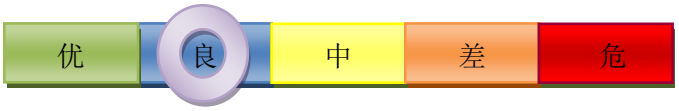
CNCERT互联网安全威胁报告

2014 年 4 月　　总第 40 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。

2014 年 4 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为345万余个；
- 境内被篡改网站数量为13526个，其中被篡改政府网站数量为579个；境内被植入后门的网站数量为4357个，其中政府网站有157个；针对境内网站的仿冒页面数量为1836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洞686个，其中，高危漏洞225个，可被利用来实施远程攻击的漏洞有635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是国家计算机网络应急技术处理协调中心的简称（英文简称为 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，为非政府非盈利的网络安全技术中心，是我国网络安全应急体系的核心协调机构。

2003 年，CNCERT 在全国 31 个省（直辖市、自治区）成立分中心。作为国家级应急中心，CNCERT 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

CNCERT 的业务能力如下：

事件发现——依托“863-917 公共互联网网络安全监测平台”，开展对基础信息网络、金融证券等重要信息系统、移动互联网服务提供商、增值电信企业等安全事件的自主监测。同时还通过与国内外合作伙伴进行数据和信息共享，以及通过热线电话、传真、电子邮件、网站等接收国内外用户的网络安全事件报告等多种渠道发现网络攻击威胁和网络安全事件。

预警通报——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，为用户单位提供互联网网络安全态势信息通报、网络安全技术和资源信息共享等服务。

应急处置——对于自主发现和接收到的危害较大的事件报告，CNCERT 及时响应并积极协调处置，重点处置的事件包括：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、涉及重要政府部门和重要信息系统的事件、用户投诉造成较大影响的事件，以及境外国家级应急组织投诉的各类网络安全事件等。

测试评估——作为网络安全检测、评估的专业机构，按照“支撑监管，服务社会”的原则，以科学的方法、规范的程序、公正的态度、独立的判断，按照相关标准为政府部门、企事业单位提供安全评测服务。CNCERT 还组织通信网络安全相关标准制定，参与电信网和互联网安全防护系列标准的编制等。

同时，作为中国非政府层面开展网络安全事件跨境处置协助的重要窗口，CNCERT 积极开展国际合作，致力于构建跨境网络安全事件的快速响应和协调处置机制。CNCERT 为国际著名网络安全合作组织 FIRST 正式成员以及亚太应急组织 APCERT 的发起人之一。截至 2013 年，CNCERT 已与 59 个国家和地区的 127 个组织建立了“CNCERT 国际合作伙伴”关系。

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

2014 年 4 月，互联网网络安全状况整体评价为良。我国基础网络运行总体平稳，互联网骨干网各项监测指标正常，未发生较大以上网络安全事件。在我国互联网网络安全环境方面，除捕获的新增恶意代码文件数量、境内被篡改网站数量和被植入后门的网站数量较上月有所下降外，其他各类网络安全事件数量均有不同程度的增长。总体上，4 月公共互联网网络安全态势较上月略有恶化，但评价指数仍在良的区间。

◆ 基础网络安全

2014 年 4 月，我国基础网络运行总体平稳，互联网骨干网各项监测指标正常，未出现省级行政区域以上的造成较大影响的基础网络运行故障，未发生较大以上网络安全事件，但存在一定数量的流量不大的针对互联网基础设施的拒绝服务攻击事件。

◆ 重要联网信息系统安全

政府网站和金融行业网站仍然是不法分子攻击的重点目标，安全漏洞是重要联网信息系统遭遇攻击的主要内因。本月，监测发现境内被篡改政府网站数量为 579 个，较上月的 602 个下降 3.8%，占境内被篡改网站的比例由 4.4%减少到了 4.3%；境内被植入后门的政府网站数量为 157 个，较上月的 246 个下降 36.2%，占境内被植入后门网站的比例由 4.1%减少到了 3.6%；针对境内网站的仿冒页面数量为 1836 个，较上月的 1794 个增长 2.3%，这些仿冒页面绝大多数是仿冒我国金融机构和著名社会机构。

本月，国家信息安全漏洞共享平台（CNVD[1]）共协调处置了 412

注1：CNVD 是 CNCERT 联合国内重要信息系统单位、基础电信企业、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。

起涉及我国政府部门以及银行、民航等重要信息系统部门以及电信、传媒、公共卫生、教育等相关行业的漏洞事件。这些事件大多数是网站程序存在 SQL 注入、弱口令以及权限绕过等漏洞，也有部分是信息系统采用的应用软件存在漏洞，可能导致获取后台系统管理权限、信息泄露、恶意文件上传等危害，甚至会导致主机存在被不法分子远程控制的风险。此外，“Nagios Remote Plugin Executor 'nrpe.c'远程代码执行漏洞”、“Xerox DocuShare'dsweb/ResultBackgroundJobMultiple/' SQL 注入漏洞”、“Sendy '/send-to' SQL 注入漏洞”、“Bluetooth Text Chat for iOS 特制蓝牙消息远程代码执行漏洞”等 0day 漏洞影响较为严重，互联网上已经出现针对上述漏洞的攻击代码。

◆ 公共网络环境安全

2014 年 4 月，根据 CNCERT 的监测数据和通信行业报送数据，我国互联网网络安全环境主要指标情况如下：网络病毒[2]活动情况方面，境内感染网络病毒的终端数为 345 万余个，较上月增长 17.5%；在捕获的新增网络病毒文件[3]中，按网络病毒名称[4]统计新增 89 个，较上月下降 29.4%，按网络病毒家族[5]统计新增 13 个，较上月下降 77.6%[6]；各安全企业报送的网络病毒捕获数量中，瑞星公司截获的病毒数量较上月下降 28.6%，新增病毒数量较上月下降 65.7%；安天公司捕获的样本总数较上月下降 48.3%，新增病毒种类较上月下降

注2：一般情况下，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。4 月，CNCERT 在对恶意代码进行抽样监测时，对 405 种木马家族和 65 种僵尸程序家族进行了抽样监测。

注3：网络病毒文件是网络病毒的载体，包括可执行文件、动态链接库文件等，每个文件都可以用哈希值唯一标识。

注4：网络病毒名称是通过网络病毒行为、源代码编译关系等方法确定的具有相同功能的网络病毒命名，完整的命名一般包括：分类、家族名和变种号。一般而言，大量不同的网络病毒文件会对应同一个网络病毒名称。

注5：网络病毒家族是具有代码同源关系或行为相似性的网络病毒文件集合的统称，每个网络病毒家族一般包含多个变种号区分的网络病毒名称。

注6：4 月，CNCERT 调整了对新增恶意代码的监测规则。

56.2%；金山公司报送的计算机病毒事件数量较上月下降 7.4%。网站安全方面，本月境内被篡改网站数量为 13526 个，较上月下降 2.3%；境内被植入后门的网站数量为 4357 个，较上月下降 27.0%；针对境内网站的仿冒页面有 1836 个，较上月增长 2.3%；各安全企业报送的网页挂马情况中，浪潮公司报送的网页挂马事件数量较上月增长 0.9%，安天公司报送的网页挂马事件数量较上月增长 50.0%，奇虎 360 公司报送的网页挂马事件数量较上月增长 4.9%。安全漏洞方面，本月 CNVD 共收集整理信息系统安全漏洞 686 个，较上月增长 6.2%。其中高危漏洞 225 个，较上月增长 5.1%；可被利用来实施远程攻击的漏洞有 635 个，较上月增长 4.3%。垃圾邮件方面，从中国互联网协会垃圾邮件受理举报中心报送数据看，本月共接收 7801 件垃圾邮件事件举报，较上月下降 5.2%。事件受理方面，CNCERT 接收到网络安全事件报告 3916 件，较上月增长 11.6%，数量最多的分别是漏洞类事件 1468 件、网页仿冒类事件 1065 件。

本月重点网络安全信息

◆ 关于 OpenSSL 存在高危漏洞可被利用发起大规模攻击的情况通报

4 月 8 日， CNVD 对 OpenSSL 存在的一个内存信息泄露高危漏洞进行分析，该漏洞与 OpenSSL TLS/DTLS 传输层安全协议扩展组件(RFC6520)相关，存在于 ssl/dl_both.c 文件的心跳部分(heartbeat)。当攻击者向服务器发送一个特殊构造的数据包，可导致内存存储数据输出。远程攻击者可以利用漏洞读取存在相关服务器内存中多达 64K 字节的数据。根据上述过程，漏洞在互联网上被称为“heartbleed bug”，中文名称叫做“心脏出血”、“击穿心脏”等。

OpenSSL 是一款开放源码的 SSL 服务软件，用来实现网络通信的加密和认证。由于 OpenSSL 应用极为广泛，包括政府、高校网站以及金融证券、电子商务、网上支付、即时聊天、办公系统、邮件系统等诸多服务提供商均受到漏洞影响，直接危及互联网用户财产和个人信息安全。CNVD 组织完成的多个测试实例表明，根据对应 OpenSSL 服务器承载业务类型，攻击者一般可获得用户 X.509 证书私钥、实时连接的用户账号密码、会话 Cookies 等敏感信息，进一步可直接取得相关用户权限，窃取私密数据或执行非授权操作。

目前，OpenSSL 官方发布的 1.0.1g 版本已修复该漏洞。为防范可能的攻击，建议网站服务提供商及时下载升级。互联网用户应注意网上应用（包括手机 APP）安全风险，如发现网银证书、账号和密码被非法使用、篡改的情况，应及时向服务商或 CNVD 报告。

本月网络安全主要数据

◆ 网络病毒监测数据分析

2014 年 4 月，境内感染网络病毒的终端数为 345 万余个。其中，境内被木马或僵尸程序控制的主机 IP 为 211 万余个，环比增长 6.2%；境内感染飞客蠕虫的主机 IP 为近 134 万个，环比增长 41.1%。

➢ *木马僵尸网络监测数据分析*

2014 年 4 月，CNCERT 监测发现境内 211 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省、湖南省、江苏省。

木马或僵尸网络控制服务器 IP 总数为 9,817 个。其中，境内木马或僵尸网络控制服务器 IP 数量为 6,038 个，按地区分布数量排名前三位的分别为广东省、云南省、江苏省。境外木马或僵尸网络控制服务器 IP 数量为 3,779 个，主要分布于美国、中国香港、韩国。其中，位于美国的控制服务器控制了境内 932,445 个主机 IP，控制境内主机 IP 数量居首位，其次是位于葡萄牙和芬兰的 IP 地址，分别控制了境内 911,151 个和 149,386 个主机 IP。

➢ *飞客蠕虫监测数据分析*

2014 年 4 月，CNCERT 监测到全球互联网 1314 万余个主机 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分别是中国大陆、印度、巴西。

境内感染飞客蠕虫的主机 IP 为近 134 万个，按地区分布感染数量排名前三位的分别是广东省、江苏省、浙江省。

➢ *网络病毒捕获和传播情况*

2014 年 4 月，CNCERT 捕获了大量新增网络病毒文件，其中按网络病毒名称统计新增 89 个，按网络病毒家族统计新增 13 个。

网络病毒主要针对一些防护比较薄弱,特别是访问量较大的网站通过网页挂马的方式进行传播。当存在安全漏洞的用户主机访问了这些被黑客挂马的网站后，会经过多级跳转暗中连接黑客最终“放马”的站点下载网络病毒。2014 年 4 月，CNCERT 监测发现排名前十的活跃放马站点域名和活跃放马站点 IP 如表 1 所示。

表 1： 2014 年 4 月活跃放马站点域名和 IP

排序	活跃放马站点域名	排序	活跃放马站点 IP
1	down.yinyue.fm	1	122.224.9.35
2	twtwtwtwtwt.org	2	60.190.218.136
3	icq.liukejun.com	3	115.47.44.107
4	idq.liukejun.com	4	121.10.104.34
5	dx2.xiazaiba.com	5	121.10.104.39
6	up.chaoqingxi.net	6	222.186.57.218
7	kunbang.yinyue.fm	7	220.161.209.177
8	soft.tai69.com	8	61.153.110.177
9	update.ie9000.com	9	61.164.241.70
10	qvodplay.44kk.org	10	61.164.154.250

网络病毒在传播过程中，往往需要利用黑客注册的大量域名。2014 年 4 月，CNCERT 监测发现的放马站点中，通过域名访问的共涉及有 186 个域名，通过 IP 直接访问的共涉及有 80 个 IP。在 186 个放马站点域名中，于境内注册的域名数为 73 个（约占 39.2%），于境外注册的域名数为 111 个（约占 59.7%），未知注册商属地信息的有 2 个（约占 1.1%）。放马站点域名所属顶级域名排名前 5 位的具体情况如表 2 所示。

表 2： 2014 年 4 月活跃恶意域名所属顶级域名

排序	顶级域名（TLD）	类别	恶意域名数量
1	.COM	通用顶级域名（gTLD）	126
2	.CN	中国顶级域名（ccTLD）	19
3	.NET	通用顶级域名（gTLD）	19
4	.ORG	通用顶级域名（gTLD）	9
5	.CC	通用顶级域名（gTLD）	6

◆ 网站安全数据分析

➢ *境内网站被篡改情况*

2014 年 4 月，境内被篡改网站的数量为 13526 个，境内被篡改网站数量按地区分布排名前三位的分别是北京市、上海市、浙江省。按网站类型统计，被篡改数量最多的是.COM 域名类网站，其多为商业类网站 ;值得注意的是 ,被篡改的.GOV 域名类网站有 579 个，占境内被篡改网站的比例为 4.3%。

截至 4 月 30 日仍未恢复的部分被篡改政府网站[7]如表 3 所示。

表 3： 截至 4 月 30 日仍未恢复的部分政府网站

被篡改网站	所属部门或地区
ahjzmz.gov.cn	安徽省六安市
hssjj.gov.cn	安徽省马鞍山市
lbrk.gov.cn	安徽省宿州市
www.tdjyw.gov.cn	广西壮族自治区百色市
wxny.gov.cn	广西壮族自治区来宾市
zzd.tour.dl.gov.cn	辽宁省大连市
wsfw.jcgaj.gov.cn	辽宁省葫芦岛市
www.jxjtw.gov.cn	山东省日照市

注7：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。

被篡改网站	所属部门或地区
www.jxfg.gov.cn	山东省日照市
jce.gov.cn	云南省大理白族自治州
hh.gov.cn	云南省红河哈尼族彝族自治州

➢ *境内网站被植入后门情况*

2014 年 4 月，境内被植入后门的网站数量为 4357 个。境内被植入后门的网站数量按地区分布排名前三位的分别是北京市、江苏省、广东省。按网站类型统计，被植入后门数量最多的是.COM 域名类网站，其多为商业类网站；值得注意的是，被植入后门的.GOV 域名类网站有 157 个，占境内被植入后门网站的比例为 3.6%。

2014 年 4 月，境外 3194 个 IP 地址通过植入后门对境内 3658 个网站实施远程控制。其中，境外 IP 地址主要位于美国、中国香港和韩国等国家或地区。从境外 IP 地址通过植入后门控制境内网站数量来看，位于阿根廷的 IP 地址共向境内 702 个网站植入了后门程序，入侵网站数量居首位，其次是位于中国香港和美国的 IP 地址，分别向境内 528 个和 528 个网站植入了后门程序。

➢ *境内网站被仿冒情况*

2014 年 4 月，CNCERT 共监测到针对境内网站的仿冒页面有 1836 个，涉及域名 1406 个，IP 地址 524 个，平均每个 IP 地址承载近 4 个仿冒页面。在这 524 个 IP 中，境外占 88.0%，主要位于美国和中国香港。

◆ 漏洞数据分析

2014 年 4 月，CNVD 收集整理信息系统安全漏洞 686 个。其中，高危漏洞 225 个，可被利用来实施远程攻击的漏洞有 635 个。受影响的软硬件系统厂商包括 Advantech、Apple、Cisco、Google、IBM、Juniper、Microsoft、Oracle、WordPress、ZyXEL 等。

根据 CNVD 的代码验证结果，本月共出现了 132 个 0day 漏洞，

其中影响较为严重的是“Nagios Remote Plugin Executor 'nrpe.c'远程代码执行漏洞”、“Xerox DocuShare'dsweb/ResultBackgroundJobMultiple/' SQL 注入漏洞”、“Sendy '/send-to' SQL 注入漏洞”、“Bluetooth Text Chat for iOS 特制蓝牙消息远程代码执行漏洞”等。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。

根据漏洞影响对象的类型，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、WEB 应用漏洞、网络设备漏洞。

◆ 网络安全事件接收与处理情况

➢ *事件接收情况*

2014 年 4 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 3916 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 106 件。

在 3916 件事件报告中，排名前三位的安全事件分别是漏洞、网页仿冒、网页篡改。

➢ *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。

2014 年 4 月，CNCERT 总部以及各省分中心共同协调处理了 3893 件网络安全事件。各类事件处理数量中漏洞、网页仿冒类事件处理数量较多。

附：术语解释

- 信息系统

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

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。

- 恶意程序

恶意程序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。恶意程序分类说明如下：

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[8]、网银木马[9]、窃密木马[10]、远程控制木马[11]、流量劫持木马[12]、下载者木马[13]和其它木马七类。

2. 僵尸程序（Bot）

   僵尸程序是用于构建大规模攻击平台的恶意代码。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

注8：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9：网银木马是用于窃取用户网银、证券等账号的木马。

注10：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11：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12：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13：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。

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。

- 僵尸网络

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木马或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。

- 拒绝服务攻击

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

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

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

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。

- 网站后门

网站后门事件是指黑客在网站的特定目录中上传远程控制页面从而能够通过该页面秘密远程控制网站服务器的攻击事件。

- 垃圾邮件

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

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

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

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。