



CNCERT互联网安全威胁报告

2011 年 1 月

总第 1 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 1 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874万个；
- 境内被篡改网站数量为5596个，其中被篡改政府网站数量为337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洞406个。其中，高危漏洞101个，可被利用来实施远程攻击的漏洞有352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

《CNCERT 互联网安全威胁报告》(以下简称“报告”)为国家计算机网络应急技术处理协调中心(简称国家互联网应急中心, CNCERT 或 CNCERT/CC)的电子刊物,由 CNCERT 编制并拥有版权。报告中凡摘录或引用内容均已指明出处,其版权归相应单位所有。本报告所有权利及许可由 CNCERT 进行管理,未经 CNCERT 同意,任何单位或个人不得将本报告以及其中内容转发或用于其他用途。

CNCERT 力争保证本报告的准确性和可靠性,其中的信息、数据、图片等仅供参考,不作为您个人或您企业实施安全决策的依据, CNCERT 不承担与此相关的一切法律责任。

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 1 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，影响较大的事件主要是 1 月 13 日 17 时至 20 时因厦门易名网络科技有限公司 DNS 服务器遭受大规模拒绝服务攻击，导致通过其进行域名解析的大量网站业务受到影响。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。

根据 CNCERT 监测结果，我国境内僵尸网络受控主机数量略有增长，境内木马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，本月公共互联网环境中网络安全事件报送数量总体呈现上升趋势，主要集中在各地通信管理局和基础电信运营企业报送的计算机病毒事件、蠕虫事件、木马和僵尸网络事件等方面，这说明通信行业加大了对公共互联网的安全监测和环境的治理。总体上，1 月公共互联网网络安全态势比上月份略好，各单位应重点关注一些对本单位信息系统运行可能构成较大威胁或可能造成较大影响的事件信息和预警信息，如：桌面操作系统和应用软件漏洞。

◆ 基础网络的运行安全

2011 年 1 月，我国互联网基础设施运行整体平稳，1 月 13 日 17 时至 20 时因厦门易名网络科技有限公司 DNS 服务器遭受大规模拒绝服务攻击，导致通过其进行域名解析的大量网站业务受到影响。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 1 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活动情况方面，境内感染网络病毒的终端数约为 874 万个；②网站安全方面，境内被篡改网站数量为 5596 个，其中被篡改政府网站数量为 337 个，占境内被篡改网站比例为 6.02%；据各安全企业的报送情况，1 月份网页挂马情况总体上较上月有所好转，但对恶意代码的捕获情况各不相同；③事件受理方面，CNCERT 接收到网络安全事件报告 723 件（不含扫描和垃圾邮件类事件²）。

◆ 网络病毒监测数据分析

2011 年 1 月，境内感染网络病毒的终端数约为 874 万个。其中，境内被木马或僵尸程序控制的主机 IP 约为 57 万个；境内感染飞客蠕虫的主机 IP 约为 785 万个；境内感染“毒媒”手机病毒的用户约为 33 万个。

➤ 木马僵尸网络监测数据分析

2011 年 1 月，CNCERT 监测发现境内 57 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、浙江。

木马或僵尸网络控制服务器 IP 总数为 29863 个。其中，境内木马或僵尸网络控制服务器 IP 数量为 22795 个；境外木马或僵尸网络控制服务器 IP 数量为 7068 个，按国家或地区分布数量排名前三位的分别为印尼、美国、日本。

➤ 飞客蠕虫监测数据分析

2011 年 1 月，CNCERT 监测到全球互联网约 4559 万个主机

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。1 月，CNCERT 在对网络病毒进行抽样监测时，对 153 种木马和 57 种僵尸程序进行了监测。

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。

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 785 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 1 月，CNCERT 通过多种渠道获得新增网络病毒名称数为 1425 个，网络病毒家族数为 253 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 1 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 1 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 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以数百计。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以数百计。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以数十计。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以数十计。注册商为境外机构。
第五组	注册在 25u.com 域外的恶意域名，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以数十计。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 1 月，境内被篡改网站的数量为 5596 个，其中代号为“soojoy”、“Cracker-Mr.X”和“冰寒”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 337 个，占境内被篡改网站的比例为 6.02%。

截至 1 月 31 日仍未恢复的部分被篡改政府网站³如表 2 所示。

表 2：仍未恢复的重要政府网站

被篡改网站	所属部门或地区
shangbao.ahjt.gov.cn	安徽省
zhuanjia.ahjt.gov.cn	安徽省
aqtj.gov.cn	安徽省安庆市
oa.tlinfo.gov.cn	安徽省铜陵市
www.xmgh.gov.cn	福建省厦门市
www.pxdjw.gov.cn	广西自治区凭祥市
www.dq12333.gov.cn	黑龙江省大庆市
www.hgqx.gov.cn	湖北省黄冈市
www.qjgt.gov.cn	湖北省潜江市
czzradio.gov.cn	湖南省郴州市
jjpc.yyjt.gov.cn	湖南省岳阳市
www.msaonline.gov.cn	江苏省南京市
www.pjdj.gov.cn	辽宁省盘锦市
smeqd.gov.cn	山东省青岛市

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。

➤ 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 1 月 31 日仍存在被挂马或被植入不正当广告链接（如：网络游戏、色情网站链接）的部分政府网站如表 3 所示。

表 3：仍存在挂马的重要政府网站

被挂马网站	所属部门或地区
www.lggs.gov.cn	广东省深圳市
www.jnarchives.gov.cn	四川省成都市
jddpc.gov.cn	浙江省建德市

◆ 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 1 月，国家信息安全漏洞共享平台（CNVD⁴）收集整理信息系统安全漏洞 406 个。其中，高危漏洞 101 个，可被利用来实施远程攻击的漏洞有 352 个。受影响的软硬件系统厂商包括 Apple、Cisco、Google、IBM、Linux、Microsoft、Mozilla、OpenOffice、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、网络设备漏洞。

根据 CNVD 的代码验证结果，本月共出现了 66 个 0day 漏洞，其中影响较为严重的是“Microsoft Windows MHTML 脚本代码注入漏洞”和“Kingsoft Antivirus 'KisKrn.sys' 驱动拒绝服务漏洞”，互联网上已经出现针对上述漏洞的攻击代码，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。

本月，CNVD 对北京亚控科技有限公司生产的工业系统管理监控

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。

软件 KingView 6.5.3 存在的一个高危漏洞进行了分析验证，并协调亚控公司对漏洞提供了修复补丁。分析结果表明，利用该漏洞可获得用户主机权限，进而对相关工业控制系统的运行安全构成严重威胁。建议有关用户采取如下防范措施：(1)及时下载亚控公司发布的安全补丁，对系统进行加固；(2)对网络加强管理，尽可能地将与工业控制系统相关的管理控制主机与互联网隔离。

◆ 用户对网络安全事件的感知情况

2011 年 1 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 1 月共接收 13212 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 29%。

本月网络安全事件接收与处理情况

◆ 事件接收情况

2011 年 1 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 723 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 170 件。

在 723 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 1 月，CNCERT 总部以及各省分中心共同协调处理了 610 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

协调处置境外投诉拒绝服务攻击事件

1 月 13 日，CNCERT 接到亚太网络安全组织 APCERT 投诉，称位于我国大陆的某主机向境外的某重要网络设施持续发起拒绝服务攻击，该主机极有可能被黑客控制。接收到事件投诉后，CNCERT 及时响应，通过主机 IP 所在地区分中心——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。

协调处置中科院重点实验室网页挂马事件

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代码（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，就会被恶意代码所感染。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。目前，该网站已暂行关闭并在整改中。

协调处置仿冒苏格兰皇家银行、中国银行、德国邮政银行的钓鱼事件

1月18日，CNCERT接到国外网络安全组织投诉，称在我国注册的、域名为rbstrade.com的网站对苏格兰皇家银行网站进行仿冒，实施钓鱼欺诈，对用户账户安全构成严重威胁。经验证核实，CNCERT协调该域名的注册机构万网公司依法暂停了对仿冒域名的解析服务。

1月24日，CNCERT接到用户投诉，称域名为www.boceed.com的网站对中国银行网站进行仿冒，实施钓鱼欺诈，对中国银行网银用户的资金安全构成严重威胁。经验证核实，CNCERT协调该域名的注册机构新网互联公司依法暂停了对仿冒域名的解析服务。

1月30日，CNCERT接到国外网络安全组织投诉，称在我国注册的多个域名被利用于对德国邮政银行进行网页仿冒攻击。该事件中，仿冒域名较多且域名所有者信息具有明显的集团化、组织化特征，对该行客户的资产安全构成了严重威胁。经验证核实，CNCERT迅速协调上述域名的注册机构新网互联公司依法暂停了对仿冒域名的解析服务。

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。