国家互联网应急中心

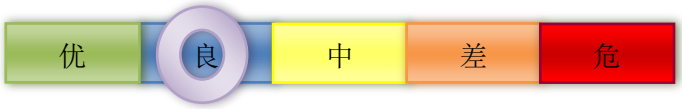
网络安全信息与动态周报

2019 年第 11 期

3 月 11 日-3 月 17 日

CNCERT/CC

本周网络安全基本态势

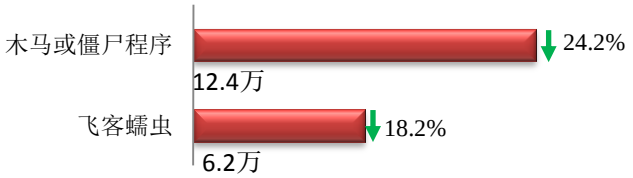


境内感染网络病毒的主机数量	• 18.6万	↓ 22.3%
境内被篡改网站总数 其中政府网站数量	• 643 • 44	↓ 8.1% ↑ 33.3%
境内被植入后门网站总数 其中政府网站数量	• 1810 • 22	↑ 220.9% ↑ 69.2%
针对境内网站的仿冒页面数量	• 1171	↓ 31.1%
新增信息安全漏洞数量 其中高危漏洞数量	• 350 • 70	↑ 45.8% ↓ 33.3%

= 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

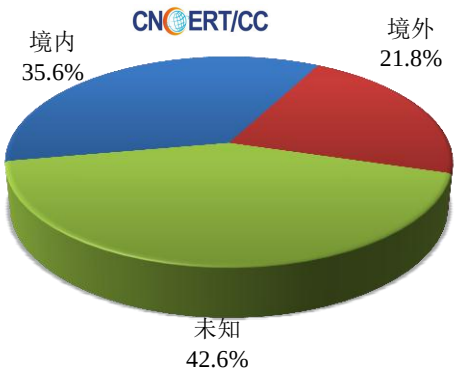
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 18.6 万个，其中包括境内被木马或被僵尸程序控制的主机约 12.4 万以及境内感染飞客（conficker）蠕虫的主机约 6.2 万。

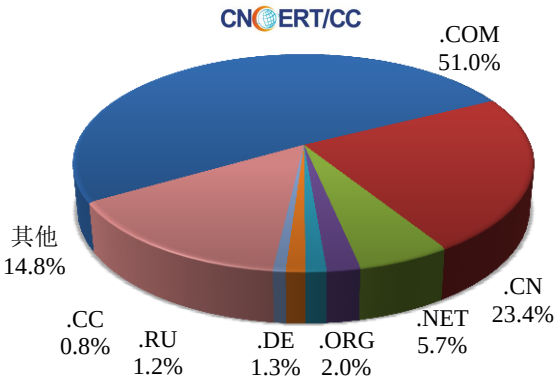


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 1982 个，涉及 IP 地址 3385 个。在 1767 个域名中，有 21.8% 为境外注册，且顶级域为.com 的约占 51.0%；在 3557 个 IP 中，有约 52.2 %位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 384 个 IP。

本周放马站点域名注册所属境内外分布
(3/11-3/17)



本周放马站点域名所属顶级域的分布
(3/11-3/17)



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。

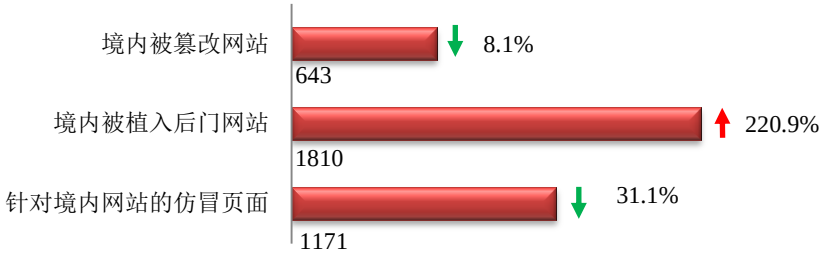
ANVA恶意地址黑名单发布地址

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。

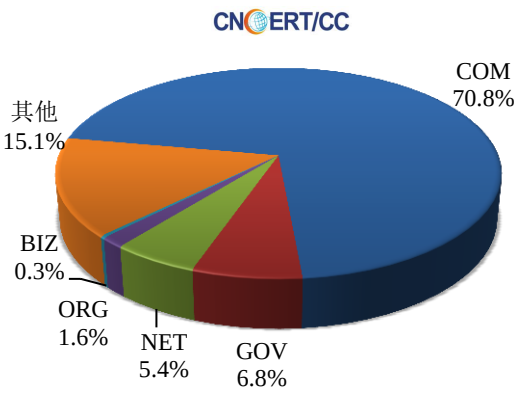
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 643 个；境内被植入后门的网站数量为 1810 个；针对境内网站的仿冒页面数量 1171 个。

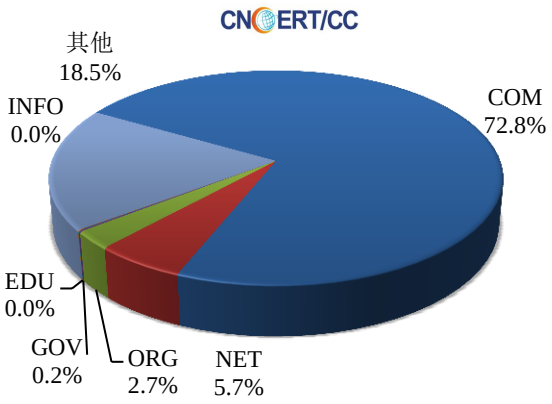


本周境内被篡改政府网站（GOV 类）数量为 44 个（约占境内 6.8%），较上周环比上升了 33.3%；境内被植入后门的政府网站（GOV 类）数量为 22 个（约占境内 0.2%），较上周环比上升了 69.2%；针对境内网站的仿冒页面涉及域名 367 个，IP 地址 215 个，平均每个 IP 地址承载了约 5 个仿冒页面。

本周我国境内被篡改网站按类型分布
(3/11-3/17)

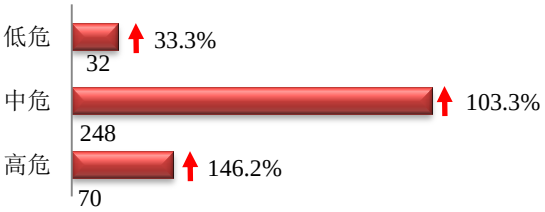


本周我国境内被植入后门网站按类型分布
(3/11-3/17)

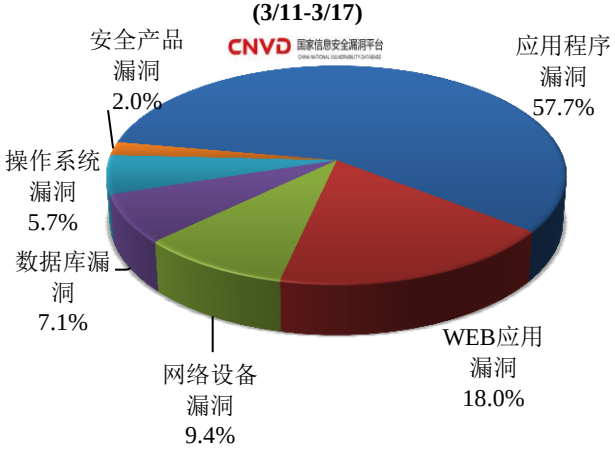


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 350 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
(3/11-3/17)



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

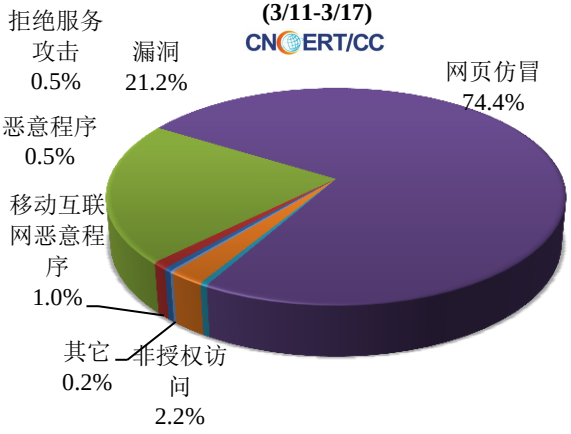
http://www.cnvd.org.cn/webinfo/list?type=4

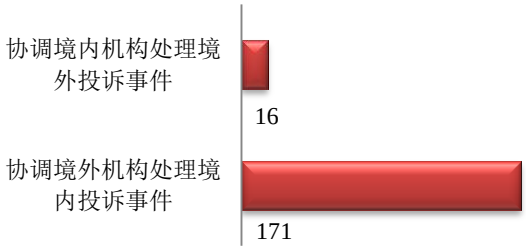
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 410 起，其中跨境网络安全事件 187 起。

本周CNCERT处理的事件数量按类型分布 (3/11-3/17)

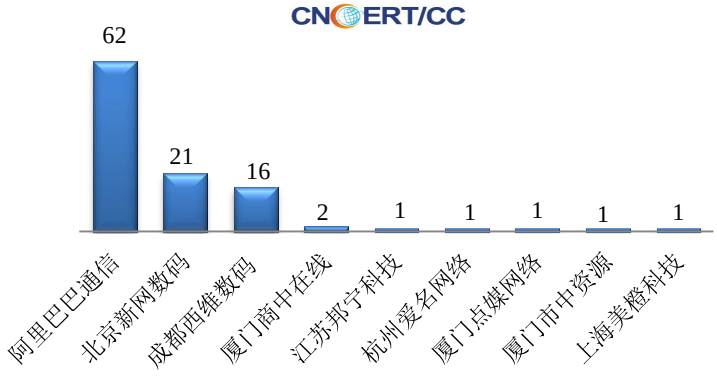




本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 305 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 296 起和政府公益事件 7 起。

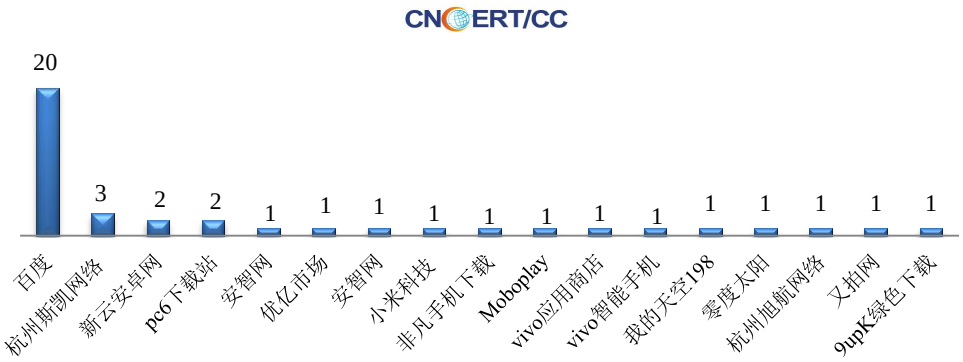
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (3/11-3/17)

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 (3/11-3/17)



本周，CNCERT 协调 17 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 40 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 (3/11-3/17)



业界新闻速递

1、教育部办公厅印发《2019 年教育信息化和网络安全工作要点》

安全内参 3 月 13 日消息 为全面落实党中央国务院对教育领域网络安全和信息化的战略部署，推动数字资源服务普及，网络学习空间应用不断深入，网络条件下的精准扶智持续推进。经教育部网络安全和信息化领导小组审议通过，印发《2019 年教育信息化和网络安全工作要点》。以习近平新时代中国特色社会主义思想为指导，深入贯彻落实党的十九大精神，全面落实全国教育大会、全国网络安全和信息化工作会议精神，围绕加快教育现代化、建设教育强国、办好人民满意的教育，以“育人为本、融合创新、系统推进、引领发展”为原则，坚持稳中求进工作总基调，深入落实《教育信息化“十三五”规划》和《教育信息化 2.0 行动计划》，实施好教育信息化“奋进之笔”，加快推动教育信息化转段升级，积极推进“互联网+教育”，坚持高质量发展，以教育信息化支撑和引领教育现代化。

2、七国集团拟制定消费者数据保护规则

参考消息网 3 月 13 日消息 日媒称，七国集团（G7）建议，针对社交网络服务等数字服务领域制定保护消费者的措施，要求企业一方在签订服务合同前完全公开信息，以防消费者在不利条件下使用网络服务。各国 IT 企业在全球持续增长，在此情况下，日美欧等发达国家将主导制定规则。据报道，不仅是被称为“GAFA”的谷歌等美国大型 IT 公司，中国的阿里巴巴、腾讯等平台企业也利用消费者数据实现了持续发展。但令人担忧的是，在网络服务便捷性增加的同时，消费者的意愿和隐私却被牺牲。

3、Citrix 收 FBI 警告：6TB 至 10TB 敏感数据被窃

2019 年 3 月 11 日 软件制造商 Citrix 近日承认公司已经沦为数据泄露的新受害者，导致国

际黑客窃取了大量的数据。公司表示美国联邦调查局（FBI）已经就此事和公司取得联系，并警告称本次网络攻击行为极有可能是伊朗黑客组织所为，窃取了 6TB 至 10TB 的商业文件。根据披露的细节显示，黑客使用了一种名为“password spraying”的策略，他们利用弱密码获取有限的访问权限，然后努力绕过其他安全系统。但真正的问题是，作为政府承包商，该公司拥有大量敏感数据。

4、户外品牌 Kathmandu 网店遭黑客攻击，客户交易信息泄露

安全内参 3 月 15 日消息 在澳洲证券交易所上市的全球户外服饰和设备零售商 Kathmandu 披露，该公司在节后销售旺季遭遇数据泄露，客户的个人和支付信息被窃取。Kathmandu 在 Magento 电子商务平台上运营网上商店，过去几年，也曾有犯罪分子在未打补丁的服务器上攻击这个平台，并植入盗卡恶意软件。被访问的信息包括客户的账单和货物名称、收件地址、电子邮件和电话号码，以及他们在网站上使用的信用卡或借记卡的详细信息。客户在 Kathmandu 俱乐部的用户名和密码，以及如提货和送货细节等订单备注也可以被访问。

5、Facebook 全面瘫痪，包括 Instagram 和 WhatsApp

凤凰科技 3 月 14 日消息 Facebook 用户报告称，在登录 Facebook 网站以及 Instagram 和 WhatsApp 时出现了无法加载和评论的问题，有些用户的屏幕上会显示出“账号暂时不可用”（Account Temporarily Unavailable）的消息。Facebook 发布 Twitter 消息承认了此次服务中断，但未给出服务中断的原因。目前，报告 Facebook 问题的报告最多达到了 11000 多。

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。截至 2017 年，CNCERT 与 72 个国家和地区的 211 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：王庆

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158