国家互联网应急中心

2016 年第 14 期

3 月 28 日-4 月 3 日

# 网络安全信息与动态周报

CNCERT/CC

## 本周网络安全基本态势

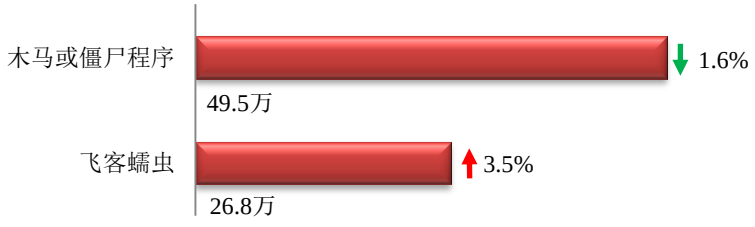
优 | 良 | 中 | 差 | 危

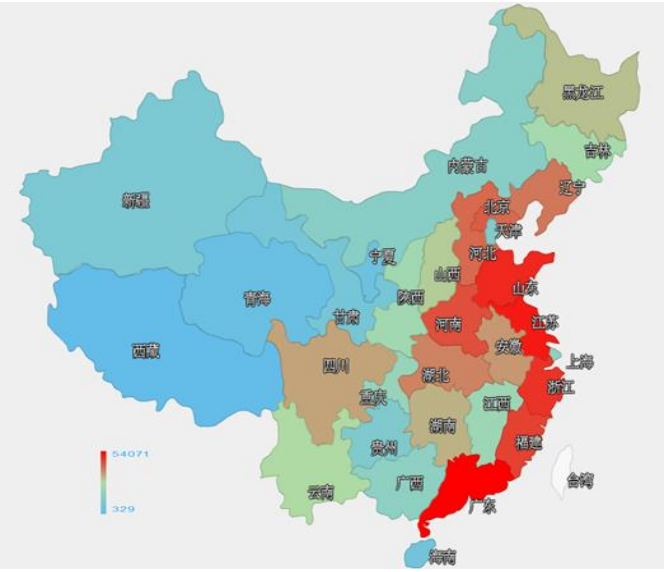
| | | |
|---|---|---|
| 境内感染网络病毒的主机数量 | •76.3万 | ↑ 0.2% |
| 境内被篡改网站总数<br>其中政府网站数量 | •4262<br>•72 | ↑ 2.5%<br>↑ 4.3% |
| 境内被植入后门网站总数<br>其中政府网站数量 | •2595<br>•88 | ↑ 33.1%<br>= |
| 针对境内网站的仿冒页面数量 | •6195 | ↑ 47.1% |
| 新增信息安全漏洞数量<br>其中高危漏洞数量 | •93<br>•22 | ↓ 19.1%<br>↓ 26.7% |

*=表示数量与上周相同　↑表示数量较上周环比增加　↓表示数量较上周环比减少*

## 本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 76.3 万个，其中包括境内被木马或被僵尸程序控制的主机约 49.5 万以及境内感染飞客（conficker）蠕虫的主机约 26.8 万。





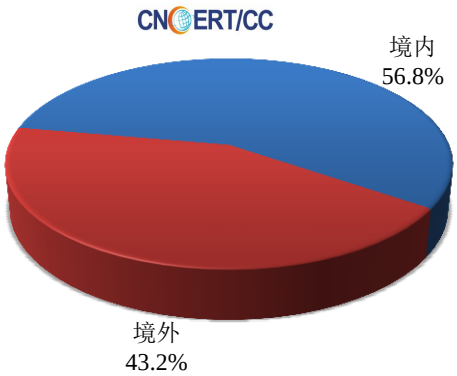

木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、江苏省和山东省。

TOP3

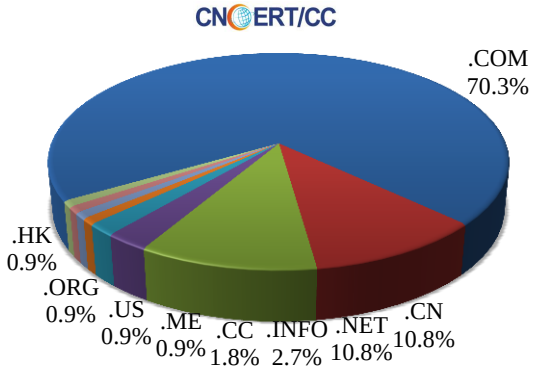
| | |
|---|---|
| 广东省 | • 约5.4万个（约占中国大陆总感染量的10.9%） |
| 江苏省 | • 约4.0万个（约占中国大陆总感染量的8.1%） |
| 山东省 | • 约3.8万个（约占中国大陆总感染量的7.7%） |

放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 111 个，涉及 IP 地址 255 个。在 111 个域名中，有约 43.2%为境外注册，且顶级域为.com 的约占 70.3%；在 255 个 IP 中，有约 10.2%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 17 个 IP。

**本周放马站点域名注册所属境内外分布**
**(3/28-4/3)**




**本周放马站点域名所属顶级域的分布**
**(3/28-4/3)**




针对 CNCERT 自主监测发现以及各单位报送数据，CNCERT 积极协调域名注册机构等进行处理，同时通过 ANVA 在其官方网站上发布恶意地址黑名单。

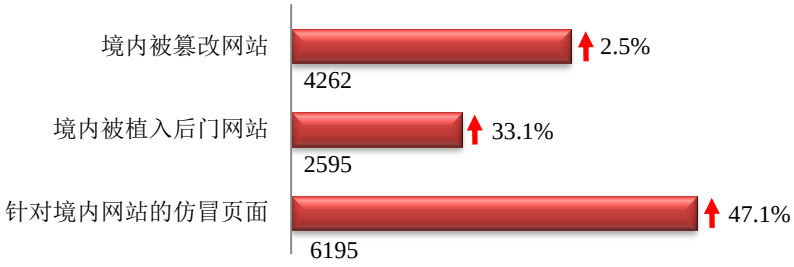
**ANVA恶意地址黑名单发布地址**

http://www.anva.org.cn/virusAddress/listBlack

*中国反网络病毒联盟（Anti Network-Virus Alliance of China，缩写 ANVA）是由中国互联网协会网络与信息安全工作委员会发起、CNCERT 具体组织运作的行业联盟。*

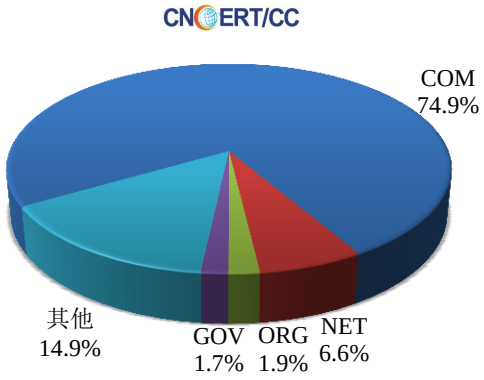
## 本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 4262 个；境内被植入后门的网站数量为 2595 个；针对境内网站的仿冒页面数量为 6195。

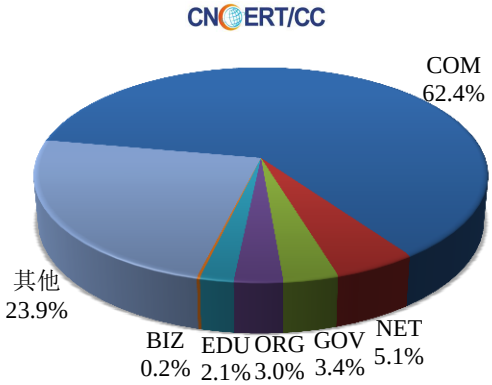



本周境内被篡改政府网站(GOV 类)数量为 72 个（约占境内 1.7%），较上周环比上升了 4.3%；境内被植入后门的政府网站（GOV 类）数量为 88 个（约占境内 3.4%），与上周持平；针对境内网站的仿冒页面涉及域名 3501 个，IP 地址 1081 个，平均每个 IP 地址承载了约 6 个仿冒页面。

**本周我国境内被篡改网站按类型分布**
**(3/28-4/3)**

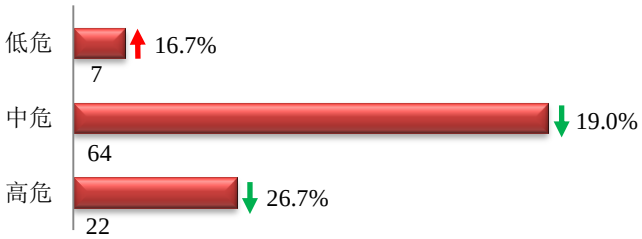



**本周我国境内被植入后门网站按类型分布**
**(3/28-4/3)**

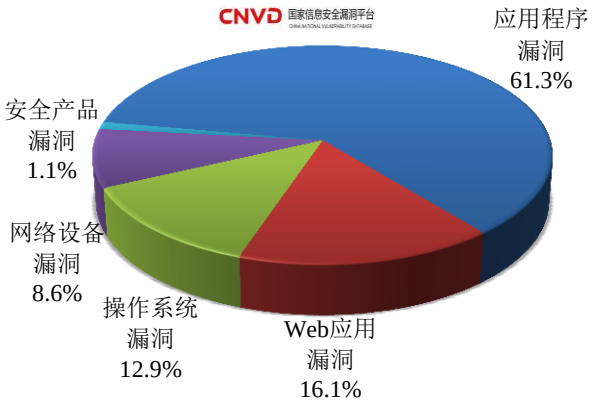


## 本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 93 个，信息安全漏洞威胁整体评价级别为中。




**本周CNVD收录漏洞按影响对象类型分布**
**(3/28-4/3)**




本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是 Web 应用漏洞和操作系统漏洞。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

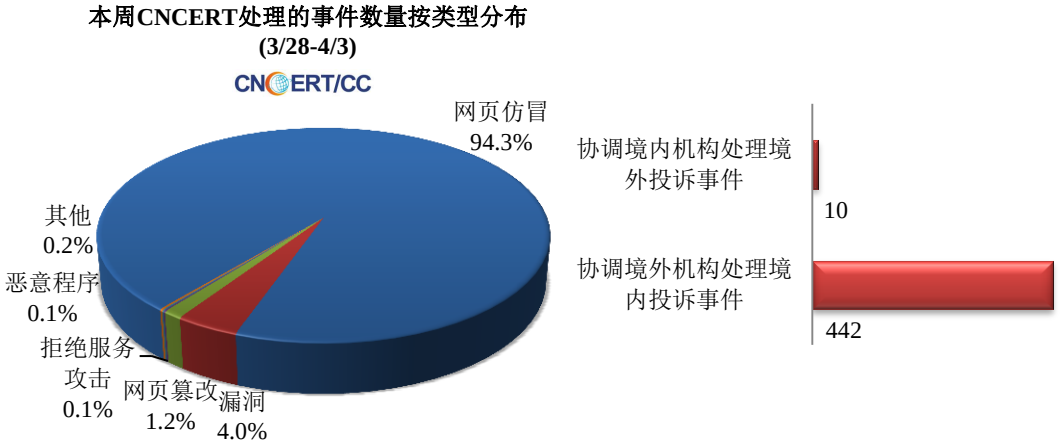
**CNVD漏洞周报发布地址**

http://www.cnvd.org.cn/webinfo/list?type=4

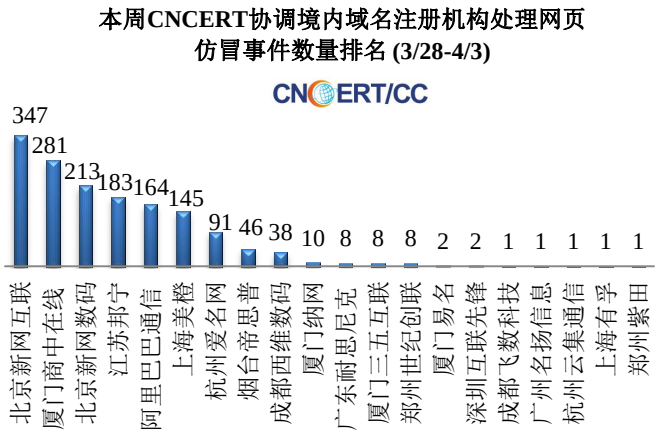
*国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。*

## 本周事件处理情况

本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 2096 起，其中跨境网络安全事件 452 起。

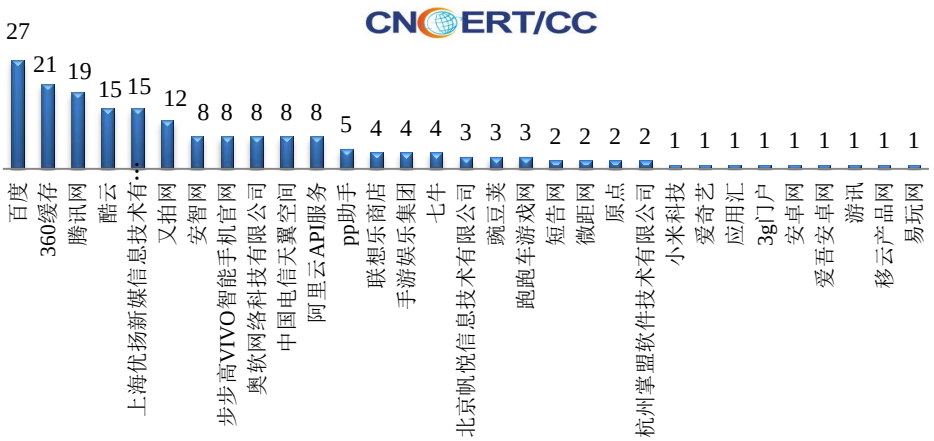



本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 1977 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事 1752 起和互联网服务提供商仿冒事件 208 起。


本周，CNCERT 协调 31 个应用商店及挂载恶意程序的域名开展移动互联网恶意代码处理工作，共处理传播移动互联网恶意代码的恶意 URL 链接 192 个。

**本周CNCERT协调手机应用商店处理移动互联网恶意代码事件数量排名**
**(3/28-4/3)**




## 业界新闻速递

### 1、中国首个网络安全领域的全国性社会团体在京成立

C114 中国通信网 3 月 28 日消息 3 月 25 日，我国首个网络安全领域的全国性社会团体——中国网络空间安全协会在京成立。据悉，该协会是由国内从事网络空间安全相关产业、教育、科研、应用的机构、企业及个人自愿结成的全国性、行业性、非营利性社会组织，发起会员共计 257 个，其中单位会员 190 多个，囊括了国内主要互联网企业和网络安全企业、权威科研机构，具有广泛的代表性。协会成立后，将着力促进网络安全行业自律，积极引导网络环境下各类企业履行网络安全责任，积极推动网络安全行业标准建设和学科建设，组织开展各类网络安全专业性群众性活动，积极参与网络安全国际交流合作。国家互联网信息办公室副主任王秀军在成立大会上指出，协会的成立顺应了我国互联网行业和社会各界共同参与维护网络安全的愿望，对加强行业自律、促进行业健康发展、维护我国网络安全、加强网络安全国际交流合作将发挥积极作用。工业和信息化部总工程师张峰出席成立大会并致辞，他指出，中国网络空间安全协会的正式成立既是为国家网络空间安全战略服务的内在需要，也是适应网络安全和信息化发展形势的客观要求，必将对组织和动员社会各方面力量参与中国网络安全建设、促进网络空间健康发展发挥积极的建设性作用。在同日召开的中国网络空间安全协会第一届理事会第一次会议上，中国工程院院士、北京邮电大学教授方滨兴当选为中国网络空间安全协会理事长，吴曼青、贾焰、马民虎、孟丹、李建华、齐向东、马化腾、肖新光、郑志彬、王海峰、杜跃进等 11 人当选为副理事长，中国网络空间研究院李欲晓当选为协会秘书长。

### 2、美英将举行联合演习模拟核设施遭受网络攻击时情景

环球网 4 月 1 日消息 据英国《卫报》3 月 31 日报道，英国和美国将在 2016 年稍晚进行一场联合演习，模拟“黑客”攻击核电站时可能会出现的情景，以此来测试政府和公用事业公司的应变能力和措施。报道称，在英国首卡梅伦准备飞往华盛顿出席核安全峰会时，有英国政府消息人士指出，此次峰会上，英美两国计划在探

索核基础设施在面对恐怖袭击时的应变力方面展开合作。相关演习将在今年晚些时候进行。据称，英美两国计划开展此次演习并不是因为接到有关核设施遭袭击的可靠情报，这只是“预防计划”，消息人士还补充说：“这一计划使我们有能力检测相关系统，并且确保我们能从中吸取经验教训。”此前，两国也曾在去年模拟过银行系统遭受网络攻击时的情景。

### 3、日本敲定网络安全人才培养计划 以应对恶意攻击

中新网 3 月 31 日消息 据日媒报道，日本政府本月 31 日在首相官邸召开阁僚与专家出席的“网络安全战略总部”（总部长：官房长官菅义伟）会议，正式敲定了担负网络安全对策中枢职能的人才培养计划。据悉，该计划的主要内容是在未来4年内培养近千名专家，着眼于2020年东京奥运会和残奥会努力加强网络攻击应对态势。菅义伟在会议伊始对日本紧缺网络攻击对策方面的专家表露了危机感，强调“为确保优秀人才，应构建人才培养系统，形成人才供需的良性循环”。根据计划，日本政府将设置一项新制度，从 2017 年度起对相关职员还给予收入上的优待。计划还要求日本政府各部门制定培养项目，设立“网络安全与信息化审议官”一职以统管人才培养等工作。计划规定，原则上要把优秀职员派遣至监控针对日本政府的网络攻击的“内阁网络安全中心”(NISC)或民营企业。

### 4、日本东京警方成立网络安全对策总部 保障网络安全

中新网 4 月 1 日消息 据日本媒体报道，为加强打击数量猛增的网络犯罪和应对网络攻击的指挥塔功能，日本东京警视厅 4 月 1 日成立了以副总监山下史雄为总部长的“网络安全对策总部”。此举是着眼于 5 月七国集团（G7）伊势志摩峰会和 2020 年东京奥运，旨在提升警方在网络空间的应对能力。在东京霞关的警视厅总部举行的网络安全对策总部成立仪式上，警视总监高桥清孝作出训示：“面向东京奥运，可能会发生运用高级技术的网络攻击。希望大家发挥组织综合能力这一警视厅的强项，积极推进应对措施。”对策总部由来自于多个部门的约 50 人组成，其中生活安全部负责调查针对企业及个人的网络犯罪，公安部则负责打击针对政府部门的攻击。对策总部将汇总受害信息并进行分析，与其他各部门合作进行调查。对策总部一方面将开展进修学习以提升警察的能力，还将举行电脑病毒破解技术的竞赛。

### 5、韩国防部召开网络安全防御对策会议 应对朝威胁

环球网 3 月 30 日消息 据韩联社 3 月 29 日报道，为应对朝鲜网络威胁，韩国国防部当天召开了韩军网络安全防御对策会议。韩国国防部相关人士透露说，一季度，朝鲜网络攻击同比大幅增长。该人士表示，与 2015 年同期相比，朝鲜发送黑客邮件以及试图通过入侵韩国高官手机等情况大幅增加。韩美联合军演结束后，朝鲜网络攻击频繁，要在全军范围内集中力量预防网络安全事故的发生。韩军网络司令部和韩军网络安全防御部门等 70 人出席会议。会议围绕“韩国全军网络威胁分析”、“全军统合保安管制体系的维持、保守情况”以及“2017 年全军病毒防御体系的构筑情况”等进行了讨论。

## 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，是一个非政府非盈利的网络安全技术协调组织，主要任务是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展中国互联网上网络安全事件的预防、发现、预警和协调处置等工作，以维护中国公共互联网环境的安全、保障基础信息网络和网上重要信息系统的安全运行。目前，CNCERT 在我国大陆 31 个省、自治区、直辖市设有分中心。

同时，CNCERT 积极开展国际合作，是中国处理网络安全事件的对外窗口。CNCERT 是国际著名网络安全合作组织 FIRST 正式成员，也是 APCERT 的发起人之一，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。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。

## 联系我们

如果您对 CNCERT《网络安全信息与动态周报》有何意见或建议，欢迎与我们的编辑交流。

本期编辑：郑亚伟

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话： 010-82990158