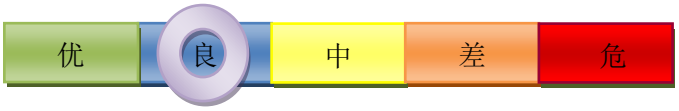
CNCERT互联网安全威胁报告

2015 年 05 月　　总第 53 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。

2015 年 05 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172万余个；
- 境内被篡改网站数量为5,668个，其中被篡改政府网站数量为193个；境内被植入后门的网站数量为7,107个，其中政府网站有450个；针对境内网站的仿冒页面数量为19,617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洞610个，其中，高危漏洞207个，可被利用来实施远程攻击的漏洞有550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 2014 年，CNCERT 已与 63 个国家和地区的 144 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

2015 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，除境内木马或僵尸程序的 IP 地址数量、境内被篡改网站的数量、仿冒境内网站的总数和网络安全事件报告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,但评价指数仍在良的区间。

◆ 基础网络安全

2015 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 151 个，较上月的 295 个下降 48.8%，占境内被篡改网站的比例由 3.3%下降到了 2.9%；境内被植入后门的政府网站数量为 782 个，较上月的 643 个增长 21.6%，占境内被植入后门网站的比例则由 12.5%下降到了 9.5%；针对境内网站的仿冒页面数量为 16,273 个，较上月的 19,583 个下降 16.9%，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 1,843

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，“Mediacoder 缓冲区溢出漏洞”、“ProjectSend 任意文件上传漏洞”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

2015 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 172 万余个，较上月增长 21.3%；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 10 个，较上月下降 88.8%；按网络病毒家族[5]统计新增 1 个，较上月下降 90.9%；境内 696 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达 41 万余次，抽样检测的 123,346 个移动互联网 APP 中有 91 个恶意程序，涉及 91 条下载链接；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 9.2%，新增病毒数量较上月增长 122.8%；安天公司捕获的样本总数较上月增长 24.9%，新增病毒种类较上月增长 107.2%；金山公司报送的计算机病毒事件数量

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 520 种木马家族和 69 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。

较上月下降 4.2%。网站安全方面，本月境内被篡改网站数量为 5,668 个，较上月增长 9.5%；境内被植入后门的网站数量为 7,107 个，较上月下降 14.1%；针对境内网站的仿冒页面有 19,617 个，较上月增长 20.5%；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 2.2%，奇虎 360 公司报送的网页挂马事件数量较上月下降 25.3%。安全漏洞方面，本月 CNVD 共收集整理信息系统安全漏洞 610 个，较上月下降 8.1%。其中高危漏洞 207 个，较上月下降 8.4%；可被利用来实施远程攻击的漏洞有 550 个，较上月下降 5.8%。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 24,101 件垃圾邮件事件举报，较上月增长 11.5%。事件受理方面，CNCERT 接收到网络安全事件报告 9,294 件，较上月增长 4.4%，数量最多的分别是网页仿冒类事件 5,803 件、漏洞类事件 1,793 件。

本月重点网络安全信息

◆ 2015 年中国计算机网络安全大会在湖北武汉召开

2015 年 5 月 27 日至 28 日，以“智能网络·安全护航”为主题的 2015 年中国计算机网络安全大会（第 12 届）在湖北省武汉市召开，来自政府和重要信息系统、企业、行业协会、科研院所等单位以及来自 CNCERT 国际合作伙伴的代表共七百余人参加了本次大会。

工业和信息化部总工程师张峰出席大会并致辞。张峰在致辞中指出，在政府、产业和社会各界的共同努力下，全功能接入国际互联网 20 多年来，中国互联网发展取得了令人瞩目的巨大成就。当前，乘着“互联网+”的新机遇，我国互联网持续高速发展，网络和终端更加智能化，应用服务更加规模化，跨界融合更加多样化。但与此同时，互联网的快速发展也伴生了一系列安全方面的挑战，包括全球网络空间环境日益复杂多变，网络安全风险不断增高，我国网络安全能力仍相对薄弱、数据安全面临巨大挑战、新技术新业务应用引发新的安全问题等，给经济社会健康发展带来了一定的风险。随后，张峰就进一步做好网络安全工作提出五点要求：一是提高思想认识，充分认识新形势下做好网络安全工作的重要性和紧迫性。二是注重统筹规划，深入推进网络安全保障体系建设。三是重视数据安全，强化网络数据和用户个人信息保护。四是深化协调协作，做好对内对外的合作与交流。五是加强人才培养，努力建设一支高素质的网络安全技术业务队伍。张峰代表工业和信息化部对本次大会的成功召开表示祝贺，并希望参会代表利用大会这个信息共享和技术交流的平台，增强交流互动，分享各自在网络安全方面对见解和思想，共享发展新机遇，共筑网络强国梦。

湖北省委副秘书长王永高致欢迎辞，并表示希望以本次大会为契机，学习借鉴先进经验，不断地加强和改进湖北省计算机网络安全工作，为全省经济社会发展营造更好、更安全的网络环境，让生活更便

捷更精彩。中国工程院沈昌祥院士应邀以《网络空间安全战略思考与启示》为题做大会报告。他指出网络空间已经成为继陆海空天之后的第五大主权领域空间，对我国网络安全提出了严峻的挑战，我们应积极应对，加快建设我国网络安全保障体系，捍卫我国网络安全国家主权。

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。大会历经十二年发展，为政府、业界及公众之间搭建起坚实的沟通桥梁，有效促进了网络安全保障成果和经验的分享，深化推动网络安全技术的交流与合作。在工业和信息化部指导下，本次大会还同期举办了 2015 中国网络安全技术对抗赛，开展了以移动互联网安全为主题的网络安全专场培训，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。

◆ 50 家单位入选第六届 CNCERT 网络安全应急服务支撑单位

2015 年 5 月 25 日，国家互联网应急中心在湖北省武汉市举行第六届 CNCERT 网络安全应急服务支撑单位评选会议，评选产生了 8 家国家级应急服务支撑单位和 42 家省级应急服务支撑单位。本次评选自 2015 年 3 月启动，经过申请材料审核、分中心提名推荐等环节，筛选出 64 家单位进入现场答辩环节。评选专门成立了委员会，成员分别由来自相关政府部门、基础电信运营企业、网络安全技术机构和科研院所的 37 位专家组成。评选委员会从企业实力、应急技术能力、应急服务规范性、支撑 CNCERT 情况等方面对参选单位进行了细致评估，其中对 CNCERT 日常工作支撑情况是一个重要考察项。

“CNCERT 网络安全应急服务支撑单位”选拔工作自 2004 年起启动，今年是第六届评选。在 CNCERT 的指导和协调下，经过十余年发展，支撑单位已成为我国互联网网络安全应急体系的重要组成部分，在网络安全应急响应和分析预警方面做出了积极贡献，为维护我国互联网网络安全发挥了重要作用。随着网络安全威胁日益复杂化，

网络安全应急工作需求日益增强，网络安全应急体系也在不断发展壮大。CNCERT 将与各支撑单位加强协作，共同推动国家网络安全应急响应支撑体系和应急工作不断完善，同时将建立支撑单位评分制度，加强对支撑单位的考察，作为今后评选的重要依据。

◆ 关于虚拟机管理组件 QEMU 存在高危漏洞的情况公告

5 月 15 日，国家信息安全漏洞共享平台（CNVD）收录了一个 QEMU 'hw/block/fdc.c' VENOM 远程内存破坏漏洞（CNVD-2015-03045，对应 CVE-2015-3456）。攻击者可以在有问题的虚拟机中进行逃逸，一定条件下可以在宿主机中获得代码执行的权限。根据评估，“毒液（VENOM）”漏洞有可能使互联网上数以百万计的虚拟机受到威胁，进而影响到全球各大云服务提供商的数据和运行安全。目前，部分 Linux 厂商已经发布了补丁修补程序。

根据 CNVD 技术组成员单位——奇虎 360 公司的测试分析，由于该漏洞为典型的堆溢出漏洞，即使虚拟机没有默认设置软驱配置，也存在利用可能。建议尽快在源码层面上对 QEME 实现补丁升级。

◆ 关于境外黑客针对我国境内网站发动攻击的情况通报

2015 年 5 月下旬，越南、菲律宾两国黑客发布声明，准备联合在 5 月 30 日中午 12 点发起针对中国政府、教育、企业等网络展开 DDoS 和网页篡改的攻击。由于事件的升级，网络攻击已提前于 5 月 29 日发动。CNCERT 对此次攻击行动进行了跟踪监测。

越南、菲律宾两国的黑客制定了针对我国境内网站的攻击行动，代号为“Op China”。近日，越菲的黑客不断通过网络发布招募黑客的信息，建立了 Facebook 行动指挥专门页面（https://www.facebook.com/events/1579947942293131/）和官网网站（http://www.op-china.net）。此次行动通过互联网（http://pastebin.com/rghEeHFv 及 http://pastebin.com/xii97KNy）公开发布境内存在高危漏洞的网站列表并制定入侵篡改页面 HTML 代码

样例，为黑客入侵提供便利。

CNCERT 监测发现，截止到 6 月 1 日 18 时，被攻击的我国境内网站或.cn 域名网站 139 个，涉及 IP 地址 101 个，其中已有 112 个网站恢复正常或处于不可访问状态。

◆ 关于“相册”系列手机恶意程序大面积泄露用户信息的情况通报

2015 年 5 月 15 日 17 时， CNCERT 接到国反网络病毒联盟成员单位安天公司举报的大面积泄露用 Android 恶意程序，通过短信内容中的 35 个 dwz.cn 短链接在国内 26 个省、直辖市传播，感染用户超过 2000 人，泄露用户短信 51 万条、通讯录联系人信息 53 万条，造成严重的用户信息泄露安全威胁。CNCERT 第一时间对该系列恶意程序进行分析，对所用的邮箱、传播服务器和控制服务器进行处置，有效控制了恶意程序的影响范围：1、协调基础电信企业对传播恶意程序和接收用户信息的恶意 URL 地址，包括 29 个恶意短地址和 http://cdn.yunguangli.com/WebApi/Index 进行阻断处理。2、协调域名注册商“成都飞数”和网易公司关停了用于接收用户信息的网站域名“yunguangli.com”和邮箱账户 a15778352422@vip.163.com。3、协调“dwz.cn”网站运营者百度公司删除 29 个恶意短地址，并要求百度公司在转换 APK 文件下载链接时，拒绝为存在恶意行为的 APK 文件下载地址进行短地址转换。

◆ 关于近日支付宝等网络故障的有关情况通报

2015 年 5 月 27 日下午 5 点半左右，全国各地大量用户反映，支付宝（www.alipay.com）出现网络故障，账号无法正常登录。支付宝官方随即回应称，故障是由于杭州市萧山区某地光纤被挖断，经紧急将用户请求切换至其他机房，故障逐步恢复。到晚上 7 点 20 分，支付宝宣布用户服务已经恢复正常，全程历时 2 个多小时。据了解，支付宝在系统上采用了“异地双活”架构，即杭州和外地两处机房同时为用户提供服务，系统会自动将全国所有用户的需求分流到两处机

房。支付宝同时强调用户的资金安全不会受到任何影响。CNCERT 监测数据显示支付宝在故障前后时间未受到 DDoS 网络攻击。

2015 年 5 月 28 日上午，携程官网（www.ctrip.com）和客户端出现故障，全部搜索功能都无法使用，搜索框中出现一段代码，而携程官网显示，“携程网站目前遇到问题，深表歉意，正在紧急修复中…”。11 时 9 分，携程官网回应称“因写成部分服务器遭到不明攻击，导致官方网站及 APP 暂时无法正常使用，目前正在紧急恢复。对用户造成的不便，我司深表歉意”。CNCERT 得知此事后第一时间核查了有关携程网站近期的相关的漏洞通告等信息，并未发现携程网站具有被外部网络攻击的漏洞。携程官方微博 29 日凌晨 4 点发布声明内容表示，确认此次事件是由于员工误操作导致。

携程网出故障后，携程网首页挂出通知，建议用户选择艺龙旅行网（www.elong.com）。然而，28 日当天 17 时，艺龙网站也出现无法访问的故障。18 时 17 分，艺龙官方回应“因遭受网络攻击，艺龙网首页出现部分用户无法访问的情况，目前已恢复正常。”CNCERT 对此事进行跟踪，因艺龙网使用了 360 的网站宝，无法得到准确 IP 地址，经协调艺龙网也未回复相关信息，故无法查询到艺龙网的相关网络流量信息。

去哪儿网（www.qunar.com）于 5 月 28 日遭受异常流量攻击。CNCERT 与去哪儿网联系并得到对方提供的受攻击 IP 地址，初步判断此次攻击主要是 UPnP 反射攻击，且伪造的流量主要是境外发起。

CNCERT 将继续跟踪事件后续情况，做好国内用户受影响情况的监测和预警工作。

本月网络安全主要数据

◆ 网络病毒监测数据分析

2015 年 5 月，境内感染网络病毒的终端数为 172 万余个。其中，境内 137 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 96 万个相比增长 43.2%；境内近 35 万个主机 IP 感染“飞客”蠕虫，与上月的 46 万余个相比下降 24.3%。

➢ *木马僵尸网络监测数据分析*

2015 年 5 月，CNCERT 监测发现境内 137 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、江苏省、浙江省。

木马或僵尸网络控制服务器 IP 总数为 7,410 个。其中，境内木马或僵尸网络控制服务器 IP 数量为 4,339 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 3,071 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 369,225 个主机 IP，控制境内主机 IP 数量居首位，其次是位于韩国和中国香港的 IP 地址，分别控制了境内 311,811 个和 192,300 个主机 IP。

➢ *飞客蠕虫监测数据分析*

2015 年 5 月，CNCERT 监测到全球互联网 301 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、巴西、埃及。

境内感染飞客蠕虫的主机 IP 为近 35 万个，按地区分布感染数量排名前三位的分别是广东省、河南省、浙江省。

➢ *网络病毒捕获和传播情况*

2015 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 10 个，按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。2015 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： 2015 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	soft.pengan119.com	1	61.153.109.193
2	www.xz9u.com	2	183.61.16.134
3	ini.8476ddd.com	3	115.231.76.17
4	down.job391.com	4	183.61.16.141
5	inix.xiaoxinrili.com	5	59.53.167.124
6	ini.ttu998d.com	6	219.239.88.67
7	down.xqt18.com	7	210.14.135.189
8	url.cncrk.com	8	203.88.164.47
9	dljxa.caloinfo.com	9	162.250.142.29
10	cache.yyupload.com	10	183.60.40.18

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。2015 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 282 个域名，通过 IP 直接访问的共涉及有 53 个 IP。在 282 个放马站点域名中，于境内注册的域名数为 174 个（约占 61.7%），于境外注册的域名数为 107 个（约占 37.9%），未知注册商属地信息的有 1 个（约占 0.4%）。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： 2015 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）	201
2	.CN	国家顶级域名（ccTLD）	34
3	.NET	通用顶级域名（gTLD）	31

4	.RU	国家顶级域名（ccTLD）	6
5	.CC	国家顶级域名（ccTLD）	3

➢ *移动互联网恶意程序监测情况*

2015 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 6,961,521 个，按地区分布感染数量排名前三位的分别是广东省、陕西省和山东省。

2015 年 5 月，CNCERT 通过应用商店在线检测平台（https://appstore.anva.org.cn）共检测 20 家手机应用商店的 123,346 个 APP（根据 MD5 去重），发现其中 91 个移动互联网程序为恶意 APP，涉及 91 条恶意下载链接，并通过在线检测平台通知相关应用商店下架恶意程序。

◆ 网站安全数据分析

➢ *境内网站被篡改情况*

2015 年 5 月，境内被篡改网站的数量为 5,668 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、广东省、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 193 个，占境内被篡改网站的比例为 3.4%。

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
lpxrsj.gov.cn	河北省承德市
wxny.gov.cn	广西壮族自治区来宾市

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。

被篡改网站	所属部门或地区
ynaz.gov.cn	云南省昆明市
irgsf.gov.cn	江苏省南京市
www.bayan.gov.cn	黑龙江省哈尔滨市

➢ 境内网站被植入后门情况

2015 年 5 月，境内被植入后门的网站数量为 7,107 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、广东省、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 450 个，占境内被植入后门网站的比例为 6.3%。

2015 年 5 月，境外 4,948 个 IP 地址通过植入后门对境内 5,979 个网站实施远程控制。其中，境外 IP 地址主要位于美国、委内瑞拉和中国香港等国家或地区。从境外 IP 地址通过植入后门控制境内网站数量来看，来自荷兰的 IP 地址共向境内 1,226 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 637 个和 558 个网站植入了后门程序。

➢ 境内网站被仿冒情况

2015 年 5 月，CNCERT 共监测到针对境内网站的仿冒页面有 19,617 个，涉及域名 16,240 个，IP 地址 2,547 个，平均每个 IP 地址承载 7 余个仿冒页面。在这 2,547 个 IP 中，境外占 66.4%，主要位于中国香港和美国。

◆ 漏洞数据分析

2015 年 5 月，CNVD 收集整理信息系统安全漏洞 610 个。其中，高危漏洞 207 个，可被利用来实施远程攻击的漏洞有 550 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 108 个 0day 漏洞，其中影响最严重的是“Mediacoder 缓冲区溢出漏洞”、“ProjectSend 任意文件上传漏洞”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、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*

2015 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 9,294 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 10 件。

在 9,294 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。

2015 年 5 月，CNCERT 以及各省分中心共同协调处理了 9,104 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。