国家互联网应急中心

网络安全信息与动态周报

2019 年第 31 期

7 月 29 日-8 月 4 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	•22.0万	4.7%
境内被植入后门网站总数 其中政府网站数量	•3433 •54	16.0% 22.7%
针对境内网站的仿冒页面数量	•498	0.4%
新增信息安全漏洞数量 其中高危漏洞数量	•308 •82	30.5% 58.6%

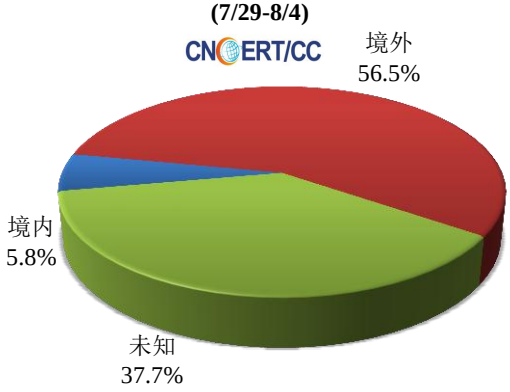
表示数量与上周相同 *表示数量较上周环比增加* *表示数量较上周环比减少*

本周网络病毒活动情况

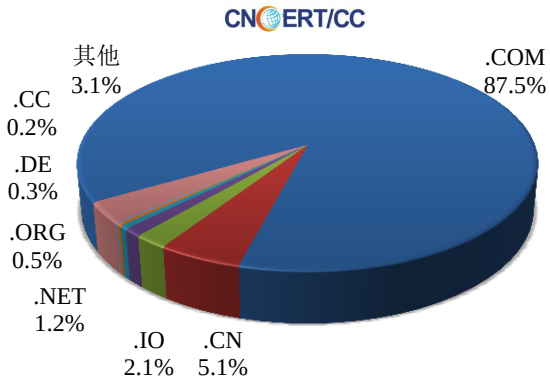
本周境内感染网络病毒的主机数量约为 22.0 万个，其中包括境内被木马或被僵尸程序控制的主机约 13.4 万以及境内感染飞客（conficker）蠕虫的主机约 8.6 万。

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 13337 个，涉及 IP 地址 4524 个。在 13337 个域名中，有 56.5%为境外注册，且顶级域为.com 的约占 87.5%；在 4524 个 IP 中，有约 50.8%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 903 个 IP。

本周放马站点域名注册所属境内外分布
(7/29-8/4)



本周放马站点域名所属顶级域的分布
(7/29-8/4)



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。

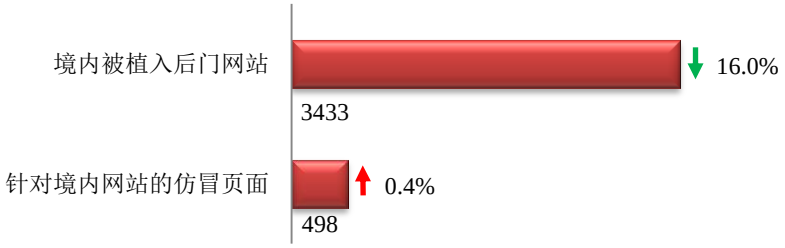
ANVA恶意地址黑名单发布地址

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。

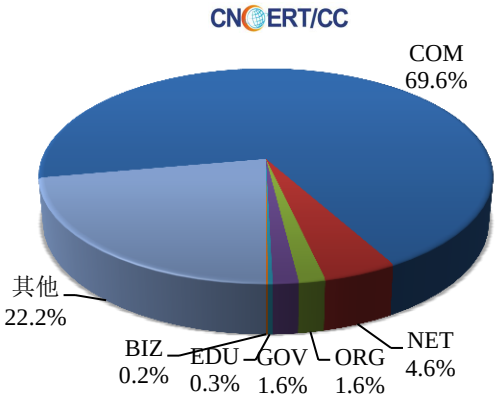
本周网站安全情况

本周 CNCERT 监测发现境内被植入后门的网站数量为 3433 个；针对境内网站的仿冒页面数量 498 个。



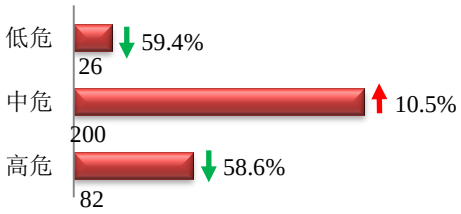
本周境内境内被植入后门的政府网站（GOV 类）数量为 54 个（约占境内 1.6%），较上周环比上涨 22.7%；针对境内网站的仿冒页面涉及域名 306 个，IP 地址 149 个，平均每个 IP 地址承载了约 3 个仿冒页面。

本周我国境内被植入后门网站按类型分布
(7/29-8/4)

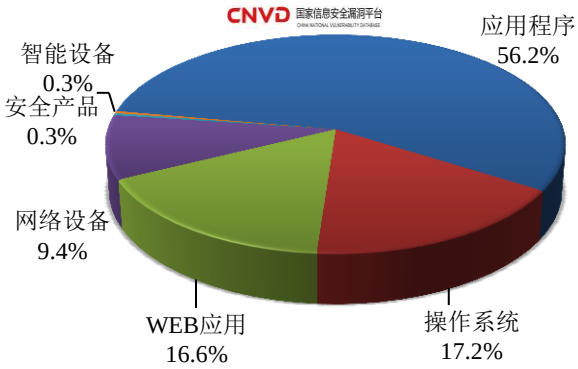


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 308 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
(7/29-8/4)



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。

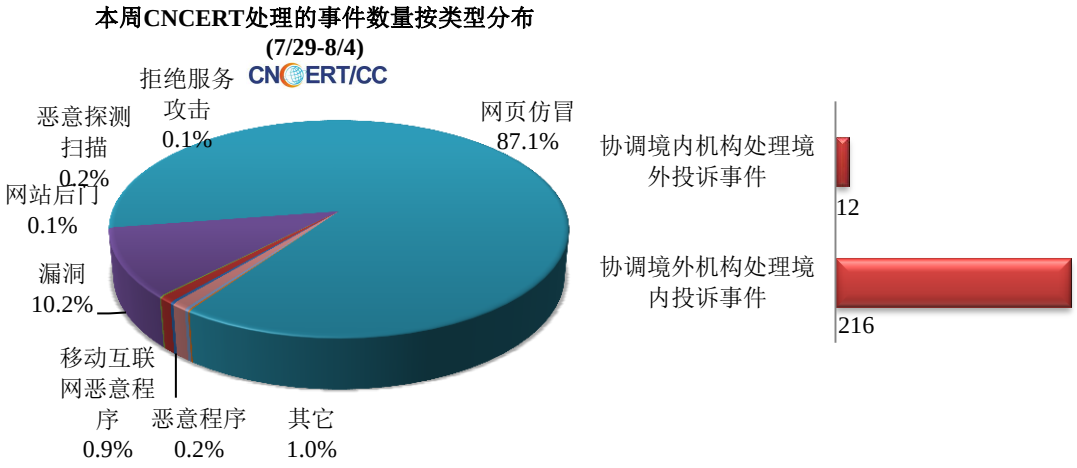
CNVD漏洞周报发布地址

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

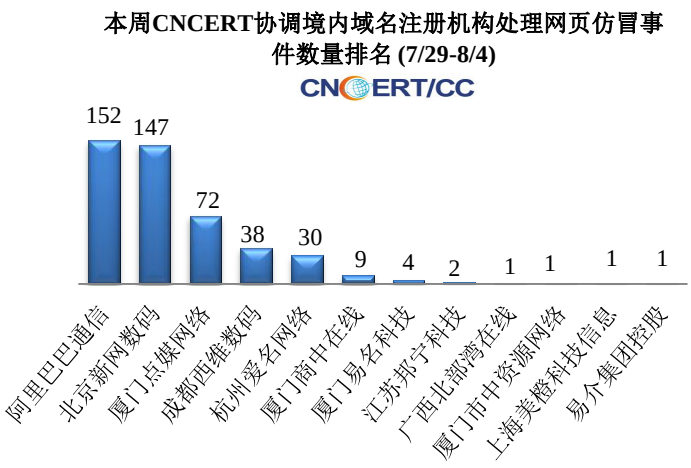
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 801 起，其中跨境网络安全事件 228 起。

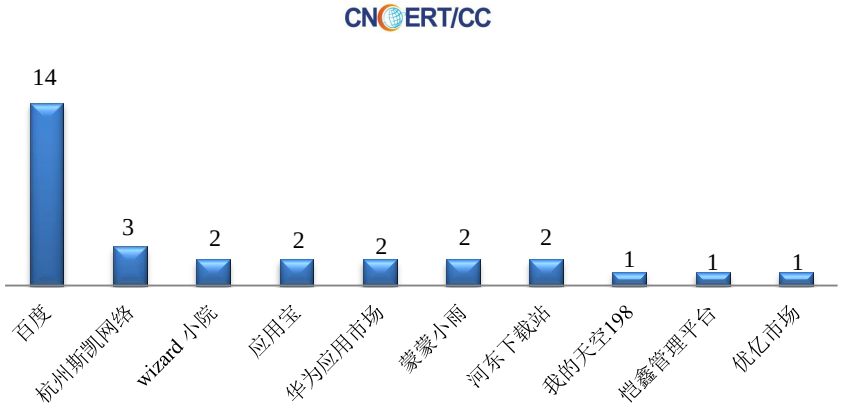


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 698 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 677 起和互联网服务提供商仿冒事件 18 起。



本周，CNCERT 协调 10 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 30 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
(7/29-8/4)



业界新闻速递

1、科技部关于印发《国家新一代人工智能开放创新平台建设工作指引》

中华人民共和国科技部官网 8 月 1 日消息 为深入贯彻落实《国务院关于印发新一代人工智能发展规划的通知》（国发〔2017〕35 号），充分发挥人工智能行业领军企业、研究机构的引领示范作用，促进人工智能与实体经济的深度融合，进一步推进国家新一代人工智能开放创新平台建设，推动我国人工智能技术创新和产业发展，科技部制定了《国家新一代人工智能开放创新平台建设工作指引》。

2、美国路易斯安那州遭遇勒索软件攻击，州长宣布进入紧急状态

E 安全 7 月 31 日消息 美国路易斯安那州在几个学区遭受网络攻击后宣布全州进入紧急状态。位于路易斯安那州北部的 Sabine，Morehouse 和 Ouachita 教区的学校系统近日都受到恶意软件袭击。黑客控制和加密了重要的网络系统，并要求勒索赎金以恢复数据。在路易斯安那州之后，过去一年中，这些类似的攻击在城市和州的袭击中显着上升，市政当局从乔治州到佛罗里达州以及美国其他地方。一种常见做法是让黑客获取并锁定城市或州的网络和文件，要求付款以扭转损害。

3、美国第一资本银行遭黑客入侵：逾 1 亿用户信息泄露

cnBeta.COM7 月 30 日消息 美国第一资本银行金融公司披露，一名黑客获取了逾 1 亿名顾客和潜在顾客的个人信息，包括姓名、地址、电话号码和生日。美国第一资本称，公司在 7 月 19 日确认了这次黑客入侵事件，

目前这名黑客已经被美国联邦调查局逮捕。在宣布这一消息后，第一资本股价在盘后交易中下跌 1%。美国第一资本表示，大约有 1 亿美国用户和 600 万加拿大用户的个人信息受到了此次事件的影响，但是黑客没有获取任何信用卡账号，超过 99%的社会安全号码没有泄露。

4、印度一公司发生信息泄漏事故

E 安全 7 月 29 日消息 一家名为 FormGet 的印度公司发生了信息泄漏事故。该公司泄露了包含“数十万”份用户上传的敏感文件，这些文件的上传时间最早可追溯到 2013 年。该公司所泄露的文件包扩：护照、驾照扫描件、工资支票以及社保号码的扫描件；银行账户报表和水电费账单的详细信息、带有姓名和电话号码的快递标签、包含联系信息的简历以及多家银行和金融公司的网络安全评估报告。

5、美妆巨头丝芙兰官网账号数据泄露

搜狐新闻 7 月 29 日消息 丝芙兰的一些客户收到了一封电子邮件，告知他们“过去两周”发现的数据泄露情况。该化妆巨头公司遭遇了数据泄露的原因在于未经授权的第三方获取了其使用在线服务的客户的个人信息。受影响的客户所在地区为新加坡、马来西亚、印度尼西亚、泰国、菲律宾、香港特别行政区（中国）、澳大利亚和新西兰等地。但对于具体受影响的客户数量，丝芙兰官方没有给出说明。

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：吕卓航

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315