国家互联网应急中心

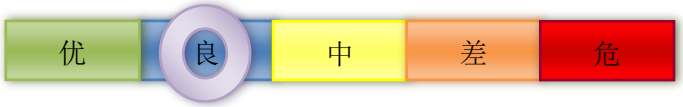
网络安全信息与动态周报

2018 年第 31 期

7 月 30 日-8 月 5 日

CNCERT/CC

本周网络安全基本态势

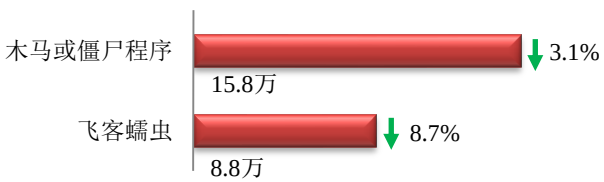


境内感染网络病毒的主机数量	•24.6万	↓ 5.2%
境内被篡改网站总数 其中政府网站数量	•1006 •36	↓ 8.0% =
境内被植入后门网站总数 其中政府网站数量	•913 •9	↑ 17.8% ↓ 18.2%
针对境内网站的仿冒页面数量	•1208	↓ 14.7%
新增信息安全漏洞数量 其中高危漏洞数量	•273 •66	↑ 27.6% ↑ 32.0%

=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

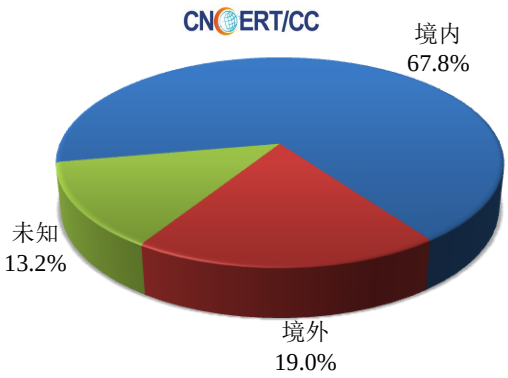
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 24.6 万个，其中包括境内被木马或被僵尸程序控制的主机约 15.8 万以及境内感染飞客（conficker）蠕虫的主机约 8.8 万。

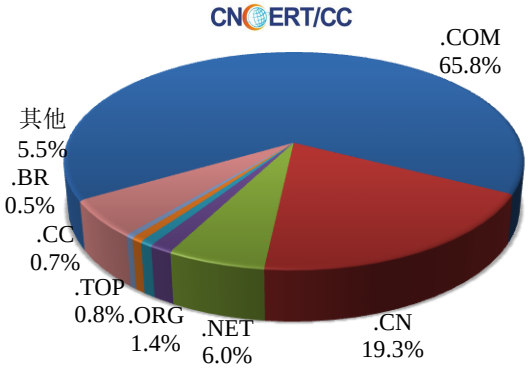


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 985 个，涉及 IP 地址 70578 个。在 985 个域名中，有 19.0%为境外注册，且顶级域为.com 的约占 65.8%；在 70578 个 IP 中，有约 25.3%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 217 个 IP。

本周放马站点域名注册所属境内外分布
(7/30-8/5)



本周放马站点域名所属顶级域的分布
(7/30-8/5)



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。

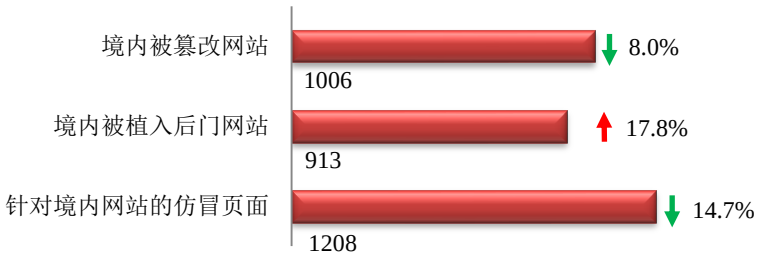
ANVA恶意地址黑名单发布地址

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。

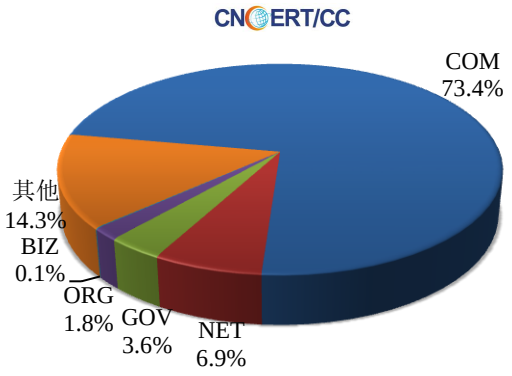
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1006 个；境内被植入后门的网站数量为 913 个；针对境内网站的仿冒页面数量为 1208。

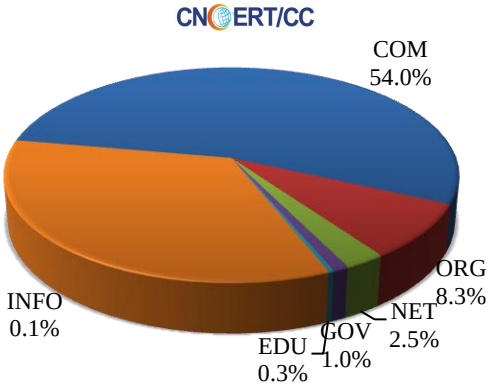


本周境内被篡改政府网站（GOV 类）数量为 36 个（约占境内 3.6%），与上周持平；境内被植入后门的政府网站（GOV 类）数量为 9 个（约占境内 1.0%），较上周环比下降了 18.2%；针对境内网站的仿冒页面涉及域名 539 个，IP 地址 253 个，平均每个 IP 地址承载了约 5 个仿冒页面。

本周我国境内被篡改网站按类型分布
(7/30-8/5)

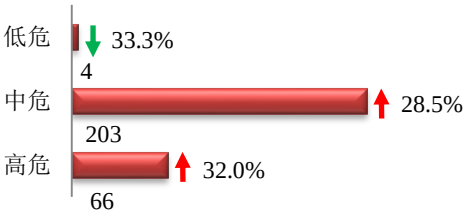


本周我国境内被植入后门网站按类型分布
(7/30-8/5)

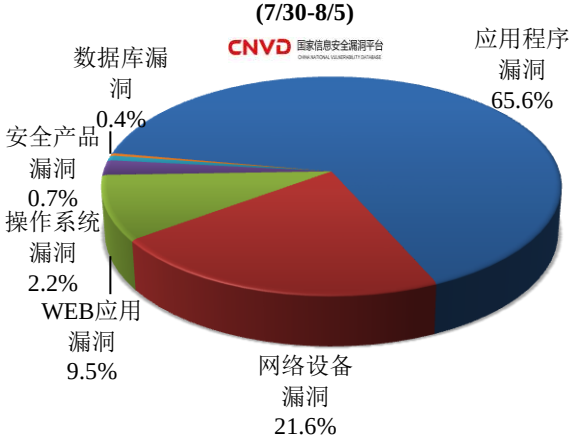


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 273 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
(7/30-8/5)



本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是网络设备漏洞和 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

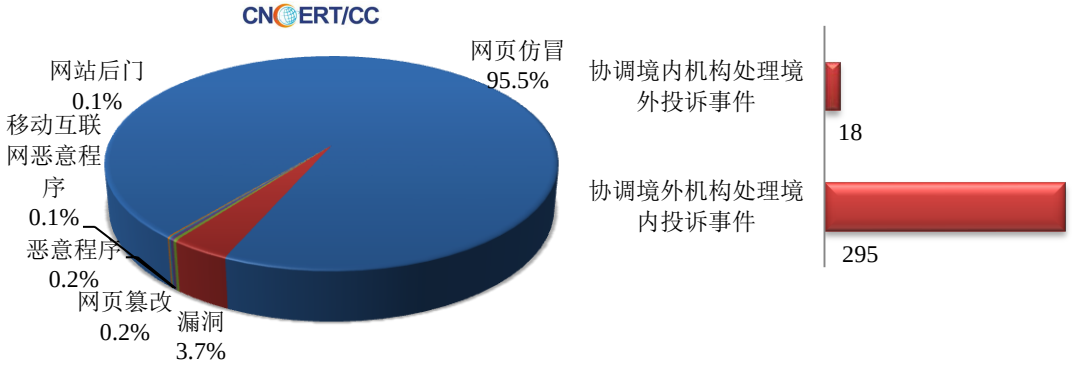
http://www.cnvd.org.cn/webinfo/list?type=4

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

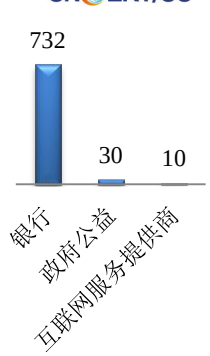
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 808 起，其中跨境网络安全事件 313 起。

本周CNCERT处理的事件数量按类型分布 (7/30-8/5)

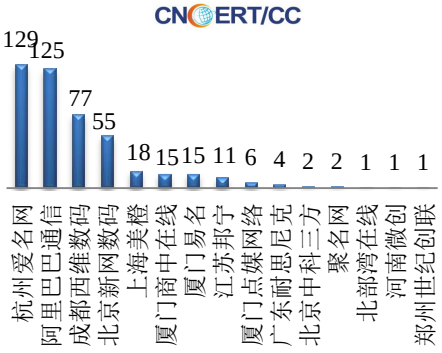


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 772 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 732 起和政府公益仿冒事件 30 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(7/30-8/5)

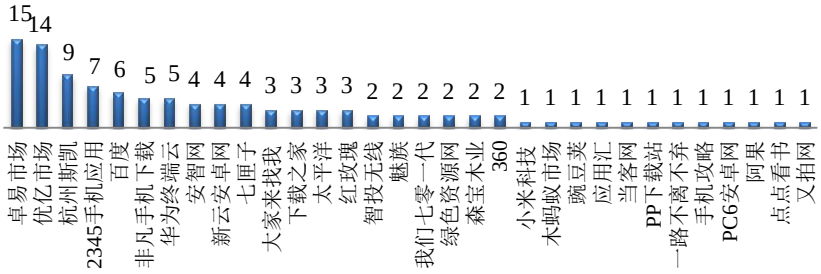


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (7/30-8/5)



本周，CNCERT 协调 32 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 109 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
(7/30-8/5)



业界新闻速递

1、工业和信息化部等多部门联合发起整治骚扰电话专项行动

新华网 7 月 30 日消息 记者 30 日从工业和信息化部获悉，工信部、最高人民法院、最高人民检察院等十三部门日前印发《综合整治骚扰电话专项行动方案》，决定自 2018 年 7 月起至 2019 年 12 月底，在全国开展综合整治骚扰电话专项行动，进一步推动骚扰电话治理工作步伐。《方案》显示，依据《网络安全法》《消费者权益保护法》《全国人大常委会关于加强网络信息保护的决定》《中华人民共和国电信条例》等法律法规，多部门将在全国范围内组织开展为期一年半的综合整治骚扰电话专项行动。据了解，专项行动将综合采用法律、行政、经济和技术等多种手段，重点对商业营销类、恶意骚扰类和违法犯罪类骚扰电话进行整治，规范通信资源管理，加强源头治理，打击非法获取个人信息的行为，合力斩断骚扰电话利益链条，实现商业营销类电话规范拨打、恶意骚扰和违法犯罪类电话明显减少的目标。

2、工业和信息化部网络安全管理局对多家涉及网络数据和用户个人信息安全突出情况的企业开展问询调查

工信部网站 7 月 31 日消息 近期，针对媒体公开报道和用户投诉较为集中的“部分应用随意调取手机摄像头权限、用户订单信息泄露引发诈骗案件、用户信息过度收集和滥用”等网络数据和用户个人信息安全突出情况，工业和信息化部网络安全管理局会同北京、上海等通信管理局积极开展调查，先后组织对涉及的上海携程商务有限公司、深圳市腾讯计算机系统有限公司、上海洋码头网络技术有限公司、北京弹幕网络科技有限公司、北京爱奇艺科技有限公司、探探文化发展（北京）有限公司等企业进行了情况问询，要求上述企业按照《网络安全法》《电信和互联网用户个人信息保护规定》有关网络数据和用户个人信息保护要求，进一步完善内部管理制度和技术保障措施，强化网络数据和用户个人信息安全保护，落实重大安全事件及时报告要求。结合情况问询及调查核实情况，部网络安全管理局初步认定上海洋码头网络技术有限公司存在用户个人信息安全管理制度不完善、用户个人信息泄露补救措施不到位等问题，对该企业相关负责人进行了约谈，责令企业限期整改，

并提交整改报告。下一步，部网络安全管理局将持续加大对网络数据和用户个人信息安全事件的监测巡查力度，指导督促企业切实履行相关法律责任，依法依规严肃处理涉事企业，切实做好网络数据和用户个人信息安全保护工作。

3、美军“网络航母”即将启航

中青在线8月2日消息 据美国科技网站《第五域》近期报道，美国国防部公布了一项名为“统一平台”（Unified Platform）的网络武器系统采购计划。该计划是美军网络司令部成立后，最大、最关键的采购项目，国防部公布了该计划前三年的预算，分别为2019年2980万美元、2020年1000万美元、2021年600万美元，但项目的总预算暂时保密。目前，整个项目的集成和运营由美国空军装备寿命管理中心负责，洛克希德·马丁、诺斯洛普·格鲁曼、雷神等军工巨头竞相参与投标。据国防部官员描述，“统一平台”系统是一种可以携带网络攻击和防御武器，在网络空间自由穿梭的标准化平台，作战人员可以对其实施指挥控制，执行攻防作战、情报获取、侦察监视等任务，由于该系统类似于海上的航母、空中的飞机和陆地的坦克，因此又被称为“网络航母”（Cyber Carrier），是美军为网络任务部队在网络空间执行作战任务打造的主战装备。

4、欧盟网络安全法案：建通用网络安全认证系统

E安全 7月30日消息 2018年5月29日，欧盟委员会发起了一项欧洲未来网络安全章程（《欧盟网络安全法案》）的提议。《欧盟网络安全法案》是一种更广泛的“网络安全数据包”（Cybersecurity Package）的表现形式，“网络安全数据包”的概念最初于2017年提出，后经过了一段时间的影响评估，并接受了各界评论。在网络风险不断增加的形势下，《欧盟网络安全法案》将把欧盟网络和信息安全署（ENISA）定位成欧盟永久性机构，从而加强ENISA的力量；还将为信息和通讯技术（ICT）等产品创建一个欧洲网络安全认证框架，旨在欧盟内部提供网络弹性和响应能力，协调各种标准以提升效率也是欧盟“数字单一市场”（Digital Singl Market）战略的核心主题。

5、日媒：日本政府为2020年奥运会制订网络安全战略

参考消息网7月30日消息 日媒称，着眼于2020年东京奥运会和残奥会，日本政府在27日的内阁会议上敲定了今后三年确保互联网安全的网络安全战略。为应对针对奥运会的网络攻击，2018年底前后将在政府内设立负责协调相关机构的新组织。此外，新战略还写明，针对会影响国民生活的大规模网络攻击，相关机构将加强应对能力。据共同社7月27日报道，新战略指出，东京奥运会“预计会受到超过历届奥运会的网络攻击”。政府内部将设立“网络安全应对协调中心”，以加强相关省厅、奥组委、东京都及基础设施企业间的合作。新战略还提出，为应对网络攻击的巧妙化，要事先同民间企业合作，开展防范攻击的“积极网络防御”。此外还将针对日益普及的虚拟货币交易、小型无人机及未来将投入实际使用的自动驾驶技术等推进安全防范措施。

6、印度拟设监管机构监管电商，要求谷歌 Facebook 等公司在本地存储数据

HackerNews.cc7月31日消息 7月30日消息，据国外媒体报道，路透社看到的一份政策文件草案显示，印度正在考虑设立一个单独监管机构并进行立法，以解决该国所有与电子商务相关的问题，消除目前监管该行业的法律不成体系现象。这份政策文件即《国家政策框架草案》中提出的一些措施包括：本地数据存储、强制使

用国内用卡支付网络 Rupay 进行网上交易，以及推动微型、小型和中型企业提供网上零售服务。该文件还表示，印度还将采取措施，发展数据存储能力，并鼓励在印度国内存储数据。这份文件还称，将给予时间让电子商务行业“在本地化成为强制性要求之前进行调整”。该政策草案表示，“在遵守隐私、许可等相关规定情况下，印度政府将有权让数据存储在印度国内，以实现国家安全和公共政策目标。”

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：马莉雅

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158