户密码）。

- 网页挂马

网页挂马是通过在网页中嵌入恶意代码或链接，致使用户计算机在访问该页面时被植入恶意代码。

- 垃圾邮件

垃圾邮件是将不需要的消息（通常是未经请求的广告）发送给众多收件人。包括：（一）收件人事先没有提出要求或者同意接收的广告、电子刊物、各种形式的宣传品等宣传性的电子邮件；（二）收件人无法拒收的电子邮件；（三）隐藏发件人身份、地址、标题等信息的电子邮件；（四）含有虚假的信息源、发件人、路由等信息的电子邮件。

- 域名劫持

域名劫持是通过拦截域名解析请求或篡改域名服务器上的数据,使得用户在访问相关域名时返回虚假 IP 地址或使用户的请求失败。

- 非授权访问

非授权访问是没有访问权限的用户以非正当的手段访问数据信息。非授权访问事件一般发生在存在漏洞的信息系统中,黑客利用专门的漏洞利用程序(Exploit)来获取信息系统访问权限。

- 路由劫持

路由劫持是通过欺骗方式更改路由信息,以导致用户无法访问正确的目标,或导致用户的访问流量绕行黑客设定的路径,以达到不正当的目的。。

感谢您阅读 CNCERT 《2009 年中国互联网网络安全报告》(预览版),如果您发现本文档存在任何问题,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。