国家互联网应急中心

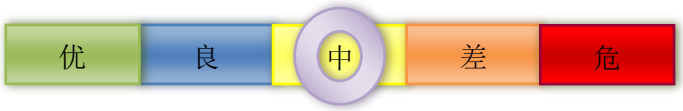
网络安全信息与动态周报

2016 年第 21 期

5 月 16 日-5 月 22 日

CNCERT/CC

本周网络安全基本态势

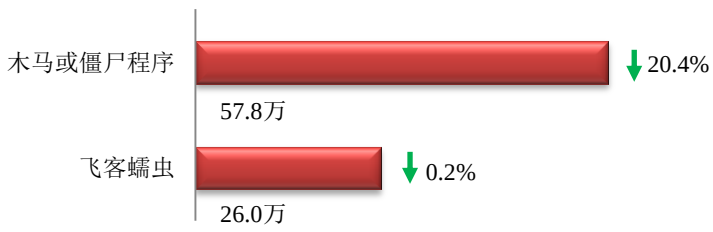


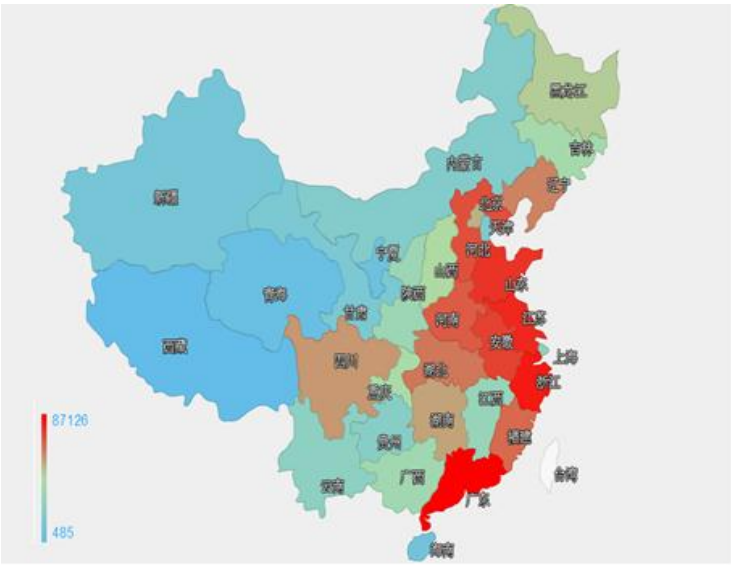
境内感染网络病毒的主机数量	•83.8万	15.0%
境内被篡改网站总数 其中政府网站数量	•3143 •76	6.0% 10.6%
境内被植入后门网站总数 其中政府网站数量	•8823 •230	37.3% 44.6%
针对境内网站的仿冒页面数量	•4861	75.9%
新增信息安全漏洞数量 其中高危漏洞数量	•219 •83	21.2% 25.9%

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

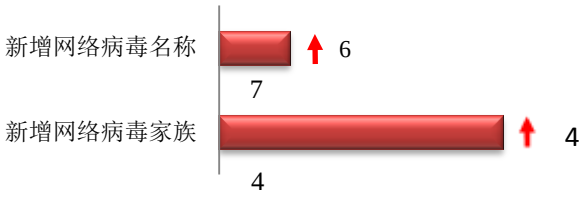
本周境内感染网络病毒的主机数量约为 83.8 万个，其中包括境内被木马或被僵尸程序控制的主机约 57.8 万以及境内感染飞客（conficker）蠕虫的主机约 26.0 万。





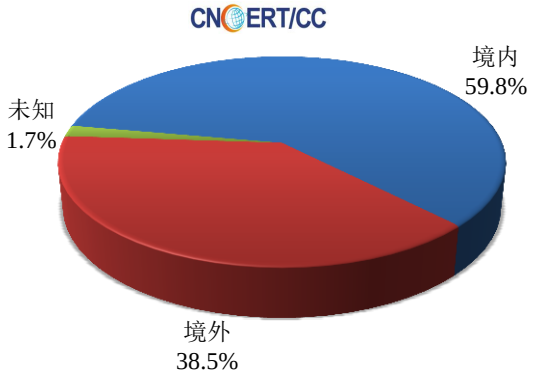
木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、浙江省和江苏省。

本周 CNCERT 捕获的新增网络病毒文件，按网络病毒名称统计新增 7 个，按网络病毒家族统计新增 4 个。

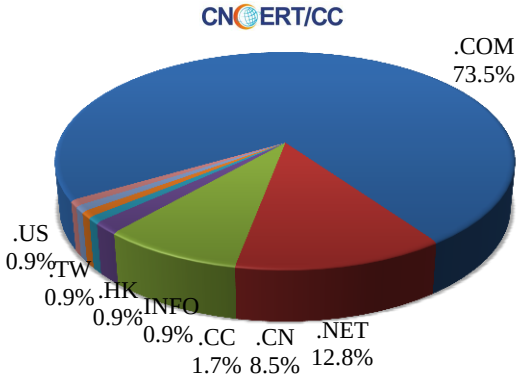


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 117 个，涉及 IP 地址 363 个。在 117 个域名中，有 38.5%为境外注册，且顶级域为.com 的约占 73.5%；在 363 个 IP 中，有约 94.2%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 26 个 IP。

本周放马站点域名注册所属境内外分布
(5/16-5/22)



本周放马站点域名所属顶级域的分布
(5/16-5/22)



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。

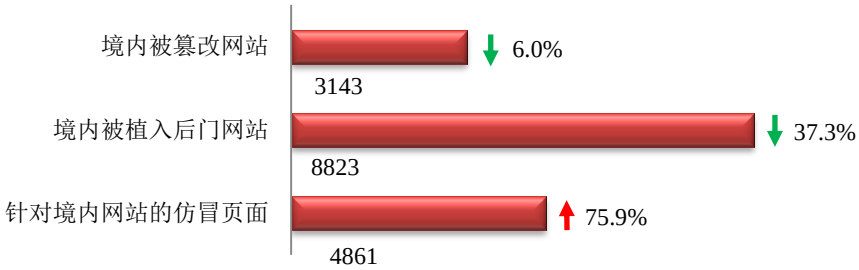
ANVA恶意地址黑名单发布地址

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。

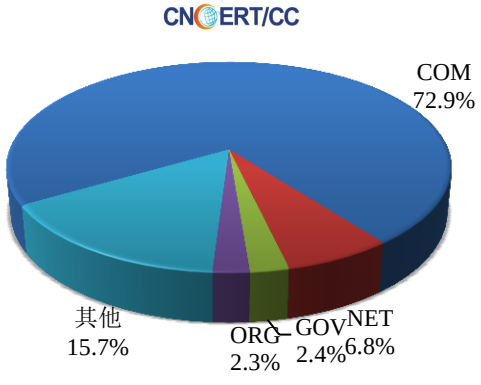
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 3143 个；境内被植入后门的网站数量为 8823 个；针对境内网站的仿冒页面数量为 4861。

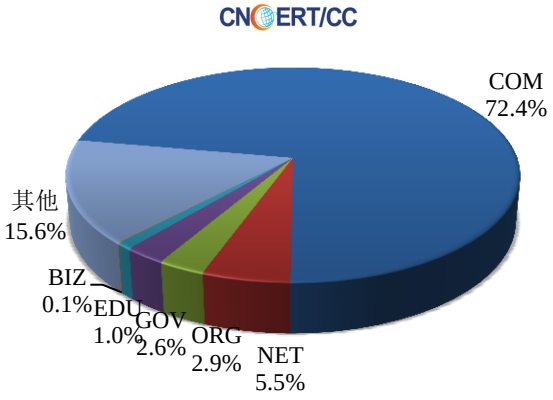


本周境内被篡改政府网站（GOV 类）数量为 76 个（约占境内 2.4%），较上周环比下降了 10.6%；境内被植入后门的政府网站（GOV 类）数量为 230 个（约占境内 2.6%），较上周环比下降了 44.6%；针对境内网站的仿冒页面涉及域名 1967 个，IP 地址 1289 个，平均每个 IP 地址承载了约 4 个仿冒页面。

本周我国境内被篡改网站按类型分布
(5/16-5/22)

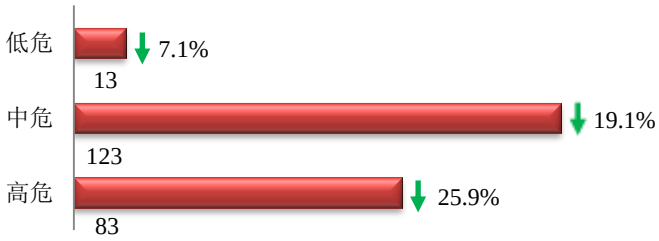


本周我国境内被植入后门网站按类型分布
(5/16-5/22)

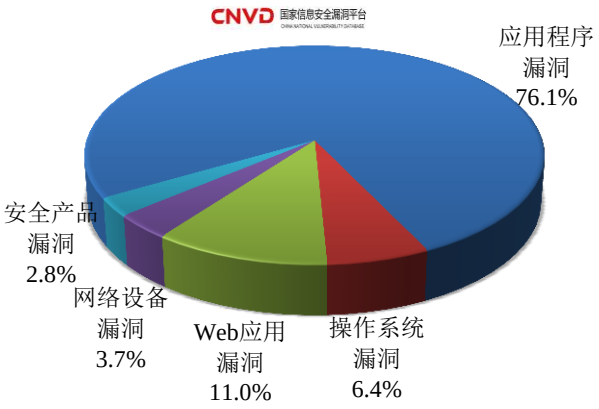


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 219 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
(5/16-5/22)



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

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

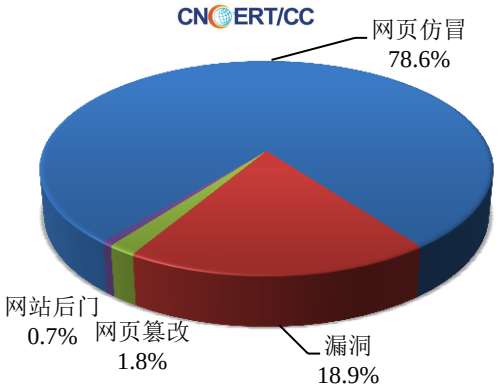
http://www.cnvd.org.cn/webinfo/list?type=4

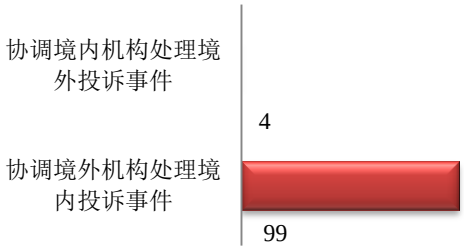
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 760 起，其中跨境网络安全事件 183 起。

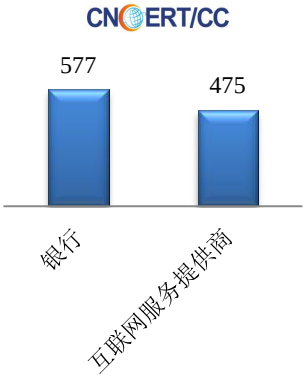
本周CNCERT处理的事件数量按类型分布
(5/16-5/22)



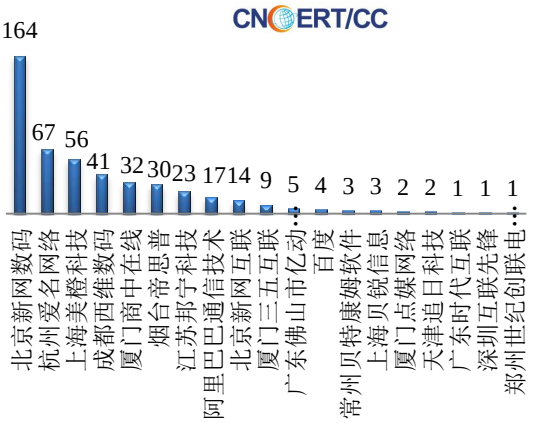


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 1052 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事 577 起和互联网服务提供商仿冒事件 475 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(5/16-5/22)

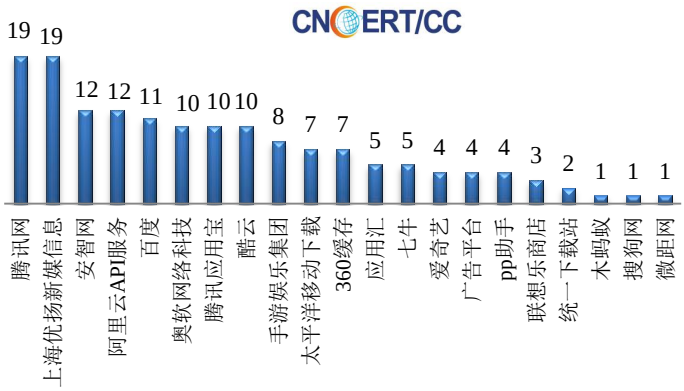


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (5/16-5/22)



本周，CNCERT 协调 21 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 155 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 (5/16-5/22)



业界新闻速递

1、工信部：《网络安全法》今年有望出台

在日前召开的“第十三届中国信息港论坛”上，工业和信息化部网络安全管理局局长赵志国表示，大数据安全面临四大问题，目前我国正积极推进《电信法》立法进程。如果顺利，今年《网络安全法》有望出台。据中国通信网 5 月 16 日消息，赵志国表示，大数据不断发展的同时，安全问题引起各方面的高度关注。赵志国强调，“从大数据安全角度来看，大数据主要面临四个问题：一方面黑客攻击、病毒等传统的网络安全问题不断向大数据领域渗透。另一方面，大数据发展带来新的问题：一是数据滥用的问题；二是数据的窃取问题；三是大数据核心技术缺乏自主可控问题；四是数据主权和权属问题。” 赵志国表示，目前大数据安全的工作主要是统筹好数据开放共享和隐私保护，以编制出台《信息通信网络与信息安全十三五规划》为牵引，重点抓好网络基础设施安全防护、大数据安全管理、网络信息安全技术保障能力建设、网络生态治理、互联网企业安全监管和人才培养等六个方面的工作。在谈到信息安全立法问题时，赵志国指出，“国家正积极推动出台《网络安全法》并抓好落地实施，积极推进《电信法》立法进程。如果顺利，今年《网络安全法》有望出台。” 业界预计，随着网络支付普及和车联网蓬勃发展，我国网络安全投入将不断增加。“十三五”规划明确指出，要实施网络强国战略的同时，将“安全”作为未来信息基础设施的重要内涵。在未来五年政府的 100 项重大建设项目中，国家网络空间建设被排在第六位，可见网络空间安全建设在政府工作中的重要程度。随着项目的启动，网络安全产业有望在“十三五”期间迈进建设高峰期，预计未来数年，行业复合增速有望达 30%。A 股中启明星辰、绿盟科技、卫士通等上市公司，涉及网络安全相关业务。

2、越南一家银行遭到黑客攻击 SWIFT 存在安全漏洞

没有枪支弹药，没有偷偷塞向柜台的小纸条，更没有耗工数月通往保险库的隐蔽密道——时隔两个月，又一家银行被洗劫一空。上周五，环球银行金融电信协会（SWIFT）表示，黑客对一家商业银行发动了恶意程序攻击，并成功绕过银行风险控制系统入侵这家银行的资金转移系统。虽然受攻击银行的名称、所属国家和损失金额等细节并未被透露，但根据英国国防网络承包商 BAE Systems Plc 的推测，这家商业银行地处越南，且与两个月前的孟加拉国央行失窃案存在颇多相似之处。此外，黑客的技术和当年日本索尼被攻击的恶意软件代码有很多相似之处，当时这起案件被疑为朝鲜黑客所为。今年 3 月初，未知黑客入侵孟加拉国央行在纽约联邦储备银行的账户，盗走 8100 万美元，作为有史以来规模最大的网络盗窃案而轰动全球。至今，受害者孟加拉国央行并未完全脱离风险。一家美国计算机安全公司的调查报告显示，黑客们仍然潜伏在孟加拉国央行的网络中，令该国有再度遭受攻击的可能。有意思的是，这两起黑客侵入事件的作案手法十分雷同：均通过恶意程序盗取转账凭证，并更改 SWIFT 软件发出虚假验证信息以隐藏汇款流向。这意味着，前次孟加拉国央行遭遇黑客入侵并非孤例。SWIFT 在声明中称，黑客使用的入侵手段显示出了“在目标银行的特定操作控制方面拥有深刻而复杂的知识”，因而很有可能存在银行内鬼或其他网络攻击协助（或者二者兼有）。根据《华尔街日报》，美国联邦调查局（FBI）特工目前已找到表明至少有一名孟加拉国央行员工充当共犯的证据。更糟糕的是，由于几个月

前 SWIFT 计算机雇员将央行的首个实时全额结算系统（RTGS）连接上了 SWIFT 的讯息平台，这使得央行变得更容易受到黑客入侵。SWIFT 此前已承认，存有某种恶意软件旨在防止银行察觉欺诈交易。作为一个全球性的电文传递网络，SWIFT 被世界各地的银行和其他金融机构用来发送支付指令，它已成为全球金融体系的重要组成部分。上个月，世界各地使用 SWIFT 支付网络的银行已被要求进行一次紧急软件升级。事实上，《金融时报》早在今年 4 月便曾报道，孟加拉国央行被窃事件很可能重演。当时，受聘调查孟加拉国央行被窃事件的网络安全公司 FireEye 也声明，已经在其他金融服务机构观察到了黑客活动，很可能出自对孟加拉国央行发起网络攻击的同一个威胁源。这一声明被认为是在警告孟加拉国央行失窃案仅是“针对目标银行的大型入侵行动”的一部分，犯罪分子将再次发起一波针对银行的攻势。世界多个大银行的接连失窃令银行界开始“人人自危”。《央行杂志》出版人卡佛表示，各国央行虽然一直在关注网络犯罪，但最初只是把目光投向国内的银行业和自己的网站，但事实证明是国际支付的神经系统 SWIFT 存在安全漏洞，这让各国央行非常担忧。

3、美网络安全演练 召集 1.4 万黑客“黑掉五角大楼”

参考消息网 5 月 17 日报道俄媒称，美国举行保障网络安全大型演练过程中，约 1.4 万名黑客尝试入侵国防部网络系统。美国国防部新闻发言人彼得·库克 16 日表示，名为“黑掉五角大楼”的项目自 4 月下旬启动，至上周结束。据俄罗斯卫星新闻网 5 月 17 日报道，库克称："国防部长阿什顿·卡特对演练结果非常满意。我们认为该项目是成功的。"他表示，此次演练参与者从志愿参加的美国公民中选出，演练有利于“发现漏洞并制定应对措施”以保护五角大楼的网络系统。“此次演练让我们注意到那些自己未能发现的东西。” 库克还表示，演练过程中黑客们要入侵国防部一些网站，演练成果不会公开，原因“众所周知”。五角大楼尚未决定是否有必要再次举行这种有上万名志愿者参与的“网络安全演练”。报道称，库克问一名到会记者，他是否也参加了这次演练。该记者在满屋笑声中说：“我没有，但我儿子参加了。”库克明确表示，在尝试突破国防部网络防护系统过程中表现出良好机敏度的“特别突出”的黑客将获得奖励。此次非常演练的总结工作将在 6 月进行。

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：徐原

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话： 010-82990158