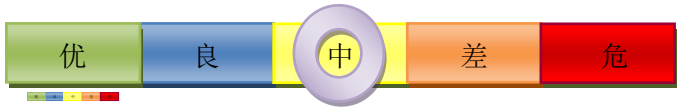
CNCERT互联网安全威胁报告

2016 年 5 月　　总第 65 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 5 月，互联网网络安全状况整体评价为中。主要数据如下：

- 境内感染网络病毒的终端数为近300万个；
- 境内被篡改网站数量为5,629个，其中被篡改政府网站数量为155个；境内被植入后门的网站数量为30,216个，其中政府网站有847个；针对境内网站的仿冒页面数量为27,734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洞888个，其中，高危漏洞306个，可被利用来实施远程攻击的漏洞有779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 5 月，互联网网络安全状况整体评价为中。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、漏洞报告数量和垃圾邮件举报总数较上月有所增长外，其他各类网络安全事件数量均有不同程度的下降。总体上，5 月公共互联网网络安全态势较上月有所恶化,但评价指数在中的区间。

◆ 基础网络安全

2016 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，监测发现境内被篡改政府网站数量为 155 个，较上月的 176 个下降 11.9%，占境内被篡改网站的比例由 2.7%上升到 2.8%；境内被植入后门的政府网站数量为 847 个，较上月的 619 个增长 36.8%，占境内被植入后门网站的比例由 5.0%下降到了 2.8%；针对境内网站的仿冒页面数量为 27,734 个，较上月的 12,209 个增长 127.2%，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 2,558

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，“PowerFolder 远程代码执行漏洞”、“Adobe Flash 任意代码执行漏洞”、“Google Chrome pdfium 堆内存错误引用漏洞”、“Foxit Reader PDF 解析内存破坏漏洞” 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 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近 300 万个，较上月增长 6.5%；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 16 个，较上月下降 48.4%；按网络病毒家族[5]统计新增 9 个，较上月增长 50.0%；境内 12,511 万余个用户感染移动互联网恶意程序，恶意程序累计传播次数近 2,459 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 1.0%，新增病毒数量较上月增长 85.8%；安天公司捕获的样本总数较上月增长 32.8%，新增病毒种类较上月下降 2.8%；猎豹移动报送的计算机病毒事件数量较上月增长

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。5 月，CNCERT 在对恶意代码进行抽样监测时，对 526 种木马家族和 84 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。

26.6%。网站安全方面，本月境内被篡改网站数量为 5,629 个，较上月下降 12.1%；境内被植入后门的网站数量为 30,216 个，较上月增长 144.4%；针对境内网站的仿冒页面有 27,734 个，较上月增长 127.2%；各安全企业报送的网页挂马情况中，奇虎 360 公司报送的网页挂马事件数量较上月下降 41.1%。安全漏洞方面，本月 CNVD 共收集整理信息系统安全漏洞 888 个，较上月增长 35.6%。其中高危漏洞 306 个，较上月增长 45.7%；可被利用来实施远程攻击的漏洞有 779 个，较上月增长 42.4%。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 8,112 件垃圾邮件事件举报，较上月增长 16.0%。事件受理方面，CNCERT 接收到网络安全事件报告 8,343 件，较上月下降了 15.2%，数量最多的分别是漏洞类事件 3,087 件、网页仿冒类事件 2,434 件。

本月重点网络安全信息

◆ 2016 中国网络安全年会在四川成都召开

2016 年 5 月 25 日至 26 日，以“聚网络英才·筑安全生态”为主题的 2016 中国网络安全年会（第 13 届）在四川省成都市顺利召开，来自工业和信息化部、国防部、科技部、公安部、人社部、交通运输部、中国人民银行、四川省人民政府等单位的领导和专家，国内金融和电力等重要信息系统单位、基础电信企业、域名服务机构、互联网和网络安全企业、科研院所等业界同仁，以及来自 CNCERT 国际合作伙伴部分代表齐聚一堂。大会主办方国家互联网应急中心主任黄澄清致大会欢迎辞，对参会代表的到来表示了热烈的欢迎，对给予本次大会大力支持的各方表示衷心的感谢。工业和信息化部党组成员、办公厅主任莫玮出席会议并致辞，莫玮指出，我国互联网事业发展取得了显著成绩，突出体现在基础设施加快演进升级、产业规模持续扩大、融合创新蓬勃发展、国际影响力稳步提升四个方面。但与此同时，网络空间面临的威胁和挑战越来越现实和紧迫。莫玮就进一步做好网络安全工作提出四点要求：一是把握机遇，推动网络安全事业迈上新台阶；二是凝心聚力，加快突破网络安全核心技术；三是增进合作，不断提升网络安全保障能力；四是多措并举，持续壮大网络安全人才队伍。莫玮强调每个人都有责任积极发挥才干，投身网络强国建设，为共同推动我国互联网的持续健康发展贡献力量，希望参会代表在此次大会期间，多沟通交流，分享经验和思想，共谋网络强国建设大计。本次大会还同期举办了 2016 中国网络安全技术对抗赛，并开展了以“黑客入侵案例重现分析与业务保障对策”为主题的网络安全专场培训，分设了“网络安全威胁情报”、“网络安全人才培养”、“漏洞安全及价值秩序”、“移动互联网安全生态”、“数据安全分论坛”、“CNCERT-CIE 网络安全学术论坛”六个主题分论坛，为网络安全技

术爱好者提供了交流、展示、学习网络安全技术的平台。大会由工业和信息化部指导，国家计算机网络应急技术处理协调中心（CNCERT）主办，中国电子学会、中国互联网协会网络与信息安全工作委员会和中国通信学会通信安全技术委员会协办。来自政府部门、重要信息系统、企业、行业协会、科研院所等单位以及 CNCERT 国际合作伙伴的代表共九百余人参加了本次大会。

◆ 2016 中国网络安全技术对抗赛在成都举办

2016 年 5 月 24 日，在工业和信息化部指导下，国家互联网应急中心（CNCERT/CC）在四川省成都市举办了 2016 中国网络安全技术对抗赛。对抗赛以宣传普及网络安全知识，提高用户网络安全防护意识，推动网络安全技术的发展与应用，培养、发现优秀网络安全技术人才为目标。这是国家互联网应急中心第三次举办此项国内顶级水平的网络安全攻防赛事。通过对比赛报名队伍的筛选，本届大赛最后确定来自全国各地的 38 支队伍共 115 名队员参加。通过节奏紧张、分阶段的对抗竞赛模式，全面考验了参赛队伍的渗透测试、漏洞分析、挖掘利用、漏洞修复、安全防护等网络攻防实战能力。经过一天的激烈对决，6 支优秀的队伍脱颖而出。其中，由北京长亭科技有限公司组建的长亭科技队获得一等奖(奖金五万元)，由四川无声信息技术有限公司组建的 PKAV 队以及由个人组建的 FlappyPig 队获得二等奖(奖金两万元)，由 CNCERT 上海分中心组建的酱油队、由北京中科三方网络技术有限公司组建的中科三方队以及由北京安普诺信息技术有限公司组建的 Anpro 队获得三等奖(奖金一万元)。工业和信息化部网络安全管理局赵志国局长以及出席本次大赛的相关领导为获奖队伍颁奖，并勉励参赛选手继续努力研究网络安全技术，加强网络安全实践能力，为保障国家和社会网络安全利益贡献自己的力量。同时，国家互联网应急中心表示将继续举办此类赛事，不断丰富比赛内容、增加比赛形式、完善比赛赛制、提高比赛技术性与观赏性，为网络安全技术爱好者提供交流、展示、学习网络安全技术的平台。本次大赛由

CNCERT 实验平台、合天智汇、永信至诚和数字冰雹提供技术支持。

◆ 2016 年中国网络安全年会“网络安全培训”成功举办

2016 年 5 月 24 日上午，以《黑客入侵案例重现分析与业务保障对策沙盘演练》为主题的 2016 年中国网络安全年会“网络安全培训”在成都成功举办，约 500 人参加了本次培训。本次培训邀请到了北京中安国发信息技术研究院院长、信息安全应急演练关键技术研究中心主任张胜生担任主讲人。本次培训借助攻防演练实战平台，分别从网络攻击方和防守方的实际操作角度进行详细讲解，培训内容涵盖：系统脆弱性识别、系统安全加固、日志分析、快速应急响应等。

◆ 中国-东盟网络安全应急响应能力建设研讨会在成都举行

2016 年 5 月 24 日至 26 日，中国-东盟网络安全应急响应能力建设研讨会在成都举行。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、马来西亚、缅甸、菲律宾、泰国、越南、新加坡等东盟国家信息通信主管部门和国家级 CERT 组织的 29 名代表参加研讨会。工业和信息化部国际合作司调研员郑凯、网络安全管理局调研员刘伯超，国家计算机网络应急技术处理协调中心副处长李佳，越南国家级 CERT 组织主任 Nguyen Trong Duong 在研讨会开幕式上致辞。

本次研讨会是 2015 年在越南举办的第十次中国 - 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、网络安全信息共享最佳实践和技术平台建设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 2016 中国网络安全年会。东盟代表表示，本次研讨会议题广泛、内容丰富、交流充分，加深了彼此了解，对于双方进一步开展务实合作具有重要意义。

◆ 第一届 CNCERT 国际合作论坛在成都召开

2016 年 5 月 24 日，由国家互联网应急中心（CNCERT）主办的第一届 CNCERT 国际合作论坛在中国成都召开。来自澳大利亚、德国、罗马尼亚、韩国、新加坡、马来西亚等十六个国家和地区的电信政府部门、网络安全应急组织和互联网企业近 50 名代表出席了本次会议。该论坛为 CNCERT、国际伙伴和网络安全企业提供一个在网络安全应急领域交流的平台，进一步增进互信，相互学习，促进开展全方面的网络安全合作。本届论坛的主题是“网络安全信息共享”，CNCERT 副主任云晓春代表主办方致辞，表示随着互联网的快速发展，面对日益复杂的网络安全形势，网络安全国际合作成为必然趋势。召开 CNCERT 国际合作论坛就是提供一个在网络安全应急领域交流的平台，并就进一步合作谈了四点想法：一是加强日常联系和交流，优化跨境事件处置的协调配合；二是加强信息共享，开展网络安全环境综合治理；三是加强网络安全项目共研，探求有效应对措施与保障技术；四是联合开展网络安全宣传教育，促进网络安全防范意识与知识水平提高。 随后，CNCERT 的代表介绍了召开该论坛的背景，以及起草的论坛愿景、使命和实施计划等内容。罗马尼亚 CERT-RO、日本 JPCERT、马来西亚 MyCERT、IT 安全认证和教育机构(ISC)2、香港 HKCERT、韩国 KrCERT、中国安天公司的代表分别就网络安全国际合作、恶意程序治理项目、网络安全能力建设、网络安全威胁趋势、恶意网站监测项目、威胁情报分析等主题展开了精彩演讲，和与会者分享了最佳实践经验。25-26 日，CNCERT 邀请国际代表参加了 2016 中国网络安全年会。国际代表表示 CNCERT 国际合作论坛和中国网络安全年会举办得很成功，其中关于网络安全政策、管理和技术方面的新视点极具实践和研究价值。

◆ 通报 ImageMagick 存在远程代码执行高危漏洞

近日，国家信息安全漏洞共享平台（CNVD）收录了 ImageMagick

远程代码执行漏洞6。远程攻击者利用漏洞通过上传恶意构造的图像文件，可在目标服务器执行任意代码，进而获得网站服务器的控制权。由于有多种编程语言对 ImageMagick 提供调用支持且一些广泛应用的 Web 中间件在部署中包含相关功能，对互联网站安全构成重大威胁。CNVD 对以上漏洞的综合评级均为“高危”。 目前，互联网上已经披露了该漏洞的利用代码，厂商尚未发布漏洞修复程序，预计近期在 ImageMagick 7.0.1-1 和 6.9.3-10 版本中修复该漏洞。CNVD 建议相关用户关注厂商主页更新，及时下载使用，避免引发漏洞相关的网络安全事件。

◆ 通报全志科技 ARM 内核系统存在预置 ROOT 权限口令漏洞

近日，国家信息安全漏洞共享平台（CNVD）收录了全志科技 ARM 内核系统存在的预置 ROOT 权限口令漏洞。 攻击者利用漏洞可获取设备 root 访问权限，且存在远程攻击可能，影响到日常使用的平板电脑、机顶盒等终端设备安全。CNVD 对该漏洞的综合评级为“高危”。漏洞影响 Linux 3.4-Sunxi 内核，进而影响到装载该内核的八核心 A83T、H8 处理器以及四核心的 H3 处理器等全志科技公司产品。根据国外安全研究者的测试分析情况，这些处理器应用广泛，诸多平板电脑和机顶盒产品都有可能受到影响。5 月 13 日，CNVD 已将该漏洞细节通报给厂商处置，请其核实漏洞并提供修复措施。目前，厂商尚未直接回应同时也未提供漏洞修复方案，用户可参考第三方厂商(Friendlyarm)提供的修复补丁或联系厂商获取修复方案，避免引发漏洞相关的网络安全事件。

注6：CNVD-2016-02721，对应 CVE-2016-3714

本月网络安全主要数据

◆ 网络病毒监测数据分析

2016 年 5 月，境内感染网络病毒的终端数为近 300 万个。其中，境内近 228 万个 IP 地址对应的主机被木马或僵尸程序控制，与上月的 212 万余个相比增长 7.3%；境内 72 万余个主机 IP 感染“飞客”蠕虫，与上月的 69 万余个相比增长 4.0%。

➢ *木马僵尸网络监测数据分析*

2016 年 5 月，境内近 228 万个 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 9,034 个。其中，境内木马或僵尸网络控制服务器 IP 数量为 4,561 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 4,473 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 739,440 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荷兰的 IP 地址，分别控制了境内 327,583 个和 177,605 个主机 IP。

➢ *飞客蠕虫监测数据分析*

2016 年 5 月，CNCERT 监测到全球互联网近 455 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 72 万余个，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 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 16 个，按网络病毒家族统计新增 9 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 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： 2016 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	down.job391.com	1	124.228.91.118
2	down.ttu998d.com	2	183.61.16.134
3	www.ctscf.com	3	218.90.204.141
4	www.xz9u.com	4	115.231.76.17
5	ini.ttu998d.com	5	218.90.204.145
6	tg.ikuaiping.com	6	123.94.10.133
7	down.8476ddd.com	7	222.186.129.198
8	soft.qwfjewfk.com	8	42.159.26.92
9	a.wbsz.com	9	222.186.46.47
10	down.tt6786.com	10	219.239.88.67

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 5 月，CNCERT 监测发现的放马站点中，通过域名访问的共涉及有 199 个域名，通过 IP 直接访问的共涉及有 551 个 IP。在 199 个放马站点域名中，于境内注册的域名数为 115 个（约占 57.8%），于境外注册的域名数为 75 个（约占 37.7%），未知注册商属地信息的有 9 个（约占 4.5%）。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 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	.COM	通用顶级域名（gTLD）	140
2	.NET	国家顶级域名（ccTLD）	21
3	.CN	通用顶级域名（gTLD）	19

4	.CC	通用顶级域名（gTLD）	5
5	.RU	国家顶级域名（ccTLD）	3

➢ *移动互联网恶意程序监测情况*

2016 年 5 月,CNCERT 抽样监测发现境内感染移动互联网恶意程序的感染用户 125,111,495 个，按地区分布感染数量排名前三位的分别是广东省、北京市和四川省。

◆ 网站安全数据分析

➢ *境内网站被篡改情况*

2016 年 5 月，境内被篡改网站的数量为 5,629 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、河南省。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 155 个，占境内被篡改网站的比例为 2.8%。

截至 5 月 31 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 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.bzqgaj.gov.cn	四川省成都市
zclgj.gov.cn	山东省济南市
ls93.gov.cn	四川省成都市
zwfw.arq.gov.cn	四川省成都市
jxwzga.gov.cn	安徽省合肥市
www.zyrs.gov.cn	贵州省贵阳市

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.hzzz.gov.cn	贵州省贵阳市
www.hanyang.gov.cn	广西省南宁市

➢ *境内网站被植入后门情况*

2016 年 5 月，境内被植入后门的网站数量为 30,216 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、浙江省。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 847 个，占境内被植入后门网站的比例为 2.8%。

2016 年 5 月，境外 5,606 个 IP 地址通过植入后门对境内 26,904 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 ,来自中国香港的 IP 地址共向境内 7,438 个网站植入了后门程序，入侵网站数量居首位；其次是来自美国和俄罗斯的 IP 地址，分别向境内 3,126 个和 1,633 个网站植入了后门程序。

➢ *境内网站被仿冒情况*

2016 年 5 月，CNCERT 共监测到针对境内网站的仿冒页面有 27,734 个，涉及域名 12,507 个，IP 地址 6,666 个，平均每个 IP 地址承载 4 余个仿冒页面。在这 6,666 个 IP 中，69.3%位于境外，主要位于中国香港和美国。

◆ 漏洞数据分析

2016 年 5 月，CNVD 收集整理信息系统安全漏洞 888 个。其中，高危漏洞 306 个，可被利用来实施远程攻击的漏洞有 779 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 73 个 0day 漏洞，

其中影响最严重的是“PowerFolder 远程代码执行漏洞”、“Adobe Flash 任意代码执行漏洞”、“Google Chrome pdfium 堆内存错误引用漏洞”、“Foxit Reader PDF 解析内存破坏漏洞”。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 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 8,343 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 8,343 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。

2016 年 5 月，CNCERT 以及各省分中心共同协调处理了 8,367 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。

- 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。