国家互联网应急中心

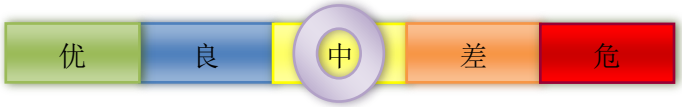
网络安全信息与动态周报

2019 年第 32 期

8 月 5 日-8 月 11 日

CNCERT/CC

本周网络安全基本态势

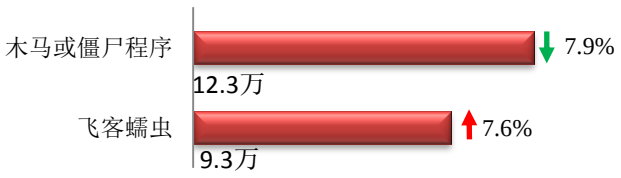


境内感染网络病毒的主机数量	•21.6万	1.9%
境内被植入后门网站总数 其中政府网站数量	•3124 •28	9.0% 48.1%
针对境内网站的仿冒页面数量	•379	23.9%
新增信息安全漏洞数量 其中高危漏洞数量	•400 •62	29.9% 24.4%

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*

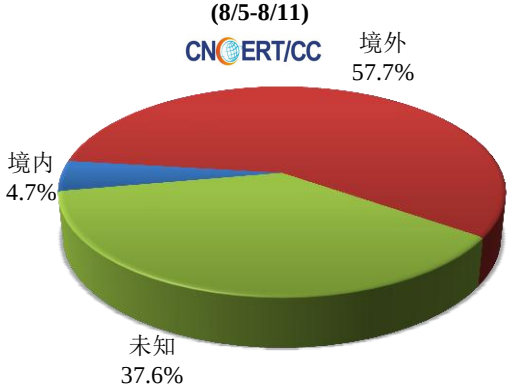
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 21.6 万个，其中包括境内被木马或被僵尸程序控制的主机约 12.3 万以及境内感染飞客（conficker）蠕虫的主机约 9.3 万。

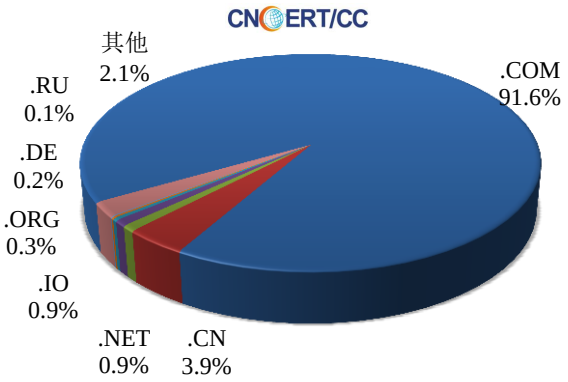


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 18816 个，涉及 IP 地址 4947 个。在 18816 个域名中，有 57.7%为境外注册，且顶级域为.com 的约占 91.6%；在 4947 个 IP 中，有约 51.0%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 838 个 IP。

本周放马站点域名注册所属境内外分布
(8/5-8/11)



本周放马站点域名所属顶级域的分布
(8/5-8/11)



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。

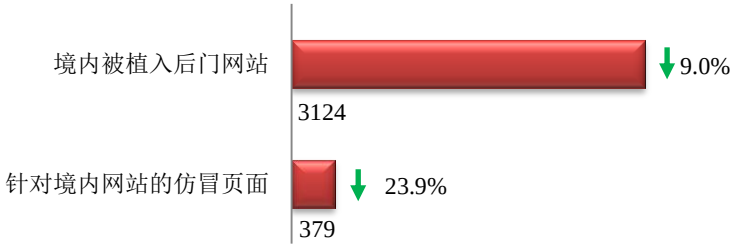
ANVA恶意地址黑名单发布地址

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。

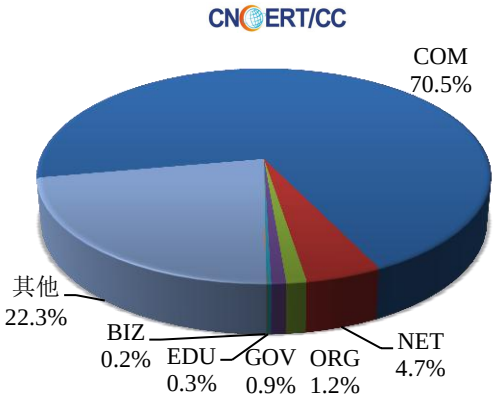
本周网站安全情况

本周 CNCERT 监测发现境内被植入后门的网站数量为 3124 个；针对境内网站的仿冒页面数量 379 个。



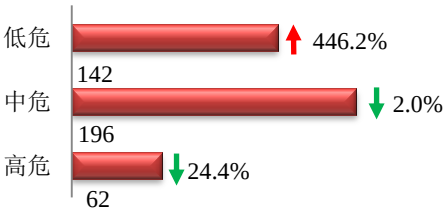
本周境内境内被植入后门的政府网站（GOV 类）数量为 28 个（约占境内 0.9%），较上周环比下降 48.1%；针对境内网站的仿冒页面涉及域名 237 个，IP 地址 145 个，平均每个 IP 地址承载了约 3 个仿冒页面。

本周我国境内被植入后门网站按类型分布
(8/5-8/11)

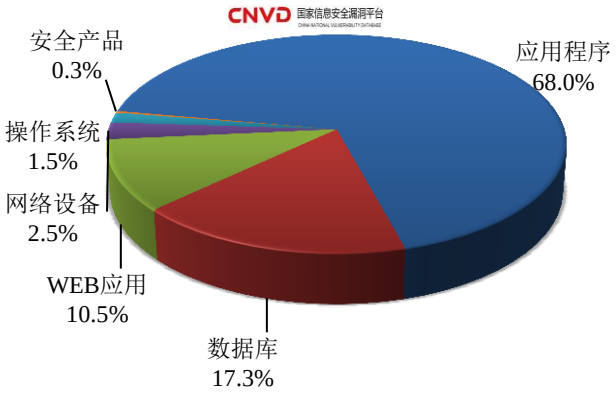


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 400 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
(8/5-8/11)



本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是数据库漏洞和 WEB 应用漏洞。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

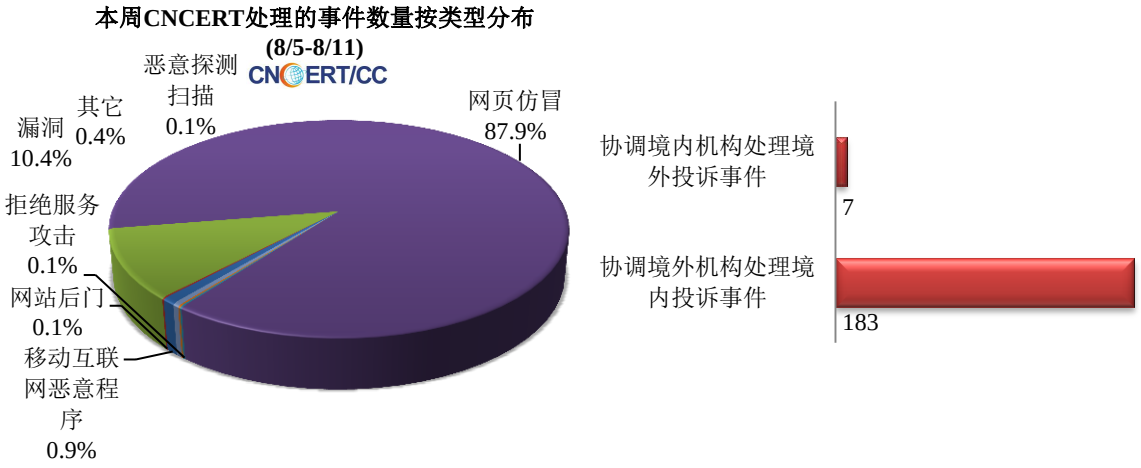
CNVD漏洞周报发布地址

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

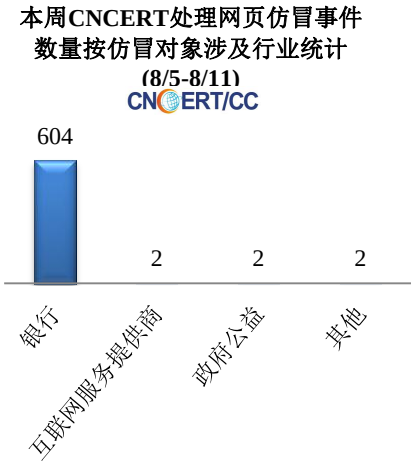
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

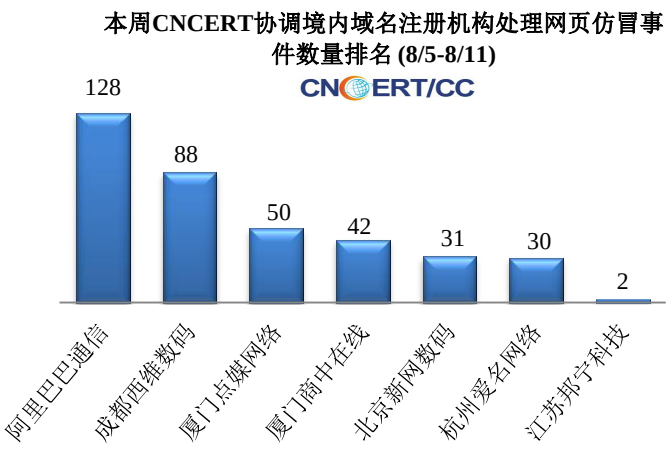
本周事件处理情况

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 695 起，其中跨境网络安全事件 190 起。



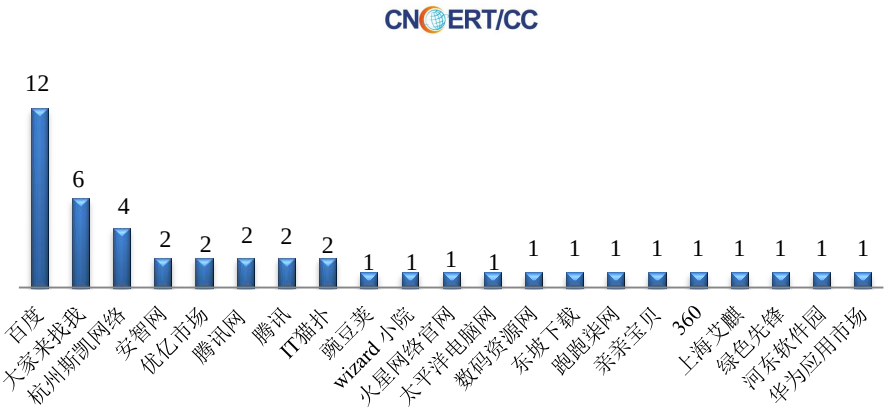
本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 610 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 604 起和互联网服务提供商仿冒事件 2 起。





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 45 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
(8/5-8/11)



业界新闻速递

1、国务院指导意见：推广大数据，加快 5G 等新一代信息基础建设

新华社8月8日消息 国务院办公厅印发《关于促进平台经济规范健康发展的指导意见》(以下简称《意见》)，为促进平台经济规范健康发展，《意见》提出了五个方面政策措施，其中包括“在实体经济中大力推广应用物联网、大数据，促进数字经济和数字产业发展”、“加强网络支撑能力建设。加快 5G 等新一代信息基础设施建设”等具体政策措施，并明确负责部门。

2、新加坡发布新的网络安全法案

E 安全 8 月 8 日消息 新加坡金融管理局（MonetaryAuthority of Singapore，简称 MAS)正式确立了旨在提高新加坡金融机构网络安全态势的新立法。立法中规定金融机构必须遵守六项主要要求，例如为着重确保 IT 系统的安全性，及时进行安全更新、并部署安全设备以限制未经授权的网络流量等。这些公司还必须实施措施以降低恶意软件感染风险、确保特特权系统帐户的安全以及加强关键系统的用户身份验证。此外，该立法还基本确定将强制要求企业执行现有的MAS技术风险管理指南(TechnologyRisk Management Guidelines)中的关键规定。

3、纽约市消防局丢失载有员工医疗记录和社会保险号的硬盘

cnBeta.COM8 月 11 日消息 纽约市消防局（FDNY）披露了 2019 年 3 月发生的“数据泄露”。与其他数据泄露事件不同，FDNY 的问题是由于一枚可移动硬盘丢失造成的。丢失的可移动硬盘包含了超过 10000 名被

FDNY EMS 运输或治疗的个人信息，该信息由员工复制到驱动器中然后丢失，目前还不清楚驱动器是否已加密。除了医疗记录外，硬盘包含 3000 名患者的社会保险号码，使他们面临身份盗窃的风险。

4、亚马逊谷歌苹果语音助手窃听风暴发酵 欧美多国开查

澎湃新闻 8 月 6 日消息 美国和欧洲的监管机构和立法机构正在对谷歌、苹果和亚马逊进行调查，审核上述三家公司是否涉嫌侵犯用户隐私，聘用专员听取用户使用电子助手时发出的指令。据美国《财富》杂志报道，苹果和谷歌公司已于近日叫停了人工审核录音的项目。此前，德国数据保护机构对苹果和谷歌曾发起调查。而亚马逊也于上周五修改了相关条例，允许用户关闭人工听取录音的功能。在欧洲地区，爱尔兰和英国的相关监管机构目前也在调查这些科技巨头是否违反了欧洲的隐私法律法规。

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：楼书逸

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315