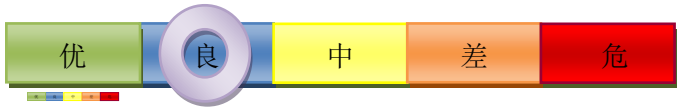
# CNCERT互联网安全威胁报告

## 2016 年 2 月　　总第 62 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。

2016 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为194万余个；
- 境内被篡改网站数量为5,744个，其中被篡改政府网站数量为87个；境内被植入后门的网站数量为4,298个，其中政府网站有123个；针对境内网站的仿冒页面数量为7,481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洞559个，其中，高危漏洞160个，可被利用来实施远程攻击的漏洞有491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“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。截止 2015 年，CNCERT 与 66 个国家和地区的 165 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

2016 年 2 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，除境内木马或僵尸程序控制服务器 IP 地址数目和境内感染木马或僵尸程序的 IP 地址数目较上月有所增长外，其他各类网络安全事件数量均有不同程度的下降。总体上，2 月公共互联网网络安全态势较上月有所好转，评价指数在良的区间。

## ◆ 基础网络安全

2016 年 2 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 87 个，较上月的 112 个下降 22.3%，占境内被篡改网站的比例由 1.8%下降到 1.5%；境内被植入后门的政府网站数量为 123 个，较上月的 335 个下降 63.3%，占境内被植入后门网站的比例由 4.0%下降到了 2.9%；针对境内网站的仿冒页面数量为 7,481 个，较上月的 14,938 个下降 49.9%，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 1,354

注1：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。

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，“LEADTOOLS ActiveX control DLL 加载任意代码执行漏洞”、“Comodo Chromodo 同源策略安全绕过漏洞”、“Buffalo LinkStation 420 拒绝服务漏洞”、“Ipswitch MOVEit DMZ 和 MOVEit Mobile 文件读取漏洞”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

2016 年 2 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 194 万余个，较上月下降 34.4%；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 62 个，较上月下降 17.3%；按网络病毒家族[5]统计新增 11 个，较上月增长 57.1%；各安全企业报送的恶意代码捕获数量中，瑞星公司截获的病毒数量较上月下降 13.0%，新增病毒数量较上月下降 73.7%；安天公司捕获的样本总数较上月下降 12.9%，新增病毒种类较上月下降 36.1%；猎豹移动报送的计算机病毒事件数量较上月下降 13.3%。网站安全方面，

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。2 月，CNCERT 在对恶意代码进行抽样监测时，对 524 种木马家族和 74 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。

本月境内被篡改网站数量为 5,744 个，较上月下降 9.7%；境内被植入后门的网站数量为 4,298 个，较上月下降 48.6%；针对境内网站的仿冒页面有 7,481 个，较上月下降 49.9%；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 3.6%，奇虎 360 公司报送的网页挂马事件数量较上月下降 33.3%。安全漏洞方面，本月 CNVD 共收集整理信息系统安全漏洞 559 个，较上月下降 17.6%。其中高危漏洞 160 个，较上月下降 5.9%；可被利用来实施远程攻击的漏洞有 491 个，较上月下降 14.8%。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 4,890 件垃圾邮件事件举报，较上月下降 36.9%。事件受理方面，CNCERT 接收到网络安全事件报告 8,034 件，较上月下降 41.2%，数量最多的分别是网页仿冒类事件 3,342 件、漏洞类事件 1,968 件。

# 本月重点网络安全信息

## ◆ 中国互联网网络安全威胁治理联盟成立 互联网网络安全威胁治理行动效果显著

2016 年 2 月 26 日，国家互联网应急中心（以下简称“CNCERT”）联合中国互联网协会网络与信息安全工作委员会在京召开互联网网络安全威胁治理行动（以下简称“行动”）总结大会，对行动所取得的积极成果予以总结，并对行动过程中表现突出的单位进行了表彰。为巩固行动取得的成果，建立互联网网络安全威胁治理长效机制，大会宣布成立“中国互联网网络安全威胁治理联盟”（以下简称“联盟”），首批共 90 家企业申请加入联盟。

行动自 2015 年 7 月 31 日启动以来，举全行业之力，通过投诉举报、情报共享、威胁认定、协同处置、信息发布等多项措施环环相扣，取得了显著治理效果。互联网黑产已经成为影响我国互联网正常有序运行的重要原因之一，如博彩或私服等网站链接通过向政府网站或知名网站植入暗链提高网络搜索排名，通过采用拒绝服务攻击（以下简称“DDoS 攻击”）对竞争对手发起网络攻击导致网络不能正常提供服务等。此次行动重点针对 DDoS 攻击、网页篡改等与互联网黑产密切相关的事件进行重点处置。行动期间共接到广大网民举报的网络安全事件 109972 起，处置网络安全事件 71220 起，发布黑名单地址 54614 条。DDoS 攻击事件次数由行动启动前的日均 1491 起下降到现在的日均 265 起，大幅下降 82.2%；境内被篡改网站相比行动启动前下降 21.4%，其中被篡改政府网站相比下降了 56.2%。此次行动直面互联网黑产背后存在巨大的利益链条，不惧触动链条上利益群体，行动参与单位排除顾虑，积极行动，对于发现的网上 DDoS 攻击售卖和传播等互联网黑产行为进行了坚决处置。

大会对行动过程中表现突出的 31 家单位进行了表彰，号召受表

彰单位充分发挥带头和模范作用，带动行业内企业发挥各自作用，坚决维护我国网络安全。会上，部分行动参与单位受邀发言，均表示积极参与联盟的有关工作，切实落实企业责任。

最后，会上讨论通过了联盟章程，公布首批联盟成员单位名单，联盟成员单位主要由境内的基础电信企业、非经营性互联单位、域名注册服务机构、互联网和安全企业、IDC、应用商店等覆盖安全产业链上下游的企业组成。该联盟的成立，提供了一个行业内公共沟通交流的平台，联盟以行业自律为主导，联合网络安全领域上下游各方面力量，充分发挥联盟成员单位作用，加强互联网网络安全威胁情报共享、相互协作，对与互联网黑产密切相关的各类威胁进行整治，有效净化网络安全环境，维护用户网络安全和利益，树立我国负责任网络大国的良好形象。

### ◆ 通报安卓短信蠕虫病毒处置情况

2 月 15 日， CNCERT 接到投诉，一款通过短信传播的安卓蠕虫病毒大量传播。该蠕虫病毒伪装成“检查更新”APP，通过伪基站或者手机肉鸡以短信方式进行传播，短信内容为“XXX，新年好。相片已经放到这上了 t.cn/RGfj6iM”。用户点击链接后，该病毒即运行并私自读取用户通讯录，向联系人发送带有蠕虫病毒下载地址的恶意短信，诱骗联系人感染。通过对病毒下载地址的域名进行溯源分析，发现该域名注册人名下还有 7 个用于传播安卓恶意程序的域名。CNCERT 立即启动针对该恶意代码的处置工作，协调多家域名注册商对以上恶意域名进行停止解析处理，切断了恶意程序的传播途径 CNCERT 第一时间对该批恶意域名进行处置，有效控制了恶意程序的影响范围。

### ◆ 通报 OpenSSL 加密算法破解漏洞

2 月，国家信息安全漏洞共享平台（CNVD）收录了 OpenSSL 存在的加密算法破解漏洞（CNVD-2016-00711，对应 CVE-2016-0701）。

远程攻击者可利用该漏洞，获取加密密钥，并发起后续攻击，获得用户的敏感信息。

OpenSSL 是一个实现安全套接层和安全传输层协议的通用开源加密库，可支持多种加密算法，包括对称密码、哈希算法、安全散列算法等。OpenSSL 存在一处加密算法破解漏洞，但是该漏洞需要同时满足以下条件：OpenSSL 版本为 1.0.2-1.0.2e；依赖于 openssl 的应用程序的签名算法生成的临时密钥必须基于 Diffie Hellman 密钥交换算法。默认情况下，由于服务器会重复使用相同的临时密钥，这使得服务器容易受到密钥覆盖攻击。当满足上述条件后，攻击者可以通过服务器发送大量的握手请求，当有足够多的计算数据完成后，攻击者可以获取部分密钥值，并结合其结果与中国剩余定理最终推导出解密密钥。 CNVD 对该漏洞的综合评级为“高危”。

目前，厂商已发布了 1.0.2f 版本修复该漏洞，CNVD 建议相关用户及时下载使用，避免引发漏洞相关的网络安全事件。

### ◆ 通报 Cisco ASA Software IKE 密钥交换协议缓冲区溢出漏洞

2 月，国家信息安全漏洞共享平台（CNVD）收录了 Cisco ASA Software IKE 密钥交换协议缓冲区溢出漏洞（CNVD-2016-00929，对应 CVE-2016-1287）。攻击者利用漏洞可致网络设备重载或远程代码执行，进而可获取目标系统的控制权限，构成信息泄露和运行安全风险。

Cisco ASA 是一款自适应安全设备，可提供安全和 VPN 服务的模块化平台，可提供防火墙、IPS、anti-X 和 VPN 服务。由于 Cisco ASA Software 分段协议中的 IKE 网络密钥交换算法存在设计缺陷，IKEv1 及 IKEv2 代码中存在缓冲区溢出漏洞。未经身份验证的远程攻击者利用漏洞发送特制的 UDP 数据包到受影响系统，可致设备重载或远程代码执行，进而可获取到目标系统的完整控制权。CNVD 对该漏洞的综合评级为“高危”，且对应的安全威胁 CVSS 基准评分为 10 分（最高分即为 10 分）。

目前，互联网上已披露针对漏洞利用原理的详细分析（暂未出现公开的攻击利用代码），厂商已发布了安全公告修复该漏洞。CNVD 建议相关用户及时下载更新，避免引发漏洞相关的网络安全事件，特别是国内电信和互联网行业以及重要行业单位注意排查本单位使用的上述设备列表情况。

### ◆ 通报 GNU glibcgetaddrinfo()堆栈缓冲区溢出漏洞

2 月，国家信息安全漏洞共享平台（CNVD）收录了 GNU glibcgetaddrinfo()堆栈缓冲区溢出漏洞（CNVD-2016-01100，对应 CVE-2015-7547）。攻击者利用漏洞可通过构建恶意 dns 服务或使用中间人的方法对受害者发起攻击，对 Linux 终端设备构成安全威胁。

GNU glibc 是一款按 LGPL 许可协议发布的开源 C 语言编译程序，是 Linux 操作系统中 C 库的实现。glibc 中 getaddrinfo 函数在处理特定 dns response 数据包时存在栈溢出漏洞。由于 glibc 通过 alloca()函数在栈中为_nss_dns_gethostbyname4_r 函数 2048 字节的空间，用于托管 DNS 响应；若响应大于 2048 字节，程序会从堆中重新分配一个缓冲区，并更新所有信息（缓冲区指针，缓冲区大小和响应大小）；在一定条件下，会出现栈缓冲区和新分配的堆内存的错误匹配，导致超过栈缓冲区大小的响应仍然存储在栈中，进而发生缓冲区溢出。攻击者利用漏洞可通过构建恶意 dns 服务或使用中间人攻击的方法对 Linux 主机或相关设备发起攻击，导致远程代码执行，进而可获取用户终端控制权。CNVD 对该漏洞的综合评级为“高危”。

目前，互联网上已披露针对该漏洞的利用原理分析及利用代码。厂商暂未发布升级补丁修复该漏洞，CNVD 建议用户采取如下临时措施：该漏洞存在于 resolv/res_send.c 文件中，当 getaddrinfo()函数被调用时会触发该漏洞，技术人员可以通过将 TCP DNS 响应的大小限制为 1024 字节，并丢弃所有超过 512 字节的 UDP DNS 数据包来缓解该问题。

# 本月网络安全主要数据

## ◆ 网络病毒监测数据分析

2016 年 2 月，境内感染网络病毒的终端数为 194 万余个。其中，境内 135 万余个 IP 地址对应的主机被木马或僵尸程序控制，与上月的近 216 万个相比下降 37.2%；境内近 59 万个主机 IP 感染“飞客”蠕虫，与 1 月的 80 余万个相比下降 26.8%。

### ➢ *木马僵尸网络监测数据分析*

2016 年 2 月 ,境内 135 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、山东省、江苏省。

木马或僵尸网络控制服务器 IP 总数为 9,296 个。其中，境内木马或僵尸网络控制服务器 IP 数量为 3,827 个 ,按地区分布数量排名前三位的分别为广东省、江苏省、北京市。境外木马或僵尸网络控制服务器 IP 数量为 5,469 个，主要分布于美国、日本、韩国。其中，位于美国的控制服务器控制了境内 302,147 个主机 IP，控制境内主机 IP 数量居首位，其次是位于韩国和澳大利亚的 IP 地址，分别控制了境内 82,972 个和 69,870 个主机 IP。

### ➢ *飞客蠕虫监测数据分析*

2016 年 2 月，CNCERT 监测到全球互联网近 495 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分别是中国大陆、印度、俄罗斯。

境内感染飞客蠕虫的主机 IP 为近 59 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*

2016 年 2 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 62 个，按网络病毒家族统计新增 11 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。2016 年 2 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： 2016 年 2 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 | down01.kuaibu8.com | 1 | 192.3.205.142 |
| 2 | 192.3.205.142 | 2 | 192.3.205.142 |
| 3 | www.go890.com | 3 | 183.60.106.54 |
| 4 | 183.60.106.54 | 4 | 192.240.106.77 |
| 5 | 192.240.106.77 | 5 | 221.11.84.131 |
| 6 | dh.3515.info | 6 | 58.158.177.102 |
| 7 | xiazai.51jetso.com | 7 | 183.131.83.222 |
| 8 | icq.liukejun.com | 8 | 117.23.6.67 |
| 9 | idq.liukejun.com | 9 | 117.23.6.63 |
| 10 | url.goosai.com | 10 | 117.23.6.68 |

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。2016 年 2 月，CNCERT 监测发现的放马站点中，通过域名访问的共涉及有 290 个域名，通过 IP 直接访问的共涉及有 598 个 IP。在 290 个放马站点域名中，于境内注册的域名数为 155 个（约占 53.4%），于境外注册的域名数为 113 个（约占 39.0%），未知注册商属地信息的有 22 个（约占 7.6%）。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： 2016 年 2 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） | 199 |
| 2 | .CN | 国家顶级域名（ccTLD） | 29 |
| 3 | .NET | 通用顶级域名（gTLD） | 25 |

| | | | |
|---|---|---|---|
| 4 | .RU | 通用顶级域名（gTLD） | 6 |
| 5 | .CLUB | 国家顶级域名（ccTLD） | 6 |

## ◆ 网站安全数据分析

### ➢ *境内网站被篡改情况*

2016 年 2 月，境内被篡改网站的数量为 5,744 个，境内被篡改网站数量按地区分布排名前三位的分别是广东省、北京市、福建省。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 87 个，占境内被篡改网站的比例为 1.5%。

截至 2 月 29 日仍未恢复的部分被篡改政府网站[6]如表 3 所示。

表 3： 截至 2 月 29 日仍未恢复的部分政府网站

| 被篡改网站 | 所属部门或地区 |
|---|---|
| ahcgw.ahinfo.gov.cn | 安徽省合肥市 |
| bhtz.gov.cn | 天津市 |

### ➢ *境内网站被植入后门情况*

2016 年 2 月，境内被植入后门的网站数量为 4,298 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广东省、北京市、江苏省。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 123 个，占境内被植入后门网站的比例为 2.9%。

2016 年 2 月，境外 2,568 个 IP 地址通过植入后门对境内 3,488 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

注6：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。

和俄罗斯等国家或地区。从境外 IP 地址通过植入后门控制境内网站数量来看，来自俄罗斯的 IP 地址共向境内 692 个网站植入了后门程序，入侵网站数量居首位；其次是来自美国和乌克兰的 IP 地址，分别向境内 430 个和 426 个网站植入了后门程序。

### ➢ *境内网站被仿冒情况*

2016 年 2 月，CNCERT 共监测到针对境内网站的仿冒页面有 7,481 个，涉及域名 6,723 个，IP 地址 1,201 个，平均每个 IP 地址承载 6 余个仿冒页面。在这 1,201 个 IP 中，92.2%位于境外，主要位于中国香港和美国。

## ◆ 漏洞数据分析

2016 年 2 月，CNVD 收集整理信息系统安全漏洞 559 个。其中，高危漏洞 160 个，可被利用来实施远程攻击的漏洞有 491 个。受影响的软硬件系统厂商包括 Adobe、Cisco、Drupal、Google、IBM、Linux、Microsoft、Mozilla、WordPress 等。

根据 CNVD 的代码验证结果，本月共出现了 63 个 0day 漏洞,其中影响最严重的是“LEADTOOLS ActiveX control DLL 加载任意代码执行漏洞”、“Comodo Chromodo 同源策略安全绕过漏洞”、“Buffalo LinkStation 420 拒绝服务漏洞”、“Ipswitch MOVEit DMZ 和 MOVEit Mobile 文件读取漏洞”。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、操作系统漏洞、WEB 应用漏洞。

## ◆ 网络安全事件接收与处理情况

### ➢ *事件接收情况*

2016 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 8,034 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 11 件。

在 8,034 件事件报告中，排名前三位的安全事件分别是网页仿冒、漏洞、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。

2016 年 2 月，CNCERT 以及各省分中心共同协调处理了 7,632 件网络安全事件。各类事件处理数量中网页仿冒、漏洞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[7]、网银木马[8]、窃密木马[9]、远程控制木马[10]、流量劫持木马[11]、下载者木马[12]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7：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8：网银木马是用于窃取用户网银、证券等账号的木马。

注9：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10：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11：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12：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。

- 移动互联网恶意程序

在用户不知情或未授权的情况下，在移动终端系统中安装、运行以达到不正当目的，或具有违反国家相关法律法规行为的可执行文件、程序模块或程序片段。