2 “您的计算机被控制了吗？”—恶意代码监测情况

恶意代码主要包括计算机病毒、蠕虫、木马、僵尸程序等。计算机病毒和蠕虫几年前是最为常见的恶意代码类型，对用户计算机的破坏力也较强。近年来，随着黑客地下产业链的进化,木马和僵尸程序以及一些助长其传播的恶意代码成为了黑客最经常利用的手段,也成为了用户侧安全防范的主要对象。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,掌握黑客最新攻击手段，以进一步深入研究信息系统必需的防护措施。

木马和僵尸程序都是非常有效的远程监听和控制手段,尤其是在网络失窃密和发动 DDoS 攻击方面，对政府部门、商业机构以及普通用户造成了严重危害，因此，国家互联网应急中心（以下用英文简称 CNCERT 代替）对这两类恶意代码进行了重点监测[1]。

2.1 木马数据分析

木马是以盗取用户个人信息,甚至是以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。按照功能分类，木马程序可进一步分为：盗号木马、网银木马、窃密木马、远程控制木马、流量劫持木马、下载者木马和其它木马七类。

2010 年 CNCERT 抽样监测结果显示，在利用木马控制服务器对主机进行控制的事件中，木马控制服务器 IP 总数为 479626 个，较 2009 年下降 21.3%，木马受控主机 IP 总数为 10317169 个，较 2009 年大幅增长 274.9%。

■ 木马控制服务器分析

2010 年，境外木马控制服务器 IP 数量约有 22 万个，较 2009 年有所增长，增幅为 34.1%，而境内木马控制服务器 IP 数量为近 26 万个，与 2009 年相比则下降了 41.9%，具体如图 2-1 所示。

[1] 2010 年 CNCERT 主要对 153 种木马家族和 57 种僵尸网络家族进行了抽样监测。

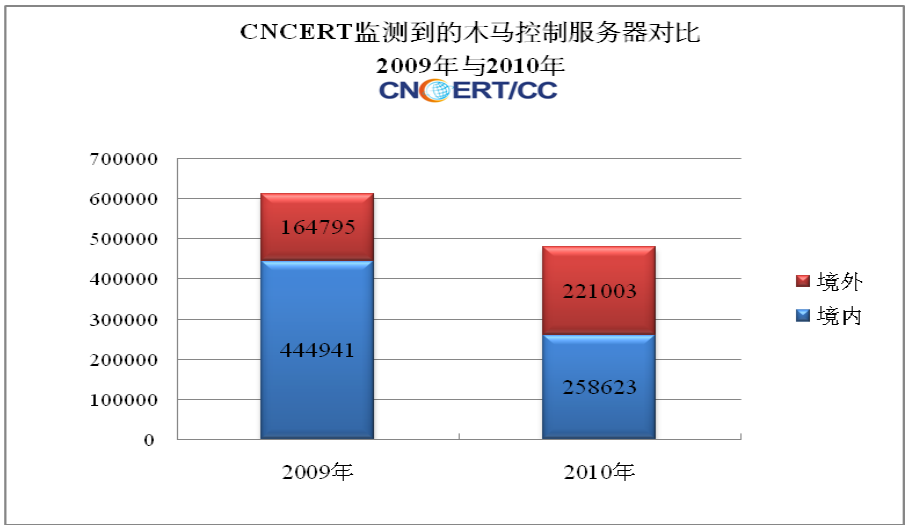

图 2-1　2009 年与 2010 年木马控制服务器数据对比

境内木马控制服务器 IP 绝对数量和相对数量（即各地区木马控制服务器 IP 绝对数量占其活跃 IP 数量的比例）前 10 位地区分布如图 2-2 所示，其中：广东省、山东省、浙江省居于木马控制服务器 IP 绝对数量前 3 位，西藏自治区、陕西省、广西壮族自治区居于木马控制服务器 IP 相对数量的前 3 位。

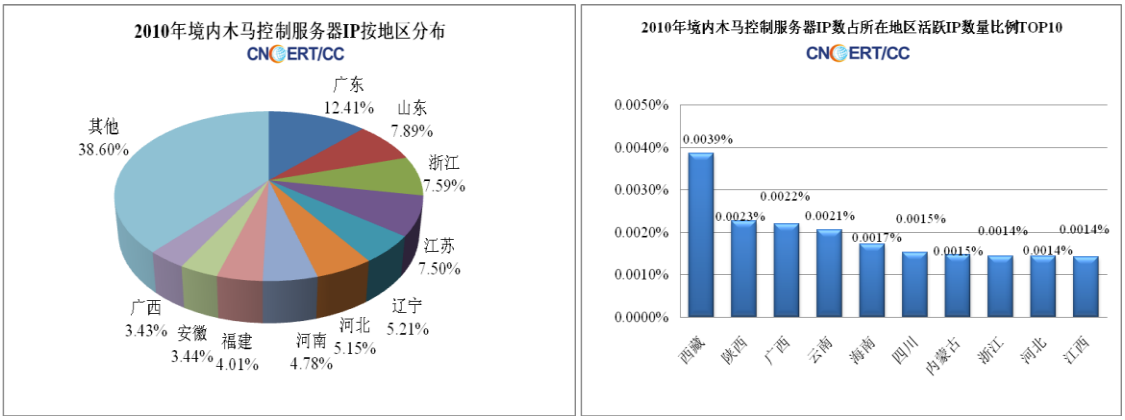

图 2-2　2010 年境内木马控制服务器 IP 按地区分布

图 2-3 所示为 2010 年境内木马控制服务器 IP 数量按运营商分布及所占比例，木马控制服务器 IP 数量无论是绝对数量，还是相对数量（即各运营商网内木马控制服务器 IP 绝对数量占其活跃 IP 数量的比例），位于中国电信网内的数量均排名第一。

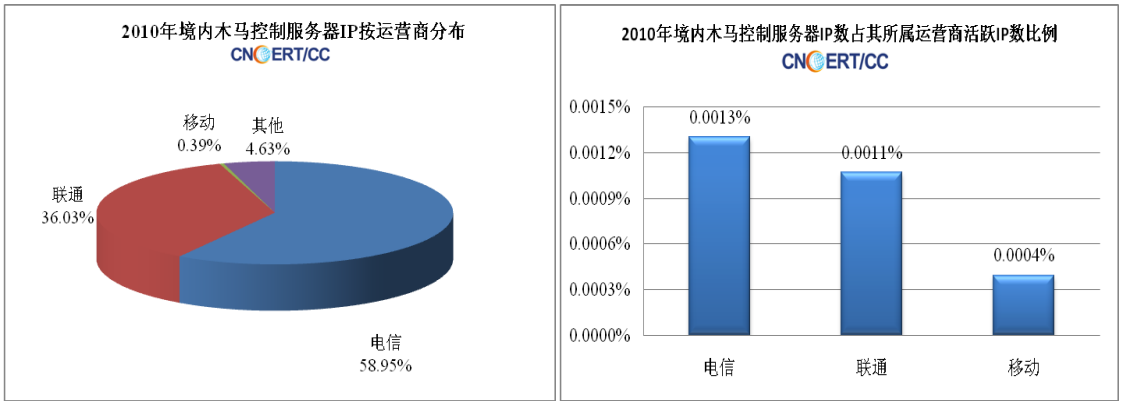

图 2-3　2010 年境内木马控制服务器 IP 按运营商分布

境外木马控制服务器 IP 数量前 10 位按国家和地区分布如图 2-4 所示，其中：美国、印度、中国台湾居于木马控制服务器 IP 数量前 3 位。

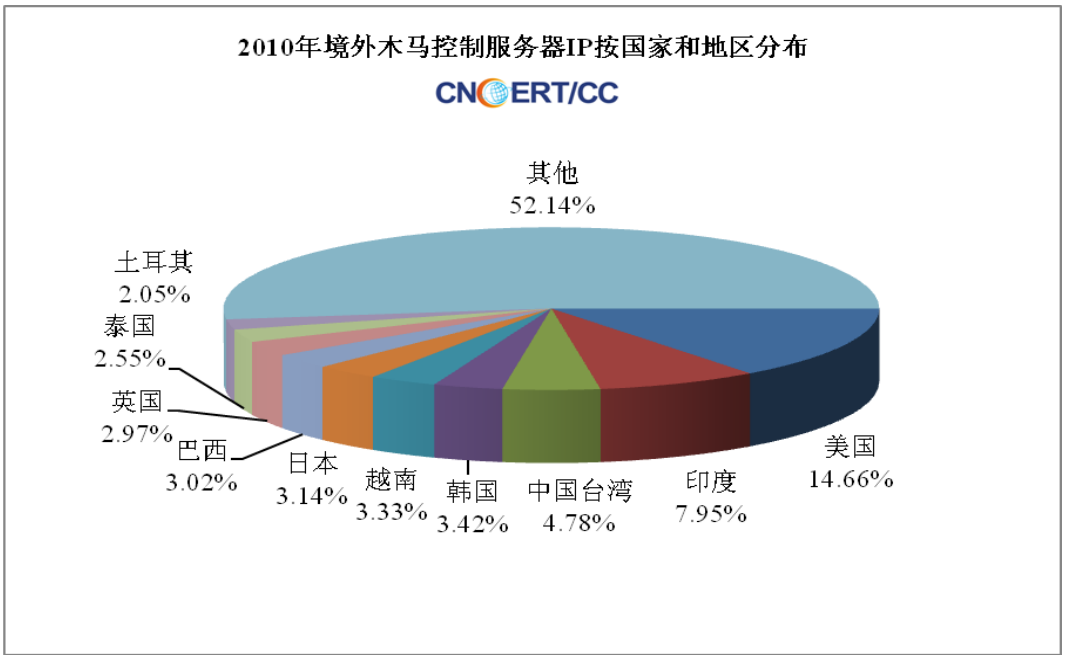

图 2-4　2010 年境外木马控制服务器 IP 按国家和地区分布

■ 木马受控主机分析

2010 年，境内共有 451 万余个 IP 地址的主机被植入木马，境外共有 580 万余个 IP 地址的主机被植入木马，数量较 2009 年均有较为明显的增长，增幅分别达到了 1620.3%和 133.1%，具体如图 2-5 所示。

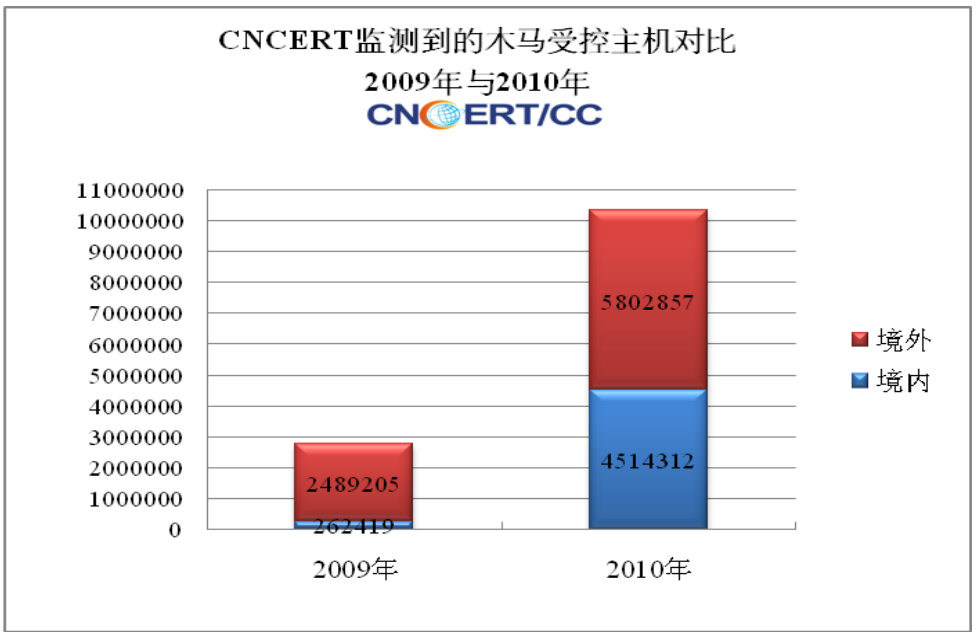

图 2-5　2009 年与 2010 年木马受控主机数据对比

2010 年木马受控主机 IP 数量呈现增长趋势，并在 2010 年下半年出现激增现象，原因是自 2010 年 6 月起，CNCERT 的监测范围新增了下载者木马、窃密木马、盗号木马、流量劫持木马和部分新型远程控制木马等。2010 年木马受控主机 IP 数量、境内木马受控主机 IP 数量、境外木马受控主机 IP 数量的月度统计分别如图 2-6、图 2-7、图 2-8 所示。

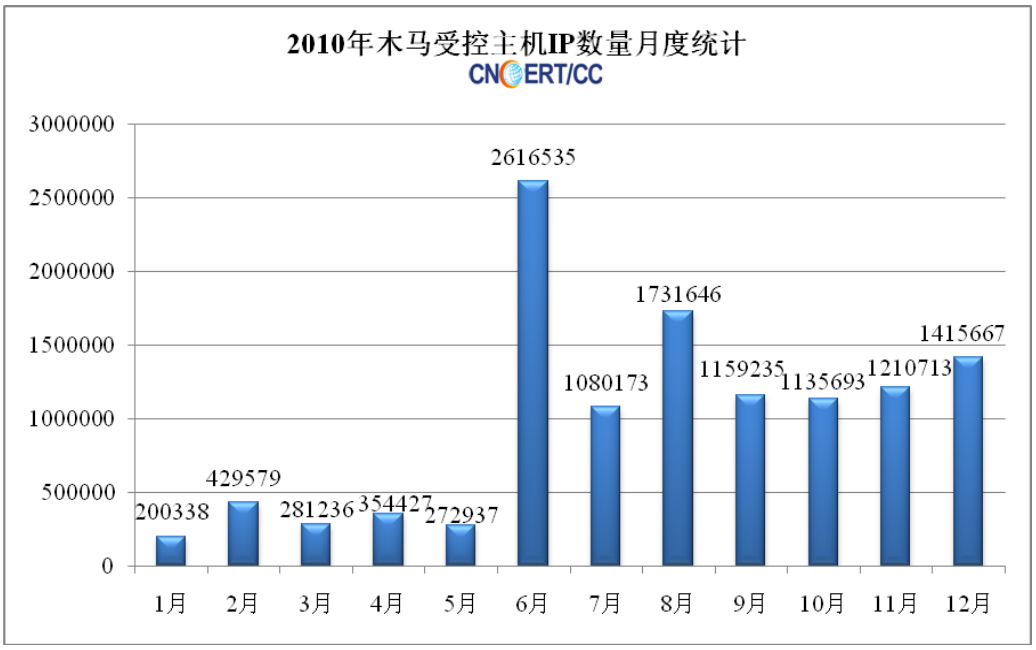

图 2-6　2010 年木马受控主机 IP 数量月度统计

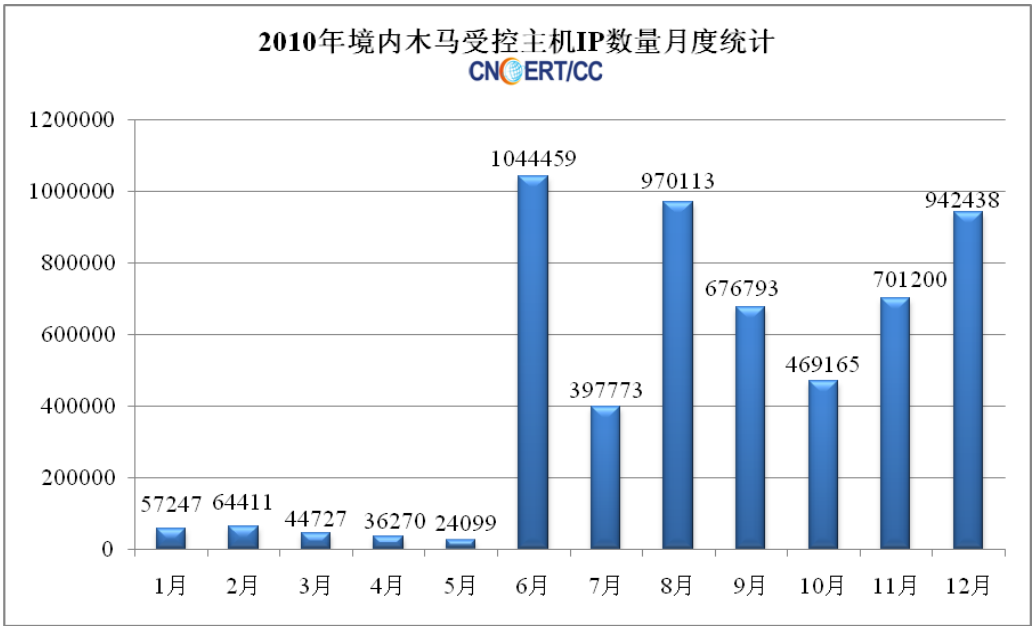

图 2-7　2010 年境内木马受控主机 IP 数量月度统计

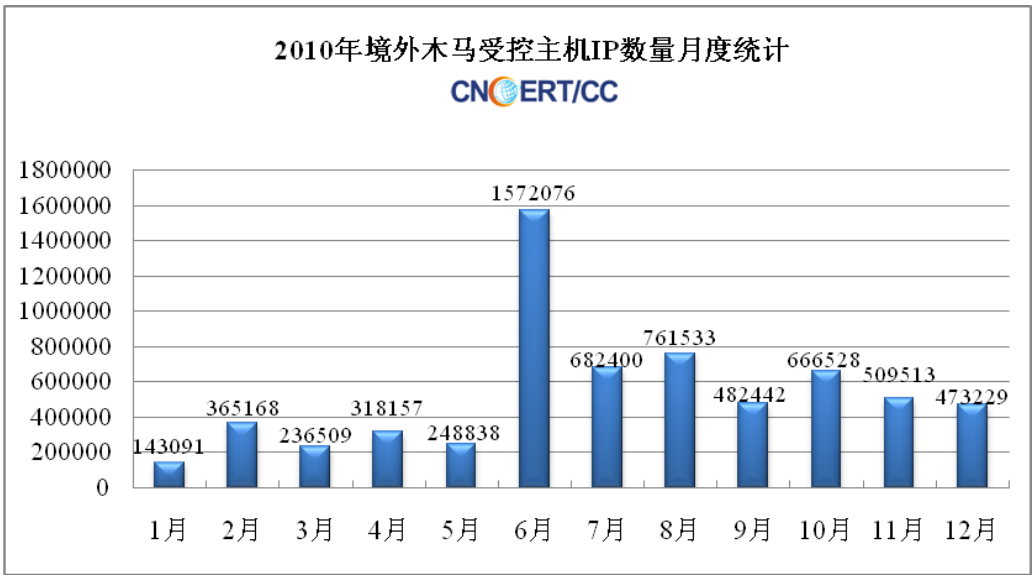

图 2-8　2010 年境外木马受控主机 IP 数量月度统计

境内木马受控主机 IP 绝对数量和相对数量(即各地区木马受控主机 IP 绝对数量占其活跃 IP 数量的比例) 前 10 位地区分布如图 2-9 所示，其中：广东省、湖南省、浙江省居于木马受控主机 IP 绝对数量前 3 位，陕西省、广西壮族自治区、湖南省居于木马受控主机 IP 相对数量的前 3 位，这在一定程度上反映出经济较为发达、互联网较为普及的东部地区因网民多、计算机数量多，使得该地区的木马受控主机 IP 绝对数量处于全国前列，而中西部地区因经济欠发达，虽网民相对较少、计算机总数较少，但相应计算机安全防护措施也更为薄弱，导致该地区木马受控主机 IP 占该地区活跃 IP 数量的比例较高，反映出该地区木马受灾较为严重。

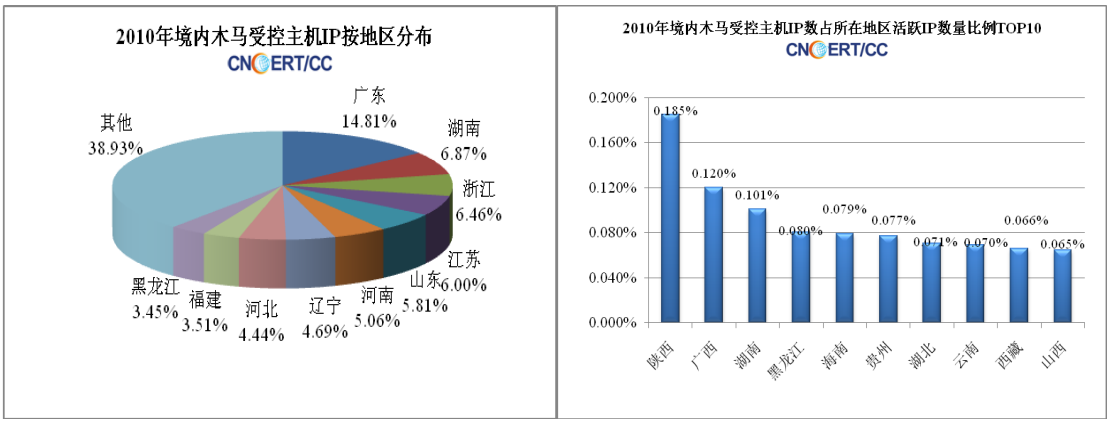

图 2-9　2010 年境内木马受控主机 IP 按地区分布

图 2-10 所示为 2010 年境内木马受控主机 IP 数量按运营商分布及所占比例，木马受控主机 IP 数量无论是绝对数量，还是相对数量（即各运营商网内木马受控主机 IP 绝对数量占其活跃 IP 数量的比例），位于中国电信网内的数量均排名第一。此外，在 CNCERT 监测到的木马受控主机 IP 中，有相当一部分 IP 属于动态 IP 地址或是虚拟主机地址，据此可以判断，终端用户（如：拨号上网用户）或虚拟主机托管用户由于安全防护措施较弱，易成为黑客攻击的目标；当黑客攻击成功取得控制权后，其可成为黑客发动新的攻击行为的跳板。

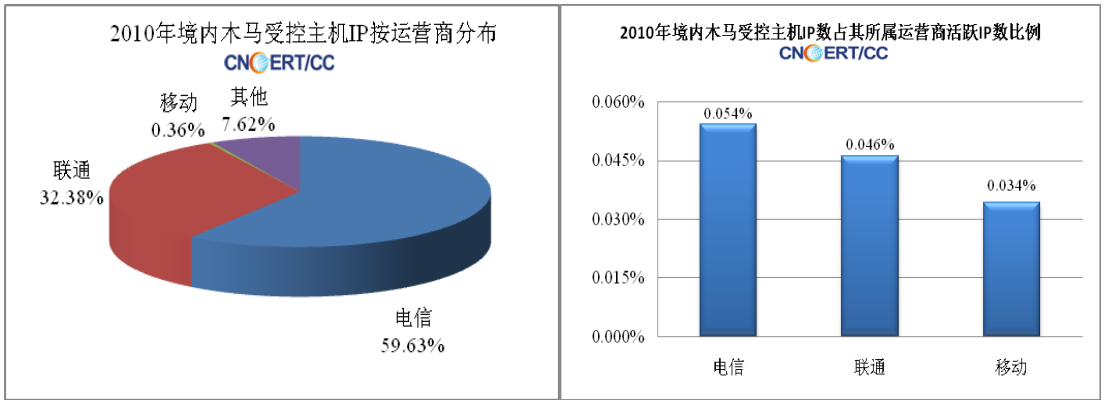

图 2-10　2010 年境内木马受控主机 IP 按运营商分布

境外木马受控主机 IP 数量前 10 位按国家和地区分布如图 2-11 所示，其中：中国台湾、美国、韩国居于木马受控主机 IP 数量前 3 位。

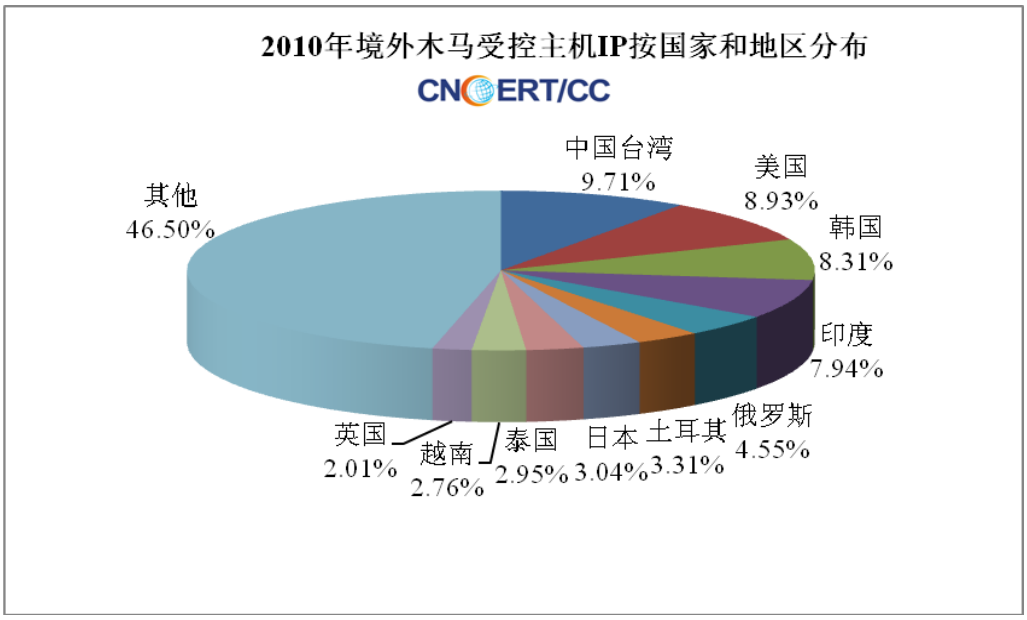

图 2-11　2010 年境外木马受控主机 IP 按国家和地区分布

2.2僵尸网络数据分析

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。多年以前，当僵尸网络刚刚出现的时候，黑客往往是通过 IRC 协议来控制的。随着恶意代码的发展，越来越多的僵尸网络被通过木马来控制，因此按照广义的概念也可以把感染木马并由同一组控制端控制的联网计算机也称之为僵尸网络，但在 2010 年的统计中，我们重点统计 IRC 和 HTTP 类型的僵尸网络。

2010 年 CNCERT 抽样监测结果显示，僵尸网络控制服务器 IP 总数约为 1.4 万个，僵尸网络受控主机 IP 地址总数为 562 万余个，较 2009 年均有较大幅度下降，降幅分别达到 39.6%和 52.8%。

■ 僵尸网络控制服务器分析

2010 年，境内僵尸网络控制服务器 IP 数量为 7251 个，较 2009 年增长 72.9%，境外僵尸网络控制服务器 IP 数量为 6531 个，与 2009 年相比则下降了 65%，具体如图 2-12 所示。

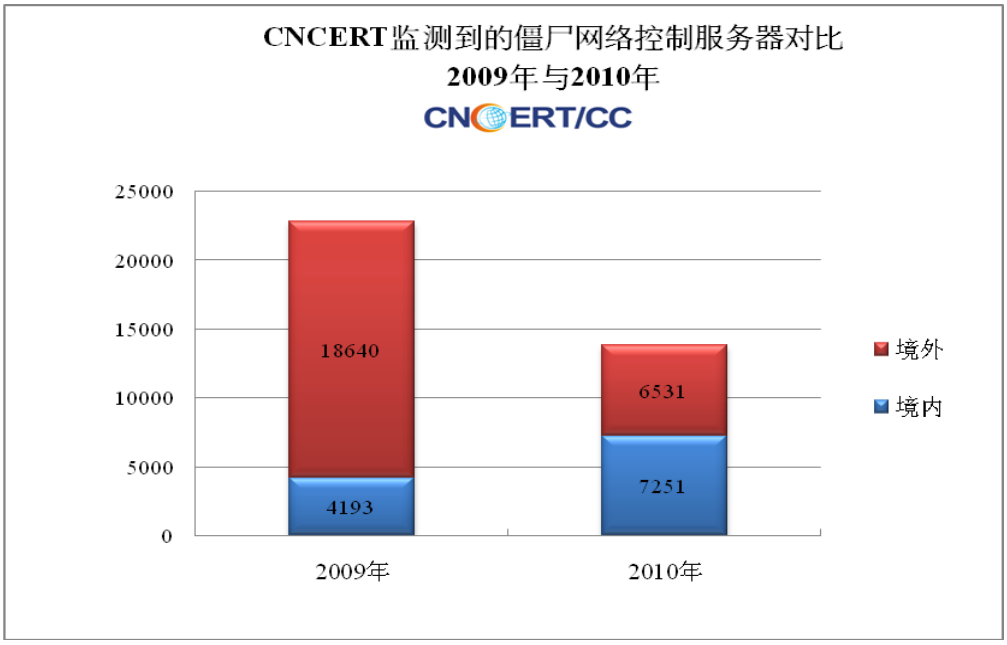

图 2-12　2009 年与 2010 年僵尸网络控制服务器数据对比

2010 年僵尸网络按规模分布如图 2-13 所示，控制规模在 1 千个主机 IP 以内的僵尸网络约占总数的 99.1% ,较 2009 年略增 1.9%。控制规模在 1000 以下、1000-5000、5000-20000、2 万-5 万、5 万-10 万以及 10 万以上的僵尸网络数量与 2009 年相比分别下降 38.5%、65.4%、82.8%、94.7%、97.4%和 93.9%。从绝对数量上看，僵尸网络的规模总体上继续保持小型化、局部化的趋势。

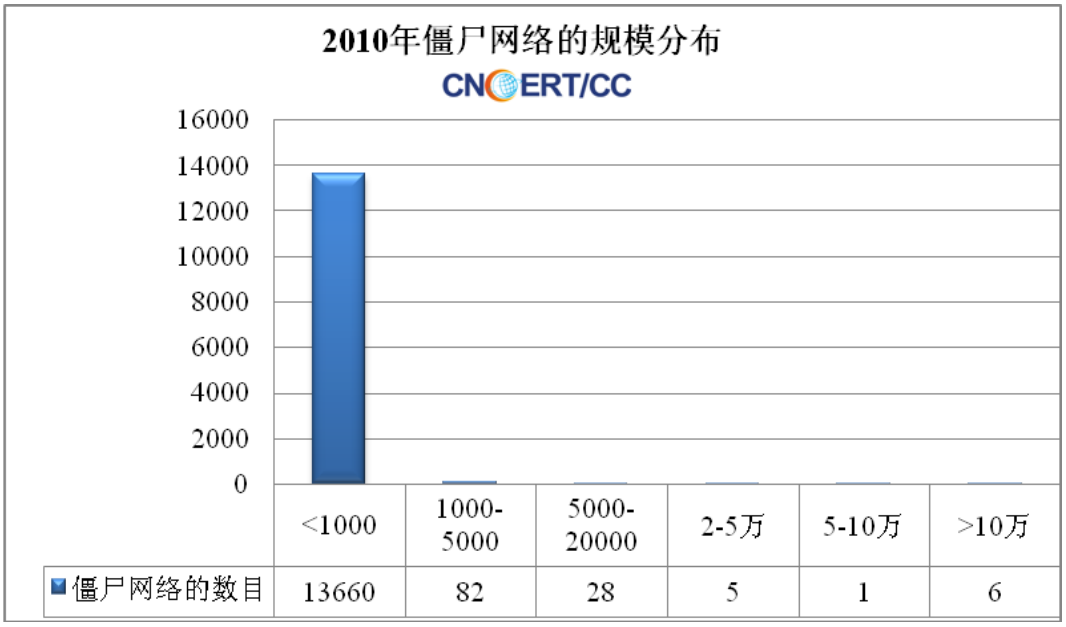

图 2-13　2010 年僵尸网络规模分布

境内僵尸网络控制服务器 IP 绝对数量和相对数量（即各地区僵尸网络控制服务器 IP 绝对数量占其活跃 IP 数量的比例）前 10 位地区分布如图 2-14 所示，

其中：广东省、北京市、浙江省居于僵尸网络控制服务器 IP 绝对数量前 3 位，江西省、辽宁省、江苏省居于僵尸网络控制服务器 IP 相对数量的前 3 位。

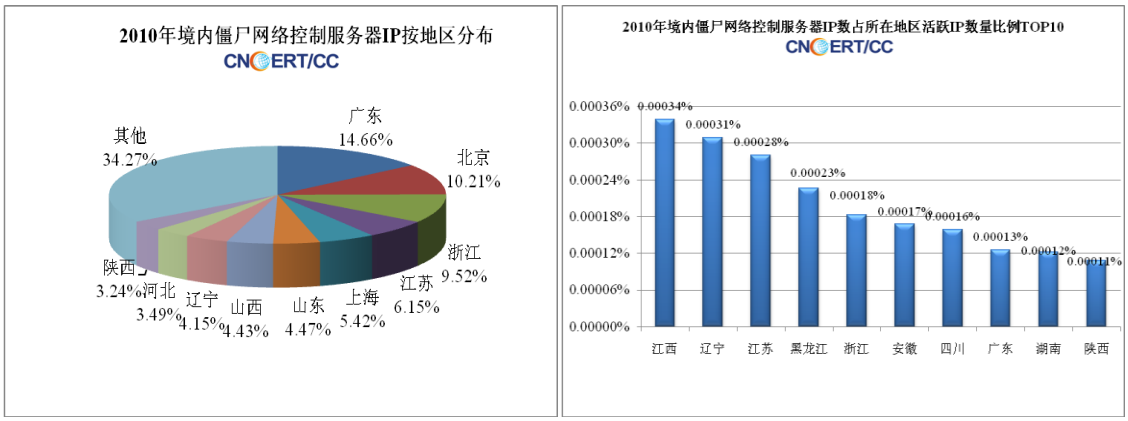

图 2-14　2010 年境内僵尸网络控制服务器 IP 按地区分布

图 2-15 所示为 2010 年境内僵尸网络控制服务器 IP 数量按运营商分布及所占比例，僵尸网络控制服务器 IP 数量无论是绝对数量，还是相对数量（即各运营商网内僵尸网络控制服务器 IP 绝对数量占其活跃 IP 数量的比例），中国电信网内数量均排名第一。

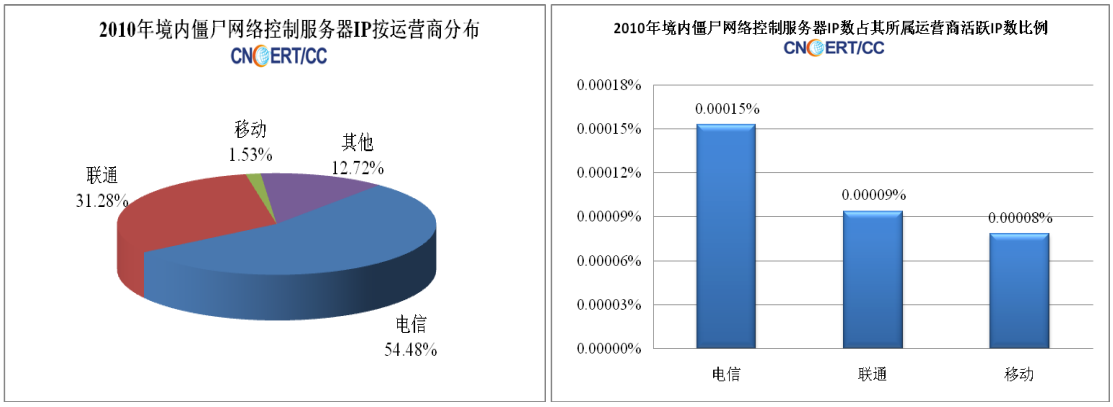

图 2-15　2010 年境内僵尸网络控制服务器 IP 按运营商分布

境外僵尸网络控制服务器 IP 数量前 10 位按国家和地区分布如图 2-16 所示，其中：美国、印度、土耳其居于僵尸网络控制服务器 IP 数量前 3 位。

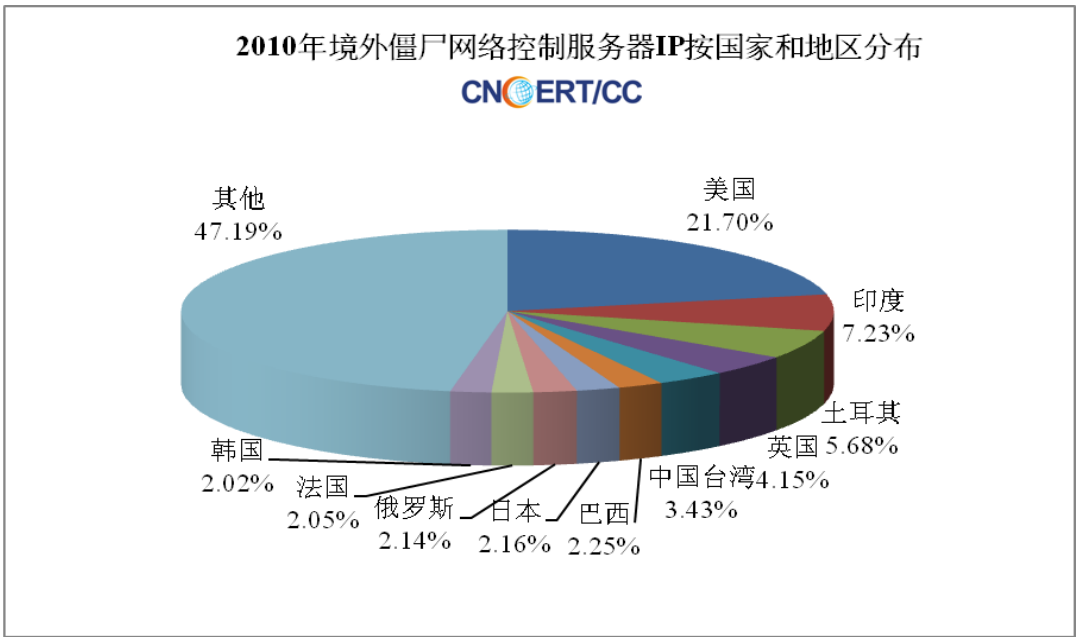

图 2-16　2010 年境外僵尸网络控制服务器 IP 按国家和地区分布

■ 僵尸网络受控主机分析

2010 年，境内有 47 万余个 IP 地址的主机感染僵尸程序，境外有 515 万余个 IP 地址的主机感染僵尸程序，数量较 2009 年均有大幅下降，降幅分别为 43.9%和 53.4%，具体如图 2-17 所示。

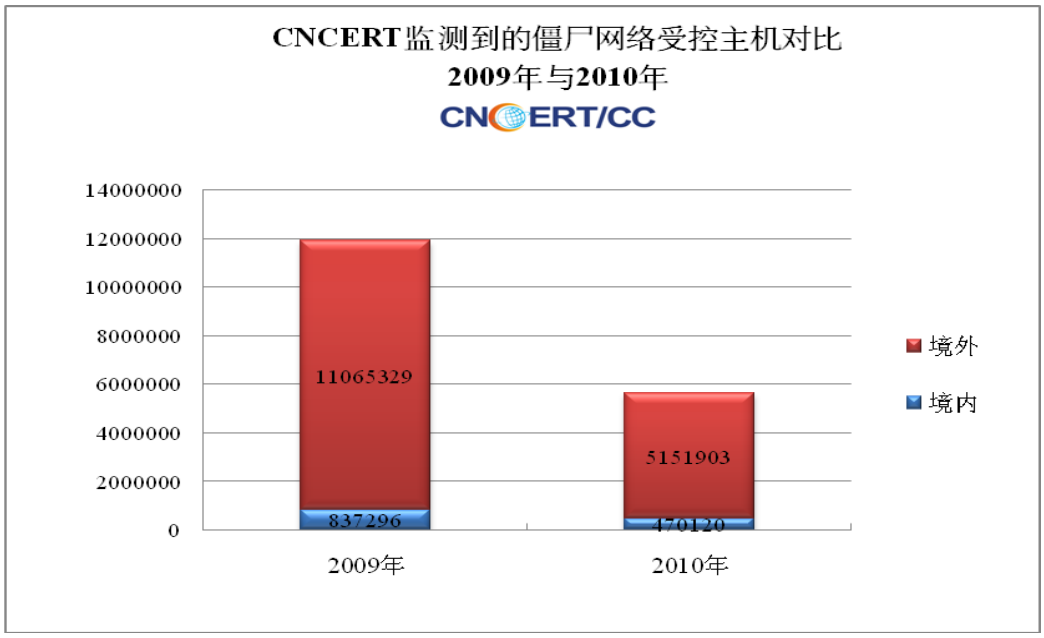

图 2-17　2009 年与 2010 年僵尸网络受控主机数据对比

2010 年僵尸网络受控主机 IP 数量、境内僵尸网络受控主机 IP 数量、境外僵尸网络受控主机 IP 数量的月度统计分别如图 2-18、图 2-19、图 2-20 所示。2010 年 3 月起僵尸网络受控主机数量明显回落，这说明 CNCERT 持续开展的僵尸网络专项治理行动取得了一定成效。因 CNCERT 的僵尸网络监测范围增加了新的监测特征，12 月境内僵尸网络受控主机 IP 数量出现激增现象。

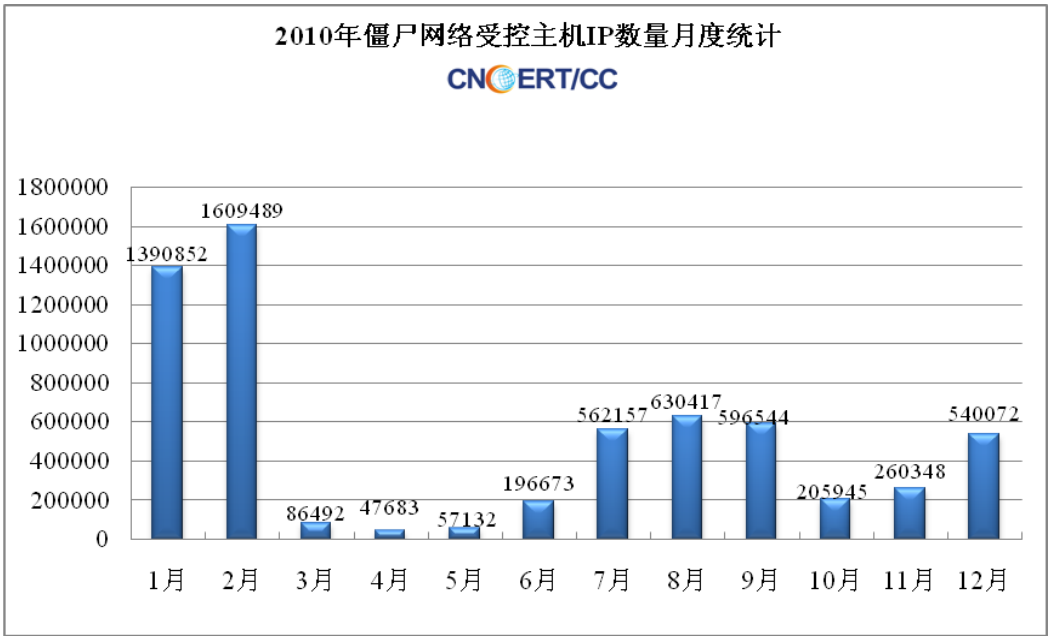

图 2-18　2010 年僵尸网络受控主机 IP 数量月度统计

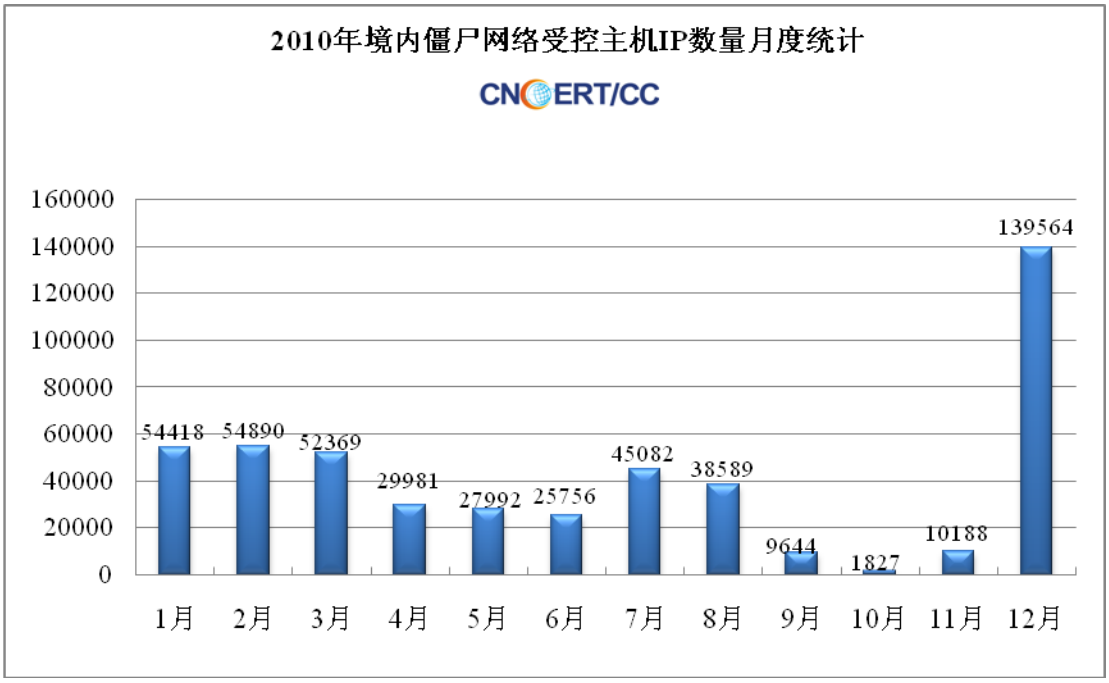

图 2-19　2010 年境内僵尸网络受控主机 IP 数量月度统计

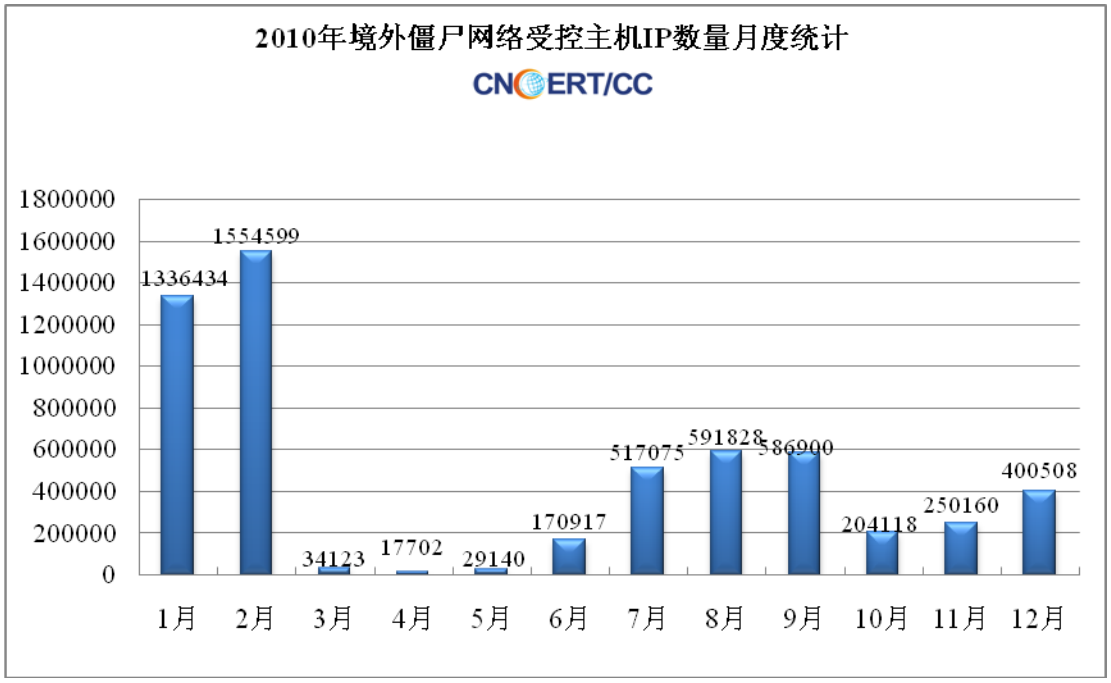

图 2-20　2010 年境外僵尸网络受控主机 IP 数量月度统计

境内僵尸网络受控主机 IP 绝对数量和相对数量（即各地区僵尸网络受控主机 IP 绝对数量占其活跃 IP 数量的比例）前 10 位地区分布如图 2-21 所示，其中：广东省、浙江省、上海市居于僵尸网络受控主机 IP 绝对数量前 3 位，黑龙江省、陕西省、江西省居于僵尸网络受控主机 IP 相对数量前 3 位。这与境内木马受控主机分布情况类似，东部沿海地区僵尸网络受控主机 IP 绝对数量较多，而中西部地区僵尸网络受控主机 IP 占该地区活跃 IP 数量的比例则较高。

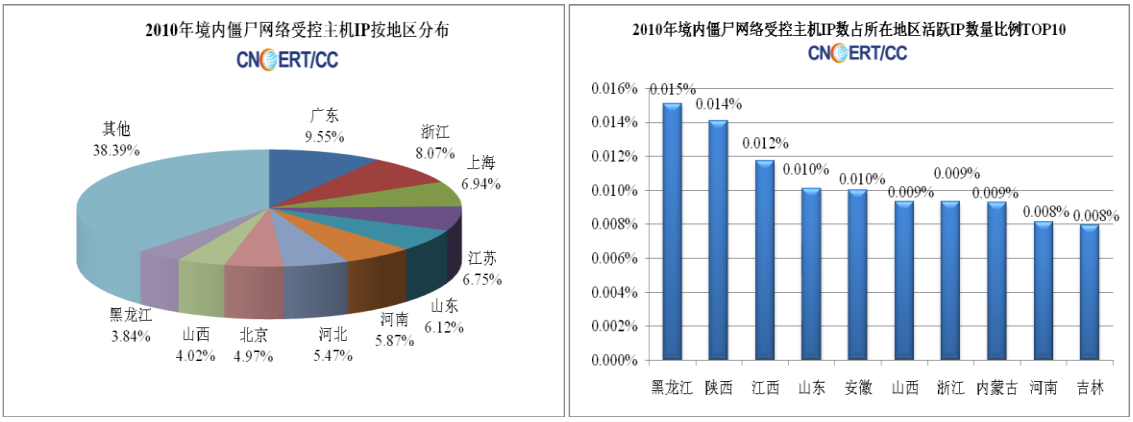

图 2-21　2010 年境内僵尸网络受控主机 IP 按地区分布

图 2-22 所示为 2010 年境内僵尸网络受控主机 IP 数量按运营商分布及所占比例，中国电信网内感染僵尸程序的受控主机 IP 绝对数量最多，中国联通网内感染僵尸程序的受控主机 IP 相对数量（即各运营商网内僵尸网络受控主机 IP 绝对数量占其活跃 IP 数量的比例）最多。与木马受控主机情况类似，在国家互联

网应急中心协调运营商处置的僵尸网络受控主机中也有相当一部分主机 IP 属于动态 IP 地址或是虚拟主机地址。木马和僵尸程序都是黑客用来控制用户主机的最为常见的手段，也是当前对互联网运行安全最为严重的威胁之一，木马和僵尸网络受控主机（包括一些 IDC 主机）已成为黑客构建大规模网络攻击平台的主要资源。

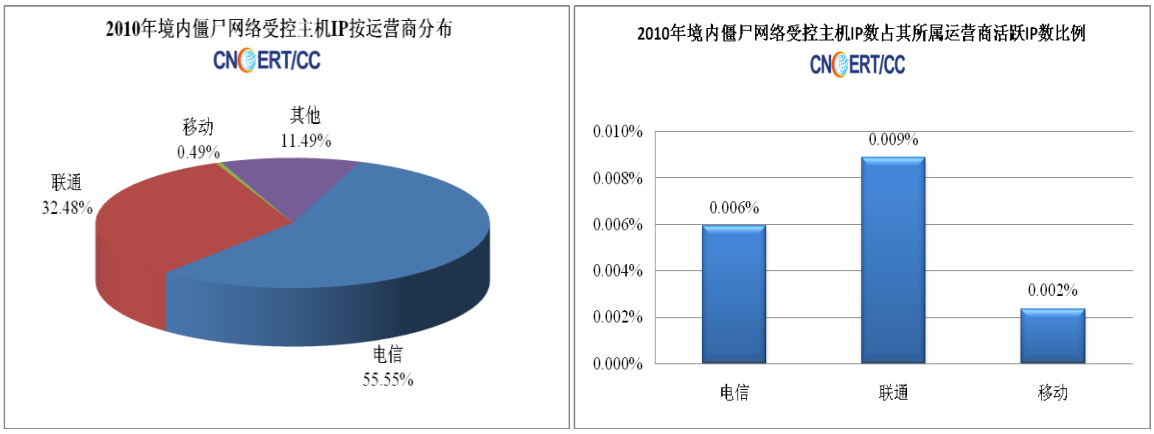

图 2-22　2010 年境内僵尸网络受控主机 IP 按运营商分布

境外僵尸网络受控主机 IP 数量前 10 位按国家和地区分布如图 2-23 所示，其中：美国、印度、泰国居于僵尸网络受控主机 IP 数量前 3 位。

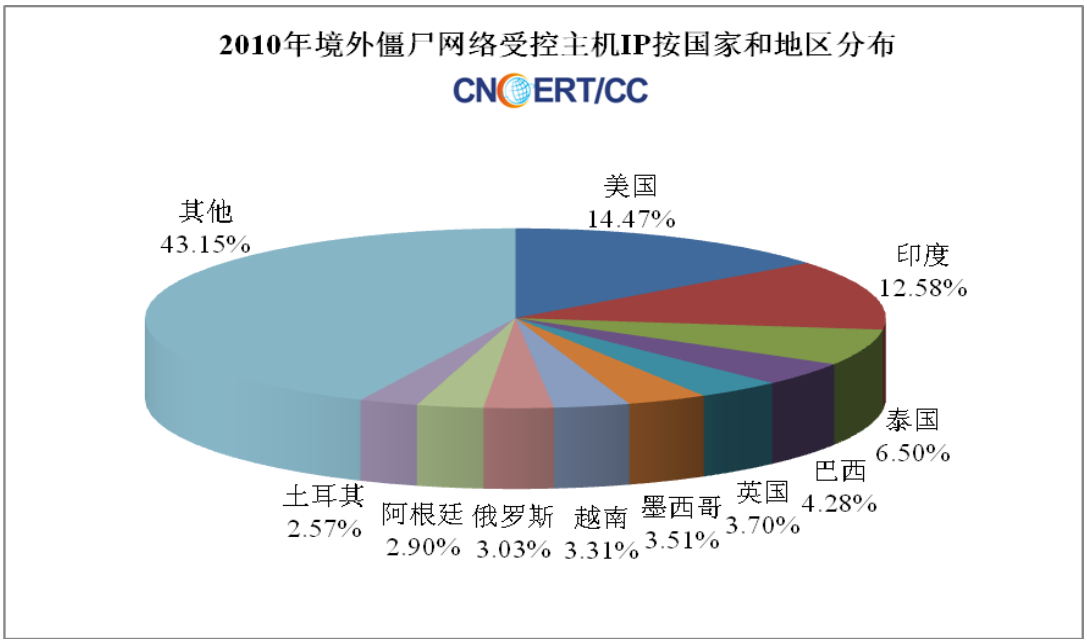

图 2-23　2010 年境外僵尸网络受控主机 IP 按国家和地区分布

2.3“飞客”蠕虫数据分析

当前黑客地下产业中，以盗号木马、窃密木马、网银木马等为代表的木马类恶意代码比较流行，与之相比，蠕虫这种能造成大范围快速传播和影响的恶意代码显得较为“古典”。自 2008 年底开始出现，持续泛滥两年的“飞客”蠕虫(Conficker) 重新引起了人们对这种古老而传统的恶意代码的关注。2010 年，“飞客”蠕虫仍然在快速传播，依旧对计算机用户产生重大的安全威胁。

与“冲击波”蠕虫类似，“飞客”蠕虫利用的也是 Windows 操作系统的 RPC 远程连接调用服务存在的高危漏洞来侵入互联网上未能进行有效防护的主机，并通过局域网、U 盘等方式快速传播。但相比以往出现的蠕虫，“飞客”蠕虫的自我保护机制大大增强，其体现出来的对抗性也是前所未有的。因此，它带来的对互联网资源的滥用以及对网络信息系统的危害性也更为严重。

“飞客“蠕虫的制造者和传播者增加了特定的安全对抗机制，防止被监测和进一步处置，其所用的传播和复制方式呈现多样化和复杂化趋势，例如它所采用的 P2P 传播机制极大地提升了“飞客”蠕虫的传染性。

2010 年的“飞客”蠕虫继续呈现“模范”蠕虫的“温柔”一面，在控制互联网主机资源过程中继续采取稳健“布局”方式，并未发动大规模网络攻击。根据 CNCERT 的 2010 年 12 月抽样监测结果，全球互联网已经有超过 6000 万个主机 IP 感染“飞客”蠕虫，境内仍然是“重灾区”，有超过 900 万个主机 IP 被感染。其中，感染“飞客”蠕虫变种 B 的主机 IP 新增数量远远超过感染变种 C 的主机 IP 新增数量。2010 年 12 月 CNCERT 监测到的全球互联网以及境内主机感染飞客蠕虫 B 变种和 C 变种的地区分布情况分别如图 2-24、图 2-25、图 2-26、图 2-27 所示。

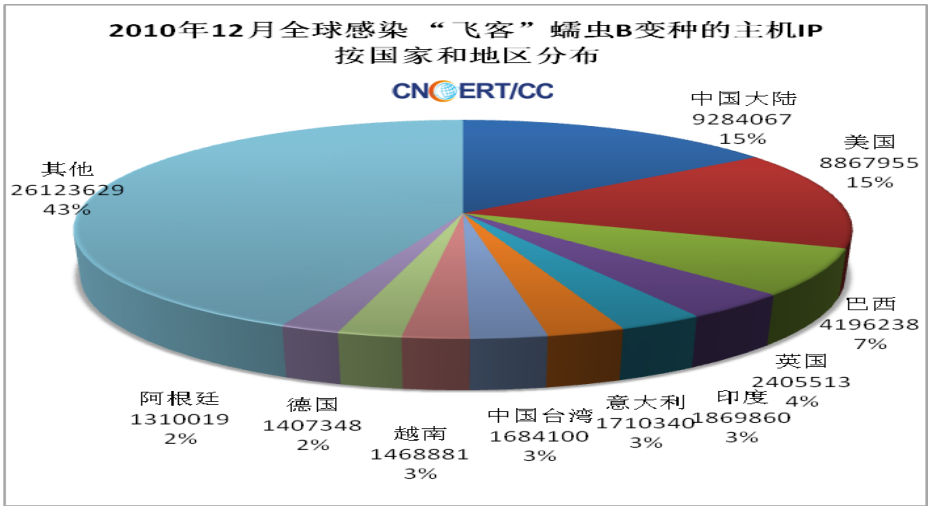

图 2-24　2010 年 12 月全球互联网感染“飞客”蠕虫 B 变种的主机 IP 按国家和地区分布

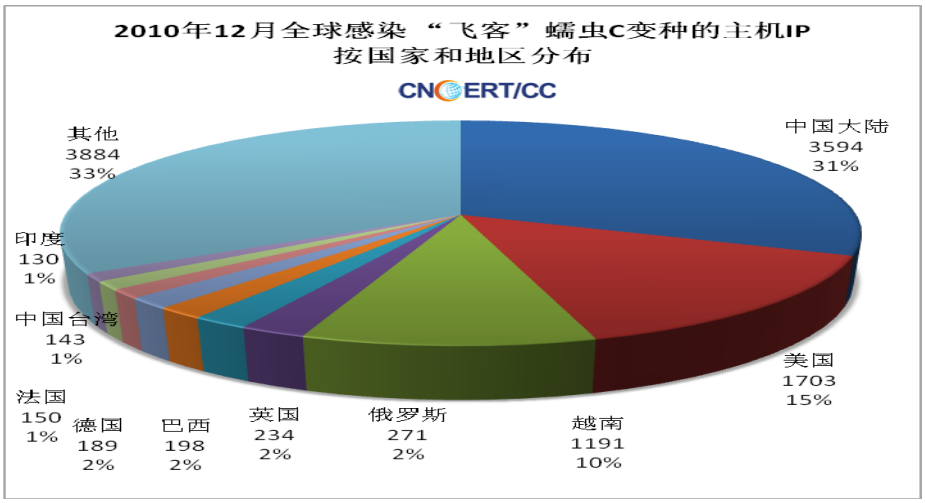

图 2-25　2010 年 12 月全球互联网感染“飞客”蠕虫 C 变种的主机 IP 按国家和地区分布

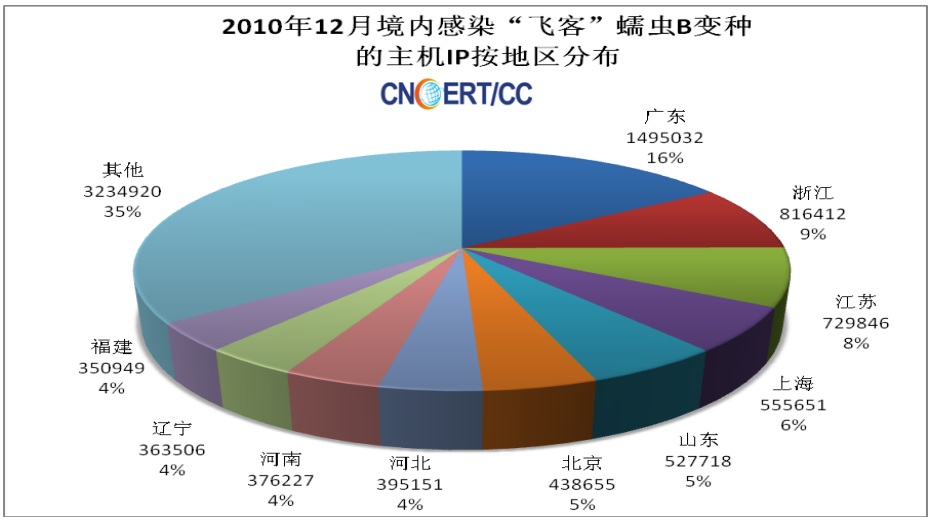

图 2-26　2010 年 12 月境内感染“飞客”B 变种的主机 IP 按地区分布

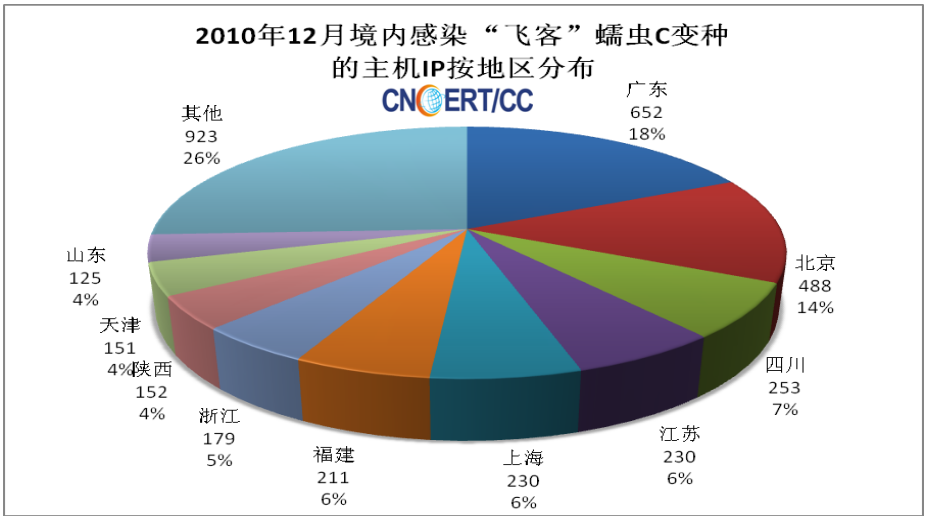

图 2-27　2010 年 12 月境内感染“飞客”C 变种的主机 IP 按地区分布

2.4 通报成员单位报送情况

■ 安天公司[2]恶意代码捕获情况

根据安天公司监测结果，2010 年共捕获恶意代码样本数量为 958 万余个，较 2009 年的 664 万[3]个增长 48%，2006 年至 2010 年捕获恶意代码数量走势如图 2-28 所示。

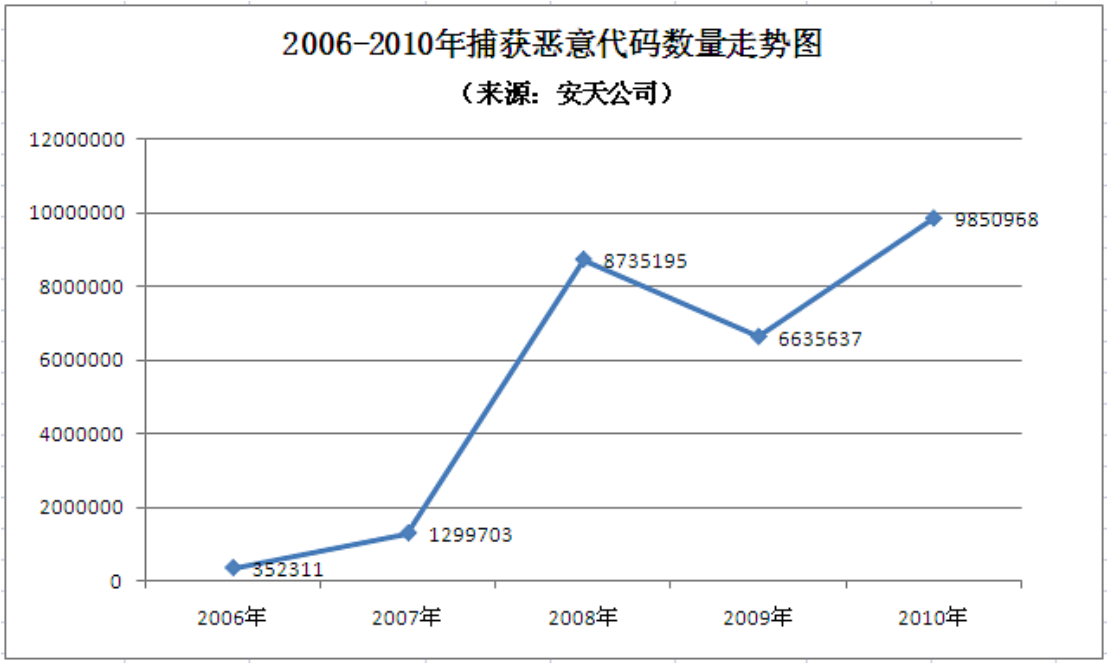

图 2-28　2006-2010 年捕获恶意代码数量走势图(来源：安天公司)

2010 年全年捕获恶意代码数量趋势呈现波浪形变化，如图 2-29 所示，其中 2 月达到全年最低值（近 45.2 万个），12 月大幅上升，达到全年最高值（近 169 万个）。

[2] 安天公司即哈尔滨安天信息技术有限公司，是通信行业互联网网络安全信息通报工作单位，同时也是 CNCERT 国家级应急服务支撑单位。

[3]安天公司对恶意代码使用了新的数据统计方式，导致当前统计的数据与以往公布的数据有所不同。

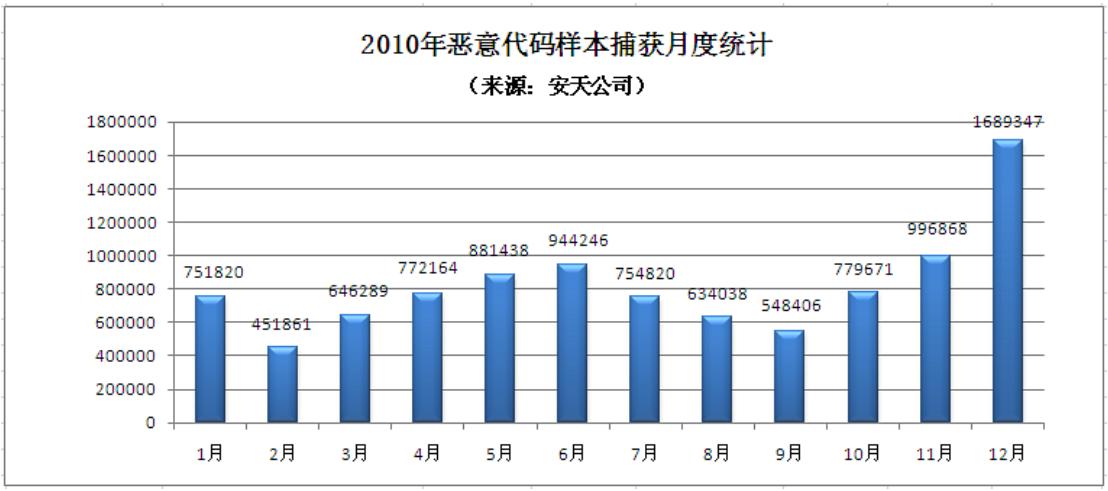

图 2-29　2010 年恶意代码样本捕获月度统计(来源：安天公司)

安天公司将捕获的恶意代码类型分为 6 大类，分别是木马、后门、蠕虫、病毒、恶意插件和黑客工具，每类恶意代码捕获数量月度统计如图 2-30 所示。其中 ,木马是对全年捕获恶意代码数量趋势影响最大的一类 ,这也是当前最为流行、黑客利用最充分的恶意代码类型 ,全年捕获木马数量共 666.5 万余个。根据 2009 年和 2010 年监测结果对比，在捕获的各类恶意代码中，绝对数量增长最多的是木马 ,下降的是病毒 ,且下降了 29.4%。各类恶意代码数量增幅位居前三位的是：黑客工具、恶意插件和木马，增幅分别为：167.7%、126.1%和 66.5%，如图 2-31 所示。

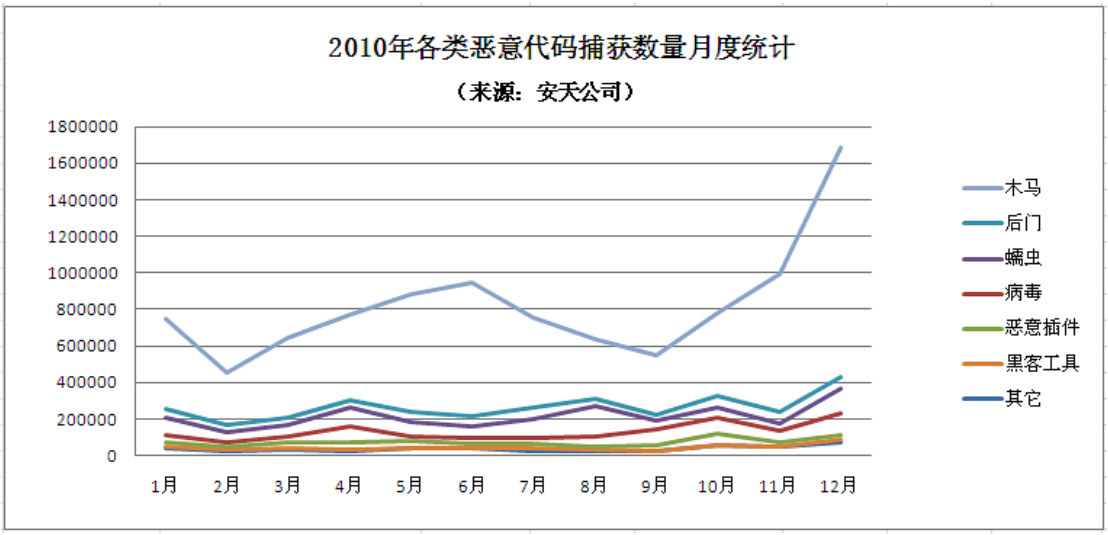

图 2-30　2010 年各类恶意代码捕获数量月度统计（来源：安天公司）

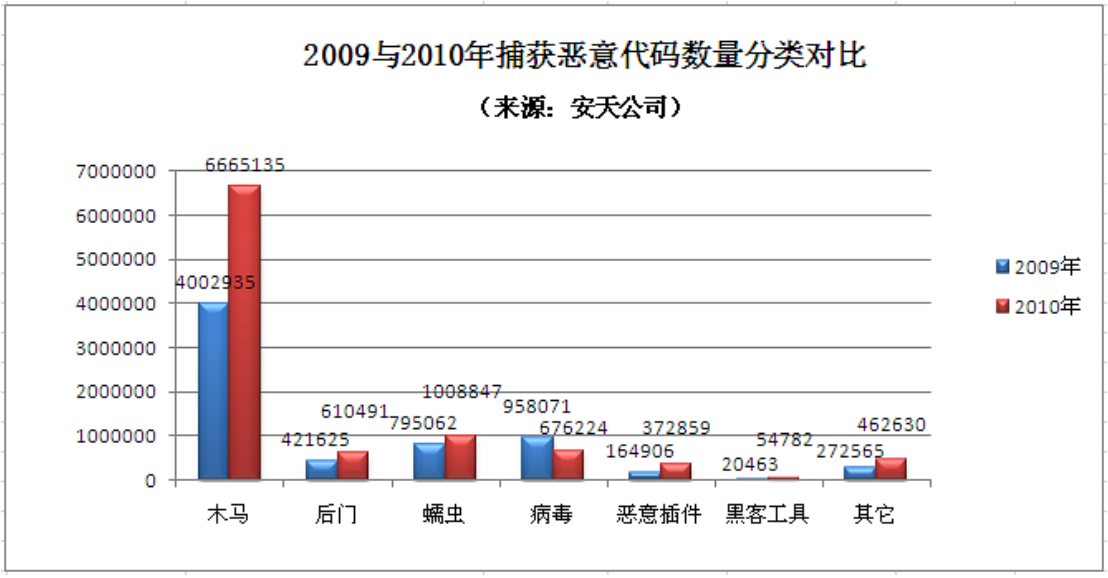

图 2-31　2009 年与 2010 年捕获恶意代码数量分类对比（来源：安天公司）

此外，从恶意代码的行为特征分析，用于窃取私密信息（Stealer）、网游盗号（GameThief）、恶意代码下载（Downloader）的恶意代码占据前三位，其数量远远高于其它用途的恶意代码，如图 2-32 所示。其中，Stealer 的数量比 2009 年增长一倍多，由 2009 年的第三位上升至第一位；GameThief 的数量下降了 46%，由 2009 年的第一位降至第二位；Downloader 的数量下降了 13%，由 2009 年的第二位降至第三位。

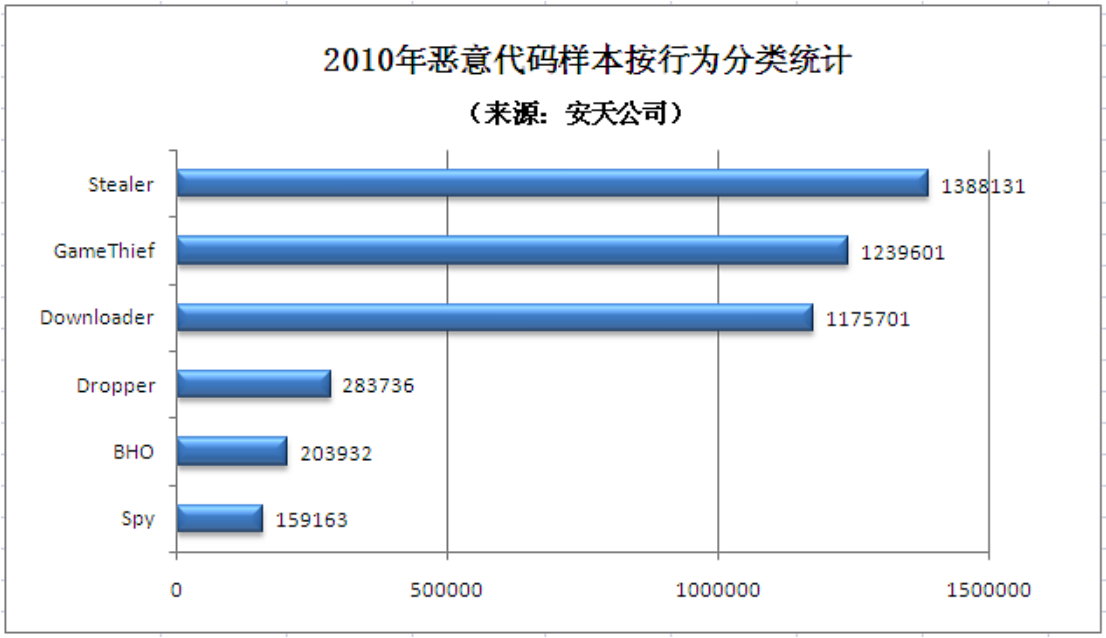

图 2-32　2010 年恶意代码样本按行为分类统计（来源：安天公司）

安天公司对恶意代码家族按捕获数量进行了统计，2010 年恶意代码家族前 10 位如表 2-1 所示。

表 2-1 2010 年恶意代码家族捕获数量 TOP10（来源：安天公司）

2010 年恶意代码家族 Top10（来源：安天公司）		
序号	家族名称	数量
1	Trojan/Win32.Kykymber	1246800
2	Trojan/Win32.OnLineGames	606301
3	Trojan/Win32.Agent	528801
4	Trojan/Win32.Lipler	427415
5	Trojan/Win32.Patched	362707
6	Trojan/Win32.Nilage	314855
7	Worm/Win32.Allaple	265082
8	Trojan/Win32.Cosmu	206260
9	Trojan/Win32.VB	193729
10	Worm/Win32.VB	186403

2010 年，恶意代码样本表现出越来越强的对抗性。恶意代码样本加壳的比例由 2009 年的 15.1%上升至 2010 年的 19.4%，如图 2-33 所示。2010 年恶意代码所使用的主要壳类型 TOP 10 列表如表 2-2 所示。

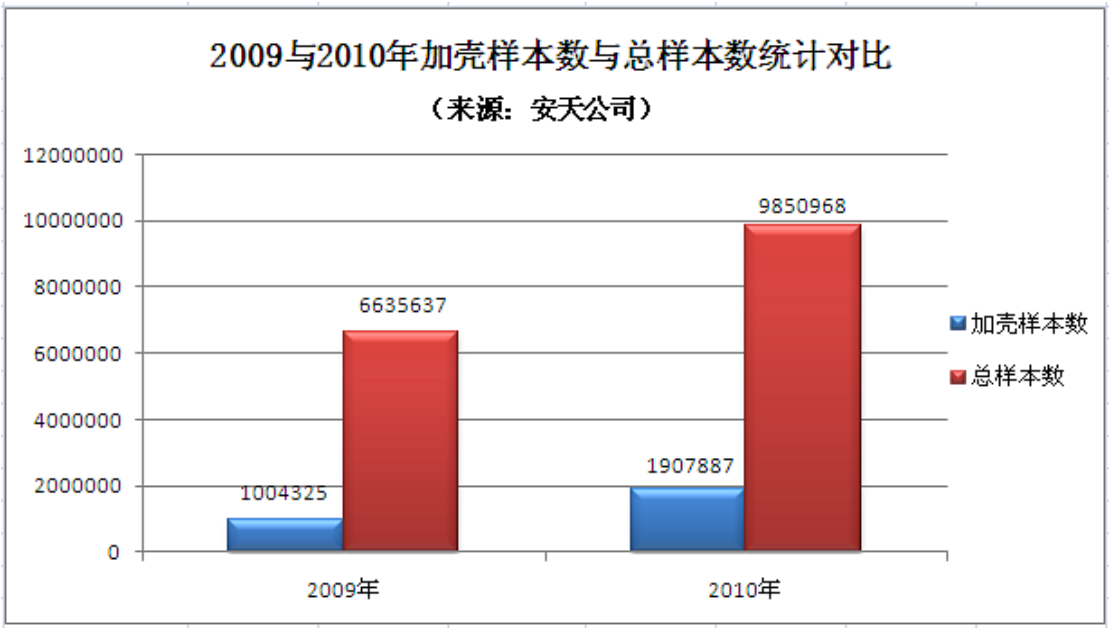

图 2-33　2009 年与 2010 年加壳样本数与总样本数统计对比（来源：安天公司）

表 2-2 2010 年恶意代码所使用的壳类型 TOP10 （来源：安天公司）

2010 年恶意代码加壳类型 Top10（来源：安天公司）		
序号	壳名称	数量
1	UPX	607559
2	MaskPE	366006
3	ASPack	339175
4	PECompact	162657
5	Petite	75980

6	NSPack	32114
7	UPack	28309
8	PecBundle	16565
9	FSG	11808
10	TeLock	6503

■ 瑞星公司[4]报送的恶意代码情况

根据瑞星公司的监测结果，2010 年全年捕获恶意代码样本总量为 11836325 个，比 2009 年的 12382547 个下降 4.41%。2010 年各月捕获数量如图 2-34 所示，其中 2 月达到全年最低值（496603 个），12 月达到全年最高值（1697269 个）。

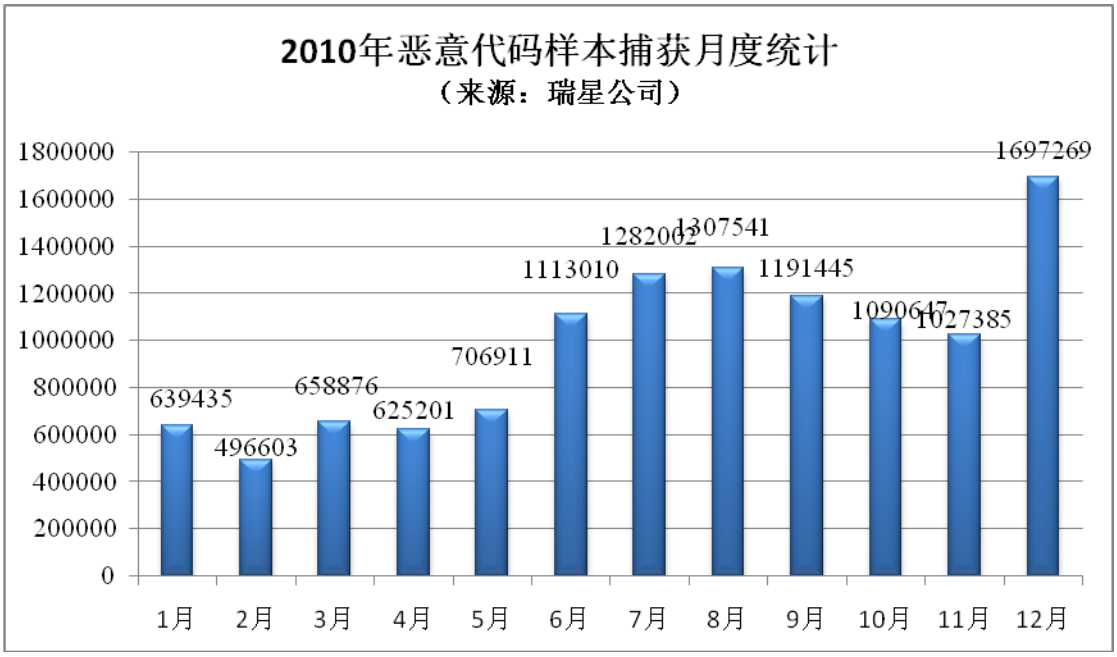

图 2-34　2010 年恶意代码样本捕获月度统计(来源：瑞星公司)

2010 年全年监测到感染恶意代码的主机 16088357 余台，11 月和 12 月大幅上升，其中感染主机数量 10 月为全年最低点（335435 台），11 月达到全年最高值（8471574 台），如图 2-35 所示。

[4] 瑞星公司即北京瑞星信息技术有限公司，是通信行业互联网网络安全信息通报工作单位。

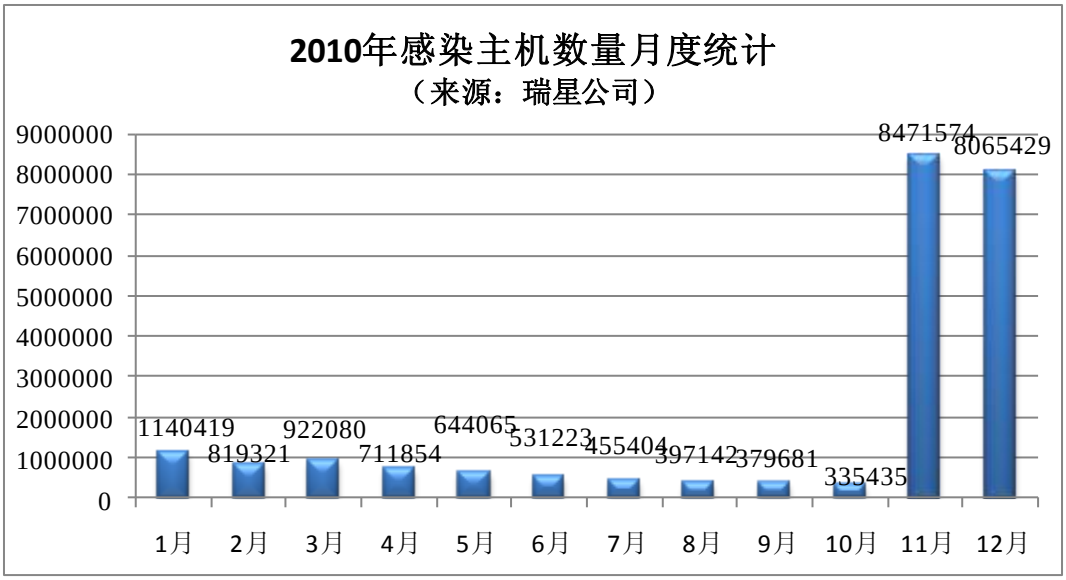

图 2-35　2010 年感染主机数量月度统计(来源：瑞星公司)

瑞星公司将捕获的恶意代码类型分为 11 大类，分别是:worm、trojan、pe、macro、joke、harm、hack、dropper、downloader、boot、backdoor，每类恶意代码捕获数量月度统计如图 2-36 所示。其中，trojan 是对全年捕获恶意代码数量趋势影响最大的一类恶意代码，全年捕获 trojan 类病毒样本数量共 10139987 余个。根据 2009 年和 2010 年监测结果对比，在捕获的各类恶意代码中，绝对数量增长最多的是 trojan，下降的是 backdoor，且下降了 78.99%。各类恶意代码数量增幅位居前三位的是：trojan、macro 和 pe，增幅分别为：69.40%、-62.05%和-63.27%，如图 2-37 所示。

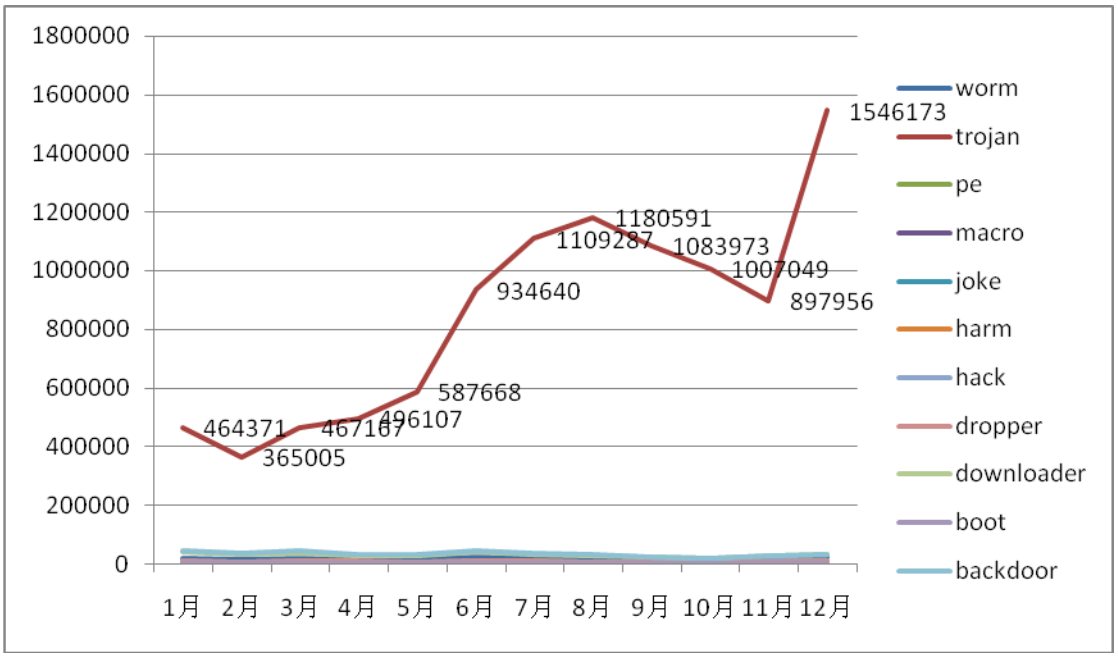

图 2-36 2010 年各类恶意代码捕获数量月度统计(来源：瑞星公司)

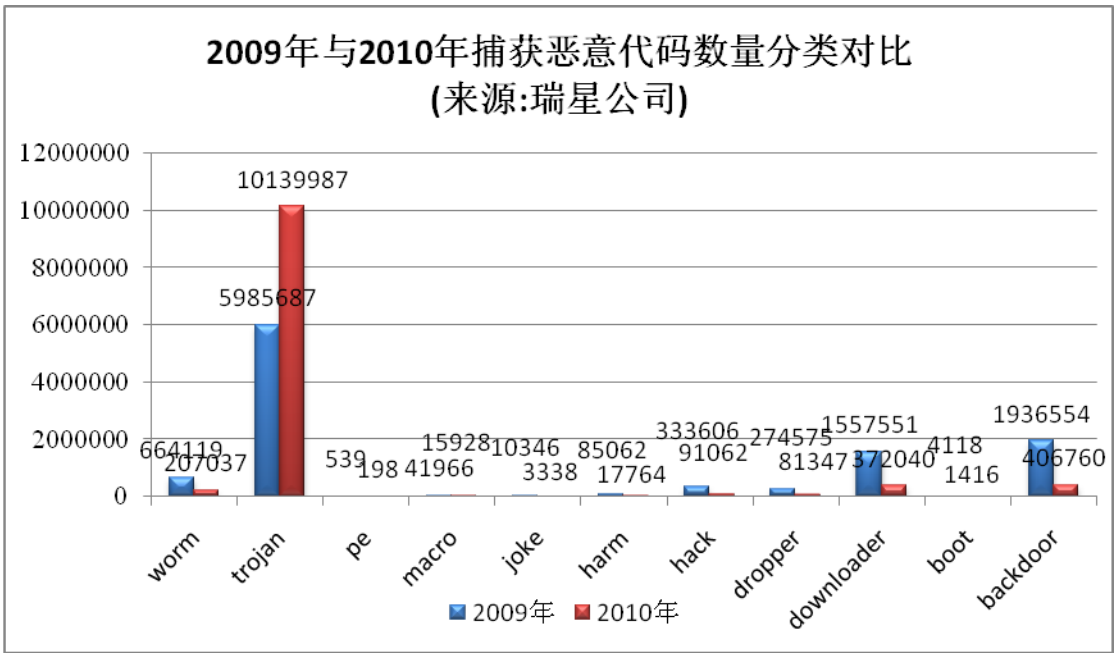

图 2-37　2009 年与 2010 年捕获恶意代码数量分类对比（来源：瑞星公司）

瑞星公司对恶意代码家族按捕获数量进行了统计，2010 年恶意代码家族前 10 位如表 2-3 所示。

表 2-3 2010 年恶意代码捕获数量 TOP10（来源：瑞星公司）

2010 年恶意代码家族 Top10（来源：瑞星公司）		
序号	家族名称	数量
1	Trojan.Win32.Generic	839257638
2	Trojan.PSW.Win32.GameOL	17432174
3	Trojan.Win32.Undef	7222360
4	Trojan.Win32.Nodef	13249633
5	Trojan.DL.Win32.Undef	6338388
6	Trojan.DL.Win32.Mnless	2895341
7	Backdoor.Win32.PcClient	1533949
8	Trojan.Win32.StartPage	25110017
9	Backdoor.Win32.Undef	9018809
10	Backdoor.Win32.Gpigeon2008	366712

2010 年，恶意代码样本加壳的比例由 2009 年的 11.94%下降至 2010 年的 4.75% ,如图 2-38 所示。2010 年恶意代码所使用的主要壳类型 TOP 10 如表 2-4 所示。

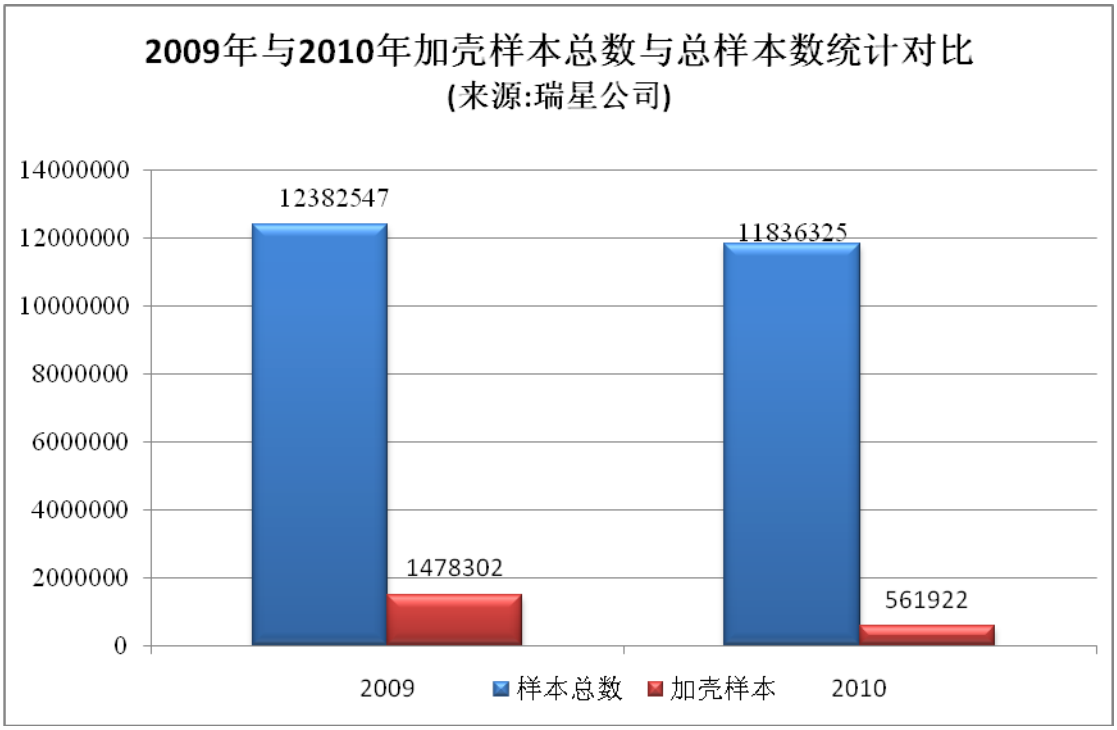

图 2-38　2009 年与 2010 年加壳样本数与总样本数统计对比（来源：瑞星公司）

表 2-4 2010 年恶意代码所使用的壳类型 TOP10 （来源：瑞星公司）

2010 年恶意代码加壳类型 Top10（来源：瑞星公司）		
序号	壳名称	数量
1	upx_c	637317
2	pecompact2x	338246
3	aspack212r	162010
4	nspack	54869
5	upack0.32	38356
6	pe_patch(23)	32980
7	fakeupx	22124
8	upack0.34	19610
9	pecompact2x-a	15061
10	fsg2.0	14692

■ 金山网络公司[5]报送的恶意代码情况

根据金山网络公司监测结果，2010 年全年捕获恶意代码样本约 5100 万次，比 2009 年的 7600 万次下降 32%。2010 年各月捕获恶意代码样本去重后的数量如图 2-39 所示，其中 10 月达到全年最低值（近 2.2 万个），3 月达到全年最高值（18.3 万余个）。

[5] 金山网络公司即金山网络科技有限公司，是通信行业互联网网络安全信息通报工作单位。

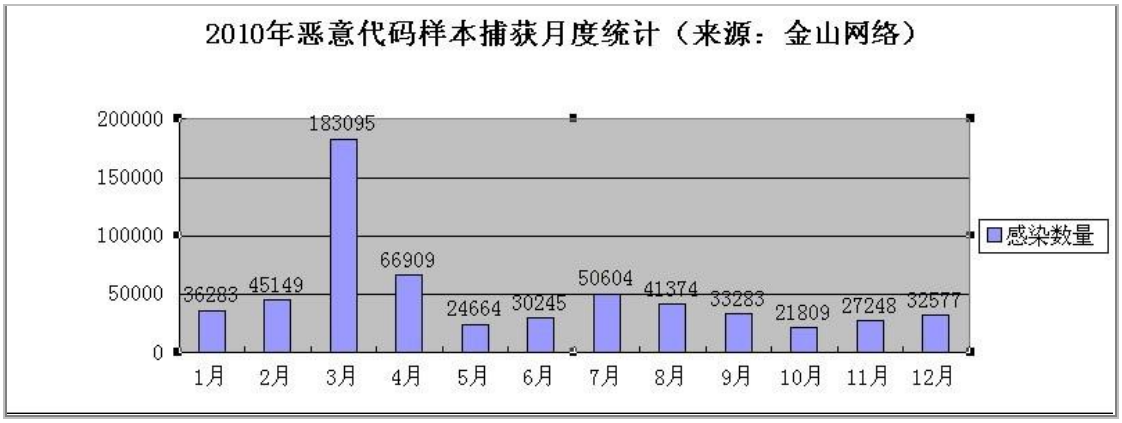

图 2-39　2010 年恶意代码样本捕获月度统计（来源：金山网络)

2010 年全年监测到感染恶意代码的主机近 7349 万台，比 2009 年的 8000 万台下降 8.8%。感染恶意代码的主机数量的趋势为：整体状况良好，其中感染主机数量 12 月为全年最低点 38.8 万余台，3 月达到全年最高值近 674.1 万台，如图 2-40 所示。

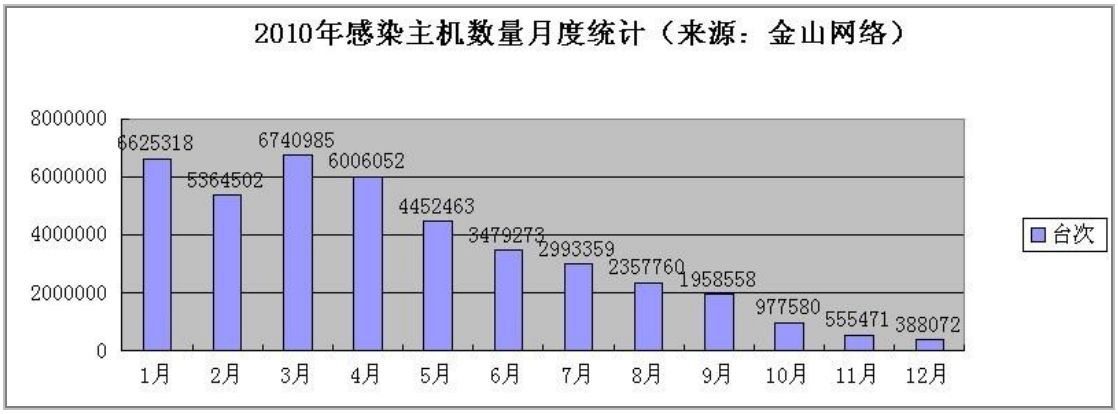

图 2-40　2010 年感染主机数量月度统计（来源：金山网络)

金山网络公司对恶意代码家族按捕获数量进行了统计，2010 年恶意代码家族前 10 位如表 2-5 所示。

表 2-5 2010 年恶意代码家族捕获数量 TOP10（来源：金山网络）

序号	家族名称
1	“极虎”病毒
2	“杀破网”病毒
3	“女人必看”类 qq 盗号木马
4	“鬼影”病毒
5	浏览器主页篡改病毒
6	牛皮癣病毒
7	数字大盗病毒
8	“伴随者”木马
9	″暴风 1 号″病毒
10	″震网″病毒

■ 奇虎 360 公司[6]报送的恶意代码情况

根据奇虎 360 公司的监测结果，2010 年全年捕获恶意代码样本总量为 56265 万个，比 2009 年的 4526 万个增长 1082.86%。2010 年各月捕获数量如图 2-41 所示，其中 2 月达到全年最低值（752 万个），11 月达到全年最高值（9785 万个）。

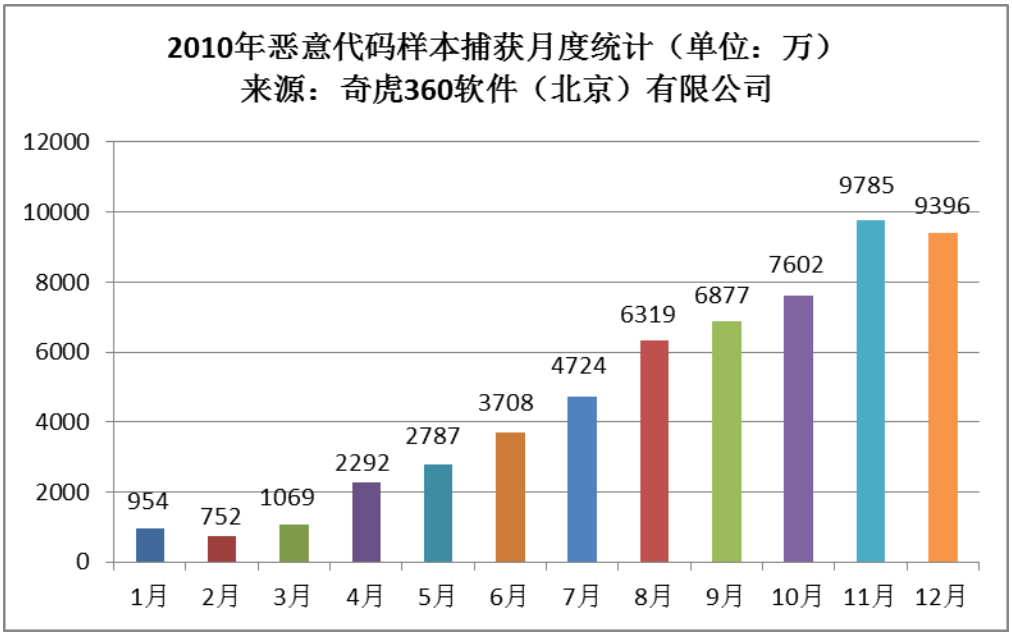

图 2-41　2010 年恶意代码样本捕获月度统计(来源：奇虎 360 公司)

2010 年全年监测到感染恶意代码的主机 210384 万余台，感染恶意代码的主机数量的趋势为上半年较为平缓而下半年增长明显，其中感染主机数量 1 月为全年最低点（2379 万个），10 月达到全年最高值（49557 万个），如图 2-42 所示。

[6] 奇虎 360 公司即奇虎 360 软件（北京）有限公司，是通信行业互联网网络安全信息通报工作单位，同时也是 CNCERT 国家级应急服务支撑单位

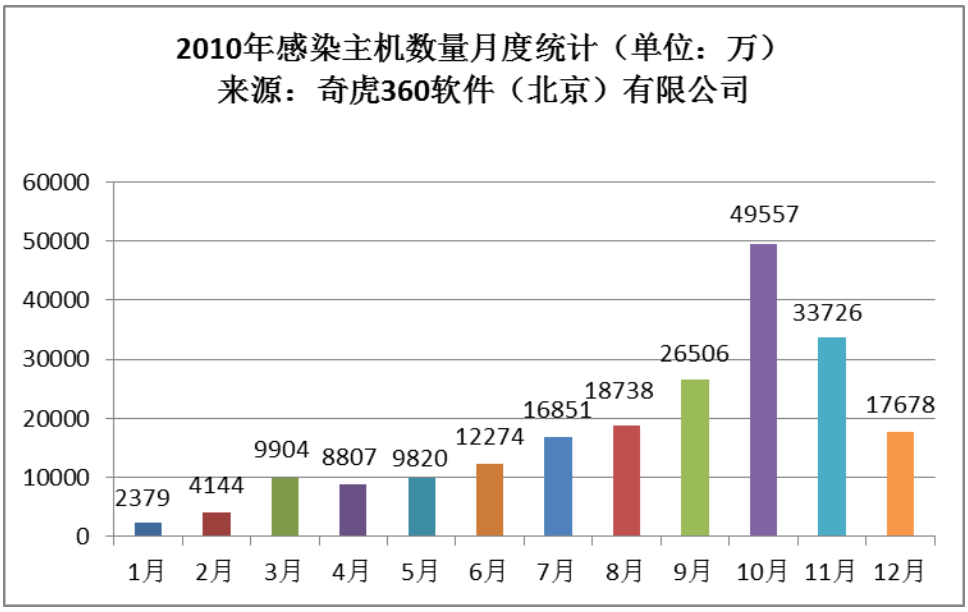

图 2-42　2010 年感染主机数量月度统计(来源：奇虎 360 公司)

2.5 国际渠道交换获得恶意代码样本情况

2010 年，CNCERT 通过国际合作渠道接收到境内感染恶意代码的主机数量为 83.1 万余个，日均 2279 个，与 2009 年相比变化不大，下半年境内感染恶意代码的主机情况有所好转，月度统计如图 2-43 所示。境内感染恶意代码的主机按地区分布如图 2-44 所示，其中广东省、浙江省和江苏省分列前 3 位。

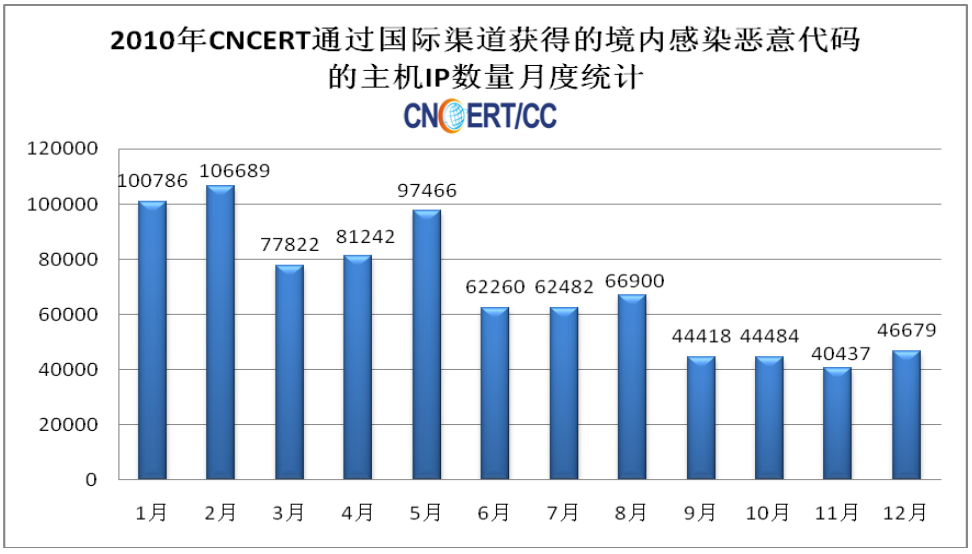

图 2-43　2010 年通过国际渠道获得的境内感染恶意代码的主机 IP 数量月度统计

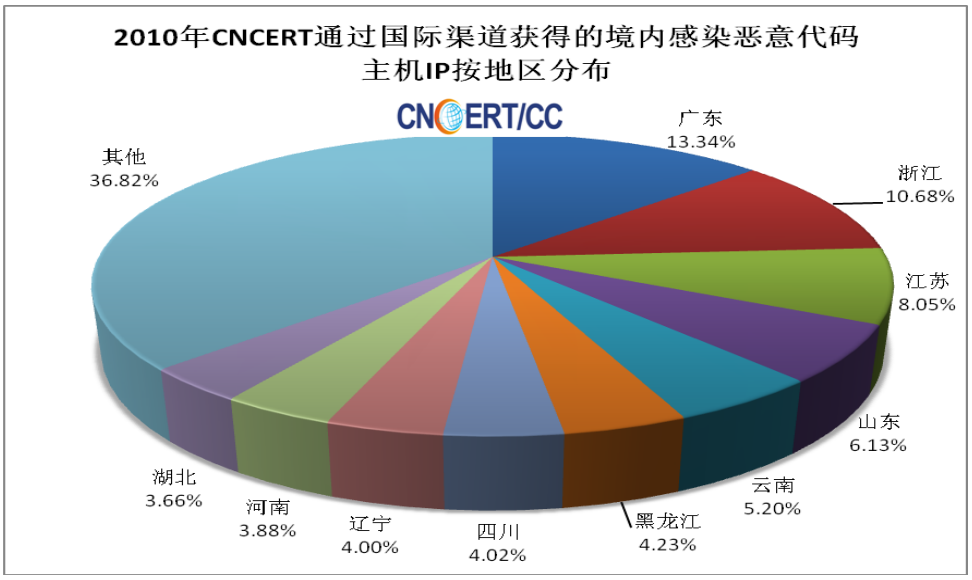

图 2-44　2010 年通过国际渠道获得的境内感染恶意代码的主机 IP 数量按地区分布