国家互联网应急中心

网络安全信息与动态周报

2016 年第 50 期

12 月 5 日-12 月 11 日

CNCERT/CC

本周网络安全基本态势

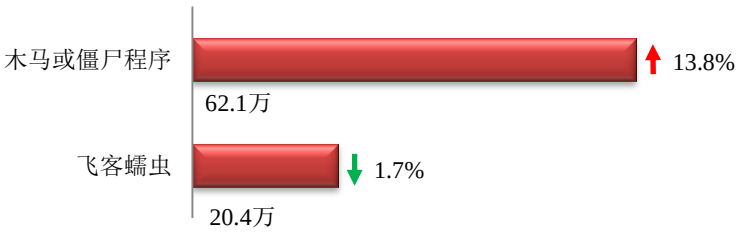
优 良 中 差 危

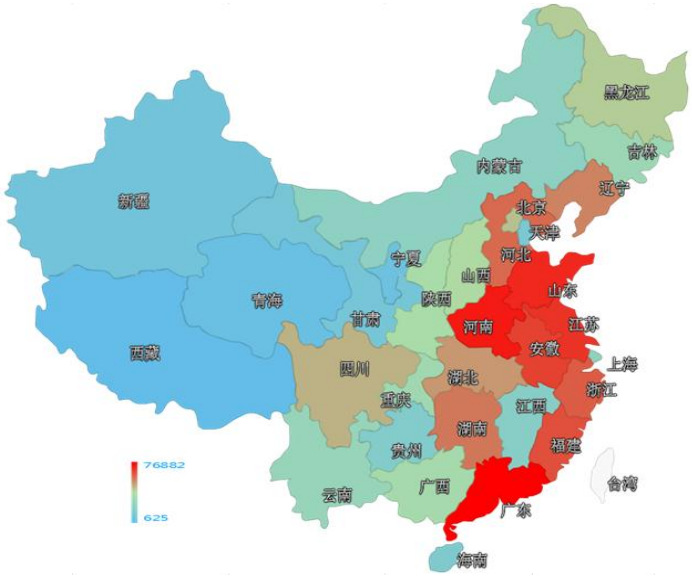
境内感染网络病毒的主机数量	•82.5万	↑ 9.5%
境内被篡改网站总数 其中政府网站数量	•3330 •85	↓ 2.6% ↓ 1.2%
境内被植入后门网站总数 其中政府网站数量	•1724 •35	↑ 8.2% ↓ 2.8%
针对境内网站的仿冒页面数量	•2417	↑ 9.9%
新增信息安全漏洞数量 其中高危漏洞数量	•175 •62	↓ 12.5% ↓ 23.5%

═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 82.5 万个，其中包括境内被木马或被僵尸程序控制的主机约 62.1 万以及境内感染飞客（conficker）蠕虫的主机约 20.4 万。





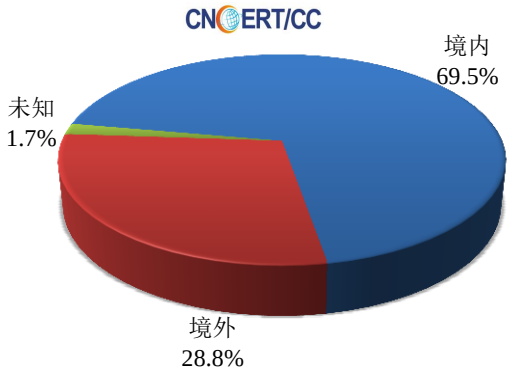
木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、河南省和山东省。

TOP3

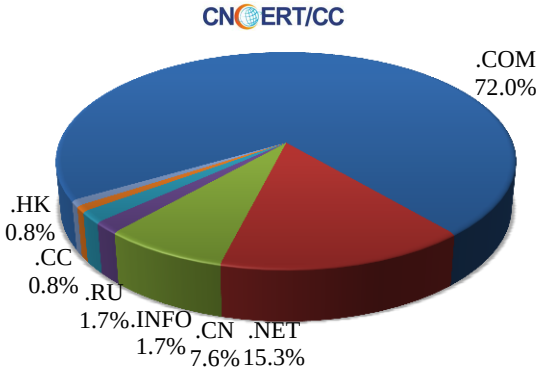
广东省	•约7.7万个（约占中国大陆总感染量的12.4%）
河南省	•约4.3万个（约占中国大陆总感染量的7.0%）
山东省	•约4.2万个（约占中国大陆总感染量的6.8%）

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 118 个，涉及 IP 地址 347 个。在 118 个域名中，有 28.8%为境外注册，且顶级域为.com 的约占 72.0%；在 347 个 IP 中，有约 5.5%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 12 个 IP。

本周放马站点域名注册所属境内外分布
(12/5-12/11)



本周放马站点域名所属顶级域的分布
(12/5-12/11)



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。

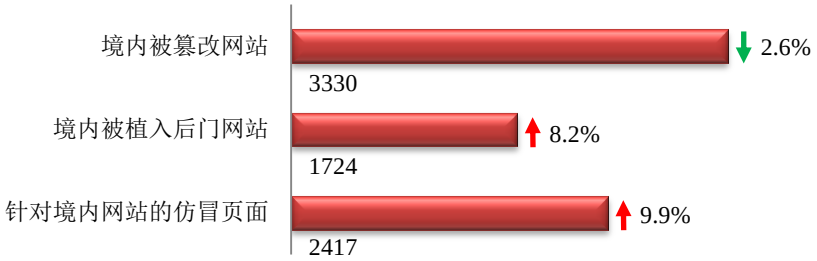
ANVA恶意地址黑名单发布地址

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。

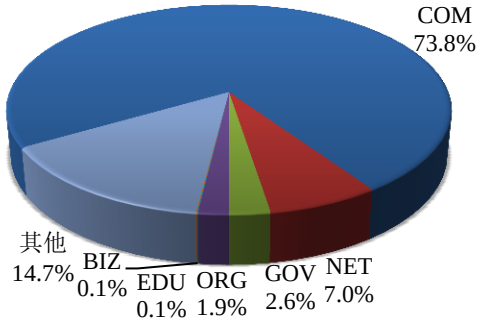
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 3330 个；境内被植入后门的网站数量为 1724 个；针对境内网站的仿冒页面数量为 2417。

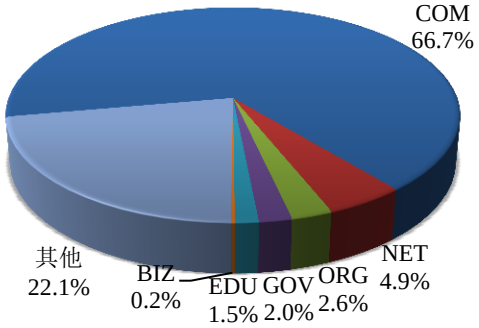


本周境内被篡改政府网站（GOV 类）数量为 85 个（约占境内 2.6%），较上周环比下降了 1.2%；境内被植入后门的政府网站（GOV 类）数量为 35 个（约占境内 2.0%），较上周环比下降了 2.8%；针对境内网站的仿冒页面涉及域名 2105 个，IP 地址 793 个，平均每个 IP 地址承载了约 3 个仿冒页面。

本周我国境内被篡改网站按类型分布
(12/5-12/11)

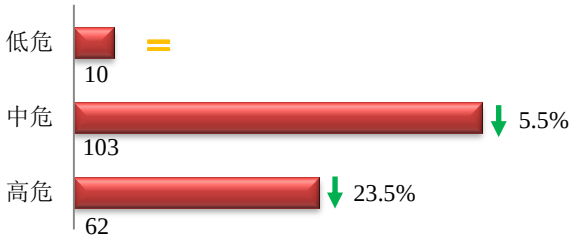


本周我国境内被植入后门网站按类型分布
(12/5-12/11)

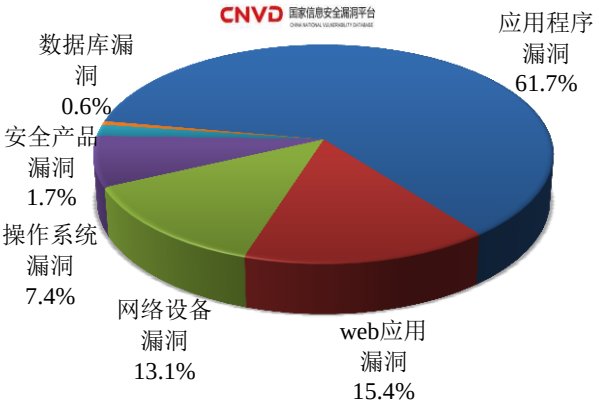


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 175 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
(12/5-12/11)



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 应用漏洞和网络设备漏洞。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

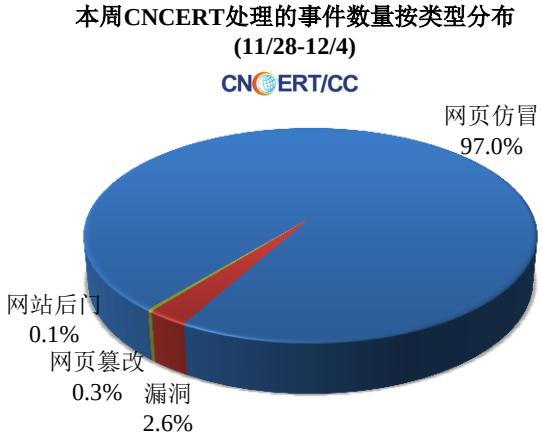
CNVD漏洞周报发布地址

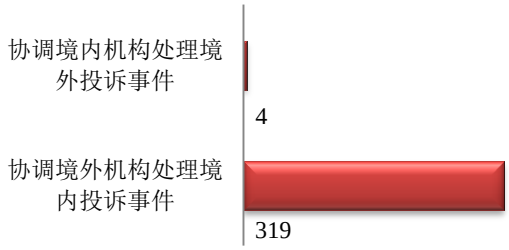
http://www.cnvd.org.cn/webinfo/list?type=4

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。

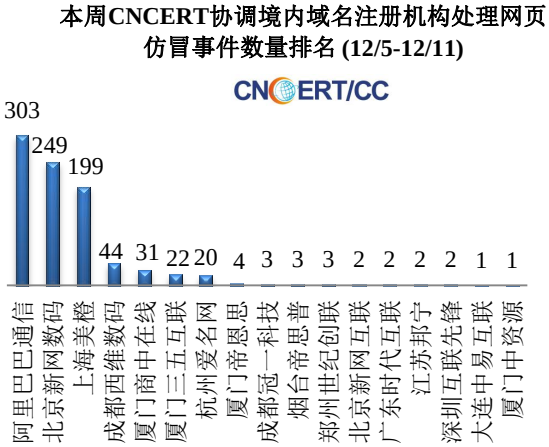
本周事件处理情况

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 1241 起，其中跨境网络安全事件 323 起。



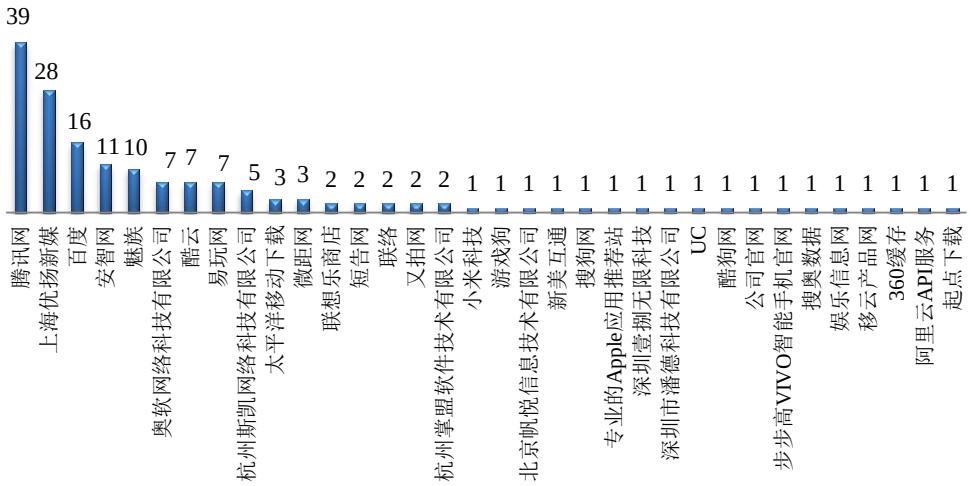


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 1204 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事 1185 起和互联网服务提供商仿冒事件 10 起。



本周，CNCERT 协调 34 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 164 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 (12/5-12/11)



业界新闻速递

1、中美举行第三次打击网络犯罪及相关事项高级别联合对话

新华网 12 月 8 日消息 第三次中美打击网络犯罪及相关事项高级别联合对话 12 月 7 日在华盛顿举行。国务委员、公安部部长郭声琨与美国司法部部长林奇、国土安全部部长约翰逊共同主持。双方回顾了首次对话以来取得的成果，充分肯定对话机制的重要性、必要性，就继续深化中美网络安全各领域合作达成诸多新共识。中美双方在此次对话中就推进打击网络犯罪、网络安全合作、完善热线联络机制、网络反恐合作、情报信息共享等达成广泛共识，取得积极成果，在落实两国元首达成的共识方面取得重要进展。双方提议 2017 年在中国举行第四次对话。公安部副部长陈智敏、国家网信办副主任王秀军、外交部副部长郑泽光、工信部副部长陈肇雄、国家安全部副部长苏德良、司法部副部长刘志强以及美国司法部、国土安全部、国务院、联邦调查局等部门负责人参加了对话。

2、美国网络安全强化委员会发布网络安全建议报告

赛迪网 12 月 7 日消息 今年 2 月，美国总统奥巴马成立了的国家网络安全强化委员会旨在通过一系列长期与短期举措改善美国的网络安全态势。近期，该强化委员出台了一份网络安全建议报告，该报告详细说明了奥巴马对网络安全的愿景、对网络威胁的演变表示了极大的关注。同时报告还对奥巴马政府和即将当选总统的特朗普提出了 16 条网络安全政策建议。建议包括整合国际网络安全政策和全球行为规范、制定评估不安全联网设备所致安全责任的法律、任命“网络安全大使”带领美国在相关战略和实践上与国际社会接触、与其它国家合作制定并推进国际网络安全标准和行为、提高政府和私有部门之间的合作等。该报告详细说明了奥巴马对网

络安全的愿景、对网络威胁的演变表示了极大的关注，并提出了确保国家基础设施的建议。

3、普京签署法令批准俄信息安全学说

亚太日报 12 月 6 日消息 据俄法律信息网站消息，普京 12 月 5 日签署了关于批准信息安全学说的法令。据报道，俄信息安全学说旨在保证俄在信息领域的国家安全，并从战略层面防止和遏制与信息科技相关的军事冲突。根据这一学说，当前俄在信息安全领域面临诸多问题，比如部分外国机构利用俄信息基础设施从事间谍活动；个别国家的情报机构利用信息在其他国家内部制造混乱，以破坏其主权和领土完整；一些国外媒体的报道对俄国家政策诋毁增多，俄媒体在国外经常遭到歧视；同时外国情报机构正试图对俄青年施加影响，以改变他们的传统道德价值观。该学说认为，近年来俄在金融借贷领域的计算机犯罪案件有所增多，在涉及经济方面的信息安全领域存在很多不足，如俄国内工业在电子元件、软件支持等领域很大程度上仍依赖外国信息科技机构。该学说强调，保证信息安全的战略意义是为了保护俄国家主权和领土完整，实现俄政治和社会稳定，并保证俄公民人权以及俄重要信息基础设施的安全。

4、澳大利亚建网络安全卓越学术中心

人民网 12 月 6 日消息 澳大利亚联邦政府近日宣布，将投入 450 万澳元（约合人民币 2290 万元）成立网络安全卓越学术中心，通过教育和研究手段，提升澳大利亚网络安全能力。澳政府希望该中心能解决该国网络安全人才短缺的问题。澳大利亚教育和培训部长伯明翰和网络安全助理部长特翰表示，该中心将对即将进入社会就业的学生加强网络安全相关的能力培训，充实国家网络安全队伍，引领世界网络安全研究，为工业部门和政府提供管理教育培训。特翰称，网络安全卓越学术中心延伸了政府的职能范围，通过澳大利亚网络安全挑战赛和女性参与网络活动等形式，鼓励更多的人投身网络安全事业。2015 年 12 月，澳大利亚总理特恩布尔宣布投入 3000 万澳元（约合人民币 1.5 亿元）成立一个以工业为主导的网络安全发展中心，作为总投入为 11 亿澳元（约合人民币 56.1 亿元）的国家科学与创新计划的一部分，以发展澳大利亚网络安全产业。2016 年 4 月，特恩布尔发布《澳大利亚网络安全战略》，旨在保卫国家免受有组织的犯罪分子及具有国家背景的黑客组织发动的网络攻击。此前，澳大利亚国防部白皮书称将投入 4 亿澳元（约合人民币 20.4 亿元）进行网络安全行动。

5、日本实施防网络攻击演习迎接奥运 约 2000 人参加

中新网 12 月 7 日消息 据日本媒体报道，作为面向 2020 年东京奥运会和残奥会的网络攻击对策，日本政府 7 日实施了以电力、铁路、金融等重要基础设施 13 个领域的企业与机构为对象的联合演习。据报道，此次演习主要在东京和大阪的两个会场实施，来自官方和民间约 500 个机构的约 2000 人参加，为迄今最大规模。演习还设想了发电站及列车操纵系统感染电脑病毒导致供电和铁路运行出现故障的严重情形。此次演习为各企业安排了不同情景，检验了初期应对及官民情报共享工作是否到位。报道称，东京奥运这一国际盛事容易成为黑客的攻击目标，预计攻击将剧增。当天在东京会场聚集了约 700 人。日本奥运相丸川珠代到场出席并致辞表示“需要做好万全准备，以防不测事态”。此外，还有一些来自通过网络互联的各企业的参加者。

6、日本化妆品行业巨头资生堂 42 万用户信息被黑客窃取

E 安全 12 月 6 日消息 日本化妆品行业巨头资生堂公司上周五宣布遭遇数据泄露事件。黑客入侵了资生堂

子公司 IPSA 茵芙莎公司运营的化妆品网店，共计 42 万顾客的个人信息数据被泄，包括财务信息。据 The Mainichi 网站报道称，“日本化妆品制造商资生堂上周五表示，其子公司 IPSA 运营的网店遭遇非法入侵，约 42 万顾客个人信息可能被泄。”这家日本媒体报道称，被盗数据包括顾客姓名和地址。IPSA 公司证实，部分顾客的财务数据可能被泄，约 5.6 万顾客的信用卡信息也可能被泄。IPSA 公司承认，信用卡数据属于 2011 年 12 月 14 日至 2016 年 11 月 4 日期间在该网店有购买记录的用户。资生堂及时向日本当局报告了这起数据泄露事件，包括日本经济、贸易和工业部。日本警方着手调查此案。IPSA 公司已暂时关闭网店。

7、国际刑警捣毁最大僵尸网络基础设施平台——雪崩 Avalanche

E 安全 12 月 5 日消息 三十多个国家的警察和检察官上周四突袭大规模跨国网络犯罪行动，搜查欧洲几十个场所，并逮捕 5 名嫌犯，查获近 40 台计算机服务器。警察和检察官调查所谓的“雪崩（Avalanche）网络”长达四年之久。雪崩网络可谓僵尸网络、恶意软件和勒索软件的托管和管理系统。欧洲刑警组织（Europol）和欧洲检察官组织（Eurojust）发表声明称，通过与互联网服务提供商（ISP）协作，该行动将超过 221 个犯罪服务器关闭。ISP 最初警告 180 多个国家的 50 万受害者，其电脑被“雪崩”管理的 20 多个恶意软件家族感染。欧洲检察官组织负责人 Michèle Coninsx 表示，“此次行动强调跨国机构之间的实际和战略重要性。德国、美国当局，欧盟以及国际伙伴，在欧洲检察官组织和欧共体的支持下，全球最大的恶意僵尸网络基础设施—雪崩被捣毁，这是有史以来对僵尸网络基础设施平台最大型的摧毁行动。”公告还表示，查获并关停超过 80 万域名地址，这是有史以来使用 URL Sinkholing 对抗恶意软件基础设施的最大型行动。

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：王英

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话： 010-82990158