2 计算机恶意程序传播和活动情况

恶意程序主要包括计算机病毒、蠕虫、木马、僵尸程序等。几年前计算机病毒和蠕虫是最为常见的恶意程序类型，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程序成为了黑客最常利用的手段，也成为了用户安全防范的主要对象。通过对恶意程序的捕获和分析，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。

2.1 木马僵尸监测数据分析

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程序。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。

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来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。随着恶意程序的发展，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。

2011 年 CNCERT 抽样监测结果显示，在利用木马或僵尸程序控制服务器对主机进行控制的事件中，控制服务器 IP 总数为 300407 个，较 2010 年下降 39.1%，受控主机 IP 总数为 27275399 个，较 2010 年大幅增长 71.1%。

■ 木马或僵尸程序控制服务器分析

2011 年，境内木马或僵尸程序控制服务器 IP 数量为 253684 个，境外木马或僵尸程序控制服务器 IP 数量为 46723 个，较 2010 年均有所下降，降幅分别为 4.6%和 79.5%，具体如图 2-1 所示。

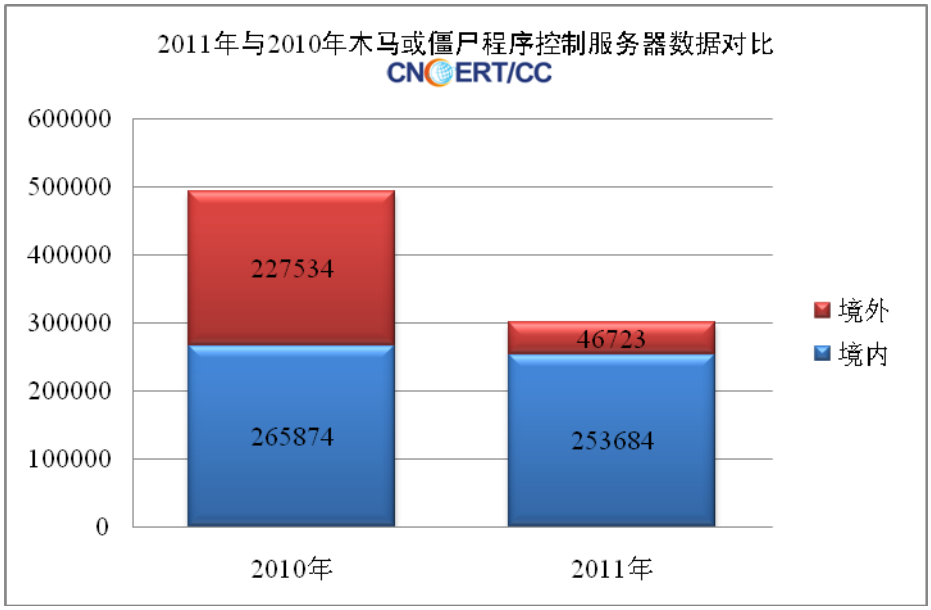


图 2-1　2011 年与 2010 年木马或僵尸程序控制服务器数据对比

2011 年, 在发现的因感染木马或僵尸程序而形成的僵尸网络[2]中, 规模在 100 至 1000 的占 80.6%以上。控制规模在 1000-5000、5000-20000、2-5 万、5-10 万及 10 万以上的主机 IP 地址的僵尸网络数量与 2010 年相比分别增加了 1386、355、90、23 和 30 个，分布情况如图 2-2 所示。

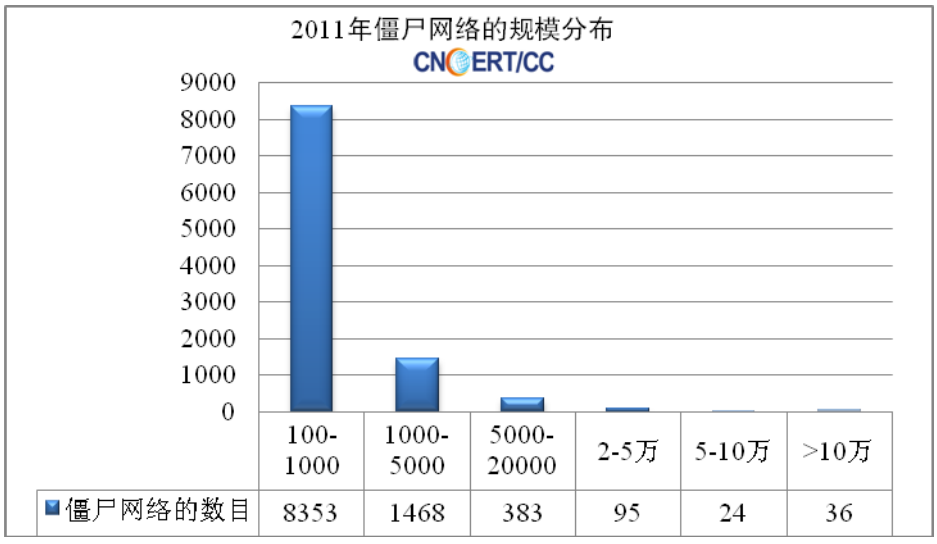


图 2-2　2011 年僵尸网络规模分布

2011 年木马或僵尸程序控制服务器 IP 数量的月度统计分别如图 2-3 所示。全年呈波动态势，12 月达到最高值 39167 个，2 月为最低值 21637 个。

[2] 统计的是受控主机 IP 数量在 100 个以上的僵尸网络。

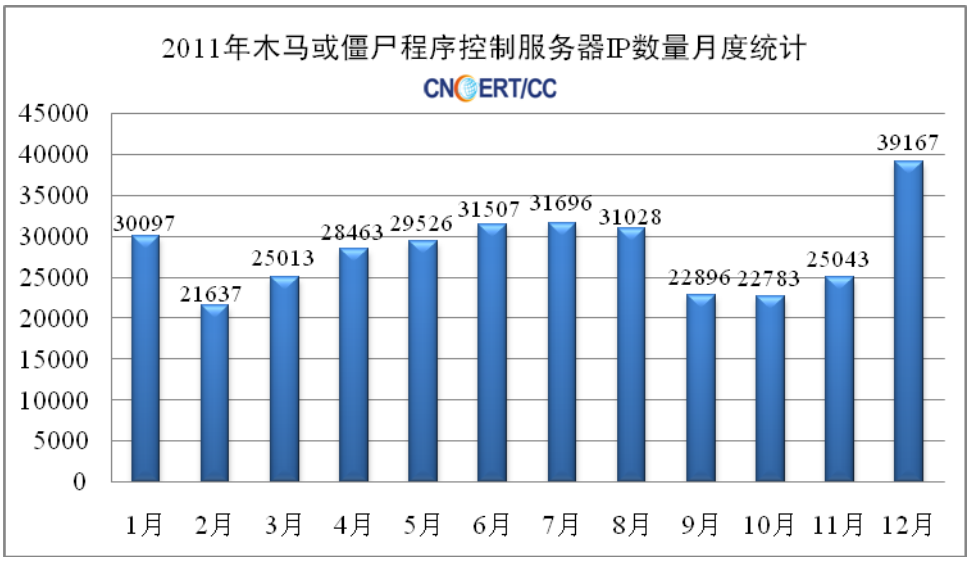


图 2-3　2011 年木马或僵尸程序控制服务器 IP 数量月度统计

境内木马或僵尸程序控制服务器 IP 绝对数量和相对数量（即各地区木马或僵尸程序控制服务器 IP 绝对数量占其活跃 IP 数量的比例）前 10 位地区分布如图 2-4 所示，其中：广东省、江苏省、浙江省居于木马或僵尸程序控制服务器 IP 绝对数量前 3 位，云南省、新疆维吾尔自治区、海南省居于木马或僵尸程序控制服务器 IP 相对数量的前 3 位。

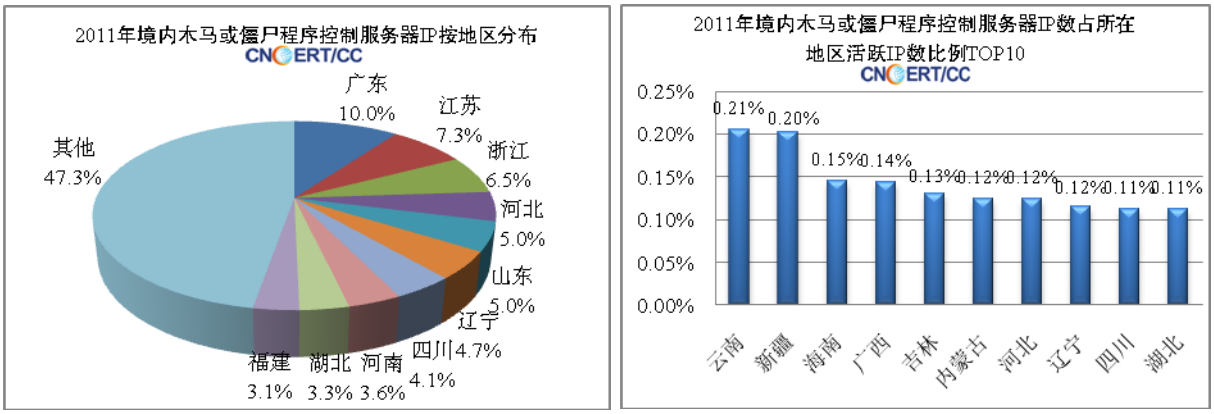


图 2-4　2011 年境内木马或僵尸程序控制服务器 IP 按地区分布

图 2-5 所示为 2011 年境内木马或僵尸程序控制服务器 IP 数量按运营商分布及所占比例，木马或僵尸程序控制服务器 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或僵尸程序控制服务器 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。

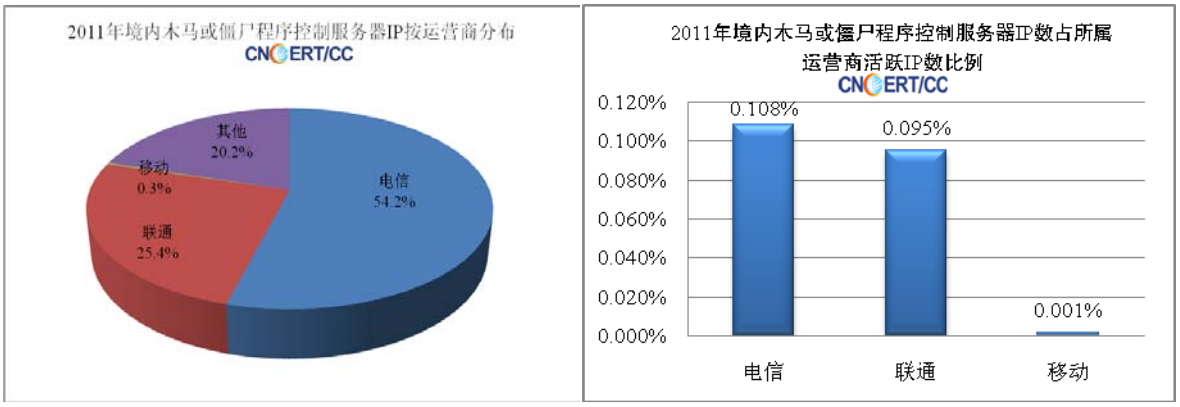


图 2-5　2011 年境内木马或僵尸程序控制服务器 IP 按运营商分布

境外木马或僵尸程序控制服务器 IP 数量前 10 位按国家和地区分布如图 2-6 所示，其中：日本、美国、韩国居于前 3 位。

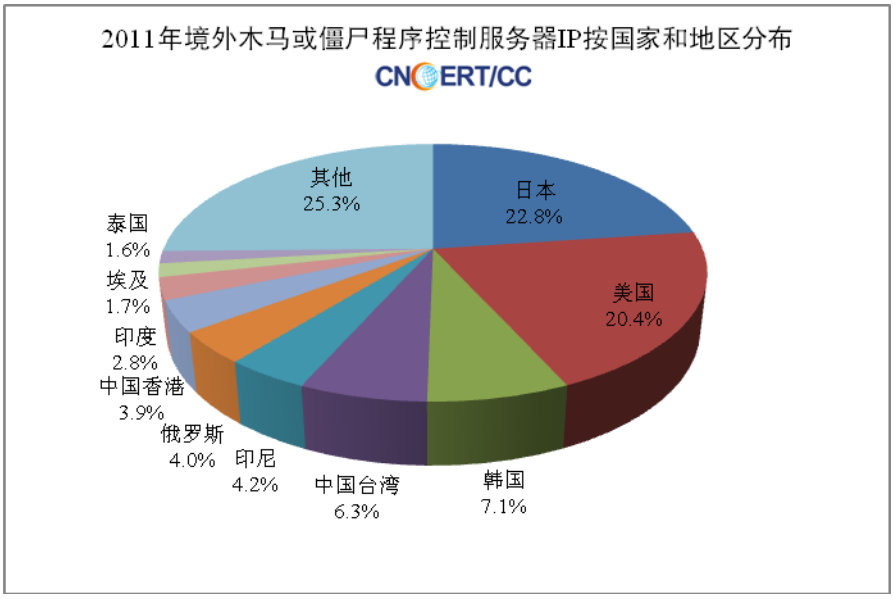


图 2-6　2011 年境外木马或僵尸程序控制服务器 IP 按国家和地区分布

■ 木马或僵尸程序受控主机分析

2011 年，境内共有 8895123 个 IP 地址的主机被植入木马或僵尸程序，境外共有 18380276 个 IP 地址的主机被植入木马或僵尸程序，数量较 2010 年均有较为明显的增长，增幅分别达到了 78.5%和 67.8%，具体如图 2-7 所示。

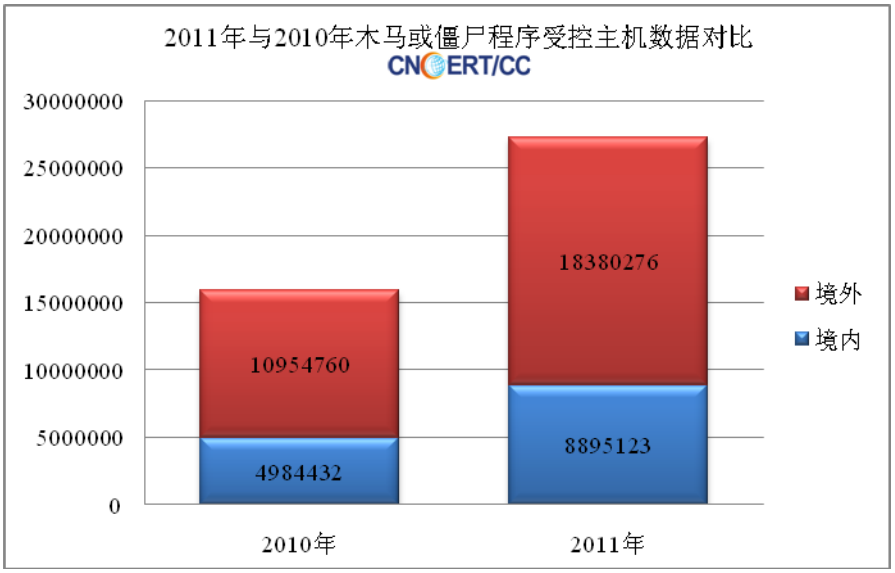


图 2-7　2011 年与 2010 年木马或僵尸程序受控主机数据对比

2011 年木马或僵尸程序受控主机 IP 数量呈现增长趋势，并在 2011 年 11 月和 12 月出现激增现象，原因是自 2011 年 11 月起，CNCERT 对木马和僵尸程序家族的监测数量增加了约 1/3。2011 年木马或僵尸程序受控主机 IP 数量的月度统计如图 2-8 所示。

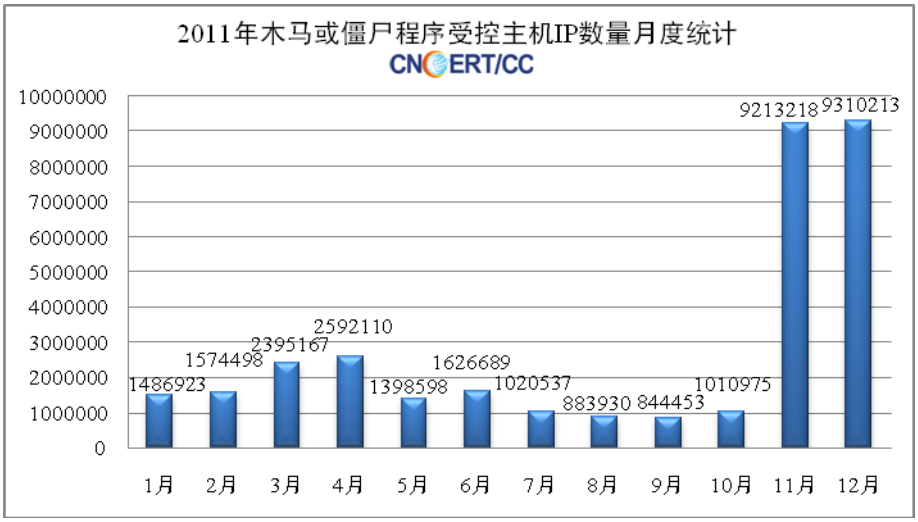


图 2-8　2011 年木马或僵尸程序受控主机 IP 数量月度统计

境内木马或僵尸程序受控主机 IP 绝对数量和相对数量（即各地区木马或僵尸程序受控主机 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、江苏省、浙江省居于木马或僵尸程序受控主机 IP 绝对数量前 3 位，新疆维吾尔自治区、黑龙江省、海南省居于木马或僵尸程序受控主机 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，使得该地区的木马或僵尸程序受控主机 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较为薄弱，导致该地区木马或僵尸程序受控主机 IP 占该地区活跃 IP 数量的比例较高。

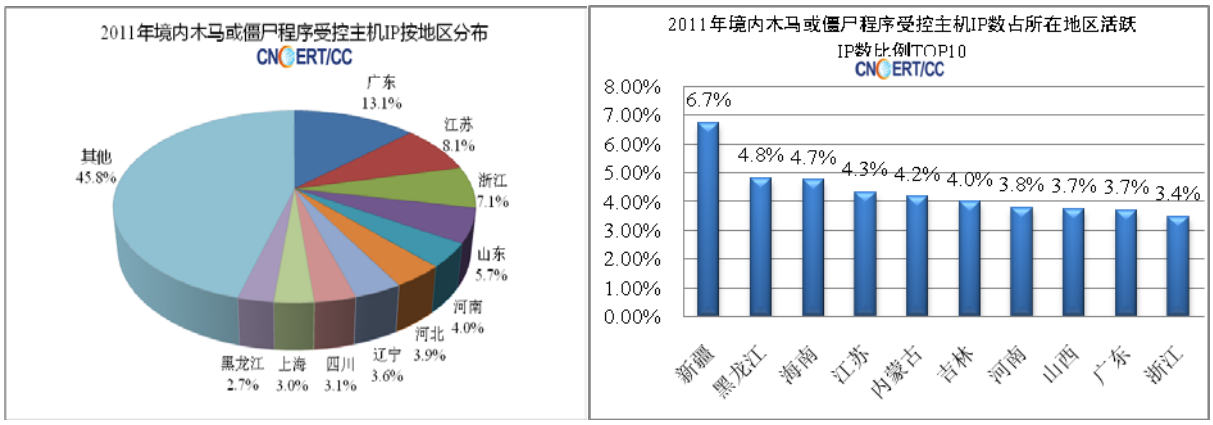


图 2-9　2011 年境内木马或僵尸程序受控主机 IP 按地区分布

图 2-10 所示为 2011 年境内木马或僵尸程序受控主机 IP 数量按运营商分布及所占比例，木马或僵尸程序受控主机 IP 无论是绝对数量，还是相对数量（即各运营商网内木马或僵尸程序受控主机 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 监测到的木马或僵尸程序受控主机 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。

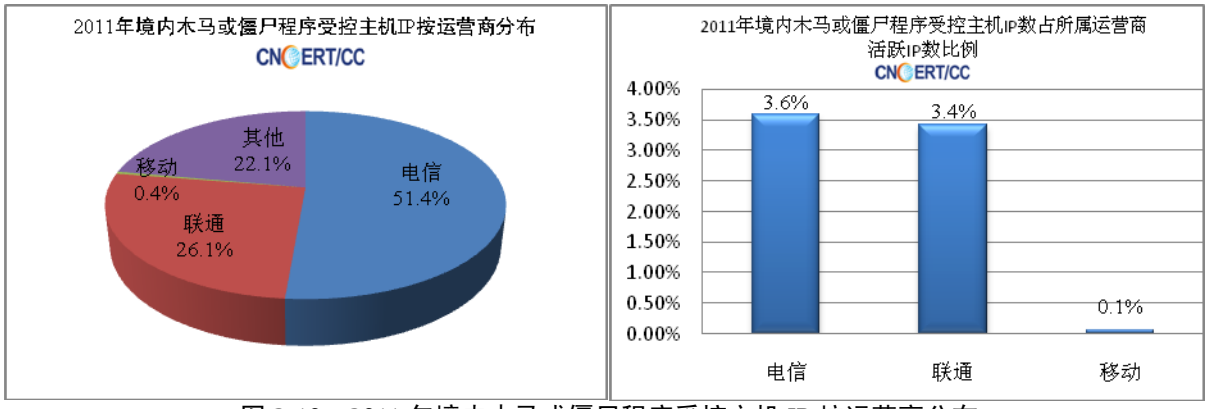


图 2-10　2011 年境内木马或僵尸程序受控主机 IP 按运营商分布

境外木马或僵尸程序受控主机 IP 数量按国家和地区分布前 10 位如图 2-11 所示，其中：印度、俄罗斯、泰国居于木马或僵尸程序受控主机 IP 数量前 3 位。

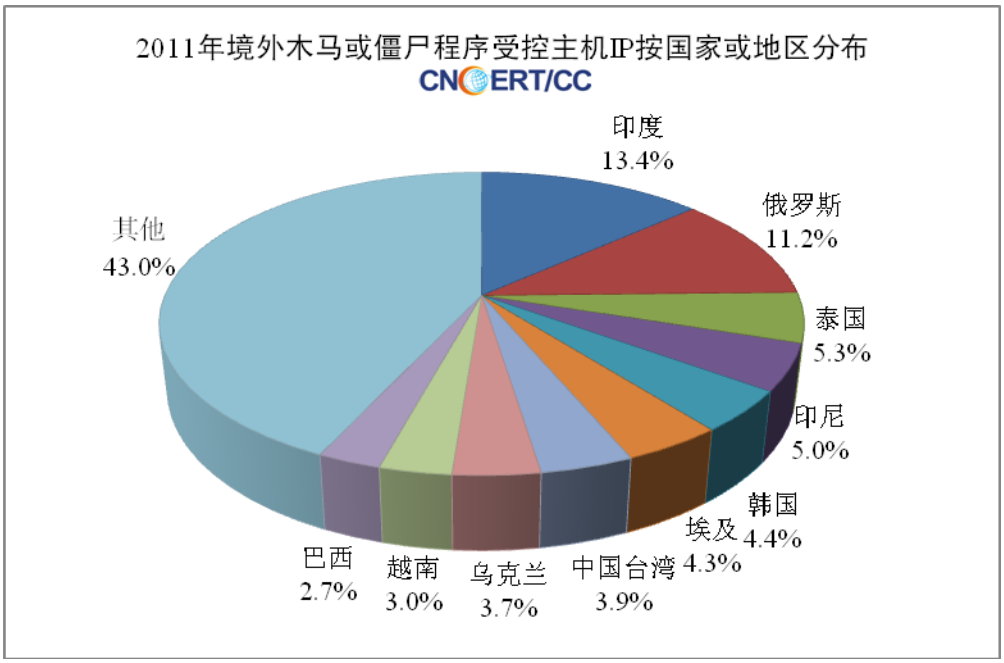


图 2-11　2011 年境外木马或僵尸程序受控主机 IP 按国家和地区分布

2.2“飞客”蠕虫数据分析

“飞客”蠕虫最早出现在 2008 年 11 月，其利用 Windows 操作系统的 RPC 远程连接调用服务存在的高危漏洞来入侵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。

与传统蠕虫相比，“飞客”蠕虫的自我保护能力大大增强，体现出前所未有的对抗性。例如，它使用了高强度的公钥加密算法对黑客发布的程序进行完整性验证；内置复杂的域名生成算法，产生数以万计的域名供黑客选择使用来实施控制及更新程序；以及采用 P2P 机制极大地提升其传播能力。

截至目前，“飞客”蠕虫已繁衍出 5 个变种（A、B、B++、C 和 E），分别出现在 2008 年 11 月 21 日、2008 年 12 月 29 日、2009 年 2 月 20 日、2009 年 3 月 4 日和 2009 年 4 月 7 日。其中，变种 E 于 2009 年 5 月 3 日自我清除，并在感染主机上保留变种 C 的恶意程序。

经过长达三年的传播，“飞客”蠕虫已经构建了一个包含数千万被控主机的攻击平台，不仅能够被用于大范围的网络欺诈和信息窃取，而且能够被利用发动无法阻挡的大规模拒绝服务攻击，甚至可能成为有力的网络战工具。截至目前，国内外安全组织尚未发现或接收到与“飞客”蠕虫有关的大规模网络攻击报告。但由于其变种 E 下载 Waledac 僵尸程序和 SpyProtect 2009 恐吓程序，而 Waledac 是用于发送垃圾邮件的大型僵尸网络，SpyProtect 2009 试图用假冒的安全警报来

欺骗用户购买一些无用的程序，因此一些安全专家推测“飞客”蠕虫可能与以盈利为目的的网络犯罪组织有某种关联。

虽然“飞客”蠕虫尚未直接被用于发动针对某一重要信息系统的大规模网络攻击，但是也有“飞客”蠕虫干扰政府和军队等重要部门正常运行的多个报道。例如：2009 年 1 月 15 日，法国海军计算机系统感染“飞客”蠕虫，随后该网络被隔离迫使几个空军基地因无法下载飞行计划而停飞；英国国防部报道，“飞客”蠕虫感染了皇家海军军舰、皇家海军潜艇、行政办公室、谢菲尔德医院等部门的 800 余台主机；2009 年 2 月 2 日，德国统一武装部队称他们有约 100 台主机被感染；2009 年 2 月，英国曼彻斯特议会 IT 系统因感染“飞客”蠕虫而中断，造成约 150 万英镑的损失；2010 年 1 月，英国曼彻斯特警方的计算机系统被感染，致使与国家警察系统中断连接三天，曼彻斯特警方对车辆和人员的例行检查不得不委托其它地区警察代为执行。

除了对互联网和重要信息系统造成威胁外，“飞客”蠕虫能够阻止用户访问与安全相关的网站，删除系统还原点，终止操作系统自身以及第三方安全软件的服务，并下载任意恶意程序文件，因此对普通的计算机用户也造成严重危害。

根据 CNCERT 监测，2011 年全球互联网月均有超过 3500 万个主机 IP 感染“飞客”蠕虫，排名前三的国家或地区分别是美国（16.1%）、中国大陆（11.6%）、和巴西（7.4%），具体分布情况如图 2-12 所示。其中，中国大陆感染的主机 IP 数量月均超过 400 万个。图 2-13 为 2011 年境内主机 IP 感染“飞客”蠕虫的数量和占全球感染数量比例的月度统计。

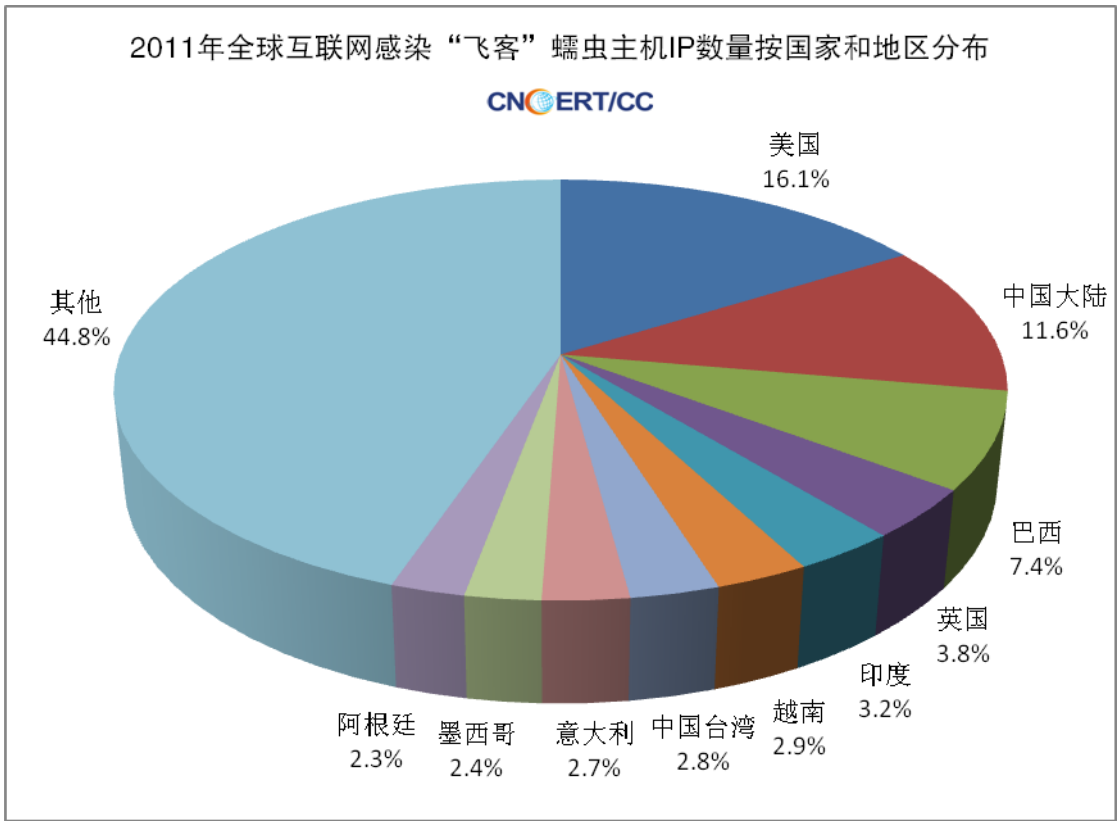


图 2-12　2011 年全球互联网感染“飞客”蠕虫的主机 IP 数量按国家和地区分布

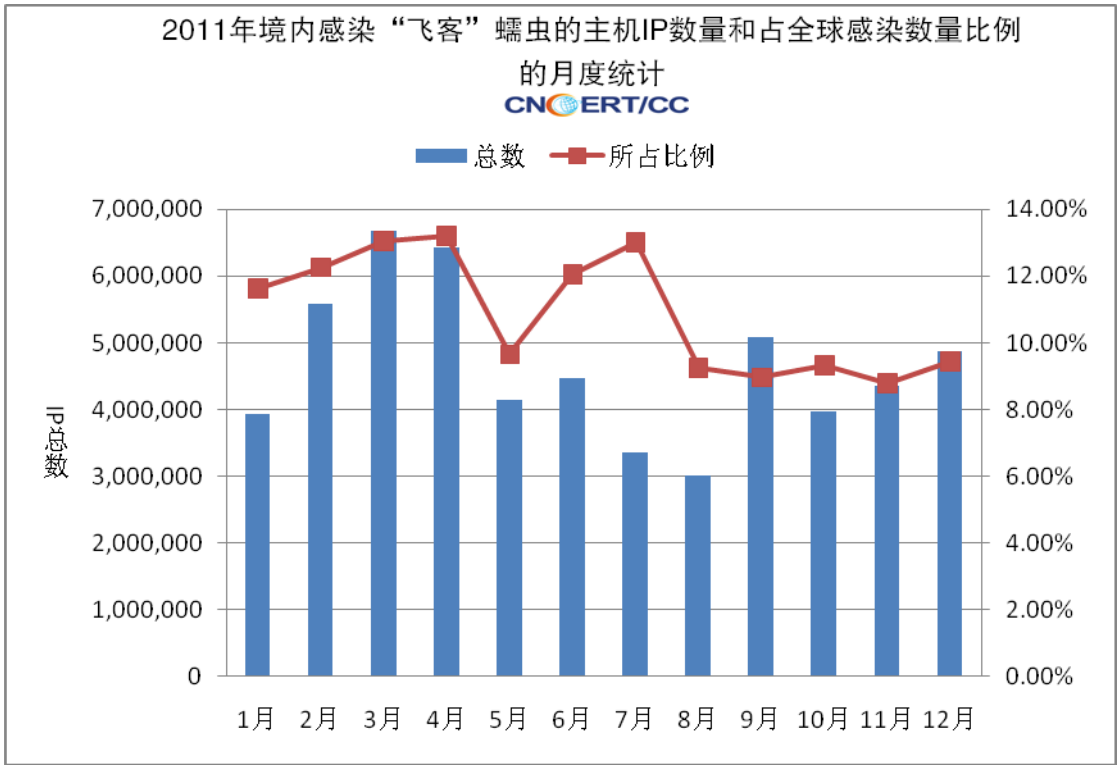


图 2-13　2011 年境内感染“飞客”蠕虫的主机 IP 数量和占全球感染数量比例的月度统计

2.3 恶意程序传播活动监测

恶意程序是攻击者开展网络攻击活动的基本工具，其主要传播方式之一是针对一些防护比较薄弱、访问量较大的网站通过网页挂马的方式进行传播。用户在浏览被挂马的页面时，如果主机程序存在安全漏洞并被成功触发，恶意脚本就会被执行，在用户不知情的条件下，跳转到攻击者存放恶意程序的网络地址（称为“放马站点”），下载并执行恶意程序。为便于大范围传播恶意程序，除少量“放马站点”直接使用 IP 地址外，攻击者通常会为“放马站点”注册域名。同时，CNCERT 还监测发现，网络下载站点、各类网盘等在线存储资源中由于对用户上传的文件缺少必要的安全检查，也会成为恶意程序的传播源，从而导致访问用户感染恶意程序。2011 年全年，CNCERT 监测发现恶意程序传播事件 35821698 次，其中恶意程序下载链接 785388 个，“放马站点”域名 67468 个，“放马站点”IP 地址 55673 个。

恶意程序传播事件的月度统计如图 2-14 所示，中间 4 月-8 月恶意程序传播活动频次相对较低，9 月后恶意程序传播事件数量维持在较高水平。

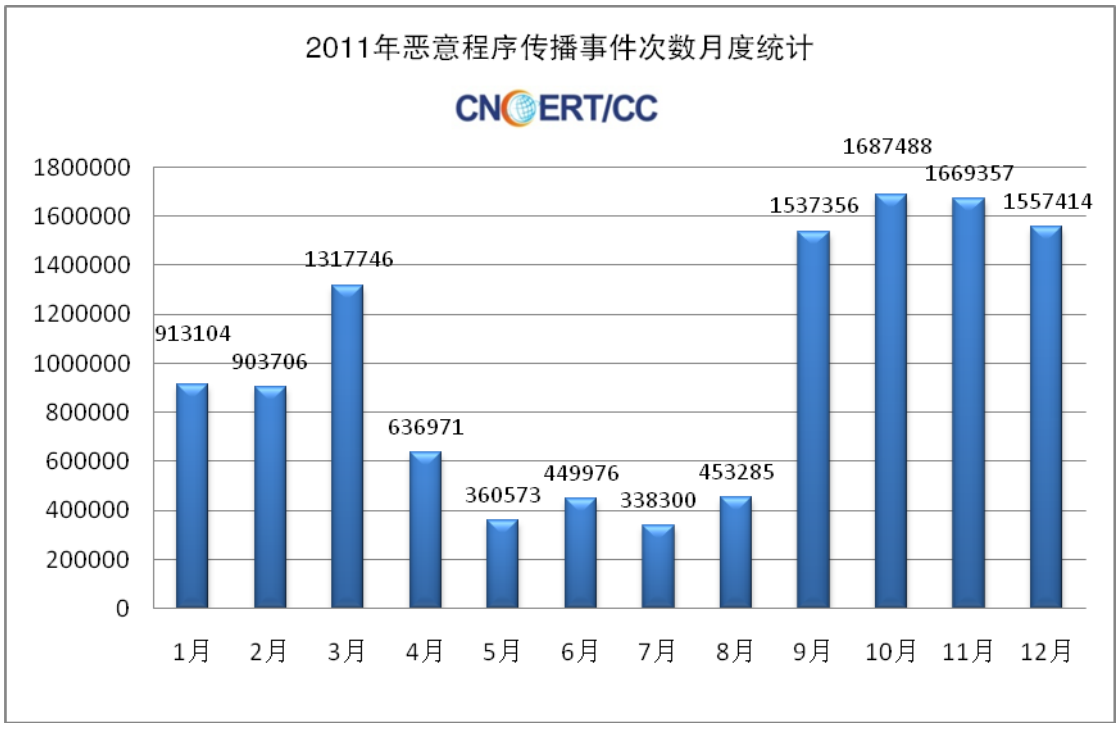


图 2-14　2011 年恶意程序传播事件次数月度统计

恶意程序传播源域名和 IP 数量的月度统计如图 2-15 所示，可以看出 9 月后传播使用的域名和 IP 数量较前几个月有了明显增长，恶意程序传播活动更加频繁，用户上网面临感染恶意程序的风险也更高，除了加大对恶意程序传播源的清理工作外，提高广大用户的安全意识也显得十分重要。

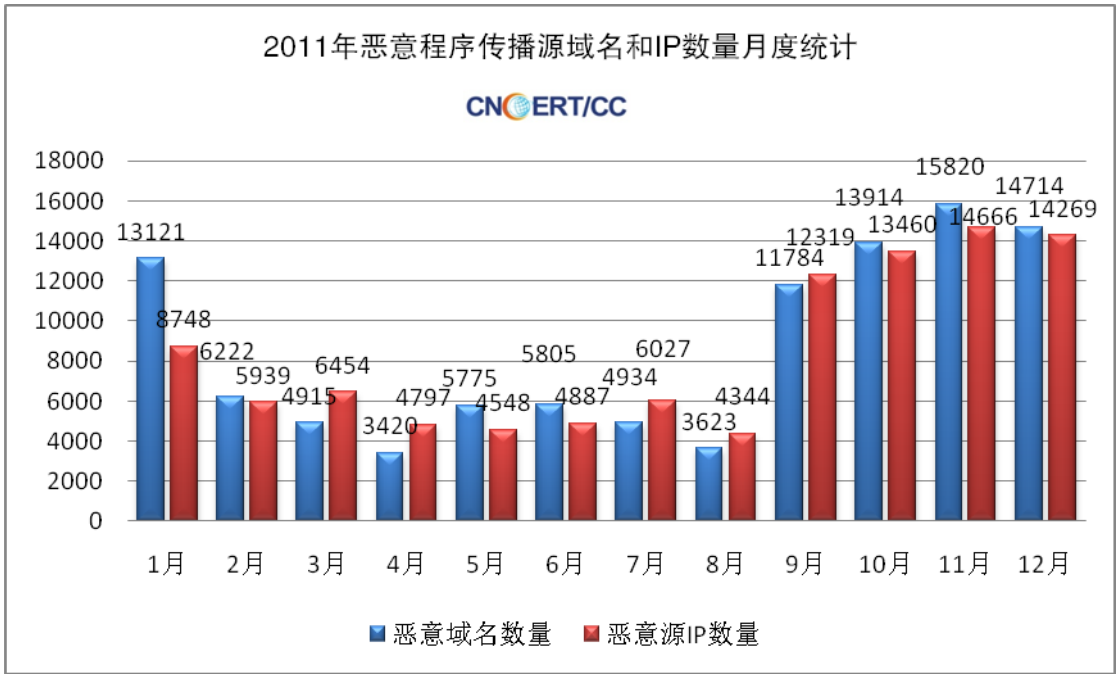


图 2-15 2011 年恶意程序传播域名和 IP 数量月度统计

监测还发现，恶意程序传播除了极少数是通过攻击者自定义的端口外，绝大部分都是通过 HTTP 协议端口，即 80 和 8080。用户上网一般都会在本机开放对远程主机 80 和 8080 端口的访问权限，这样恶意程序的下载传播过程就不会受到防火墙设备的阻断，对用户来说防范的难度更高。2011 年 CNCERT 监测到的恶意程序传播源端口分布统计如图 2-16 所示。

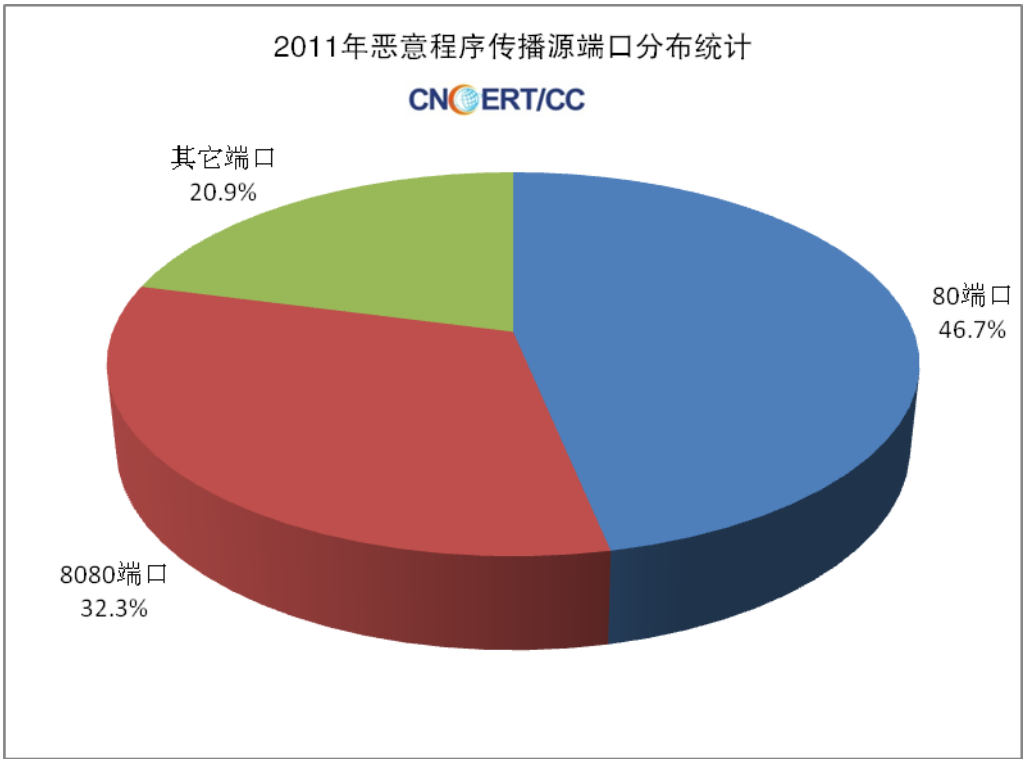


图 2-16 2011 年恶意程序传播源端口分布统计

2.4通报成员单位报送情况

■ 安天公司[3]恶意程序捕获情况

根据安天公司监测结果，2011 年全年捕获恶意程序样本总量为 11532980 个，比 2010 年的 9851180 个增长 17.1%，2007 年至 2011 年捕获恶意程序样本数量走势如图 2-17 所示。

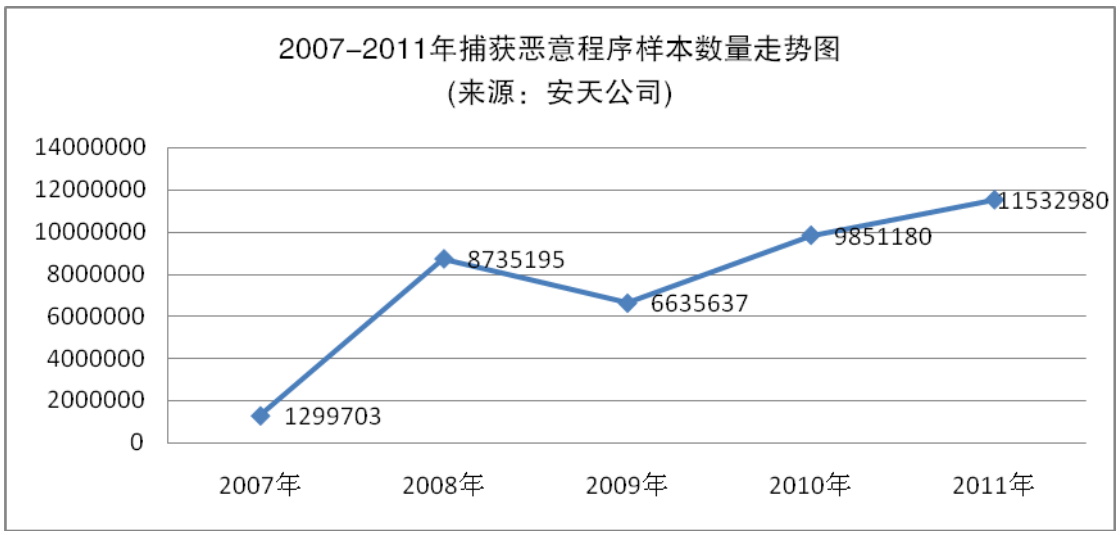


图 2-17　2007-2011 年捕获恶意程序样本数量走势图(来源：安天公司)

2011 年全年捕获恶意程序样本数量呈现波动态势，如图 2-18 所示。其中 7 月达到全年最低值 718682 个，8 月达到全年最高值 1388173 个。

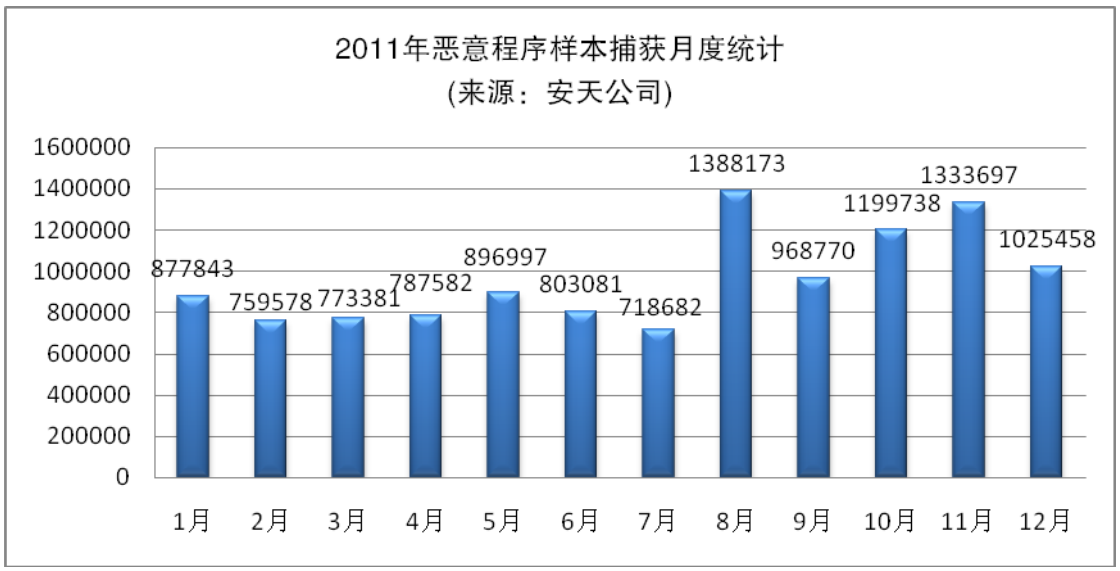


图 2-18　2011 年恶意程序样本捕获月度统计(来源：安天公司)

[3] 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。

2011 年全年监测到感染恶意程序的主机为 175375 余台，如图 2-19 所示。其中感染主机数量 12 月为全年最低值 8086 个，5 月达到全年最高值 23465 个。

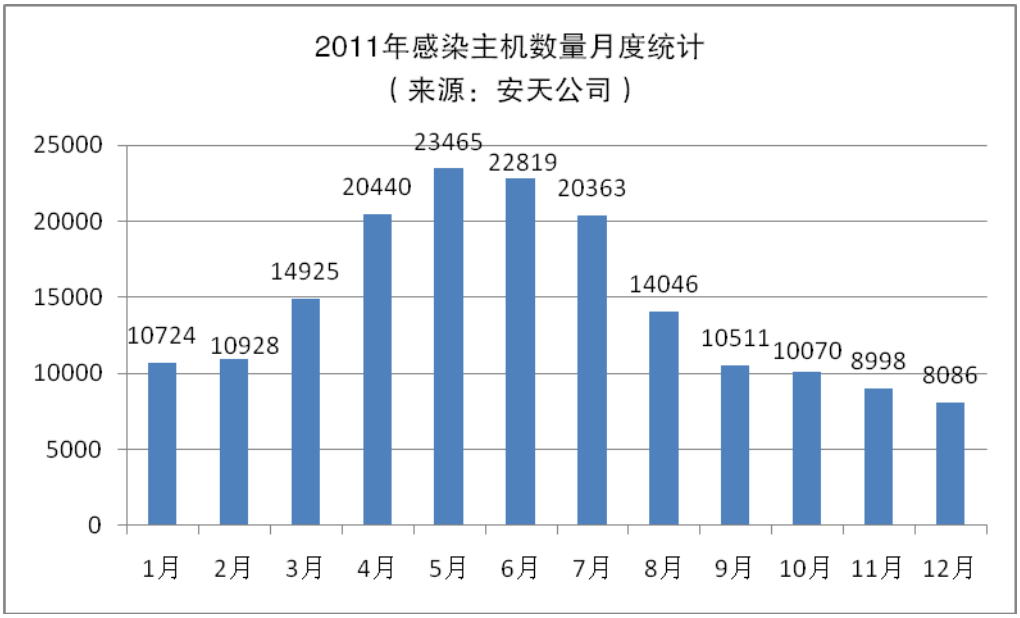


图 2-19　2011 年感染主机数量月度统计(来源：安天公司)

安天公司将捕获的恶意程序类型分为 8 大类，分别是木马、后门、蠕虫、病毒、广告软件、间谍软件、黑客工具和病毒工具，每类恶意程序捕获数量月度统计如图 2-20 所示。其中，木马是对全年捕获恶意程序数量趋势影响最大的一类恶意程序，全年捕获木马数量共 7021942 个。

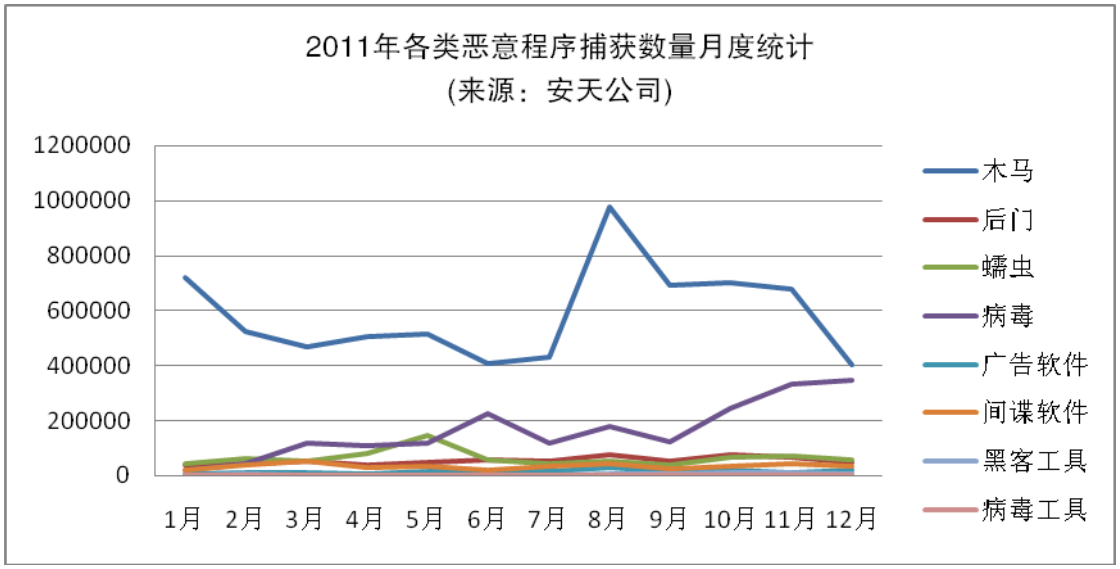


图 2-20　2011 年各类恶意程序捕获数量月度统计（来源：安天公司）

根据对比 2010 年和 2011 年的监测结果，在捕获的各类恶意程序中，绝对数量增长最多的是病毒，下降的是蠕虫，下降幅度为 29.8%。各类恶意程序数量增幅位居前三位的是：广告软件、病毒和黑客工具，增幅分别为：244.1%、196.9%

和 137.0%，如图 2-21 所示。

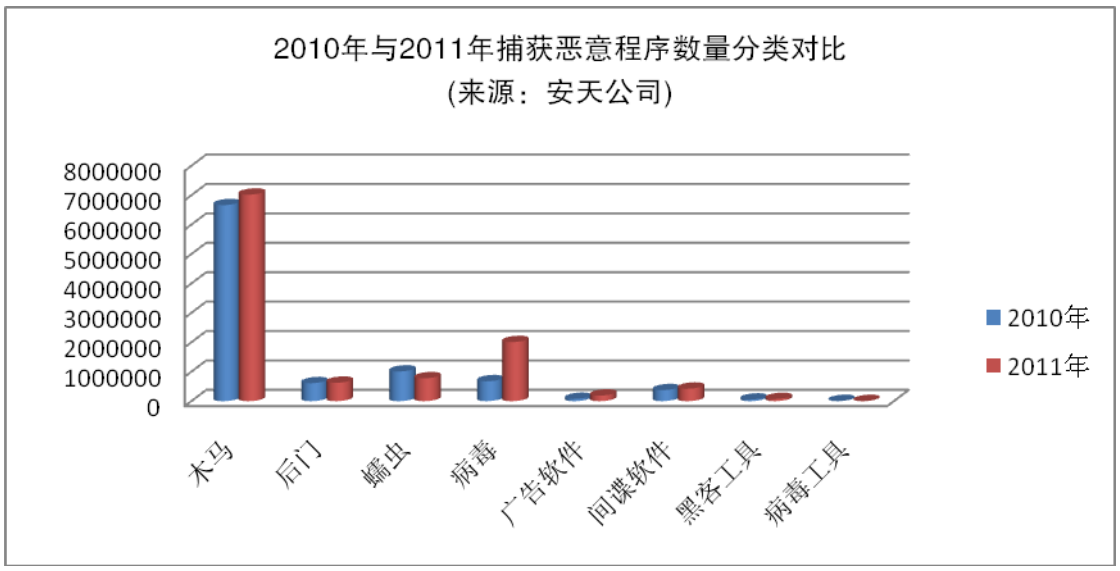


图 2-21　2010 年与 2011 年捕获恶意程序数量分类对比（来源：安天公司）

此外，从 2011 年恶意程序的行为特征分析，用于窃取信息（Stealer）、恶意程序下载（Downloader）、捆绑类（Dropper）的恶意程序占据前三位，如图 2-22 所示。其中，Stealer 的数量比 2010 年减少了 25.5%，仍排名第一；Downloader 的数量比 2010 年减少 33.2%，但排名由 2010 年的第 3 位上升至第 2 位；Dropper 的数量比 2010 年增加了 13.9%，由 2010 年的第 4 位升至第 3 位；而网游盗号（GameThief）的数量大幅下降 78.3%，由第 2 位降至第 4 位。

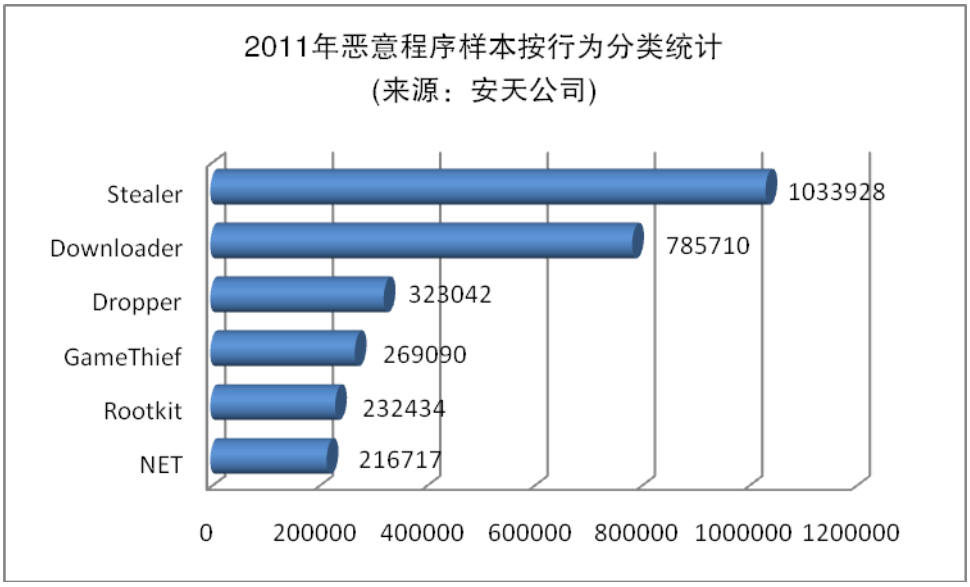


图 2-22　2011 年恶意程序样本按行为分类统计（来源：安天公司）

安天公司对恶意程序样本家族按捕获数量进行了统计，2011 年共有样本家族 20374 个，比去年新增家族 1129 个。2011 年恶意程序家族前 10 位如表 2-1 所示。

表 2-1　2011 年恶意程序样本家族捕获数量 TOP10（来源：安天公司）

2011 年恶意程序样本家族 Top10（来源：安天公司）		
序号	家族名称	数量
1	Trojan/Win32.Patched	1762610
2	Trojan/Win32.Kykymber	942787
3	Virus/Win32.Parite	740292
4	Virus/Win32.Virut	588248
5	Packed/Win32.Krap	283333
6	Trojan/Win32.Vilsel	267122
7	Trojan/Win32.VBKrypt	234991
8	Trojan/Win32. CodecPack[Downloader]	191106
9	Rootkit/Win32.TDSS	172861
10	Trojan/Win32.Buzus	150482

恶意程序样本加壳的比例由 2010 年的 19.1%下降至 2011 年的 14.3%，如图 2-23 所示。2011 年恶意程序所使用的主要壳类型 TOP 10 列表如表 2-2 所示。

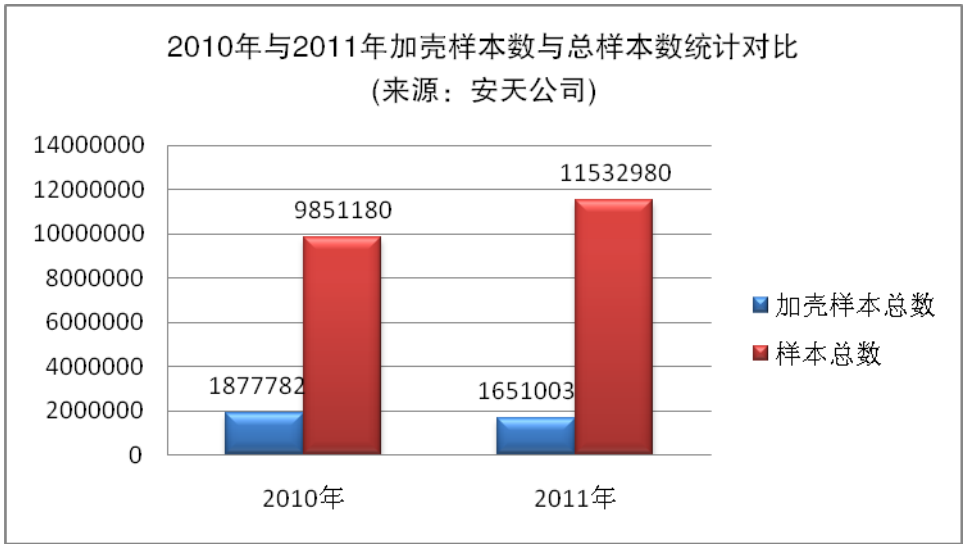


图 2-23　2010 年与 2011 年加壳样本数与总样本数统计对比（来源：安天公司）

表 2-2　2011 年恶意程序所使用的壳类型 TOP10 （来源：安天公司）

2011 年恶意程序加壳类型 Top10（来源：安天公司）		
序号	壳名称	数量
1	UPX	986797
2	PE_Patch.PECompact	131770
3	ASPack	101946
4	PECompact	92655
5	PecBundle	76928
6	PE_Patch	53906
7	PE_Patch.MaskPE	27942
8	UPack	20392
9	NSPack	17030
10	FSG	14290

■ 瑞星公司[4]报送的恶意样本情况

根据瑞星公司的监测结果，2011 年全年累积截获流行病毒 2536602 个，比 2010 年的 11836325 个大幅下降 78.6%。2011 年各月捕获数量呈现逐步递减趋势，如图 2-24 所示。其中 12 月达到全年最低值 318119 个，1 月达到全年最高值 1201266 个。

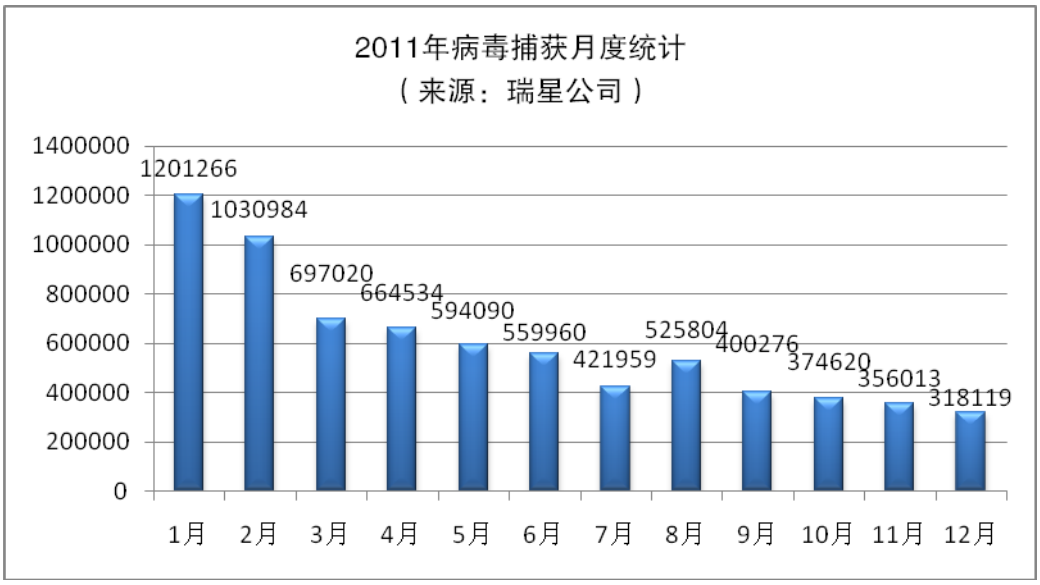


图 2-24　2011 年病毒捕获月度统计(来源：瑞星公司)

2011 年全年监测到感染病毒的主机 125099803 余台，其中感染主机数量 1 月为全年最高值 69795324 台，12 月达到全年最低值 5645378 台，如图 2-25 所示。

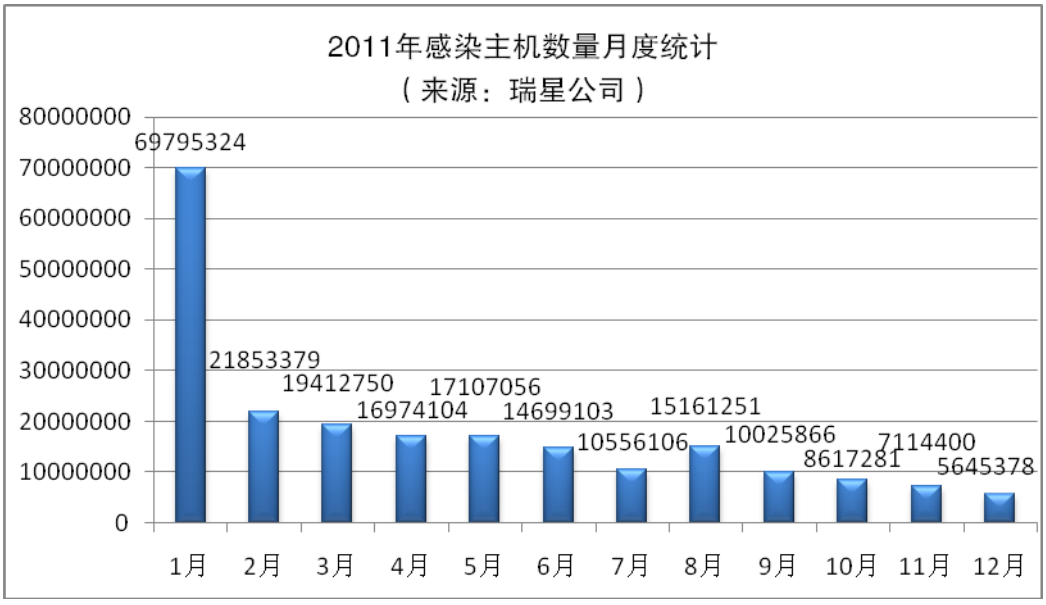


图 2-25　2011 年感染主机数量月度统计(来源：瑞星公司)

[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，同时也是 CNCERT 省级应急服务支撑单位。

瑞星公司全年累积截获流行病毒种类分类统计如图 2-26 所示。其中，木马（Trojan）是对全年捕获病毒数量趋势影响最大的一类，全年捕获木马类病毒样本占总数量的 90.0%，其次是下载者（Downloader）和后门（Backdoor）类。

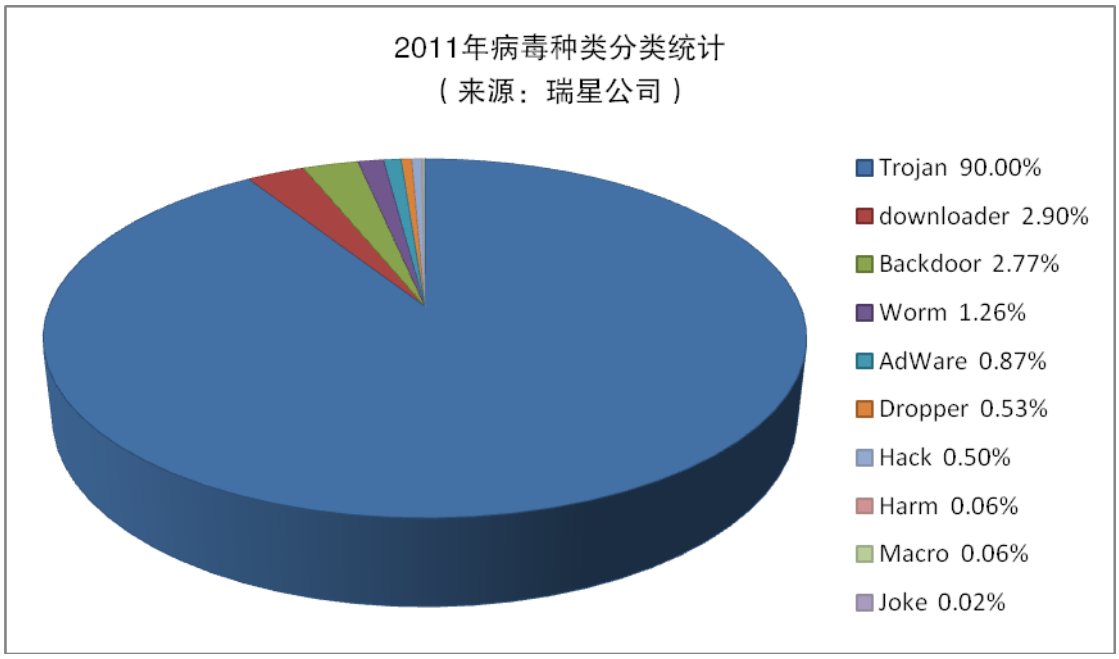
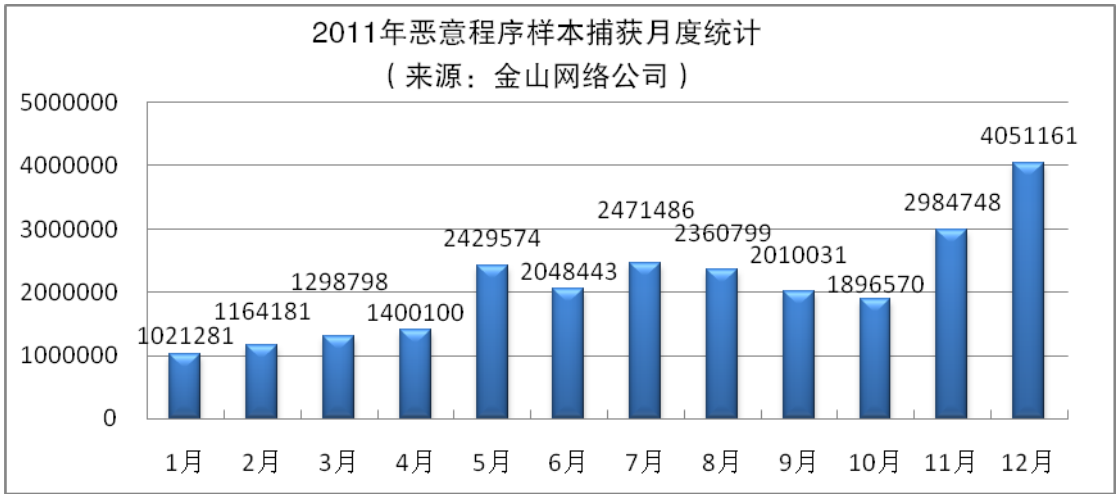


图 2-26　2011 年病毒种类分类统计(来源：瑞星公司)

■ 金山网络公司[5]报送的恶意程序情况

根据金山网络公司的监测结果，2011 年全年捕获恶意程序样本总量为 25137172 个，比 2010 年的 593240 个增长 4137%[6]。2011 年各月捕获数量如图 2-27 所示，其中 1 月达到全年最低值 1021281 个，12 月达到全年最高值 4051161 个。



[5] 金山网络公司即金山网络技术有限公司，是通信行业互联网网络安全信息通报工作单位。
[6] 2011 年金山网络公司的监控平台和 2010 年的区别较大，所以监测到的数据有很大的变化。

图 2-27　2011 年恶意程序捕获月度统计（来源：金山网络公司）

2011 年全年捕获新增恶意程序特征总量为 268483 个，比 2010 年的 563330 个下降 52.3%。2011 年各月捕获数量如图 2-28 所示，其中 10 月达到全年最低值 14018 个，1 月达到全年最高值 34408 个。

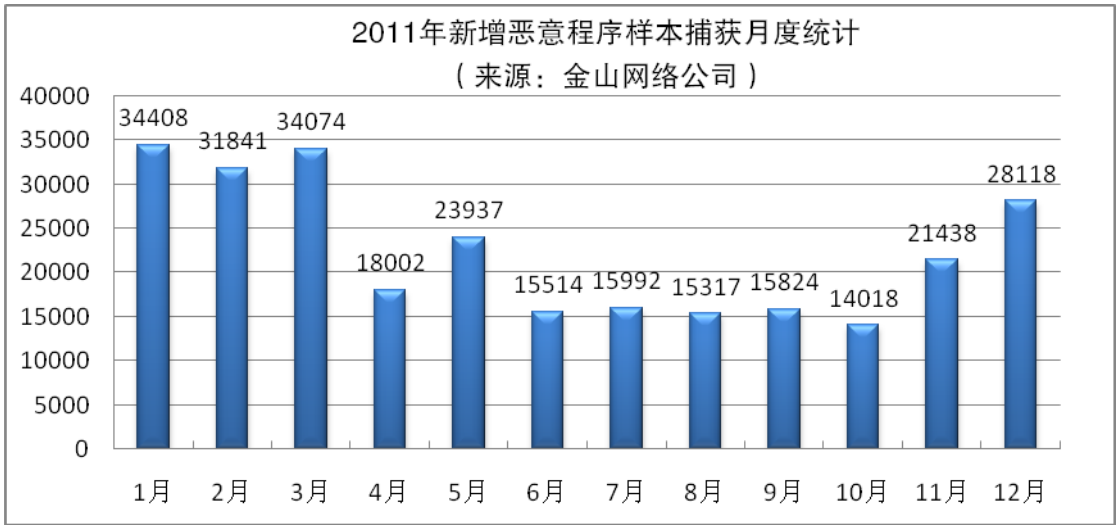


图 2-28　2011 年新增恶意程序样本捕获月度统计（来源：金山网络公司）

2011 年全年监测到感染恶意程序的主机 273698154 余台，比 2010 年的 41899393 个增长 553.2%[7]。其中感染主机数量 3 月为全年最低值 12945250 个，7 月达到全年最高值 34363191 个，如图 2-29 所示。

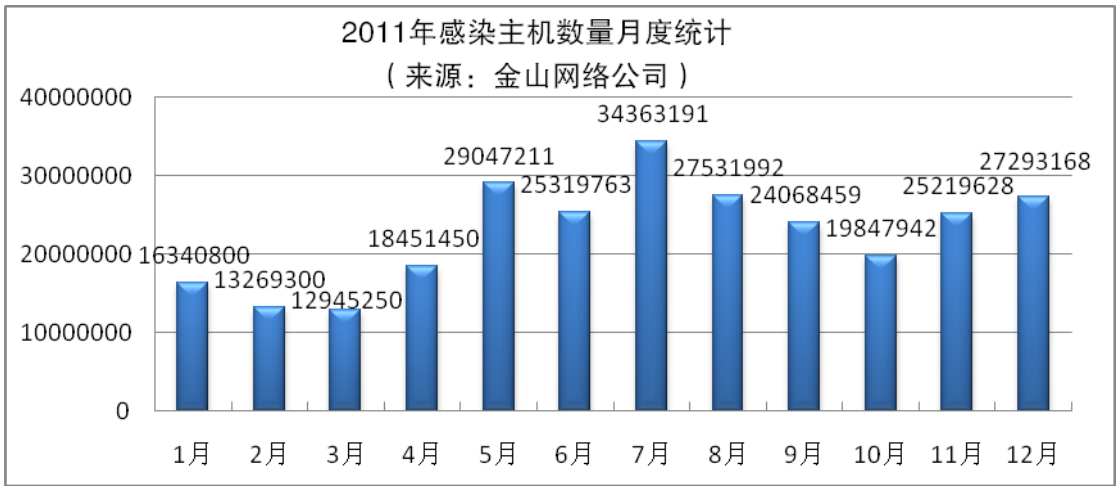


图 2-29　2011 年感染主机数量月度统计(来源：金山网络公司)

金山网络公司将捕获的恶意程序类型分为 8 大类，分别是木马病毒、恶意软件、黑客后门、漏洞攻击病毒、风险程序、脚本病毒、其他病毒和蠕虫病毒，每类恶意程序所占比例如图 2-30 所示。其中，木马病毒是对全年捕获恶意程序数量趋势影响最大的一类恶意程序。各类恶意程序数量位居前三位的是：木马病毒、

[7] 用户量上升量很大，所以监控到感染机器数量也有所上升。

恶意软件和黑客后门病毒，所占比例分别为：77.9%、15.6%和 4.9%。

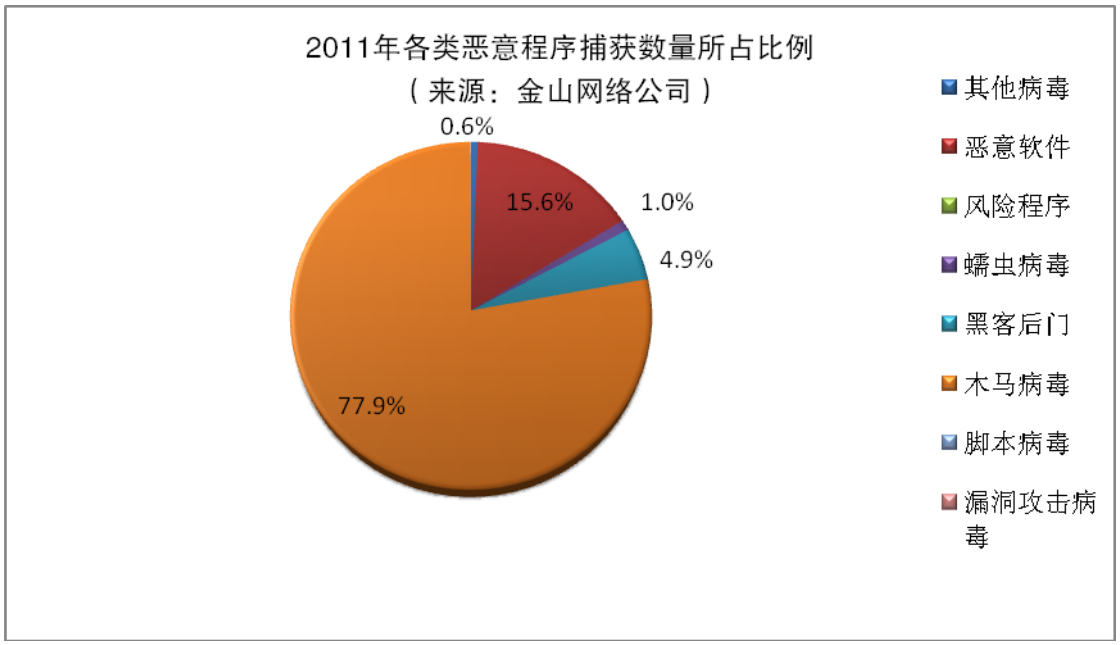


图 2-30　2011 年各类恶意程序捕获数量所占比例（来源：金山网络公司）

金山网络公司对恶意程序样本家族按捕获数量进行了统计，2011 年共有样本家族 145 个，比去年新增家族 111 个。2011 年恶意程序家族前 10 位如表 2-3 所示。

表 2-3　2011 年恶意程序样本家族捕获数量 TOP10（来源：金山网络公司）

2011 年恶意程序样本家族 Top10（来源：金山网络公司）		
序号	家族名称	数量
1	ZF	1266663
2	LS	667405
3	SIFU-私服	634300
4	WLB	141464
5	ZC	6671
6	456游戏	1241
7	桌面广告	408
8	色播 BRF	204
9	时代 TV	41
10	工具条	22

■ 奇虎 360 公司[8]报送的恶意程序情况

根据奇虎 360 公司的监测结果，2011 年全年捕获恶意程序样本总量为 10.56 亿个，比 2010 年的 5.63 亿个增长 87.6%。2011 年各月捕获数量如图 2-31 所示，

[8] 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。

其中 7 月达到全年最低值 3020 万个，11 月达到全年最高值 1.4 亿个。

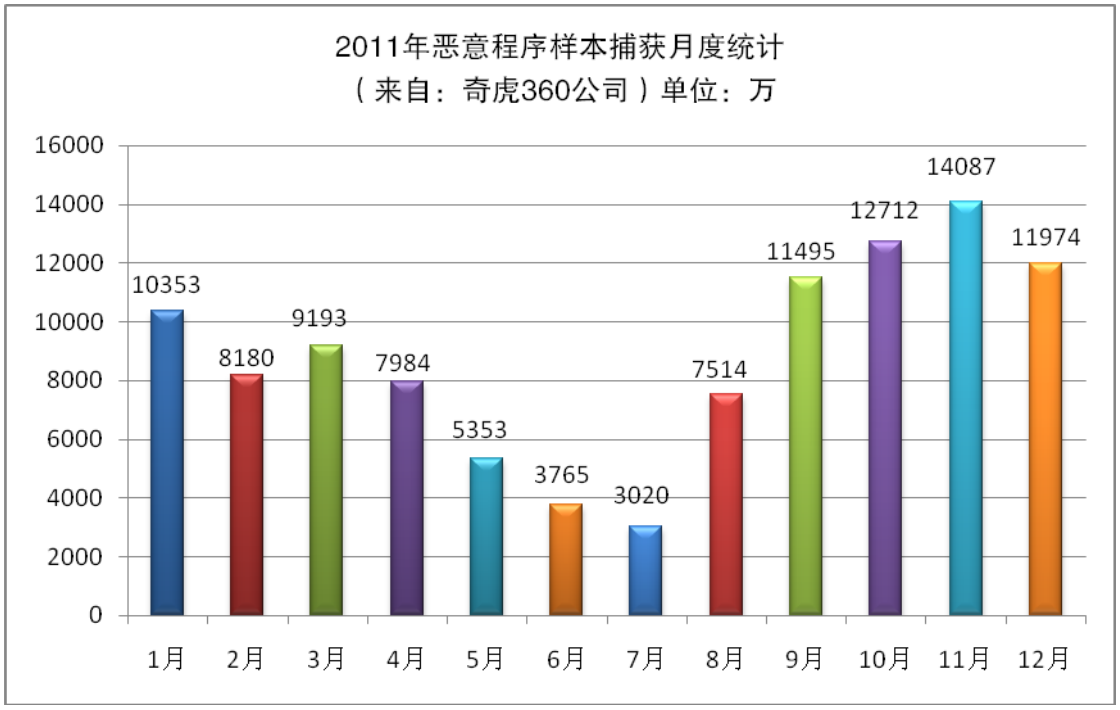


图 2-31　2011 年恶意程序样本捕获月度统计（来源：奇虎 360 公司)

2011 年全年监测到感染恶意程序的主机 311393 万余台，比 2010 年的 310384 万台增长 48.0%，感染恶意程序的主机数量的趋势为逐渐增长。其中感染主机数量 2 月为全年最低值，平均每天 318 万台；11 月达到全年最高值，平均每天 2023 万台，如图 2-32 所示。

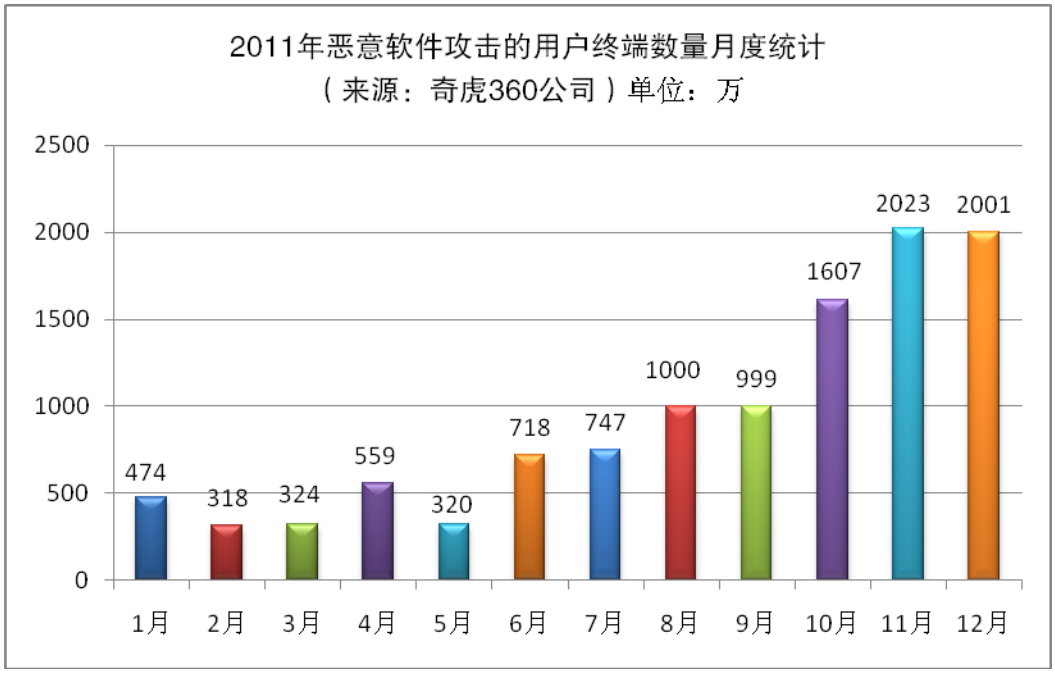


图 2-32　2011 年恶意软件攻击的用户终端数量月度统计(来源：奇虎 360 公司)

2011 年恶意程序所使用的主要壳类型 TOP 10 列表如表 2-4 所示[9]。

表 2-4　2011 年恶意程序所使用的壳类型 TOP10 （来源：奇虎 360 公司）

2011 年恶意程序加壳类型 Top10（来源：奇虎 360 公司）		
序号	壳名称	数量
1	SFX	65845246
2	UPX	45171949
3	ASPack	15385134
4	PECompact	9153613
5	Patch	1866401
6	Upack	1346737
7	ASProtect	1194829
8	NSPack	832360
9	E-Patch	408683
10	Armadillo	401890

[9]加壳类型统计自 2011 年 4 月开始统计，表中数据不代表完整数据情况。