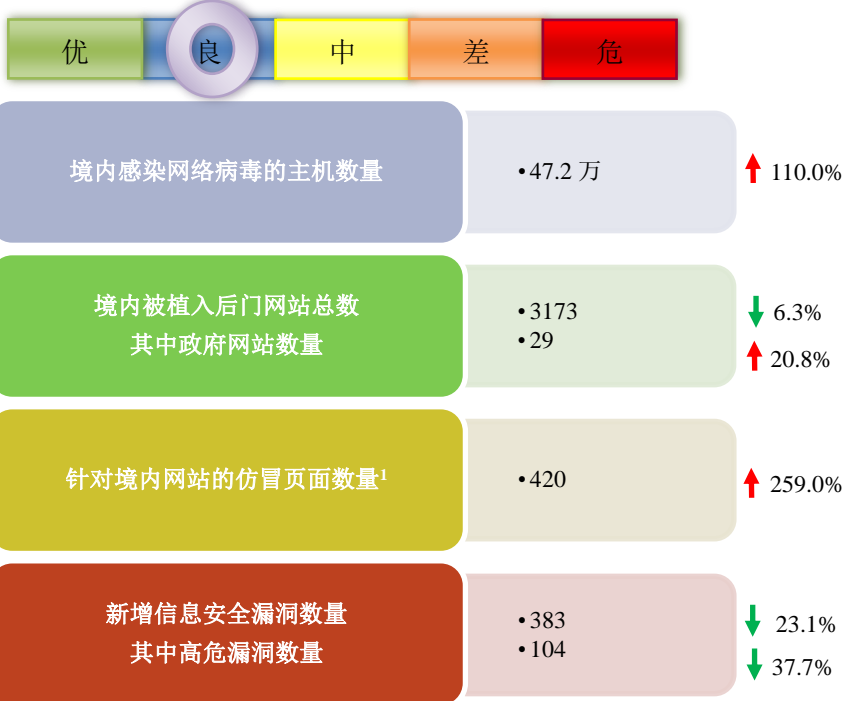


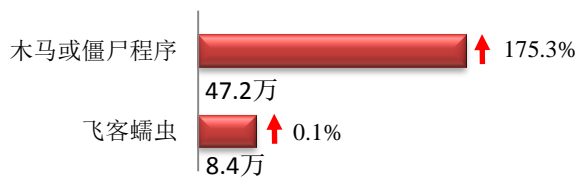
## 本周网络安全基本态势



▬ 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

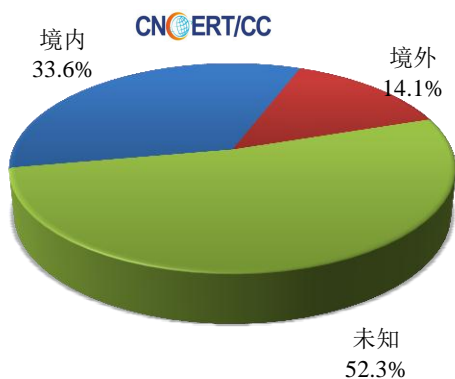
本周境内感染网络病毒的主机数量约为 47.2 万个，其中包括境内被木马或被僵尸程序控制的主机约 38.8 万以及境内感染飞客（conficker）蠕虫的主机约 8.4 万。



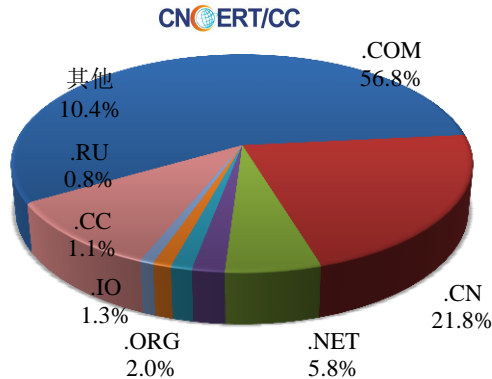
1. 本期针对境内网站的仿冒页面数量受监测数据范围扩大影响，波动较大。

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 1790 个，涉及 IP 地 3068 个。在 1790 个域名中，有 14.1% 为境外注册，且顶级域为 .com 的约占 56.8%；在 3068 个 IP 中，有约 43.9% 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 489 个 IP。

本周放马站点域名注册所属境内外分布  
(8/19-8/25)



本周放马站点域名所属顶级域的分布  
(8/19-8/25)



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。

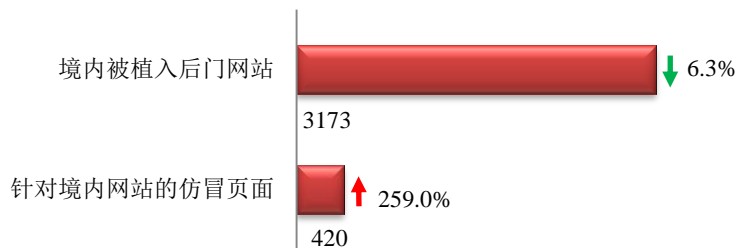
ANVA 恶意地址黑名单发布地址

<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。

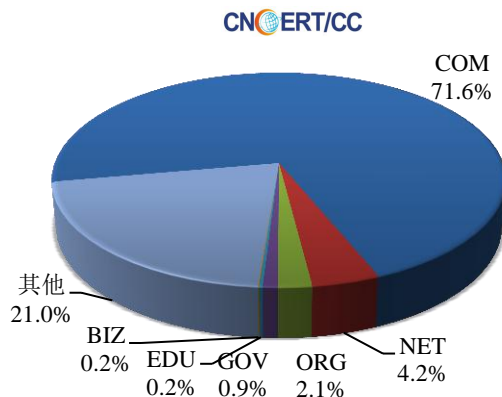
## 本周网站安全情况

本周 CNCERT 监测发现境内被植入后门的网站数量为 3173 个；针对境内网站的仿冒页面数量 420 个。



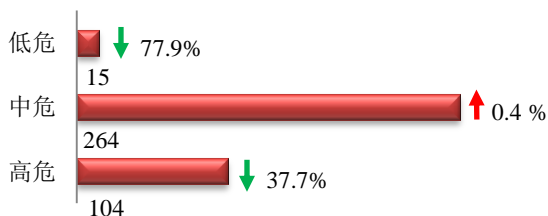
本周境内境内被植入后门的政府网站(GOV类)数量为29个(约占境内0.9%),较上周环比上涨20.8%;针对境内网站的仿冒页面涉及域名286个,IP地址154个,平均每个IP地址承载了约3个仿冒页面。

本周我国境内被植入后门网站按类型分布  
(8/19-8/25)

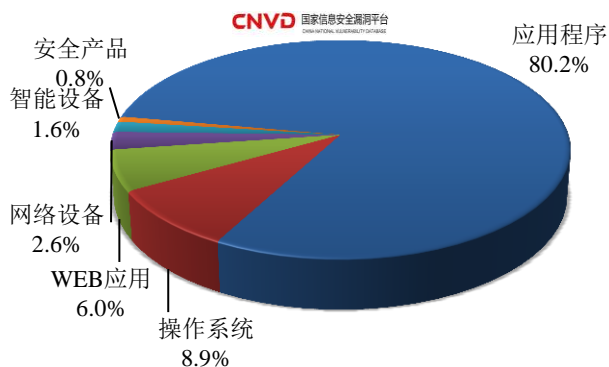


### 本周重要漏洞情况

本周,国家信息安全漏洞共享平台(CNVD)新收录网络安全漏洞383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  
(8/19-8/25)



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

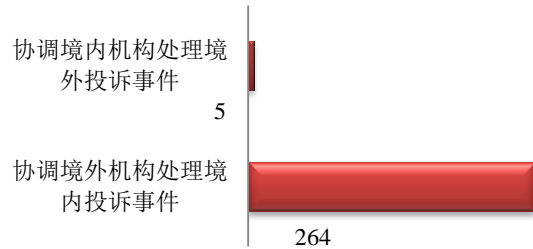
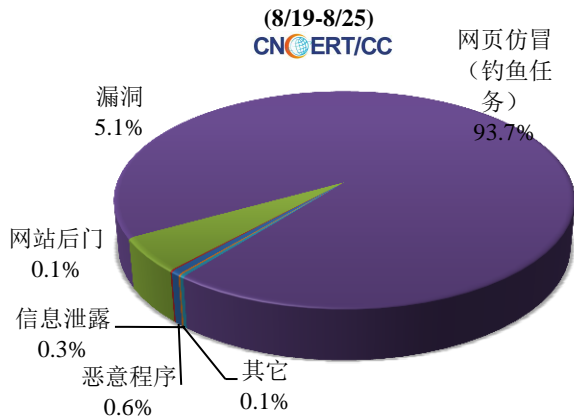
<http://www.cnvd.org.cn/webinfo/list?type=4>

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

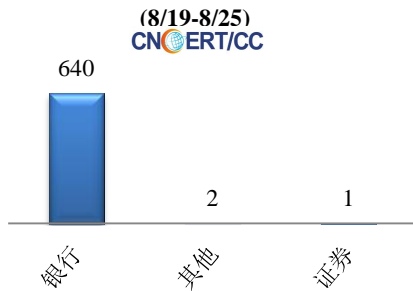
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 686 起，其中跨境网络安全事件 269 起。

### 本周CNCERT处理的事件数量按类型分布

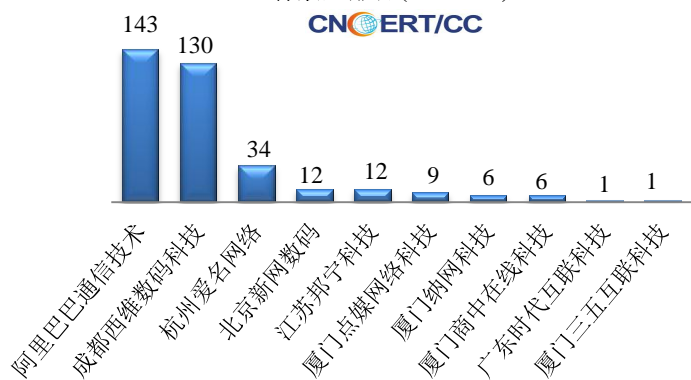


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 643 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 640 起和政府公益事件 2 起。

### 本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计



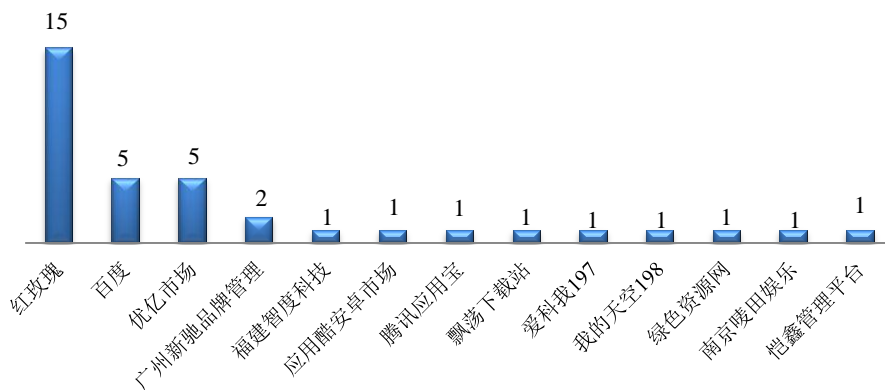
### 本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (8/19-8/25)



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  
(8/19-8/25)



本周，CNCERT 协调 15 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 38 个。



## 业界新闻速递

### 1、国家网信办发布《儿童个人信息网络保护规定》

8月23日新华社消息，国家互联网信息办公室23日发布《儿童个人信息网络保护规定》。规定自2019年10月1日起施行，并明确任何组织和个人不得制作、发布、传播侵害儿童个人信息安全的信息。针对网络运营者落实儿童个人信息安全管理责任不到位、存在较大安全风险或者发生安全事件的，由网信部门依据职责进行约谈，网络运营者应当及时采取措施进行整改，消除隐患。

### 2、工信部副部长：应坚持总体国家安全观，树立正确的网络安全观

8月21日澎湃新闻消息，由中国电子和奇安信集团等单位共同主办的2019北京网络安全大会于21日在北京国家会议中心举行。工信部副部长陈肇雄在致辞中表示，网络安全关乎社会经济发展，国家长治久安。

### 3、美国土安全部网络安全与基础设施安全局公布战略意图

8月22日网络安全与基础设施安全局（CISA, Cybersecurity and Infrastructure Security Agency）官网消息，22日正式公布了其成立以来的首份战略意图文档。根据CISA的《战略意图》文档所述，CISA的使命是：领导国家力量去理解和管理我们关键基础设施的网络及物理风险愿景：为美国人民带来安全和弹性的关键基础设施。“通过汇集不同的利益相关者来协同识别风险，确定风险的优先级，从而引领国家风险管理工作”

#### 4、乌克兰某核电厂发生严重网络安全事故

8月22日据外媒ZDNet报道，近日，位于乌克兰南部的 Yuzh-noukrainsk 市附近的核电站出现严重安全事故，数名雇员将核电厂内部网络连上了公共网络，以供其挖掘加密货币。报道指出，因为某些国家机构中的设备拥有强大计算能力，且此类机构通常拥有稳定的电力供应，所以一些国家机构雇员会利用职务之便为其挖掘加密货币。俄罗斯核能中心、罗马尼亚国家核物理和工程研究所，以及澳大利气象局就曾曝出类似事件。

### 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：王英

网址：[www.cert.org.cn](http://www.cert.org.cn)

email：[cncert\\_report@cert.org.cn](mailto:cncert_report@cert.org.cn)

电话：010-82990315

