国家互联网应急中心

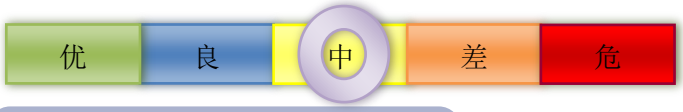
网络安全信息与动态周报

2019 年第 33 期

8 月 12 日-8 月 18 日

CNCERT/CC

本周网络安全基本态势

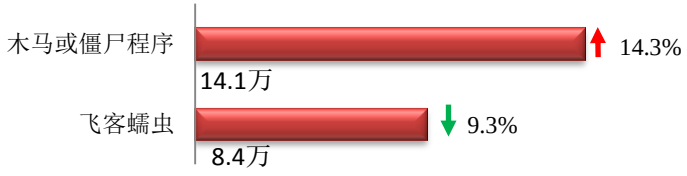


境内感染网络病毒的主机数量	•22.5万	↑ 4.2%
境内被植入后门网站总数 其中政府网站数量	•3385 •24	↑ 8.4% ↓ 14.3%
针对境内网站的仿冒页面数量	•117	↓ 69.1%
新增信息安全漏洞数量 其中高危漏洞数量	•498 •167	↑ 24.5% ↑ 169.4%

═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

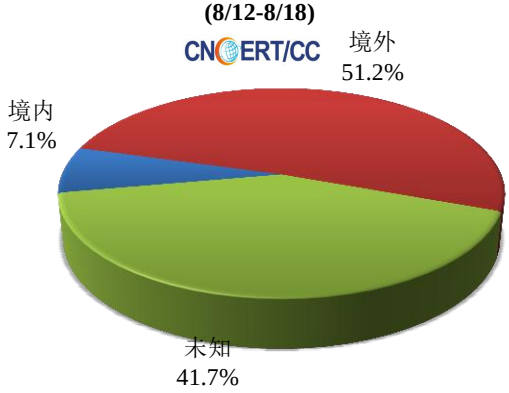
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 22.5 万个，其中包括境内被木马或被僵尸程序控制的主机约 14.1 万以及境内感染飞客（conficker）蠕虫的主机约 8.4 万。

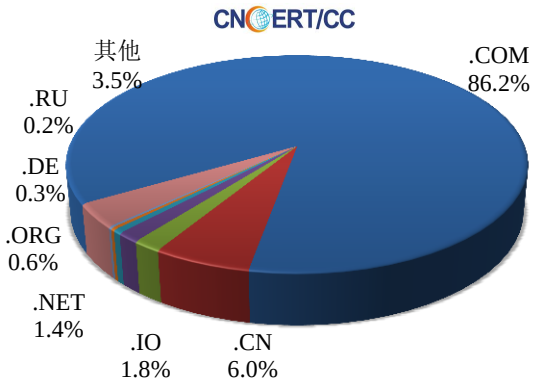


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 9893 个，涉及 IP 地址 4174 个。在 9893 个域名中，有 51.2 %为境外注册，且顶级域为.com 的约占 86.2%；在 4174 个 IP 中，有约 51.4%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 760 个 IP。

本周放马站点域名注册所属境内外分布
(8/12-8/18)



本周放马站点域名所属顶级域的分布
(8/12-8/18)



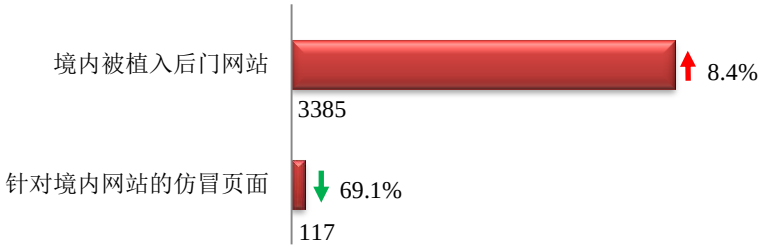
针对 CNCERT 自主监测发现以及各单位报送数据，CNCERT 积极协调域名注册机构等进行处理，同时通过 ANVA 在其官方网站上发布恶意地址黑名单。

ANVA恶意地址黑名单发布地址

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。

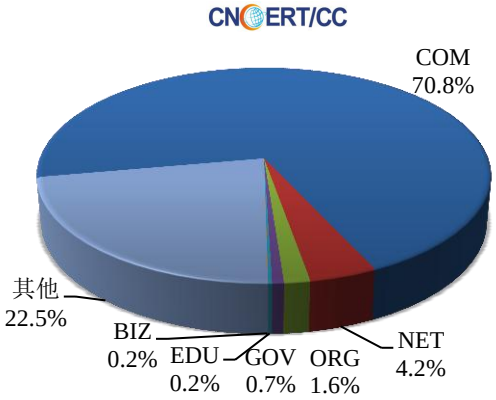
本周网站安全情况

本周 CNCERT 监测发现境内被植入后门的网站数量为 3385 个；针对境内网站的仿冒页面数量 117 个。



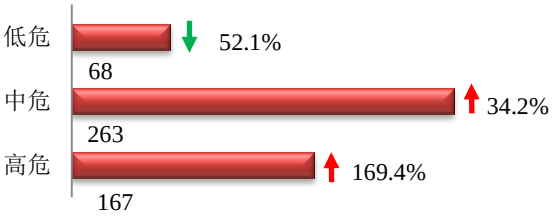
本周境内境内被植入后门的政府网站（GOV 类）数量为 24 个（约占境内 0.7%），较上周环比下降 14.3%；针对境内网站的仿冒页面涉及域名 262 个，IP 地址 47 个，平均每个 IP 地址承载了约 2 个仿冒页面。

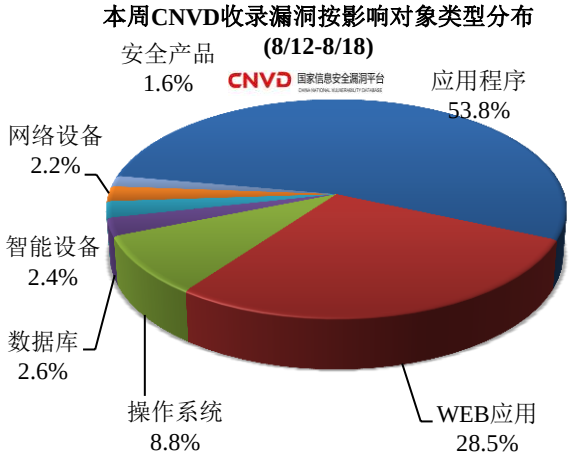
本周我国境内被植入后门网站按类型分布
(8/12-8/18)



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 498 个，信息安全漏洞威胁整体评价级别为中。





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 应用漏洞和操作系统。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

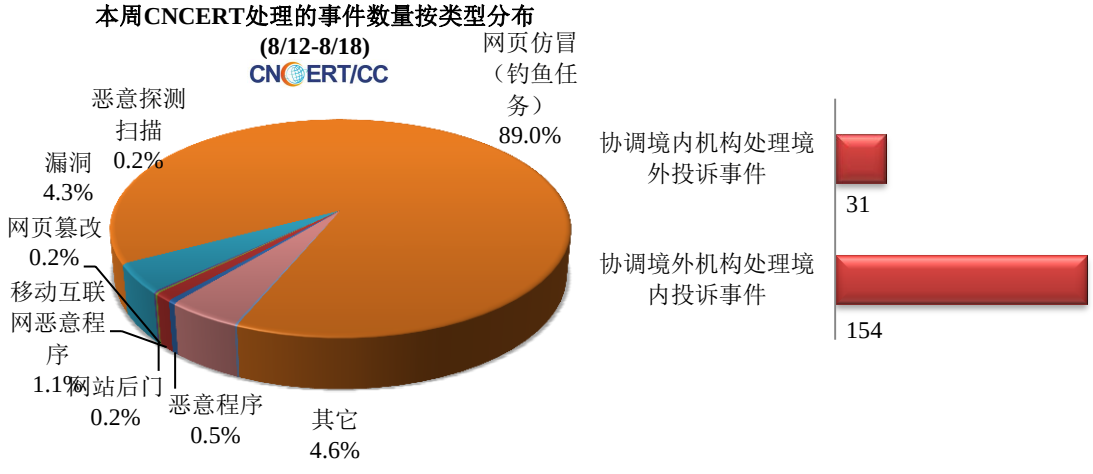
CNVD漏洞周报发布地址

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。

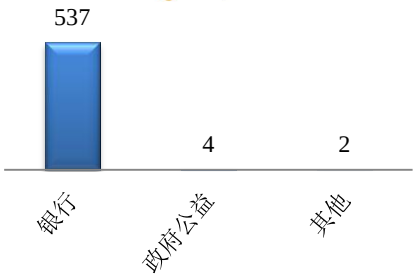
本周事件处理情况

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 610 起，其中跨境网络安全事件 185 起。

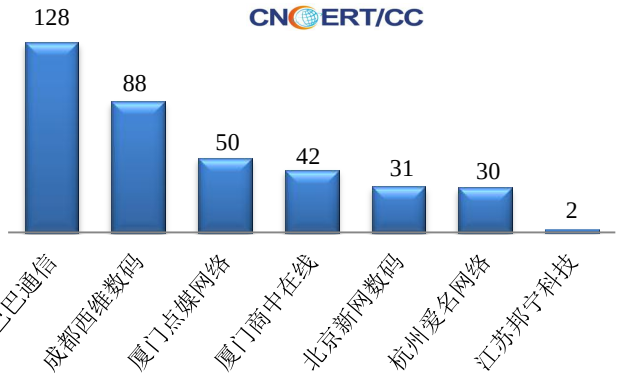


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 543 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 537 起和政府公益事件 4 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计
(8/12-8/18)

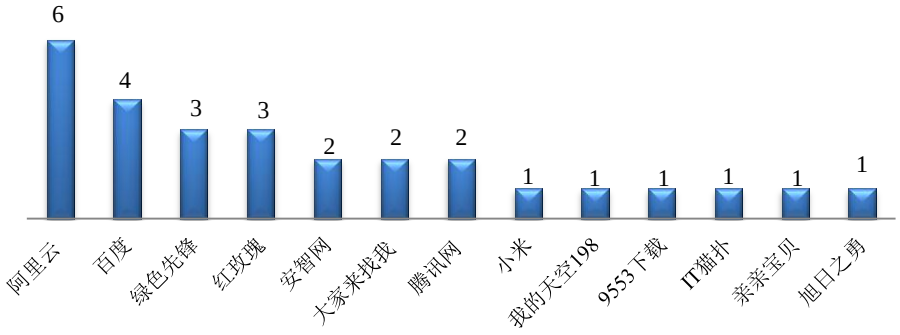


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (8/12-8/18)



本周，CNCERT 协调 13 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 28 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
(8/12-8/18)



业界新闻速递

1、水利部印发水利网络安全管理办法（试行）

8 月 16 日中华人民共和国水利部消息，为贯彻落实习近平总书记网络强国战略思想，依据《中华人民共和国网络安全法》，水利部网信办组织制定了《水利网络安全管理办法（试行）》，并于近日通过审议印发。

2、腾讯在世界顶级黑客大会中创纪录

8 月 12 日中文科技资讯消息,腾讯安全团队近日参加了美国拉斯维加斯举办的世界顶级黑客大会，在 Black Hat& DEF CON 的比赛中多项成绩领跑国内企业。这也是腾讯安全连续第四年征战 DEF CON CTF 全球总决赛赛场，再次向全球安全领域展示了中国极客力量。

3、微软 CTF 协议曝出漏洞 影响 Windows XP 发布以来的所有系统

8 月 14 日 Google Project Zero 安全团队的研究报告称微软 CTF 协议存在漏洞，很容易被利用。已在受害者计算机获得立足之地的黑客或恶意程序可以利用该漏洞劫持任何 Windows 应用，接管整个操作系统。

4、欧洲中央银行遭到黑客入侵导致用户数据泄露

8 月 15 日,欧洲中央银行（ECB）公布了 BIRD 通讯中的数据泄露事件，攻击者可以获取数月数百名金融业订阅者的联系信息。欧洲央行在定期维护工作中发现了入侵活动，黑客至少于去年 12 月入侵 BIRD，在位于银行综合报告字典(BIRD)的外部服务器上部署了恶意软件。黑客可以访问 BIRD 通讯 481 名订阅者的电子邮件地址、姓名和职位，密码也已被暴露。欧洲央行正在向可能受影响的人通报此事件。

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：文静

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315