6 “欢迎您向我们举报！”—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和重要信息系统部门的事件，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

2010 年，CNCERT 共接收了 10433 件非扫描类网络安全事件报告（2010 年不再计入垃圾邮件类事件投诉，而是建议投诉方直接向中国互联网协会反垃圾邮件中心投诉，并将接收到的此类投诉事件转至反垃圾邮件中心处理），其中，国外报告事件数量为 5070 件。事件接收数量的月度变化情况如图 6-1 所示。由图可见，2010 年 1 至 8 月的每月投诉受理事件数量基本上在 700 件左右波动，而 9 月至 12 月则稳定在每月 1 千件以上。

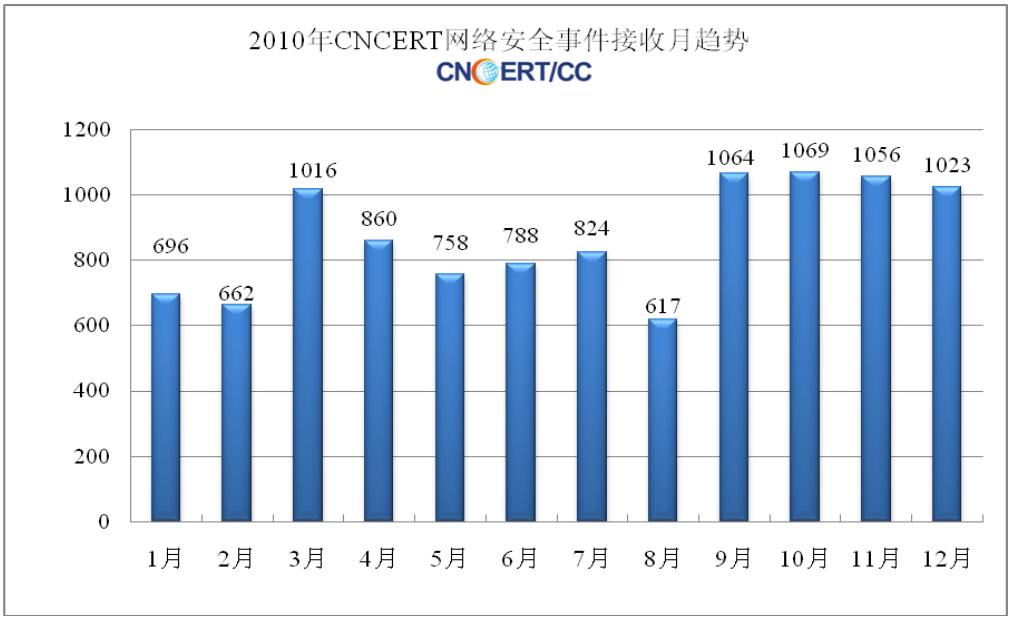

图 6-1　2010 年 CNCERT 网络安全事件接收月趋势图

2010 年，CNCERT 接收到的网络安全事件报告主要来自于政府、企业、网络安全组织、以及普通互联网用户。所报告的网络安全事件集中在信息系统漏洞、

恶意代码、网页挂马、网页仿冒等类型[1]，从图 6-2 所示的统计分布情况可以看出，各类型事件的数量在 2010 年的排名较 2009 有明显变化。

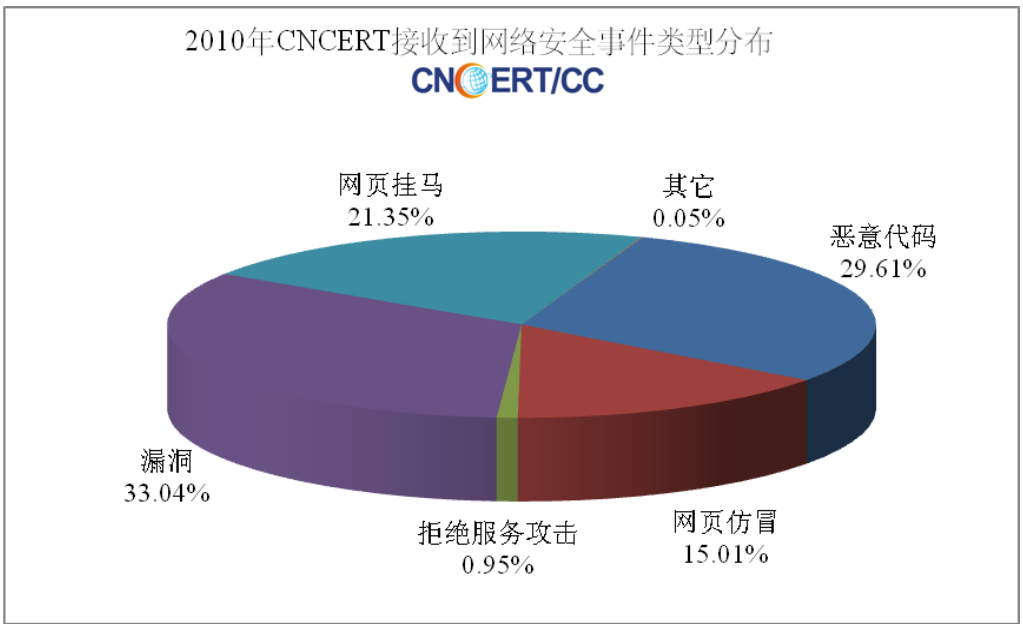

图 6-2　2010 年 CNCERT 接收到网络安全事件类型分布

信息系统漏洞事件数量最多，共 3447 件，较 2009 年的 338 件显著增多，这主要是因为专门负责漏洞信息收集和整理工作的 CNVD 漏洞信息库 2010 年取得长足发展，在启明星辰、神州绿盟、恒安嘉新、安天科技、知道创宇、东软、安氏领信等 20 余家共建单位的大力协助下，CNVD 漏洞信息库取得长足发展，不仅完成了 CNCERT 已有漏洞信息的收录，全年还收录了新增信息安全漏洞 3447 个。因此，本年度漏洞事件受理比例快速提升至 33%，跃居各类事件投诉数量首位。恶意代码类事件的数量为 3089 件，较 2009 年的 673 件明显增多。与上述原因类似，2009 年 CNCERT 发起成立了中国反网络病毒联盟（ANVA），团结行业力量共同开展网络恶意代码信息的收集工作。2010 年，在奇虎 360、瑞星、安天、江民、网秦等联盟成员单位的协助下，恶意代码样本信息收集工作成效显著，恶意代码类事件所占比例从 2009 年的 3.1%上升至 30%。

网页挂马事件为 2227 件，较 2009 年下降 54.6%，占全年投诉事件数量的 21%。

网页仿冒事件的数量为 1566 件，较 2009 年 1200 件上升 30%，占所有接收事件的比例为 15%。

总体来看，2010 年对广大互联网用户构成较严重威胁的是恶意代码事件、

[1] 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。

漏洞事件及网页挂马事件，而这几类事件往往又彼此存在关联，比如，利用信息系统的漏洞是恶意代码进行主动传播并感染用户的重要条件之一，而网页挂马又是恶意代码进行广泛传播的重要手段之一。网页仿冒事件（或称网络钓鱼）是传统欺诈活动在网络时代新的表现形式，对广大网民危害直接，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严重威胁。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。

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。2010 年，CNCERT 共成功处理各类网络安全事件 3236 件，较 2009 年的 1176 件增长了 175%。2010 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，这主要是出于配合上海世博、广州亚运保障工作需要，CNCERT 逐渐加大了事件处置工作的力度，开展了多次针对木马、僵尸网络的专项清理行动；同时，分中心、基础电信运营企业和域名注册机构的大力协助也帮助提高了事件处置的效率。

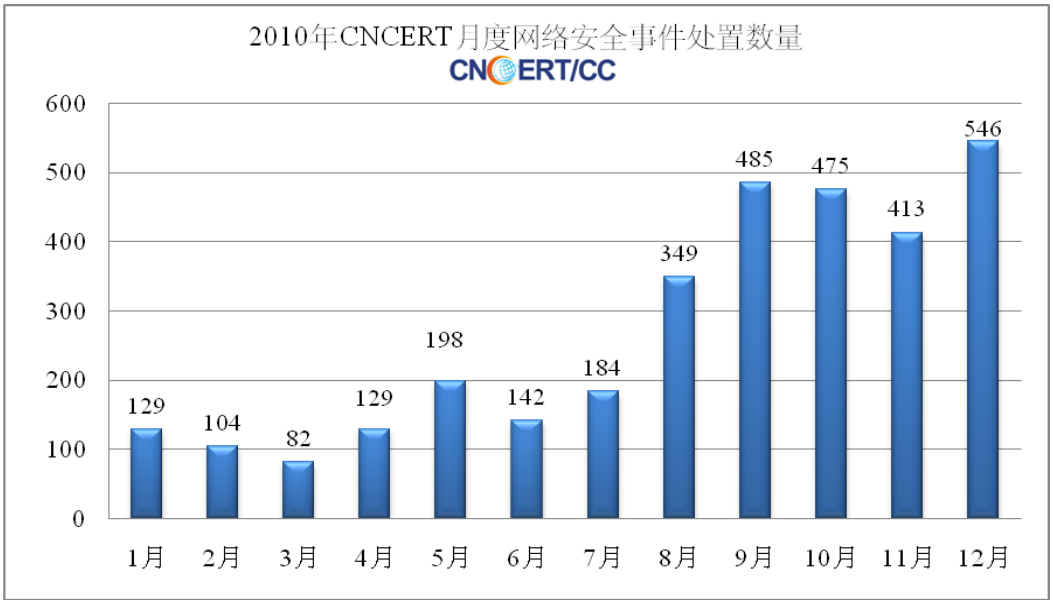

图 6-3　2010 年 CNCERT 月度网络安全事件处置数量

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。2010 年各分中心共参与处理各类网络安全事件 1059 起，较 2009 年增长 30.1%。各分中心处理事件的数量如图 6-4 所示，北京市、广东省、辽宁省、江苏省和安徽省位居前 5 位。

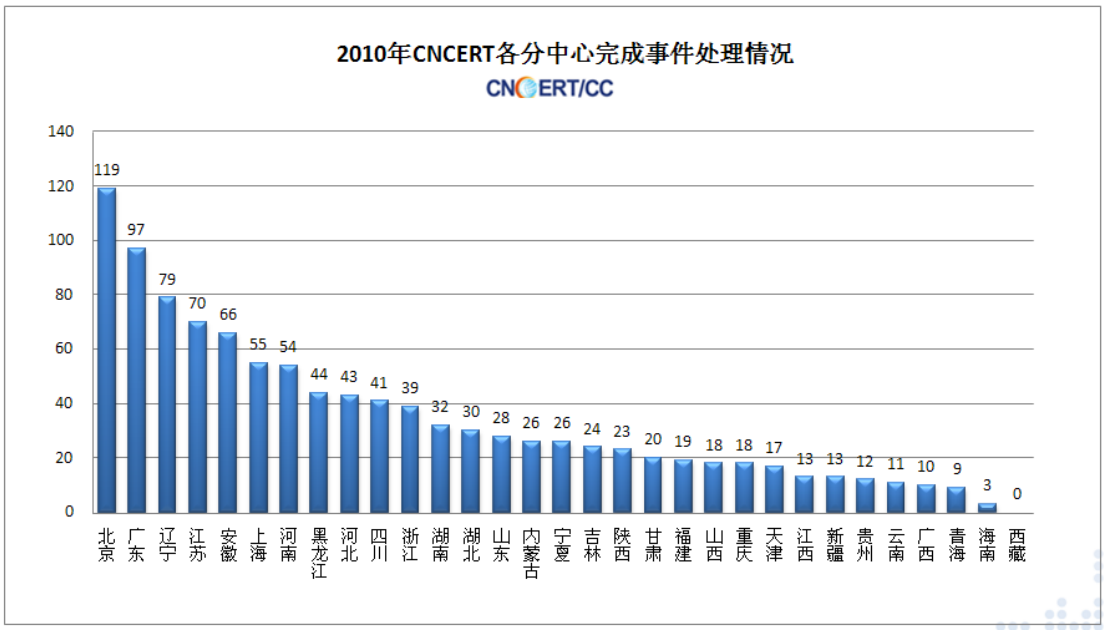

图 6-4　2010 年 CNCERT 各分中心完成事件处理情况

CNCERT 处理的网络安全事件的类型构成如图 6-5 所示，恶意代码事件最多，共 1463 件，占 45%；网页挂马事件 649 件，较 2009 年的 515 件增长了 26%。网页挂马依然是恶意代码传播的主要方式之一，所以 CNCERT 将网页挂马事件列为处置的重点，意在通过清理挂马网页打击和遏制互联网黑色地下产业活动。

2010 年，CNCERT 处理网页仿冒事件 631 件，较 2009 年的 293 件增长了 115%，涉及汇丰银行、美国银行、中国工商银行、中国银行、中国农业银行、ebay、淘宝等境内外著名金融机构和大型电子商务网站，甚至还涉及了美国财政部。在这些事件中，黑客试图通过仿冒页面诱骗用户网银、信用卡等账号信息，进而窃取用户资金。此外，2010 年 CNCERT 进一步加大了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力度，全年共处置事件 410 起，较 2009 年的 284 起增加了 44.3%。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、信息系统漏洞事件也是 2010 年 CNCERT 事件处理的重点。

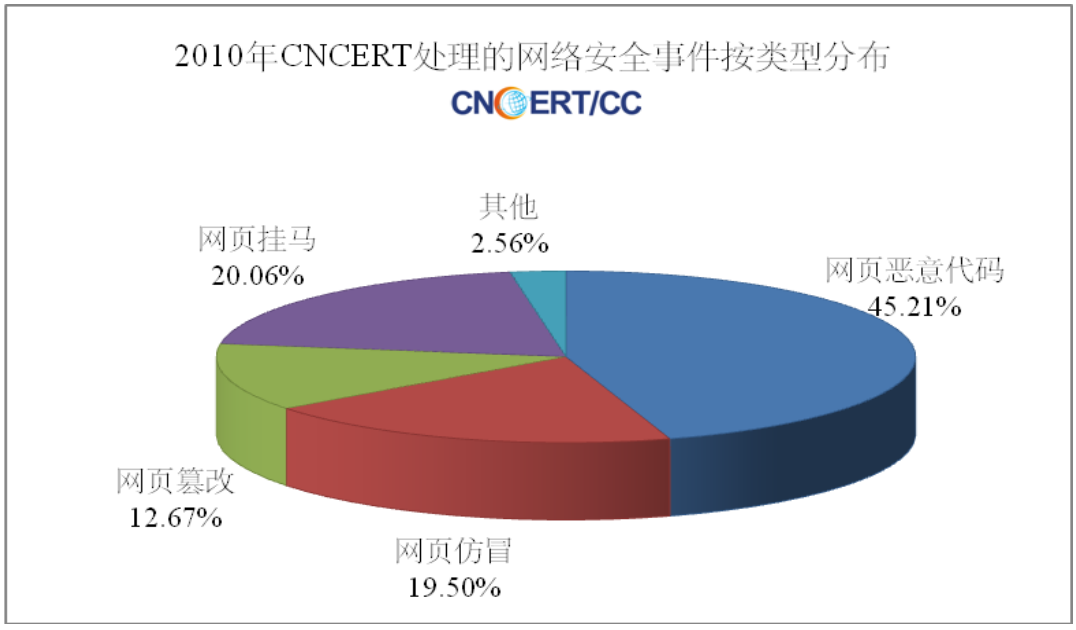

图 6-5　2010 年 CNCERT 处理的网络安全事件按类型分布

6.3 事件处理典型案例介绍

■ 一月十二日百度公司网站无法访问事件处置情况

2010 年 1 月 12 日上午 7 时左右，百度公司网站(baidu.com)突然无法访问。鉴于此事引起互联网用户的广泛关注，造成一定影响，工业和信息化部立即要求百度公司采取有效措施，尽快恢复网站的正常访问。在工业和信息化部的领导下，CNCERT 积极协调百度公司、CNNIC 和基础电信运营企业采取应急处置措施。12 日上午 11 时左右，百度公司网站访问逐步恢复正常。

12 日下午 1 时，工业和信息化部召集百度公司、基础电信运营企业、CNCERT 以及 CNNIC 召开专家研判会，对事件相关情况进行汇总研判。经查，百度公司网站的域名 baidu.com 是在美国域名注册服务商 register.com 公司注册的；综合各方提供的技术报告，与会专家分析认为，造成本次事件的原因是 baidu.com 域名的注册信息被非法篡改，致使 baidu.com 域名在全球的解析被错误指向，最终导致全球互联网用户无法正常访问 baidu.com 网站。

会上，工业和信息化部要求百度公司以此为鉴，高度重视域名安全，加强安全防护、监测预警、信息上报和应急处置，完善应急预案，避免此类事件再次发生。针对本次事件反映出的域名安全问题，CNCERT 建议重要信息系统部门和互联网企业，一方面要尽可能地使用.CN 域名作为主用域名，另一方面要在国内具备相应资质的域名注册服务机构中注册。

■ CNCERT 快速处置一批仿冒 CCTV 的钓鱼网站

2010 年 1 月底，CNCERT 接到举报，一些不法分子通过飞信、聊天工具以及垃圾邮件大量传播假冒央视“非常 6+1 栏目”的钓鱼网站信息，极易使用户受到蒙骗，造成经济损失。示例如：“恭喜您，非常 6+1 栏目小组正面向所有飞信用户举行砸金蛋抽奖活动，您的号码已被主持人李咏砸中成为幸运用户，您将获得由非常 6+1 栏目组提供的 X 万元奖金及手机，详情请登陆 www.cctv-2.vip2009.me 领取，验证码为×××××，咨询电话为 08988803×××”。 早在 2009 年 10 月，CNCERT 就专门处置过此类事件 。

由于此次事件发生时正值春节临近，不法分子借用“中奖”、“送礼品”等幌子进行网络欺诈的活动再次抬头。根据 CNCERT 掌握的情况，当时假冒“非常 6+1 栏目”的钓鱼网站多达数十个。针对上述情况，CNCERT 于 2010 年 1 月底组织协调万网志成和新网数码等国内域名注册商对监测发现的钓鱼网站域名再次开展专项清理行动，共关闭 27 个钓鱼网站，有效地打击了不法分子进行网络钓鱼的猖獗势头，保护了广大用户利益不受侵害。 同时，CNCERT 建议各单位在春节前夕加强宣传，提醒广大用户不要轻信各种形式的“中奖”消息，避免上当受骗。

■ 中美欧网络安全组织联手清除全球互联网大型僵尸网络

2010 年 2 月底，CNCERT 与美国微软公司以及欧美一些网络安全机构联手，成功打击一个名叫 Waledac 的全球大型僵尸网络。根据微软公司和其他研究机构的监测数据，Waledac 僵尸网络所使用的控制服务器大多位于德国、荷兰、瑞典和俄罗斯等欧洲国家，控制了全球数十万台计算机，预计每天能发出超过 15 亿封垃圾邮件。

由于 Waledac 僵尸网络的危害严重，微软公司除在美国通过法律诉讼途径暂时断开了僵尸网络控制服务器有关域名的互联网通信外，还协调中国和欧洲的网络安全机构开展同步处置。其中 2 月 26 日，微软公司请求 CNCERT 协助关闭 Waledac 僵尸网络所使用的部分在中国注册的域名。CNCERT 在进行技术验证后，依据我国应急处置体系的工作机制和有关管理办法，迅速采取行动，协调国内相关域名注册机构在数小时内就关闭了微软提供的全部 16 个恶意域名。

打击 Waledac 僵尸网络行动成功后，微软公司于 3 月 17 日向 CNCERT 发来了感谢信，“感谢 CNCERT 在打击 Waledac 僵尸网络中采取的迅速而果断的行动”，认为“CNCERT 的行动对整个打击行动获得成功非常重要”，并“期待将来开展更紧密的合作”。微软公司还在 3 月初于肯尼亚举办的第 37 届 ICANN 会议上发表演讲，感谢包括 CNCERT 在内的所有合作伙伴在打击 Waledac 僵尸网络中采取的快速及

时的行动。此次中美欧业界合作对僵尸网络问题采取的大胆积极行动，对净化国际互联网环境起到十分积极的作用，保护了广大网民的利益。

■ CNCERT 监测发现并处置“手机骷髅”病毒事件

2010 年 3 月，一款名为“手机骷髅”的病毒爆发，该病毒因为发送的彩信中包含一个骷髅头的图片而得名。“手机骷髅”主要感染 Symbian S60 系列第 3 版操作系统的手机，目前大量诺基亚和部分三星手机使用该系统。 感染该病毒的手机会在用户不知情的情况下，暗中联网且向手机通信录中的联系人大量群发带有病毒链接的彩信和短信。用户点击链接后会感染病毒，不仅会导致手机运行异常，频繁关机或重新启动，更为严重的是会导致用户手机因大量发送短信、彩信，而被收取高额费用。

对此，CNCERT 于 3 月 21 日发布紧急安全公告，并通过在中央电视台进行配图视频播发，广而告之。此外，CNCERT 还及时向工业和信息化部报告情况，并积极协调运营商和相关厂商进行处置。

■ CNCERT 协调韩国 CERT 组织处置基础电信运营企业受攻击事件

5 月底，CNCERT 与韩国安全组织 KrCERT 跨国联动，成功处置了一起针对我国运营商业务系统的网络攻击事件。

5 月 25 日，宁夏移动向 CNCERT 宁夏分中心投诉，称宁夏移动彩铃网站系统（nx.12530.com）遭受持续的恶意扫描。在短短一周内，针对目标系统的扫描次数就高达百万余次，对业务系统运营造成一定影响。CNCERT 在对攻击事件进行技术验证和数据分析后，发现恶意扫描数据包中大多数源 IP 地址位于韩国。对此，CNCERT 利用近年来建立的国际网络安全事件应急处置工作机制，紧急联系韩国 KrCERT，请其协助处置此次攻击事件。韩国 KrCERT 迅速响应，很快就协调其国内互联网运行单位对三个危害较大的攻击源 IP 进行了处置。5 月 26 日下午，针对宁夏移动彩铃网站系统的攻击趋缓，至 5 月 27 日攻击完全停止，系统业务运行恢复正常。

本次事件的成功处置再次表明，各国各地区安全组织加强网络安全协作，建立通畅的应急处置渠道，有助于应对当前日益严峻的网络安全威胁。

■ CNCERT 处置国外网络安全组织投诉的手机病毒事件

6 月中旬，CNCERT 分别收到诺基亚和芬兰 CERT 组织（CERT-FI）的报告，称发现针对 Symbian S60 系统的手机短信木马，并且相关恶意链接位于中国境内。

根据 CNCERT 对木马的技术分析，该木马会在用户不知情的情况下执行一些非法操作，如发送用户手机信息至一些不明网址。

此外，根据 F-Secure 公司的确认，该木马为 SymbOS/MerogoSMS 木马的变种，会影响 Symbian 60 系列第 3 版和第 5 版操作系统的手机。该木马通过中文手机短信传播，其中包括一个恶意链接。一旦用户点此链接，会立即安装一个应用。该木马会在手机启动时启动，并通过 GPRS 或 3G 尝试连接另外的恶意网址 http://rec[...]rzwxdsu.com，从而达到感染手机和重启短信服务的目的。卡巴斯基也在同一时间确认了该手机病毒。此外，在一段时间内的监测情况表明，该木马当时尚且仅限于在我国境内传播。根据上述情况，CNCERT 对涉嫌传播该手机恶意代码的网址进行了处理，并将相关情况向国外安全组织进行了及时反馈。

■ CNCERT 处置威胁工业控制系统的 Stuxnet 蠕虫事件

2010 年 7 月世界上出现了第一个有针对性的感染现实世界中工业控制系统的计算机蠕虫——Stuxnet，在国内被命名为“超级工厂”、“震网”、“双子”等。这个针对西门子公司的数据采集与监控系统 SIMATIC WinCC 进行攻击的超级蠕虫，由于攻击了伊朗布什尔核电站的工业控制设施并最终导致该核电站推迟发电，而引起了全球媒体的广泛关注。

CNCERT 高度重视该蠕虫的出现，组织中国反网络病毒联盟（ANVA）成员单位对之进行了深入分析并及时对我国感染情况进行监测。监测结果显示，Stuxnet 蠕虫在我国并没有出现大规模爆发的趋势，截止到 2010 年底，我国境内仅有 578 个 IP 被感染。尽管如此，在传统工业与信息技术的融合不断加深、传统工业体系的安全核心从物理安全向信息安全转移的趋势和背景下，此次 Stuxnet 蠕虫的爆发标志着全球网络信息安全进入一个新的时代。对此，CNCERT 通过官方网站以及中国反网络病毒联盟（ANVA）网站发布紧急安全公告，并将相关情况通报政府和重要信息系统部门，提出解决方案。

■ CNCERT 监测并处置“毒媒”手机病毒事件

9 月中旬，CNCERT 与 ANVA 成员单位——网秦公司联合监测发现一个名为“毒媒（DuMusicPlay）”的恶意代码在手机用户中大量传播。“毒媒”主要针对 Symbian S60 系统，会影响 Symbian S60 系列第 3 版和第 5 版操作系统的手机（诺基亚大部份智能手机都使用该操作系统）。CNCERT 监测发现，手机感染“毒媒”后，会自动连接互联网，向网上特定的控制服务器上传本机手机号、手机型号、IMEI 号码、IMSI 号码、信息中心号码等，同时会接受来自该服务器的指令，实现删除指定手

机软件的功能，包括关闭和删除各类手机杀毒软件。如果用户发现手机自动连接互联网，以及各类应用程序无法正常启动，手机程序卸载功能无法使用，那么就有可能已经感染该恶意代码。

CNCERT 监测结果显示，至 9 月中旬全国已经有近一百万部智能手机被该恶意代码所控制。对此，CNCERT 于 9 月 19 日在官方网站发布了 ANVA 安全公告，提醒用户警惕该恶意代码。随后，为了避免受控手机进一步遭受黑客侵害，CNCERT 协调相关域名注册服务机构对黑客使用的控制域名采取处置措施，并向运营商通报了“毒媒”的感染情况，将监测得到的已经感染该恶意代码的准确用户信息通过分中心提供给当地运营商进行处置。为了逃避监测，黑客在 11 月中旬对该恶意代码进行了一次大范围升级，并启用了几个新的控制域名，CNCERT 发现以后立刻对新的控制域名采取紧急处置措施，并再次发布安全公告。在各方的共同努力下，截至 2010 年底最后一周，CNCERT 监测到全国感染“毒媒”的用户数量下降至 17 万左右。

■ CNCERT 加大对银行网站、增值服务商相关的仿冒事件的处置力度

11 月中旬，CNCERT 监测发现我国台湾地区一个免费域名服务网站（二级域名为：163.to）通过域名指向跳转的方式，为数十个仿冒我国一些互联网增值服务商（如：新浪、腾讯、网易）的钓鱼网站提供跳转服务。在 CNCERT 监测发现的仿冒页面中，还有一些借广州亚运会的名义实施欺诈活动。为此，CNCERT 向台湾地区 CERT 组织——TWCERT 进行投诉，并提供了 43 个跳转域名的事件证据。TWCERT 及时响应，协调当地 ISP 移除了相关域名的跳转服务。

11 月底，CNCERT 监测发现涉及银行的网页仿冒事件日渐增多，对广大网银用户的财产安全构成直接威胁。为此，CNCERT 加大对网银仿冒类事件的处置力度。11 月最后一周，CNCERT 对涉及中国工商银行、中国农业银行等国内重要金融机构的 55 个仿冒网站进行集中处置。其中，有 5 个域名由国内域名注册服务商提供解析服务，CNCERT 在新网数码、万网志成等域名注册机构的大力协助下迅速进行清除；其余 50 个均为境外注册域名，CNCERT 通过协调 KrCERT（韩国 CERT）、US-CERT（美国 CERT）、Phishlab（国际反网络钓鱼组织）等国外网络安全机构及时有效地进行了治理。