6　网络安全事件接收与处理

为了能够及时响应、处置互联网上发生的攻击事件，CNCERT 通过多种公开渠道接收公众的网络安全事件报告，如热线电话、传真、电子邮件、网站等。对于其中影响互联网运行安全的事件、波及较大范围互联网用户的事件或涉及政府部门和重要信息系统的事件，CNCERT 国家中心以及各省分中心积极协调基础电信运营企业、域名注册管理和服务机构以及应急服务支撑单位进行处理。网络安全事件的接收与处理数量在一定程度上反映了我国互联网的网络安全状况。

6.1事件接收情况

2011 年，CNCERT 共接收国内外报告网络安全事件 15366 起，较 2010 年增加了 47.3%；其中，国外报告的网络安全事件数量为 2100 起，较 2010 年下降了 58.6%。2011 年 CNCERT 网络安全事件接收数量月度变化情况如图 6-1 所示。由图可见，2011 年 3 月起，每月接收事件报告数量均超过 1 千起，并在 8 月份达到全年最大值 1785 起。相比其他月份，1 月、2 月、10 月接收事件数量较少，主要原因是这几个月包含国家法定假日（如元旦、春节、国庆等）时间较长，故而 CNCERT 接收到的事件投诉数量也有所回落。

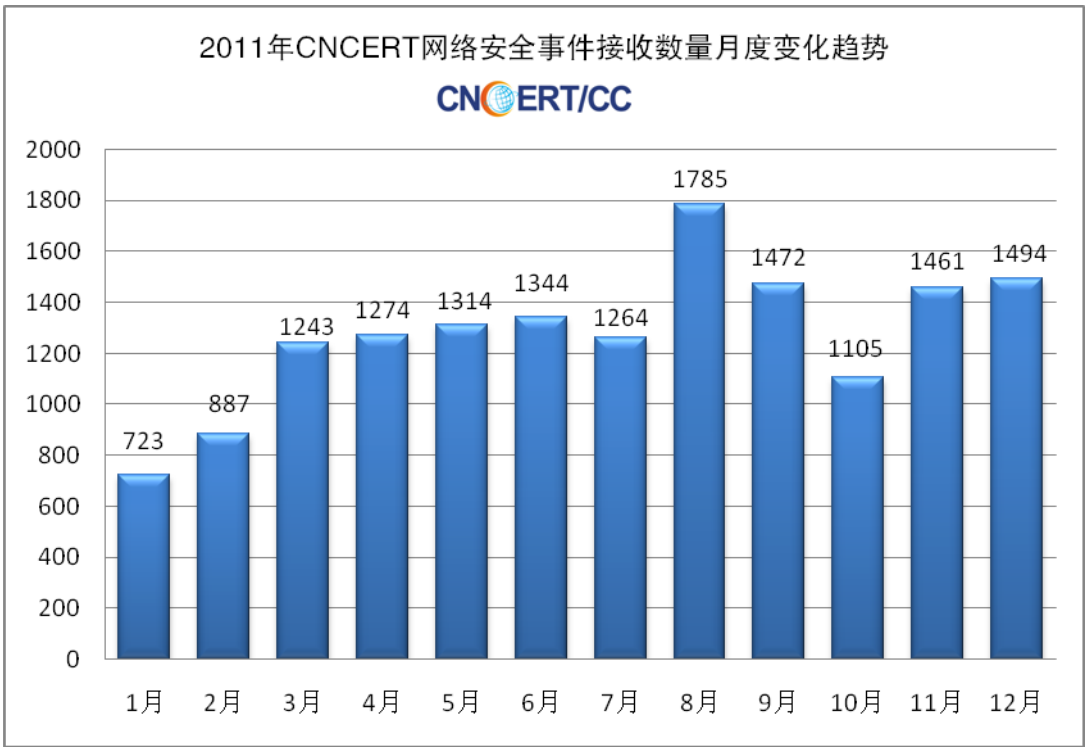

图 6-1　2011 年 CNCERT 网络安全事件接收月趋势图

2011 年，CNCERT 接收到的网络安全事件报告主要来自于政府部门、金融机构、电信运营商、互联网企业、域名服务机构、IDC、安全厂商、网络安全组织以及普通网民等。2011 年 CNCERT 接收到的网络安全事件类型主要包括信息系统漏洞、网页仿冒、恶意程序、网页篡改、网页挂马等[14]，具体分布如图 6-2 所示。

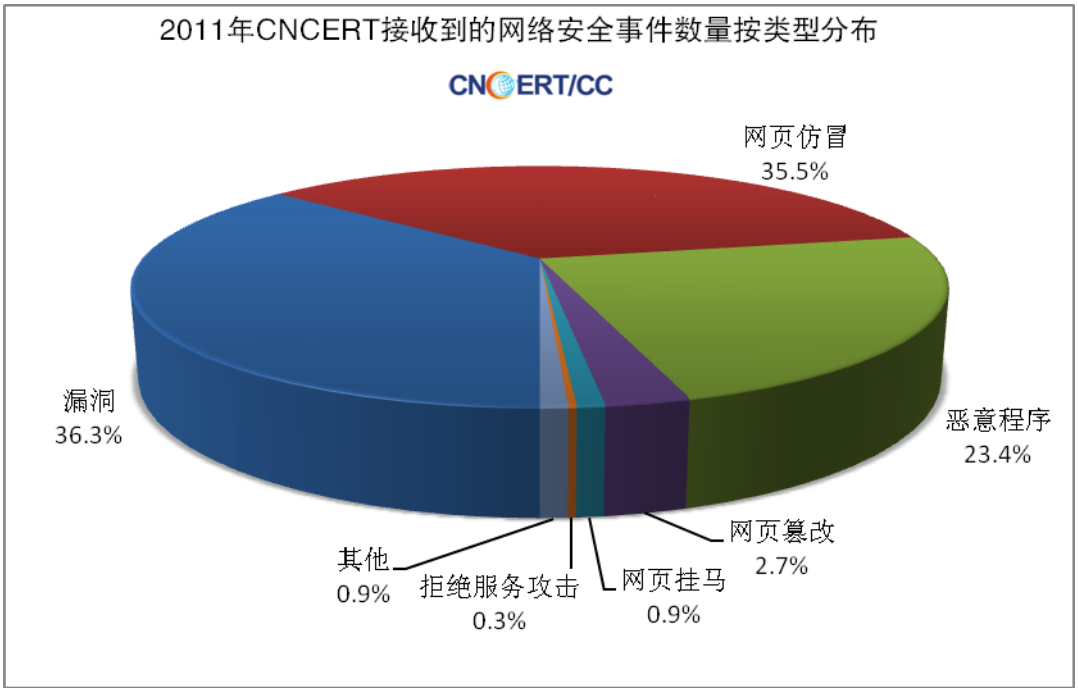

图 6-2　2011 年 CNCERT 接收到网络安全事件数量按类型分布

2010 年，CNCERT 接收到的事件数量排在前 3 位分别是信息安全漏洞、恶意程序、网页挂马事件；2011 年，CNCERT 接收的事件数量排在前 3 位的事件类型发生变化，分别是信息安全漏洞、网页仿冒和恶意程序事件。对比可见，信息安全漏洞仍是接收的重点事件，排名第一位；网页仿冒事件数量随着互联网支付和应用的普及而出现显著增长，从 2010 年的第四位跃居到 2011 年的第二位，并且与位于第一位的漏洞事件数量差距不大；恶意程序事件数量虽然排名下降了一位，但事件数高于 2010 年，仍然是对互联网用户构成严重威胁的安全事件之一。

信息系统漏洞事件数量最多，共 5583 起，较 2010 年的 3447 起增加了 62.0%，占所有接收事件的比例为 36.3%。漏洞事件数量在各类投诉事件中居于首位主要是因为在启明星辰、神州绿盟、恒安嘉新、安天、安氏领信、知道创宇、奇虎 360 等 20 余家共建单位的大力协助下，CNVD 漏洞信息库新增信息安全漏洞数量

[14] 根据 2010 年 CNCERT 推出了《网络安全术语解释》（第一版），将事件归为恶意代码、网页仿冒、拒绝服务攻击、垃圾邮件、漏洞、网页挂马和其它共七类，前六类基本对应往年分类中的病毒、蠕虫或木马、网络仿冒、拒绝服务攻击、垃圾邮件、漏洞和网页恶意代码六类事件。

在 2011 年继续保持了平稳增长势头。

网页仿冒事件数量为 5459 起，较 2010 年的 1566 起增加了 248.6%，跃居总体排名的第二位，占所有接收事件的比例为 35.5%。正如前述，网页仿冒事件数量随着互联网支付、互联网增值服务等各类互联网应用的普及和增多而不断增加，并有不断增长之势。在 CNCERT 接收的网页仿冒事件中，银行类仿冒事件数量最多。

恶意程序类事件的数量为 3593 起，较 2010 年的 3089 起有所增长，增长幅度约为 16.3%。在中国反网络病毒联盟（ANVA）行业自律框架下，CNCERT 团结行业力量共同开展网络恶意程序信息的收集工作。2011 年，在安天、奇虎 360、瑞星、金山网络、网秦、江民、洋浦科技、华为等 ANVA 成员单位的协助下，恶意程序样本信息收集工作成效显著，恶意程序类事件数量在接收事件总数中的比例为 23.4%。

总体来看，2011 年对广大互联网用户构成较为严重威胁的仍然是恶意程序的疯狂传播，恶意程序事件、漏洞事件、网页挂马事件三者是威胁互联网用户安全上网的三大要素。其中信息系统存在漏洞是恶意程序传播、感染的重要内因，网页挂马是恶意程序广泛传播的重要手段，恶意程序事件则最终造成网络失泄密等严重危害。对广大互联网用户构成较为严重威胁的另一类安全事件则是网页仿冒事件。网页仿冒事件（俗称“网络钓鱼”）是传统欺诈活动在网络时代新的表现形式，对广大网民危害较大，特别是针对网上银行、电子支付等金融类应用的网页仿冒事件，对用户的财产安全构成直接威胁。网页仿冒已成为金融行业及网络安全组织向 CNCERT 报告的重点事件类型，也是 CNCERT 重点处置的事件类型。

6.2事件处理情况

对上述投诉事件中危害大、影响范围广的事件，CNCERT 积极进行协调处理，以消除其威胁。2011 年，CNCERT 共成功处理各类网络安全事件 10924 件，较 2010 年的 6683 件[15]增长 63.5%。2011 年 CNCERT 网络安全事件处置数量的月度统计如图 6-3 所示。由图可见，全年月度事件处置数量基本呈上升趋势。针对互联网恶意程序及网页仿冒事件日益猖獗的发展趋势，CNCERT 加大了事件处置工作的力度，全年共开展了 14 次针对木马和僵尸网络的专项清理行动，并重点加

[15] 2011 年 CNCERT 将漏洞事件的处理也纳入事件处理总数中进行统计，因此也与 2010 年包括漏洞事件的处置总数 6683 件作比较。

强了针对银行类的仿冒事件的处置工作。在事件处置工作中，各分中心、基础电信运营企业和域名注册服务机构的积极配合有效提高了事件处置的效率。

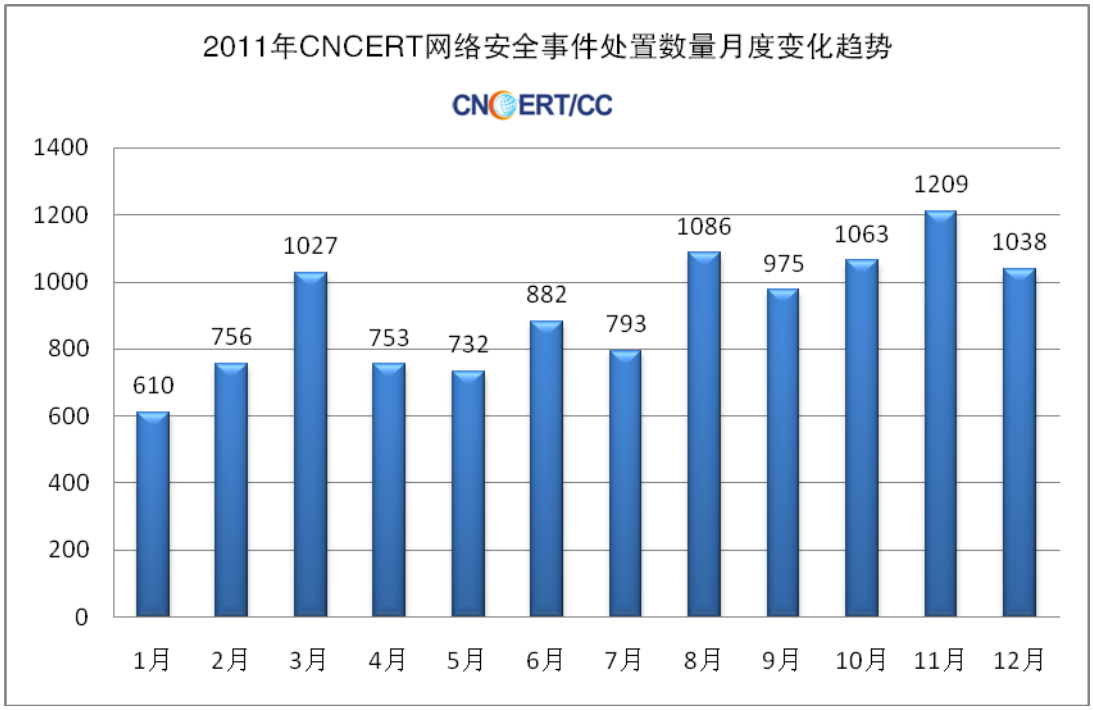

图 6-3　2011 年 CNCERT 月度网络安全事件处置数量

CNCERT 在境内各省、自治区、直辖市设立了分中心，协助 CNCERT 国家中心处理各类网络安全事件。2011 年各分中心共参与处理各类网络安全事件 1405 起，较 2010 年增长 32.6%。各分中心处理事件的数量如图 6-4 所示，广东省、辽宁省、江苏省、北京市和黑龙江省位居前 5 位。

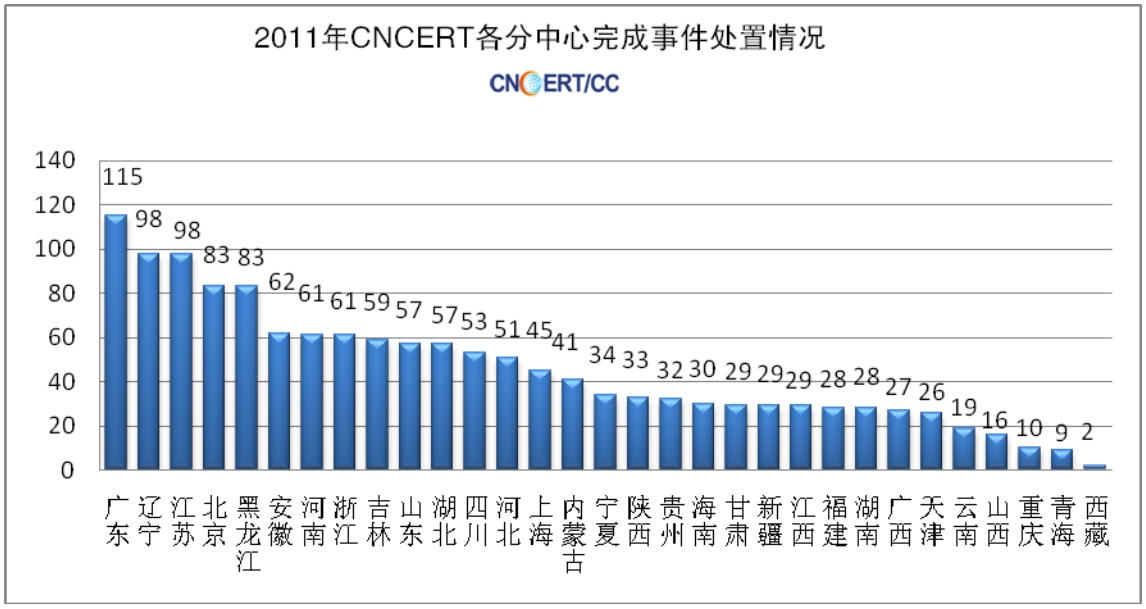

图 6-4　2011 年 CNCERT 各分中心完成事件处理情况

CNCERT 处理的网络安全事件的类型构成如图 6-5 所示，漏洞事件最多，共

5568 件，占 51.0%。漏洞事件的处置情况详见第五章。

恶意程序事件处置数量排名第二，2011 年共处置 2495 件，占 22.8%，较 2010 年的 1463 件增长了 70.5%。恶意程序是威胁互联网安全的重要因素，所以 CNCERT 将恶意程序事件列为日常处置的重点工作，意在通过清理恶意程序传播和控制的源头来降低互联网的安全风险，尽可能消除上网用户被恶意程序感染或远程控制的隐患。

2011 年，CNCERT 处理网页仿冒事件 1833 件，较 2010 年的 631 件增长了 190.5%，境内重点处理的仿冒事件主要涉及中国农业银行、中国工商银行、中国银行、中国邮政储蓄银行、淘宝等境内著名金融机构和大型电子商务网站。在这类仿冒事件中，黑客通过仿冒页面诱骗用户网银、信用卡等账号密码信息，进而窃取用户帐户中的现金。同时，还处理了大量由中国互联网协会 12312 举报中心接收用户投诉的涉及央视网、湖南卫视、腾讯、新浪、搜狐等知名媒体网站的仿冒事件，这类事件通过仿冒知名网站开展网络欺诈活动，CNCERT 通过及时处理有效避免了更多普通用户由于防范意识薄弱而导致的可能的经济损失。

此外，2011 年 CNCERT 继续开展对涉及境内政府机构和重要信息系统部门的网页篡改事件的处置，全年共处置事件 642 起，较 2010 年的 410 起增加了 56.6%。在其他类型事件中，针对政府部门和重要信息系统的拒绝服务攻击事件和网页挂马等事件也是 2011 年 CNCERT 事件处理的重点。

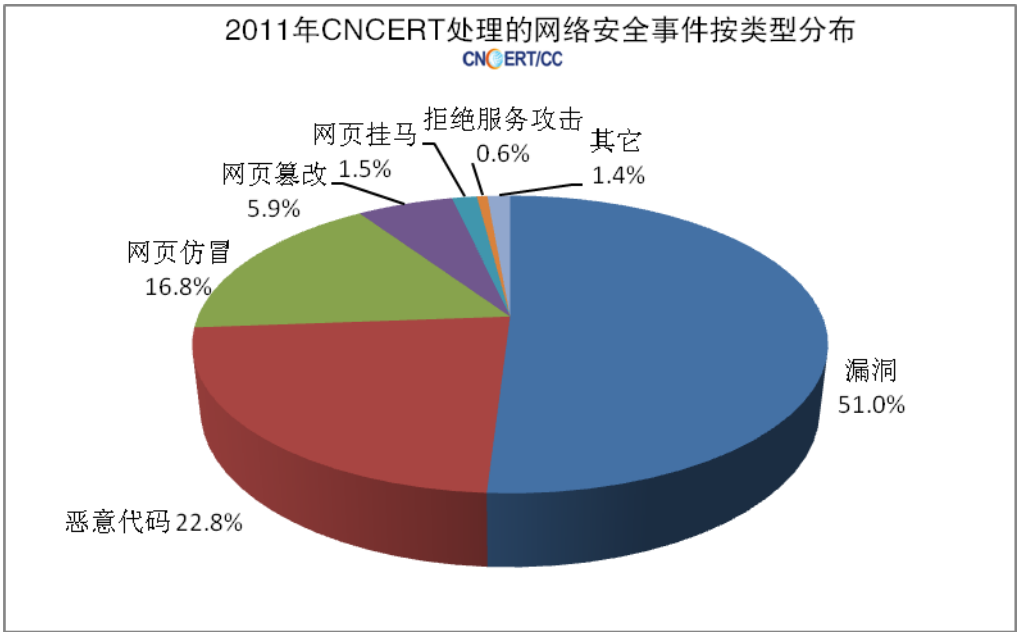

图 6-5　2011 年 CNCERT 处理的网络安全事件按类型分布

6.3 事件处理典型案例介绍

■ CNCERT 协调处置厦门易名 DNS 服务器遭攻击事件

2011 年 1 月 13 日 17 时起，厦门易名网络科技有限公司（以下简称厦门易名）位于杭州、茂名、东莞和福州等地的全部 6 台 DNS 服务器遭受大规模拒绝服务攻击，使用厦门易名域名解析服务的约 20 万个网站业务受到影响。攻击持续到 20 时左右，21 时后解析服务逐步恢复正常。据厦门易名自身分析，此次攻击不是针对其主 DNS 服务器，而是针对其代为解析的网游私服网站 uc530.com。

CNCERT 于当日 18 时接到 CNNIC 和厦门易名的共同报告后，立即依照《互联网网络安全应急预案》启动了快速处置流程。CNCERT 监测发现，针对厦门易名的攻击为伪造源地址的 DNS 请求攻击，攻击流量峰值达到 800Mbps，其中浙江、广东、福建和江苏四个省的攻击现象最为明显。经与厦门易名核实，上述四个省均为厦门易名 DNS 服务器部署的位置。厦门易名联系了相关 IDC 机房实施流量清洗，有效缓解了攻击。

本次攻击事件后，CNCERT 推动和协助厦门易名对受攻击的三台服务器加装了防护措施，在 IDC 出口加装防火墙，对伪造源 IP 包进行过滤，提高了其抵御类似攻击的能力。

■ CNCERT 快速处理针对 APCERT 的 DDoS 攻击事件

2011 年 1 月 13 日，CNCERT 接到亚太网络安全组织 APCERT 投诉，称位于我国的某主机对其某服务器持续发起拒绝服务攻击，该主机极有可能被黑客控制。CNCERT 及时响应，通过主机 IP 所在地的 CNCERT 湖北分中心协调当地基础电信运营企业进行查证。在确认该主机存在恶意网络行为后，立即联系相关用户进行了有效处理，清除了针对 APCERT 的攻击流量。

■ CNCERT 协调清理某国家重点实验室网站感染恶意程序事件

2011 年 1 月 26 日，CNCERT 监测发现中国科学院直属某国家重点实验室网站被黑客植入恶意程序（即网页挂马）。如用户在主机安全措施不到位的情况下访问该网站，就会被恶意程序所感染。鉴于该实验室访问用户较多，CNCERT 将事件情况立即向中国科学院网络管理机构——中国科技网通报，由其协调网站所属单位进行处置，并建议该网站采取暂行关闭和进行整改等措施。

■ CNCERT 快速处置韩国多家政府部门和企业网站受攻击事件

2011 年 3 月 4 日，韩国多家政府部门和企业网站受到拒绝服务攻击，韩国

网络安全应急组织 KrCERT 紧急请求 CNCERT 协助消除源自中国境内 30 多个 IP 地址的攻击流量。接到 KrCERT 请求后，CNCERT 立即开始利用自身技术手段对投诉情况进行验证，并积极调查和定位攻击流量的真实来源。从 3 月 5 日至 7 日，CNCERT 先后协调 CNCERT 北京分中心，以及中国电信、中国联通、中国移动等我国主要基础电信运营企业对攻击 IP 地址对应的主机进行排查，并对发现存在问题的主机进行了及时有效的处理。

■ CNCERT 快速处置某中央重点新闻网站访问流量异常事件

2011 年 3 月 7 日，某中央重点新闻网站联系 CNCERT，反映其访问流量异常，请 CNCERT 协助监测、调查，并消除攻击流量。接到投诉后，CNCERT 迅速启动了调查处置流程。根据监测情况，初步判断该网站正在遭受较大规模的拒绝服务攻击，随后 CNCERT 对异常流量进一步调查、定位，并对流量特点进行深入分析，发现针对该网站的拒绝服务攻击为 UDP Flood 类型，攻击流量主要源自位于福建和湖南的 4 个 IP 地址。CNCERT 通过福建分中心和湖南分中心协调当地运营商对发动攻击的主机进行清理，针对该网站的攻击流量随即消失，该网站的流量和服务也迅速恢复正常。

■ CNCERT 与微软公司联手清除 Rustock 僵尸网络

2011 年 3 月，CNCERT 接到美国微软公司举报，请求协助其联合打击名为 Rustock 的全球大型僵尸网络。据微软公司等多方监测数据，Rustock 僵尸网络在 2010 年发展成为全球规模最大范围最广的僵尸网络之一，至 2011 年初，发现其已感染 130 多万个 IP 地址，并且能够每天发送超过 300 亿封垃圾邮件，被公认为全球最大的垃圾邮件制造者。

由于 Rustock 僵尸网络危害严重，微软公司除在美国通过法律诉讼途径暂时切断该僵尸网络控制服务器有关 IP 的互联网通信外，还协调其他国家和地区的网络安全机构也进行同步处置。微软公司向 CNCERT 提供了 2010 年 9 月至 2013 年 6 月可能在.CN 顶级域下注册并用于控制 Rustock 僵尸网络的一万多个域名，希望 CNCERT 能够对这些域名进行有效监测和处置。在接到该请求后，CNCERT 积极与微软公司交流合作，并立即运用自身技术手段展开调查。在了解和验证相关情况后，CNCERT 依据我国应急处置体系的工作机制和相关管理办法，协调 CNNIC 迅速采取行动，将 Rustock 僵尸网络可能在.CN 顶级域下注册的全部控制端域名都指向黑洞地址，从而进一步切断了黑客对僵尸网络的控制信道。

微软公司对 CNCERT 的配合行动高度赞赏，多次来邮件表示感谢，并在其发布的安全报告专刊《Battling the Rustock Threat》中提及了与 CNCERT 的相关合作

情况。此次针对全球大型僵尸网络的国际化联合处置行动，积极净化了全球互联网环境，有效保护了广大网络用户的利益。

■ CNCERT 跨境协调处置某省人民政府网站遭攻击事件

2011 年 4 月 15 日，CNCERT 接到分中心报告，称某省人民政府网站服务器遭受拒绝服务攻击。经分析，本次事件是由于某网络游戏私服网站将其域名非法指向该政府网站，将原本针对该游戏私服网站的攻击流量恶意转嫁到政府网站而导致的。CNCERT 立即联系该游戏私服网站的境外域名注册商，成功协调其停止了对该游戏私服网站域名的解析，及时消除了转嫁到政府网站的攻击流量，使政府网站服务恢复正常。

■ CNCERT 处理某运营商分公司网站遭受手机病毒攻击事件

2011 年 5 月 6 日上午起，某运营商分公司业务门户网站遭受大量高频次移动互联网内 HTTP 访问请求攻击，当日下午网站已无法提供正常服务。CNCERT 监测发现，大量高频次访问的 IP 地址都来自移动互联网内，其中攻击流量最大的前 21 位手机用户的访问量最高达一天 4 万多次。

CNCERT 根据自身的手机病毒监测系统数据，并结合受害公司对上述 21 位手机用户的访谈情况进行综合分析，判定其中 17 个手机用户感染了“毒媒”病毒变种。CNCERT 进一步分析捕获到的“毒媒”病毒变种样本后发现，该样本具备接收控制端指令频繁访问特定网站的能力。为及时切断发起攻击流量的控制源头，CNCERT 根据相关法律法规，立即协调有关域名服务机构停止了对该变种控制服务器所使用的域名的解析，受害公司也及时采取紧急措施，使受攻击网站恢复了正常服务。

■ CNCERT 与境外网络安全组织相互协作加强我国政府网站的漏洞处置

2011 年 6 月，CNCERT 密切关注国外黑客组织“LulzSec”对全球政府部门网站的攻击情况，并与境外网络安全组织相互协作，加强我国政府部门网络安全事件的处置。6 月 28 日，根据澳大利亚 CERT 组织的通报，CNCERT 协调多个分中心对涉及 www.shuangliu.gov.cn 、 www.ykzzb.gov.cn 、 jsfgj.yeda.gov.cn 、 www.investhg.gov.cn、www.ahshx.gov.cn、www.ccpitzj.gov.cn 等多个境内政府部门网站存在的 SQL 注入等漏洞事件进行了验证和处置，并通过该事件，再次警示相关部门要加强重视我国政府部门网站的安全问题。

■ 协调处置 8.18、8.19 新疆某运营商域名系统遭受攻击事件

2011 年 8 月 18 日、19 日，CNCERT 监测发现，新疆某运营商的两台 DNS 递归服务器出现明显流量异常，峰值流量均超过当日正常流量的 10 倍。流量异常期间，访问受攻击 DNS 服务器的客户端 IP 地址数急剧增加。另据该运营商集团公司监测数据，18 日晚攻击期间，其域名系统缓存命中率由正常的 90%下降到 60%，出省流量峰值下降了 43%。

CNCERT 通过自身监测平台，对流量异常情况、域名解析异常情况、攻击源进行了仔细调查，并及时将该事件的调查结果向通信行业主管部门进行汇报，深入分析事件的影响，积极提供应对措施和建议。随后，CNCERT 协助通信行业主管部门召开互联网网络安全应急专家组会议，与来自中国电信、中国联通、中国移动、CNNIC、中国信息安全测评中心和我国部分网络安全企业的专家一起，对事件的性质、程度、反映的问题和宜采取的对策等进行了研判。

与会专家建议各单位应高度重视域名系统安全，加强国家层面的网络安全监测和应急处置体系建设，构建跨省、跨运营商的域名容灾备份系统，以提高对服务能力和技术能力的复用水平；认真贯彻互联网网络安全信息通报工作有关要求，落实责任；升级和修改网络应急处置预案，根据各类攻击的特点对处置措施进行分类，以实现对攻击进行有针对性的处置；切实提高域名系统安全监测能力，下沉监测位置，细化监测粒度，推动各基础电信运营企业加快在全网范围内切实认真实施源地址验证。

最后，CNCERT 以发布信息安全通报的方式将该事件的具体情况和处理建议告知各基础电信运营企业等相关单位，提醒其加强防范类似攻击的意识和能力。

■ CNCERT 预警 Carrier IQ 软件收集手机用户隐私信息

2011 年 11 月，CNCERT 获悉移动智能服务厂商 Carrier IQ 的产品存在严重的隐私搜集行为。Carrier IQ 是一款无线网络测试诊断软件，主要被各移动运营商和手机制造商用来诊断电话掉线、电池续航等问题。2011 年 11 月，CNCERT 注意到有国外研究人员披露该软件除记录网络测试诊断所需的必要信息外，还记录了按键、位置、语音、视频等用户隐私信息。从 2011 年下半年开始，国外多个第三方定制 ROM 提供商开始有计划地从提供的所有 ROM 中移除 Carrier IQ 软件相关的组件。12 月 3 日，Carrier IQ、HTC、三星三家公司已经收到美国密苏里州、伊利诺伊州等多个地区用户的集体诉讼。

CNCERT 对此事件高度重视，委托 ANVA 成员单位安天公司对 Carrier IQ 样本及国内传播情况等进行了深入的分析。按照《移动互联网恶意程序描述规范》，CNCERT 最终认定该软件为信息窃取类恶意程序，相关样本的命名为

a.privacy.CarrierIQ.a。为保护我国广大手机用户的个人隐私信息免遭窃取，CNCERT 及时向公众发布信息安全通报，向普通手机用户提供了详细易懂的处置建议。

■ CNCERT 监测发现境内域名放大攻击事件并及时预警

2011 年 12 月 7 日至 9 日，CNCERT 先后接到境外多家域名注册商和域名服务机构投诉，称从 11 月 28 日左右开始接收到大量源自我国 IP 地址的异常域名查询请求。除收到上述域名服务商的投诉邮件外，CNCERT 还进一步调查发现从 12 月 2 日开始在 Dyn 博客和 OARC 邮件列表的域名技术讨论区中，有多家境外域名服务商的技术维护人员反映在同期都接收到了大量类似的异常域名查询请求。

CNCERT 立即对境外域名服务商反映的情况展开调查，发现确实有很多源自境内的异常域名查询请求发往境外的域名解析服务器。经过综合分析调查结果，CNCERT 判断该事件是境内攻击者采用伪造源地址方式，借助域名系统放大攻击流量，实现针对多家游戏私服网站的拒绝服务攻击。攻击者通过将源地址伪造为攻击目标（即游戏私服网站），向众多境外域名解析器发送大量 ANY 类型的 DNS 请求，导致境外域名服务器将各类应答报文回送给攻击目标，由于应答流量远大于请求流量，从而实现利用域名系统放大攻击效果。该攻击方式属于典型的域名放大攻击。

CNCERT 及时将该事件的投诉情况和调查结果向通信行业主管部门进行汇报，并协助召开互联网网络安全应急专家组会议，就该事件的严重程度、潜在危害和影响、后续处置和防范措施等问题展开讨论。专家组根据 CNCERT 汇报的情况形成以下主要结论：该事件中的攻击方法为典型的域名放大攻击，攻击目标为游戏私服网站，事件的现有影响和危害有限，但潜在安全风险值得引起各方重视；CNCERT 后续将向运营商提供攻击线索信息，请运营商协助进一步调查和追溯攻击流量的真实来源位置；为长远消除众多伪造源地址的网络攻击隐患，需加快推动运营商全面部署和实施源地址认证，并借鉴垃圾邮件处置经验，探索为运营商域名服务器建立白名单等技术方案。

■ CNCERT 协调处理网站用户信息泄露事件

从 2011 年 12 月 21 日开始，互联网上陆续披露并流传 CSDN 中文社区、天涯社区等多家网站发生用户信息泄露事件。CNCERT 一方面密切关注事态发展，于 12 月 22 日通过网站向公众通报了 CSDN 中文社区大量用户账号和明文密码遭泄露的情况，一方面及时向通信行业主管部门汇报相关情况。

在通信行业主管部门的指导下，CNCERT 紧急联系协调相关网站和论坛开展

应急处置，并协助召开了互联网网络安全应急专家组会议。会议同时邀请了 CSDN 中文社区、开心网、天涯社区、网易、人人网、百度、新浪、搜狐、腾讯、阿里巴巴、卓越亚马逊等互联网企业的代表参会。会上，各互联网企业分别介绍了各自关注事件发展及自身防范用户信息泄露的技术措施。通信行业主管部门表示将以加强网络安全防护为工作重点，进一步做好互联网网络安全监管工作，并针对一系列用户信息泄漏事件提出以下意见：各企业要高度重视用户信息安全，明确保障用户信息安全是应尽的义务；各企业要做好事件的善后工作；通信行业主管部门将加大对相关企业用户数据安全、日志留存和审计等方面的检查力度，落实安全责任，推动增值电信运营企业网站加强内部管理，做好信息系统的安全防护工作；各方将合作加强对互联网用户的宣传教育，提醒用户养成良好的上网习惯，防范重要信息泄露。

截至 12 月 29 日，CNCERT 通过公开渠道获得疑似泄露的数据库 26 个，涉及账号、密码 2.78 亿条。经抽查核实，并与相关网站、论坛联系核对后，CNCERT 确认 CSDN 社区、天涯社区两家网站发生了用户数据泄漏事件，但泄漏原因还有待进一步分析；对于其他网站、论坛，虽然曝光数据中个别条目有效，但不能判定发生了网站、论坛用户数据泄漏事件。此次事件给互联网用户带来了严重的个人信息安全威胁，引起社会广泛关注，也再一次给互联网企业和互联网用户敲响了安全警钟。

■ CNCERT 协调处置近千起境内、外网页仿冒事件

针对犯罪分子越来越普遍使用跨境注册域名构建仿冒网站以逃避打击的现象，CNCERT 特别加强了与国际网络安全应急处置机构、境外运营商、域名注册商和国际网络安全组织等的合作，显著提高了对跨境网页仿冒事件的处置和打击能力。

2011 年，CNCERT 监测发现或接投诉举报后，协调境外域名注册商，处理在境外注册、被用于仿冒我国重要金融网站的恶意域名的典型案例有：仿冒中国农业银行、中国银行、中国邮政储蓄银行、中国光大银行、深圳发展银行、中国建设银行、中国人民银行征信中心、中国工商银行、台州银行等银行或重要金融机构网站等的众多事件。同时，CNCERT 接到境外投诉请求，协调境内域名注册商，处理在境内注册、被用于仿冒境外政府等权威信息发布机构网站的恶意域名的典型案例有：应加拿大网络事件响应中心（CCIRC）请求协助处置仿冒加拿大税务总局网站、应 KrCERT 请求协助处置仿冒韩国政府网站；协助处置被用于仿冒境外银行等重要金融机构网站的恶意域名的典型案例有：仿冒苏格兰皇家银行网

站、仿冒德国邮政银行网站、仿冒美国金融机构 Wells Fargo 网站、仿冒希腊国家银行网站、仿冒韩国农协银行网站等的多起事件。

通过监测发现和协调处置以上述典型事件为代表的众多仿冒我国或他国政府网站或重要信息系统、以及仿冒境内外银行或重要金融机构的网络安全事件，CNCERT 有效打击了不法分子进行网络钓鱼的猖獗势头，净化了网络环境，保护广大互联网用户能够更可靠、更方便的利用互联网获取权威信息和处理经济事务。