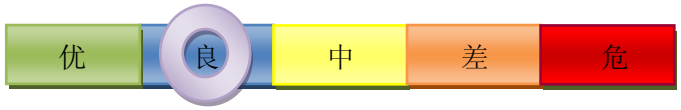
CNCERT互联网安全威胁报告

2011 年 2 月　　总第 2 期



摘要：

本报告以 CNCERT 监测数据和通报成员单位报送数据作为主要依据，对我国互联网面临的各类安全威胁进行总体态势分析，并对重要预警信息和典型安全事件进行探讨。

2011 年 2 月，互联网网络安全状况整体评价为良。主要数据如下：

- 境内感染网络病毒的终端数约为900万个；
- 境内被篡改网站数量为4796个，其中被篡改政府网站数量为288个；
- 国家信息安全漏洞共享平台（CNVD）收集整理信息系统安全漏洞398个，其中，高危漏洞155个，可被利用来实施远程攻击的漏洞有356个。

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

电子邮件：cncert@cert.org.cn

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

网址：http://www.cert.org.cn/

关于国家互联网应急中心（CNCERT）

国家互联网应急中心的全称是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 在我国大陆 31 个省、自治区、直辖市成立分中心，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 作为国家互联网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）共同处理互联网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，目前已具备对安全漏洞、恶意代码、网页篡改、网页挂马、拒绝服务攻击、域名劫持、路由劫持等各种网络威胁或攻击的监测发现能力。

- 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和与涉及国计民生的重要信息系统部门及执法机关密切合作机制实现网络安全事件的快速处置；同时作为国际著名网络安全合作组织 FIRST 和 APCERT 的重要成员，与多个世界著名的网络安全机构和各个国家级应急组织建立了网络安全事件处理合作机制。面向国内外用户受理网络安全事件报告，及时掌握和处置突发重大网络安全事件。

版权及免责声明

编者按：

感谢您阅读《CNCERT 互联网安全威胁报告》，如果您发现本报告存在任何问题，请您及时与我们联系，来信地址为：cncert@cert.org.cn。

本月网络安全基本态势分析

2011 年 2 月，互联网网络安全状况整体评价为良。我国互联网基础设施整体运行平稳，全国范围或省级行政区域内未发生造成较大影响的基础设施运行安全事件。针对政府、企业以及广大互联网用户的主要网络安全威胁来自于信息系统高危漏洞、恶意代码传播以及网站攻击。2 月 25 日至 26 日，为保障温家宝总理在线访谈活动的顺利进行，CNCERT 组织基础电信运营企业和域名注册服务机构开展了木马和僵尸网络专项清理行动。对控制规模较大的 709 个木马和僵尸网络恶意控制端 IP 和 154 个恶意 URL 进行了有效的清除，降低了总理在线访谈活动期间发生大规模网络攻击的风险。

根据 CNCERT 监测结果，我国境内木马受控主机数量略有增长，境内僵尸网络受控主机和网页篡改数量有所下降。根据通信行业报送的信息，本月网络安全事件报送总数量较上月减少。总体上，2 月公共互联网网络安全态势比上月略好，这与 2 月春节放假以及 CNCERT 组织开展专项清理等工作密切相关。

◆ 基础网络的运行安全

2011 年 2 月，我国互联网基础设施运行整体平稳，未出现全国或省级行政区域内造成较大影响的基础网络运行故障。针对境内互联网设施的主要网络攻击仍然是拒绝服务攻击。

◆ 公共互联网的网络安全

2011 年 2 月，根据 CNCERT 的监测数据和通信行业报送数据，全国公共互联网网络安全状况的主要指标情况如下：①网络病毒[1]活

注1：一般情况下，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。其中，网络病毒是特指有网络通信行为的恶意代码。2 月，CNCERT 在对网络病毒进行抽样监测时，调整了木马和僵尸网络的监测范围，监测范围总数为 177 种木马和 65 种僵尸网络。为保证数据的可比性，仍取近两月相同种类木马和僵尸网络的监测数据做环比分析。

动情况方面，境内感染网络病毒的终端数约为 900 万个，同种类网络病毒感染量较上月增长 3%；②网站安全方面，境内被篡改网站数量为 4796 个，较上月下降 14%，其中被篡改政府网站数量为 288 个，较上月的 337 个下降 15%，占境内被篡改网站比例由 6.02%减少到 6.01%；据各安全企业的报送情况，2 月份网页挂马情况总体上较上月好转，恶意代码的捕获数量呈下降趋势；③事件受理方面，CNCERT 接收到网络安全事件报告 887 件（不含扫描和垃圾邮件类事件[2]），数量较上月增长 23%。

◆ 网络病毒监测数据分析

2011 年 2 月，境内感染网络病毒的终端数约为 900 万个。其中，境内被木马或僵尸程序控制的主机 IP 约为 69 万个，同种类木马或僵尸程序感染量环比增长 17%；境内感染飞客蠕虫的主机 IP 约为 808 万个，环比增长 3%；境内感染“毒媒”手机病毒的用户约为 23 万个，环比下降 30%。

➢ *木马僵尸网络监测数据分析*

2011 年 2 月，CNCERT 监测发现境内 69 万余个 IP 地址对应的主机被木马或僵尸程序控制，按地区分布感染数量排名前三位的分别是广东、山东、江苏。

木马或僵尸网络控制服务器 IP 总数为 22100 个。其中，境内木马或僵尸网络控制服务器 IP 数量为 18181 个；境外木马或僵尸网络控制服务器 IP 数量为 3919 个，按国家或地区分布数量排名前三位的分别为美国、日本、韩国。

➢ *飞客蠕虫监测数据分析*

2011 年 2 月，CNCERT 监测到全球互联网约 4559 万个主机 IP 地址感染飞客蠕虫，按国家或地区分布感染数量排名前三位的

注2：因 CNCERT 一般不对扫描类事件和垃圾邮件类事件报告进行处置，故未做统计。对于垃圾邮件事件报告，CNCERT 直接转中国互联网协会反垃圾邮件中心处置。

分别是中国大陆、巴西、俄罗斯。

境内感染飞客蠕虫的主机 IP 约为 808 万个，按地区分布感染数量排名前三位的分别是广东、浙江、江苏。

➢ *恶意代码捕获和传播情况*

2011 年 2 月，CNCERT 通过多种渠道获得新增网络病毒名称数为 497 个，网络病毒家族数为 46 个。网络病毒主要通过网页挂马方式进行传播，其中往往需要利用黑客注册的大量域名。根据 CNCERT 对活跃恶意域名的分类跟踪，2011 年 2 月侵害境内网站和用户的恶意域名主要有以下几组，如表 1 所示。从下表可以看出，目前，侵害境内网站的恶意域名其注册商主要为境外机构。

表 1： 2011 年 2 月侵害境内网站的恶意域名组

组别	恶意域名组特征和数量描述
第一组	注册在 conna.dtdns.net、office.1s.fr、keccs.be.ma、3-a.net 等域上的恶意域名，主要用于构建恶意跳转链接，监测发现的三级域名数量数以百计。注册商为境外机构。
第二组	注册在 2288.org、3322.org、8800.org、8866.org、9966.org 等域上的恶意域名，被发现用于网页挂马的各个环节，如：恶意跳转链接、网页木马集成页面、漏洞触发页面以及恶意代码下载服务器，监测发现的三级域名数量数以百计。注册商主要为境内机构。
第三组	注册在 isgre.at 域上的恶意域名，三级域名命名呈现有规律的按字母顺序变换，用于构建恶意跳转链接，监测发现的三级域名数量数以百计。注册商为境外机构。
第四组	注册在.info 域上的恶意域名，用于构建恶意跳转链接，监测发现的三级域名数量数以十计。注册商为境外机构。

◆ 网站安全情况分析

➢ *境内网站被篡改情况*

2011 年 2 月，境内被篡改网站的数量为 4796 个，其中代号为“冰寒”、“s4r4d0” 和“Dirk”的攻击者对境内网站进行了大量篡

改。

境内被篡改网站数量按地区分布排名前三位的分别是江苏、北京、福建。按网站类型统计，被篡改数量最多的是.com 和.com.cn 域名类网站，其多为商业类网站；值得注意的是，被篡改的.gov.cn 域名类网站有 288 个，占境内被篡改网站的比例为 6.01%。

截至 2 月 28 日仍未恢复的部分被篡改政府网站[3]如表 2 所示。

表 2： 仍未恢复的部分政府网站

被篡改网站	所属部门或地区
gl.lzzjj.gov.cn	甘肃省兰州市
yd.lzzjj.gov.cn	甘肃省兰州市
yz.lzzjj.gov.cn	甘肃省兰州市
www.zhenyuan.gov.cn	贵州省黔东南自治州
al.yanlingagri.gov.cn	河南省许昌市
wt.yanlingagri.gov.cn	河南省许昌市
lxx.rc.gov.cn	湖南省郴州市
szw.rc.gov.cn	湖南省郴州市
gxjbz.gov.cn	江西省赣州市
www1.ganxian.gov.cn	江西省赣州市
gxka.ganxian.gov.cn	江西省赣州市
www.gxtc.gov.cn	江西省赣州市
www.nmzlt.gov.cn	内蒙古自治区通辽市
www.lszrsj.gov.cn	四川省凉山州
www.scms.gov.cn	四川省雅安市
www.yrjy.gov.cn	云南省楚雄州
nhcs.gov.cn	浙江省宁波市

➢ *境内网站被挂马情况*

根据 CNCERT 监测和通信行业报送数据，截至 2 月 28 日仍存在被挂马或被植入不正当广告链接（如：网络游戏、色情网站

注3：政府网站是指英文域名以“.gov.cn”结尾的网站，但不排除个别非政府部门也使用“.gov.cn”的情况。表格中仅列出了被篡改网站或被挂马网站的域名，而非具体被篡改或被挂马的页面 URL。

链接）的部分政府网站如表 3 所示。

表 3： 仍存在挂马的部分政府网站

被挂马网站	所属部门或地区
www.gzst.gov.cn	贵州省
www.zznj.gov.cn	河南省郑州市
www.weihaifda.gov.cn/	山东省威海市
www.sjly.gov.cn	上海市松江区
www.xjwh.gov.cn	新疆维吾尔自治区

◆ 网络安全的主要威胁

近期披露的一些严重安全漏洞是互联网所面临的主要安全威胁。2011 年 2 月，国家信息安全漏洞共享平台（CNVD[4]）收集整理信息系统安全漏洞 398 个。其中，高危漏洞 155 个，可被利用来实施远程攻击的漏洞有 356 个。受影响的软硬件系统厂商包括 Adobe、Cisco、Google、HP、IBM、Linux、Microsoft 、Oracle 等。

按照所涉及的软件类型，漏洞可分为操作系统漏洞、应用程序漏洞、WEB 应用漏洞、数据库漏洞、网络设备漏洞（如路由器、交换机等）和安全产品漏洞（如防火墙、入侵检测系统等）。本月 CNVD 收集整理的漏洞中，按漏洞类型分布排名前三位的分别是应用程序漏洞、操作系统漏洞、WEB 应用漏洞。

本月，域名解析服务器软件 BIND 9 部分版本被披露存在一个高危漏洞，可被利用发起远程拒绝服务攻击；此外，“Microsoft Active Directory 'BROWSER ELECTION'缓冲区溢出漏洞”和 “Sun Java 浮点值拒绝服务漏洞”影响较为严重，互联网上已经出现有关攻击代码，为避免受到漏洞影响，请广大用户及时采取补丁修复、提高主机操作系统安全防范等级等防御措施。

注4：CNVD 是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库，致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。

◆ 用户对网络安全事件的感知情况

2011 年 2 月，互联网用户感知最为强烈的事件是垃圾邮件事件和恶意代码事件。从中国互联网协会反垃圾邮件中心报送数据看，其 2 月共接收 11737 件垃圾邮件事件举报；从 CNCERT 接收国内外投诉事件情况看，恶意代码事件占 42%。

本月网络安全事件接收与处理情况

◆ 事件接收情况

2011 年 2 月，CNCERT 收到国内外通过电子邮件、热线电话、网站提交、传真等方式报告的网络安全事件 887 件（合并了通过不同方式报告的同一网络安全事件，且不包括扫描和垃圾邮件类事件），其中来自国外的事件报告有 234 件。

在 887 件事件报告中，排名前三位的安全事件分别是漏洞、恶意代码、网页仿冒。

◆ 事件处理情况

对国内外通过电子邮件、热线电话、传真等方式报告的网络安全事件，以及自主监测发现的网络安全事件，CNCERT 每日根据事件的影响范围和存活性、涉及用户的性质等因素，筛选重要事件进行协调处理。

2011 年 2 月，CNCERT 总部以及各省分中心共同协调处理了 756 件网络安全事件。各类事件处理数量中漏洞和恶意代码类事件处理数量较多，本月网页仿冒和网页篡改类事件也是处置的重点。

◆ 本月网络安全重点事件

CNCERT 开展木马和僵尸网络专项清理行动

2 月 25 日至 26 日，为保障温家宝总理在线访谈活动的顺利进行，CNCERT 组织基础电信运营企业中国电信、中国联通、中国移动以及域名注册服务机构希网网络、新网数码、广东时代互联、新网互联、万网等单位开展了木马和僵尸网络的专项清理行动。行动中，CNCERT 共对控制规模较大的 709 个木马和僵尸网络恶意控制端 IP 和 154 个恶意 URL 进行了有效的清除。清除行动实施后，CNCERT 监测捕获的木马和僵尸网络恶意控制端数量较前几日出现较大幅度下降，有效降低了总理在线访谈活动期间发生大规模网络攻击的风险。

域名系统软件 BIND 9 存在远程拒绝服务漏洞

2 月下旬，CNCERT 获知互联网上应用广泛的域名解析服务器软件 BIND 9.7.1、9.7.2 版本存在一个高危漏洞，可被利用发起远程拒绝服务攻击。依托国家信息安全漏洞共享平台（CNVD），CNCERT 及时对漏洞进行了跟踪分析，认为该漏洞可能对国内众多采用相应版本软件的域名服务器构成较为严重的威胁。CNCERT 提醒使用相应版本软件作为域名服务器的用户做好防范工作，一是建议使用受漏洞影响 BIND 版本的用户做好软件更新及相关应用部署工作，二是可临时在系统启动时使用参数“-n 1”，即强制域名服务器使用单线程处理所有数据，避开带有攻击意图的域名请求。

协调处置涉及期货、证券、政府、高校等重要单位的恶意代码事件

2 月 1 日，CNCERT 监测发现归属某期货公司的主机感染了恶意程序并被利用作木马网络控制端，频繁与木马受控主机进行通信；同时还发现分别归属于某证券公司、某市信息服务网及在京两所著名高校的 4 个 IP 感染木马和僵尸程序，被恶意远程控制。CNCERT 及时将上述事件向相关管理部门进行了通报，建议其尽快切断上述主机的网络连接并及时进行全面清理。

协调处置某知名域名注册机构遭拒绝服务攻击事件

2 月 3 日，CNCERT 接到某知名域名注册机构的投诉，称该公司某服务器持续遭受大规模的拒绝服务攻击，对该公司的域名解析服务业务构成严重影响。经调查分析，发现该事件是一起典型的通过非授权修改域名解析指向而导致的攻击转嫁事件，事件起因是游戏私服间的相互争斗。在查明事件因原后，CNCERT 协调域名注册机构新网数码、新网互联、三五互联与中国万网等公司对恶意域名进行了清理，有效消除了攻击。

协调处置马来西亚通讯与多媒体管理委员会遭受恶意扫描事件

2 月 18 日，CNCERT 接到马来西亚通讯与多媒体管理委员会投诉，称我国某主机利用 DCOM RPC 缓冲区溢出漏洞对其服务器进行扫描并尝试性攻击。经验证核实，CNCERT 通过河南分中心协调当地基础电信运营企业对参与攻击的主机进行了清理。

协调处置仿冒加拿大税务总局、中国银行、中国农业银行、中国邮政储蓄银行、深圳发展银行等的钓鱼事件

2 月中旬，CNCERT 接到加拿大网络事件响应中心（CCIRC)举报，称一位于我国的服务器对加拿大税务总局网站进行仿冒，非法采集用户个人信息，对公众隐私安全构成威胁。经验证核实，CNCERT 协调接入服务商北京中电华通通信有限公司对仿冒页面进行了有效的清除。

2 月，CNCERT 对自主监测和投诉受理工作中发现的十多起仿冒国内银行网站的钓鱼事件进行了处理，分别涉及中国银行、中国农业银行、中国邮政储蓄银行、深圳发展银行等国内多家银行机构。这些钓鱼网站使用了 www.boccnh.com 、 www.bocgq.com 、www.abchinq.com、www.pswc.tk、www.sdbck.com 等极具迷惑性的域名，个别还辅以假冒银行名义向用户发送短信提醒的方式实施欺诈。CNCERT 协调有关域名的注册机构新网互联、新网数码、江苏邦宁，及国外域名注册机构 DOT TK 和 NETEARTH ONE 依法暂停了仿冒域名的解析服务，降低了上述银行网银用户的财产安全风险。

附：术语解释

- 信息系统（Information System）

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（Vulnerability）

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（Malicious Code）

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[5]、网银木马[6]、窃密木马[7]、远程控制木马[8]、流量劫持木马[9]、下载者木马[10]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

注5：盗号木马是用于窃取用户电子邮箱、网络游戏等账号的木马。

注6：网银木马是用于窃取用户网银、证券等账号的木马。

注7：窃密木马是用于窃取用户主机中敏感文件或数据的木马。

注8：远程控制木马是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。

注9：流量劫持木马是用于劫持用户网络浏览的流量到攻击者指定站点的木马。

注10：下载者木马是用于下载更多恶意代码到用户主机并运行，以进一步操控用户主机的木马。

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（Denial of Service）

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（Website Distortion）

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（Phishing）

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（Website Malicious Code）

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（Spam）

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（DNS Hijack）

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（Unauthorized Access）

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（Routing Hijack）

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。