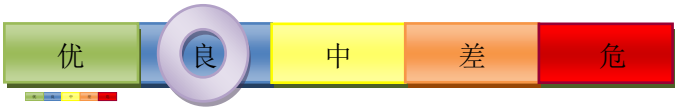
CNCERT互联网安全威胁报告

2017 年 5 月　　总第 77 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。

2017 年 5 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159万余个；
- 境内被篡改网站数量为6,245个，其中被篡改政府网站数量为145个；境内被植入后门的网站数量为4,916个，其中政府网站有228个；针对境内网站的仿冒页面数量为1,696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洞1399个，其中，高危漏洞543个，可被利用来实施远程攻击的漏洞有1226

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 2016 年，CNCERT 与 69 个国家和地区的 185 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

2017 年 5 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，除境内感染飞客蠕虫的 IP 地址数量、境内被篡改网站的总数和仿冒境内网站的页面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，5 月公共互联网网络安全态势较上月有所恶化，但评价指数在良的区间。

◆ 基础网络安全

2017 年 5 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，监测发现境内政府网站被篡改的数量为 145 个，与上月的 194 个相比下降 25.3%，占境内被篡改网站的比例由 3.1%下降到 2.3%；境内政府网站被植入后门的数量为 228 个，与上月的 200 个相比增长 14.0%，占境内被植入后门网站的比例由 5.1%下降到 4.6%；针对境内网站的仿冒页面数量为 1,696 个，较上月的 1,810 个下降 6.3%，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 1289

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。

◆ 公共网络环境安全

2017 年 5 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 159 万余个，较上月增长 10.8%；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 4 个，较上月下降 60.0%；按恶意代码家族[5]统计新增 1 个，较上月下降 66.7%；移动互联网恶意程序累计传播次数近 1 万次；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 7.7%，新增病毒数量较上月增长 19.7%；安天公司捕获的样本总数较上月增长 3.2%，新增病毒种类较上月下降 9.6%；猎豹移动报送的计算机病毒事件数量较上月增长 58.7%。网站安全方面，本月境内被篡改网站数量为 6,245 个，较上月下降 1.1%；境内被植入后门的网站数量为 4,916 个，较上月增长 24.8%；针对境内网站的仿冒页面有 1,696 个，较上月下降 6.3%；各安全企业报送的网页挂马情况中，奇虎 360 公司报

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 530 种木马家族和 80 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：恶意代码家族是具有代码同源关系或行为相似性的恶意代码文件集合的统称，每个恶意代码家族一般包含多个变种号区分的恶意代码名称。

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 1399 个，较上月增长 9.4%。其中高危漏洞 543 个，较上月增长 13.8%；可被利用来实施远程攻击的漏洞有 1226 个，较上月增长 6.1%。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 7,147 件垃圾邮件事件举报，较上月下降 36.1%。事件受理方面，CNCERT 接收到网络安全事件报告 8,580 件，较上月增加了 11.4%，数量最多的分别是漏洞类事件 2,772 件、网页仿冒类事件 1,765 件。

本月重点网络安全信息

◆ 2017 中国网络安全年会在青岛召开

5 月 22 日—24 日，以“融合促进发展　协作共建安全”为主题的 2017 中国网络安全年会在青岛召开。本次大会由工业和信息化部指导，国家互联网应急中心（CNCERT）和中国通信学会联合主办。来自政府和重要信息系统、企业、行业协会、高校和科研院所等单位以及来自 CNCERT 国际合作伙伴的代表共九百余人参加了大会。工业和信息化部党组成员、副部长陈肇雄，山东省副省长王书坚出席大会并致辞。

陈肇雄指出，当前，以互联网为代表的新一代信息技术迅猛发展、加快普及、广泛应用，在支撑经济转型、推动社会进步、深化人文交流、消弭数字鸿沟等方面发挥了积极作用。同时，也带来了一些新问题、新挑战，尤其是，网络安全威胁和风险日益突出，并加快向政治、经济、文化、社会、生态、国防等领域传导渗透，成为世界各国面临的共同难题。

陈肇雄表示，我国高度重视网络安全工作。习近平总书记就网络安全工作发表了系列重要讲话，对加强网络空间国际合作，共建网络空间命运共同体提出重要倡议。国家陆续出台了《网络安全法》、《国家网络空间安全战略》和《网络空间国际合作战略》等法律、战略和规划，对网络安全工作作出系统部署。陈肇雄就进一步做好网络安全工作提出四点要求：一是提高认识，切实增强维护网络安全的紧迫感；二是加强创新，不断突破网络安全核心关键技术；三是协同联动，推动形成网络安全保障工作合力；四是开放合作，共同应对网络安全威胁。

王书坚指出，山东省始终高度重视网络安全工作，着力提升互联网网络安全技术手段及大数据分析能力，扎实开展打击电信诈骗专项行动，采取多种形式持续开展互联网网络安全威胁治理行动，有效防

范处置各类网络安全隐患。维护网络安全成为事关国家安全、国家主权和人民群众合法权益等重大问题。正如习近平总书记指出的那样，网络安全为人民，网络安全靠人民，维护网络安全是全社会共同责任，需要政府、企业、社会组织、广大网民共同参与，共筑网络安全防线。同时，维护网络安全迫切需要在核心技术上取得突破，大力发展、积极使用自主可控的技术和产品，争取实现弯道超车，掌握互联网发展主动权，保障互联网安全、国家安全。

青岛市市长孟凡利，工程院院士王恩东，工业和信息化部相关司局、有关单位负责同志一同出席会议。大会为期共 3 天，共 5 个分论坛，同期还举办了 2017 中国网络安全技术对抗赛、第二届 CNCERT 国际合作论坛、网络安全企业领袖高峰论坛，并开展了网络安全防护专题培训。

◆ 中国-东盟网络安全应急响应能力建设研讨会在青岛举行

2017 年 5 月 22 日至 24 日，中国-东盟网络安全应急响应能力建设研讨会在青岛举行。本次研讨会由工业和信息化部主办，国家计算机网络应急技术处理协调中心承办。来自柬埔寨、印度尼西亚、老挝、缅甸、菲律宾、泰国、越南等东盟国家信息通信主管部门和国家级 CERT 组织的近 20 名代表参加研讨会。国家计算机网络应急技术处理协调中心主任黄澄清,工业和信息化部国际合作司副司长刘子平，印度尼西亚国家级 CERT 组织 ID-SIRTII/CC 副主席 Muhammad Salman Saefuddin 在研讨会开幕式上致辞。

本次研讨会是 2016 年在文莱举办的第十一次中国 - 东盟电信部长会议确定的重要合作项目之一，主要聚焦于提高中国和东盟的网络安全应急响应能力。与会代表就国家网络安全新挑战、网络安全业界合作和技术培训等议题进行了广泛深入交流，会议期间，东盟代表还应邀参加了 2017 中国网络安全年会、第二届 CNCERT 国际合作论坛暨 FIRST 技术研讨会。东盟代表表示，本次会议议题设置丰富、各方交流充分，对于双方进一步开展务实合作具有重要意义。

◆ 大数据分析与网络安全的化学反应——2017 中国网络安全技术对抗赛在青岛落下帷幕

2017 年 4 月 20 日至 2017 年 5 月 22 日，在工业和信息化部指导下，国家互联网应急中心（CNCERT/CC）举办了 2017 中国网络安全技术对抗赛（赛事官方网站：http://contest.cert.org.cn）。这是国家互联网应急中心第四次举办此项国内顶级水平的网络安全赛事。

本次比赛与前三届攻防对抗赛的形式不同，采用了新的赛制赛题形式，通过网络安全数据分析的比赛形式，选定“被黑和钓鱼网站分析”、“网站后门行为分析”、“网络攻击溯源分析”、“漏洞攻击和恶意代码通信报文分析”等四个典型安全场景，联合国内多家知名安全企业提供的来源于一线业务系统和生产场景的网络安全监测大数据，面向全国优秀数据科学人才与网络安全人才征集优秀解决方案，着力解决当前大数据背景下的网络安全攻击威胁分析、溯源、判定等应用问题。

最终，“观安-无相实验室”队获得一等奖(奖金五万元)，“极地社”队和“云堤”队获得二等奖(奖金两万元)，“Gtensor“队、“黄埔江畔”队以及“sh4d0w”队获得三等奖(奖金一万元)，“生活充满节奏感”队、“老铁来调参”队、“BUPT_901”队以及“广州阿戈比特”队获得优胜奖(奖金一万元)。

本次比赛得到了上海交通大学、科赛网、奇虎 360、天融信、阿里云、知道创宇、安恒信息、微步在线、白帽汇、永信至诚、启明星辰、绿盟科技等业内单位的技术支持，融汇了安全业界的精华数据。今后，国家互联网应急中心将继续举办此类数据分析赛事，不断丰富赛题类型、完善比赛赛制、提高比赛技术性与观赏性，进一步促进数据科学技术在网络安全领域的应用，为网络安全技术人才和数据科学人才提供思想碰撞，交流学习的平台。

◆ 关于警惕“影子经纪人”事件系列漏洞威胁的预警通报

北京时间 5 月 12 日，全球互联网遭受 Wannacry 勒索软件蠕虫感染。截止 17 日 16 时，CNCERT 监测发现全球近 356.3 万个 IP 地址遭受“永恒之蓝”SMB 漏洞攻击，其中位于我国境内的 IP 地址数量接近 12.5 万个，对我国互联网造成严重的安全威胁。综合 CNCERT 和国内网络安全企业已获知的样本情况和分析结果，该勒索软件蠕虫在传播时基于 445 端口并利用 SMB 漏洞（对应微软漏洞公告：MS17-010），可以判断是由于“影子经纪人”（Shadow Brokers）组织此前公开披露漏洞攻击工具而导致的后续勒索软件蠕虫攻击。

2017 年 4 月 14 日晚，“影子经纪人”组织在互联网上发布“方程式”（Equation Group）组织的部分工具文件，包含针对 Windows 操作系统以及其他办公、邮件软件的多个高危漏洞攻击工具，这些工具集成化程度高、部分攻击利用方式较为高效。针对可能引发的互联网上针对 Window 操作系统主机或应用软件的大规模攻击，4 月 16 日，CNCERT 主办国家信息安全漏洞共享平台（CNVD）发布《关于加强防范 Windows 操作系统和相关软件漏洞攻击风险的情况公告》（访问链接：http://www.cnvd.org.cn/webinfo/show/4110）。时隔不到一个月，Wannacry 勒索软件蠕虫大范围感染事件也印证了当时推测的严重危害。

针对“影子经纪人”发布的黑客使用的大量针对 Windows 操作系统以及其他广泛应用的软件产品的工程化工具及其对应的利用安全漏洞，CNCERT 进行了详细梳理，并提供相应处置建议，提醒广大互联网用户及时做好应急处置，避免被恶意攻击或利用。

◆ 关于一种蠕虫式勒索病毒的风险提示

据境内外媒体报道，近日一种新型的勒索病毒在全球范围内发作，在工业和信息化部指导下，我中心立即组织进行了研判。经研判，确实是一款新型病毒从 5 月 12 日起在全球范围传播扩散，已影响到包括我国用户在内的多个国家的用户。该勒索病毒利用 Windows 操

作系统 445 端口存在的漏洞进行传播，并具有自我复制、主动传播的特性。勒索病毒感染用户计算机后，将对计算机中的文档、图片等实施高强度加密，并向用户勒索赎金。 在此提醒广大用户及时采取如下措施进行防范：

一、及时升级 Windows 操作系统，目前微软公司已发布相关补丁程序 MS17-010，可通过微软公司正规渠道进行升级。

二、安装并及时更新杀毒软件。

三、不要轻易打开来源不明的电子邮件。

四、及时关闭计算机、网络设备上的 445 端口。

五、定期在不同的存储介质上备份计算机上的重要文件。

本月网络安全主要数据

◆ 网络病毒监测数据分析

2017 年 5 月，境内感染网络病毒的终端数为 159 万余个。其中，境内 105 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 89 万个相比增长 18.7% ,境内近 54 万个主机 IP 感染“飞客”蠕虫，与 4 月的近 55 万个相比下降 1.9%。

➢ *木马僵尸网络监测数据分析*

2017 年 5 月 ,境内 105 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、浙江省、江苏省。

木马或僵尸网络控制服务器 IP 总数为 27,514 个。其中，境内木马或僵尸程序控制服务器 IP 有 16,206 个，按地区分布数量排名前三位的分别为安徽省、浙江省、江苏省。境外木马或僵尸程序控制服务器 IP 有 11,308 个，主要分布于美国、韩国、英国。其中，位于美国的控制服务器控制了境内 406,706 个主机 IP，控制境内主机 IP 数量居首位，其次是位于中国台湾和中国香港的 IP 地址，分别控制了境内 181,906 个和 52,781 个主机 IP。

➢ *飞客蠕虫监测数据分析*

2017 年 5 月，CNCERT 监测到全球互联网近 294 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 54 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*

2017 年 5 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 4 个，网络病毒家族统计新增 1 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。2017 年 5 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： 2017 年 5 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	www.go890.com	1	183.60.106.54
2	cl.xzqxzs.com	2	120.26.127.170
3	down.nxwb.net	3	61.133.192.170
4	nc-dl.wdjcdn.com	4	106.37.238.1
5	i.kpzip.com	5	36.42.32.220
6	cl.gxjsxq.com	6	117.23.6.67
7	dl.wandoujia.com	7	117.23.6.64
8	dl.cdn.wandoujia.com	8	222.28.152.177
9	idq.liukejun.com	9	221.230.141.238
10	icq.liukejun.com	10	117.23.6.63

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。2017 年 5 月，CNCERT 监测发现的放马站点中，通过域名访问的共涉及有 3687 个域名，通过 IP 直接访问的共涉及有 167 个 IP。在 3687 个放马站点域名中，于境内注册的域名数为 3650 个（约占 99.0%），于境外注册的域名数为 35 个（约占 0.9%），未知注册商属地信息的有 2 个（约占 0.1%）。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： 2017 年 5 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	.NET	通用顶级域名（gTLD）	3564
2	.COM	通用顶级域名（gTLD）	109
3	.CN	国家顶级域名（ccTLD）	7

4	.INFO	通用顶级域名（gTLD）	2
5	.TV	通用顶级域名（gTLD）	1

◆ 网站安全数据分析

➢ *境内网站被篡改情况*

2017 年 5 月，境内被篡改网站的数量为 6,245 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、河南省、北京市。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 145 个，占境内被篡改网站的比例为 2.3%。

截至 5 月 31 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 5 月 31 日仍未恢复的部分政府网站

被篡改网站	所属部门或地区
www.ybdj.gov.cn	吉林省延边市
xxzx.ahxx.gov.cn	安徽省宿州市

➢ *境内网站被植入后门情况*

2017 年 5 月，境内被植入后门的网站数量为 4,916 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、河南省。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 228 个，占境内被植入后门网站的比例为 4.6%。

2017 年 5 月，境外 2,502 个 IP 地址通过植入后门对境内 4,916 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

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。

量来看，来自俄罗斯的 IP 地址共向境内 621 个网站植入了后门程序，入侵网站数量居首位；其次是来自中国香港和美国的 IP 地址，分别向境内 466 个和 386 个网站植入了后门程序。

➢ *境内网站被仿冒情况*

2017 年 5 月，CNCERT 共监测到针对境内网站的仿冒页面有 1,696 个，涉及域名 1,360 个，IP 地址 486 个，平均每个 IP 地址承载 3 余个仿冒页面。在这 486 个 IP 中，95.1%位于境外，主要位于中国香港和美国。

◆ 漏洞数据分析

2017 年 5 月，CNVD 收集整理信息系统安全漏洞 1399 个。其中，高危漏洞 543 个，可被利用来实施远程攻击的漏洞有 1226 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、操作系统漏洞。

◆ 网络安全事件接收与处理情况

➢ *事件接收情况*

2017 年 5 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 8,580 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 19 件。

在 8,580 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、恶意程序。

➢ *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。

2017 年 5 月，CNCERT 以及各省分中心共同协调处理了 8,709 件网络安全事件。各类事件处理数量中漏洞、恶意程序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。