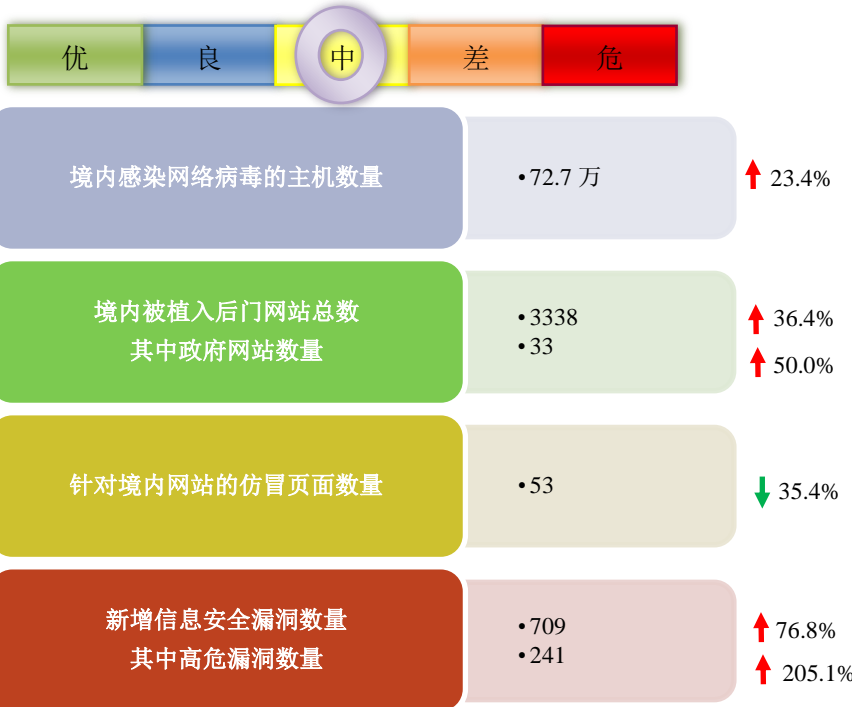


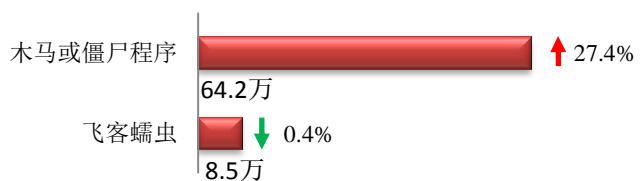
## 本周网络安全基本态势



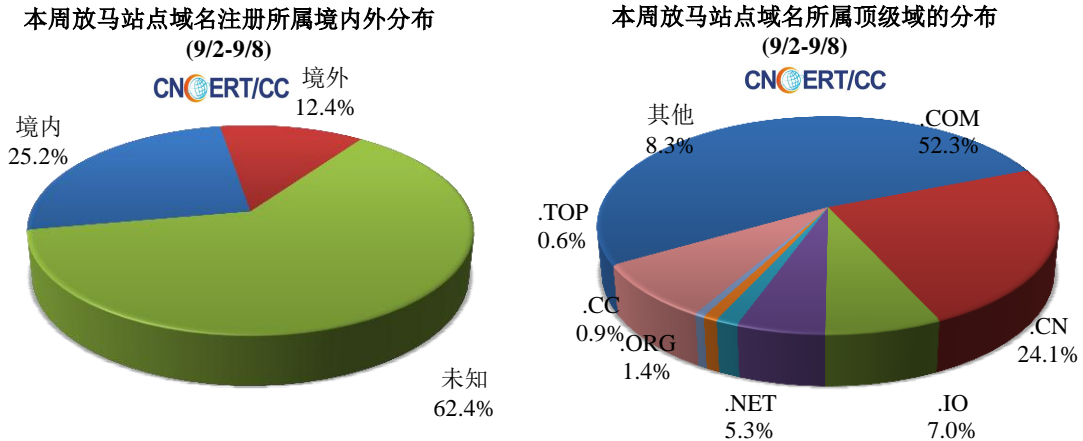
■ 表示数量与上周相同    
 ↑ 表示数量较上周环比增加    
 ↓ 表示数量较上周环比减少

## 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 72.7 万个，其中包括境内被木马或被僵尸程序控制的主机约 64.2 万以及境内感染飞客（conficker）蠕虫的主机约 8.5 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 2134 个，涉及 IP 地 3735 个。在 2134 个域名中，有 12.4% 为境外注册，且顶级域为 .com 的约占 52.3%；在 3735 个 IP 中，有约 29.2% 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 528 个 IP。



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**

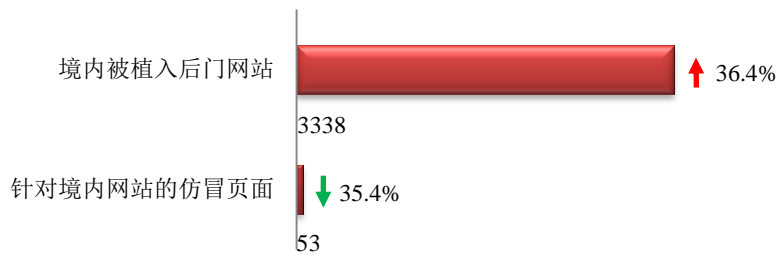
<http://www.anva.org.cn/virusAddress/listBlack>

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。



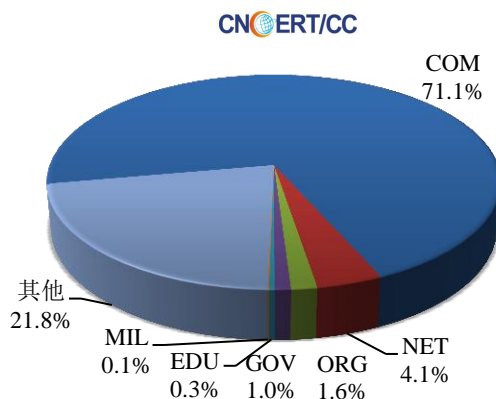
### 本周网站安全情况

本周 CNCERT 监测发现境内被植入后门的网站数量为 3338 个；针对境内网站的仿冒页面数量 53 个。



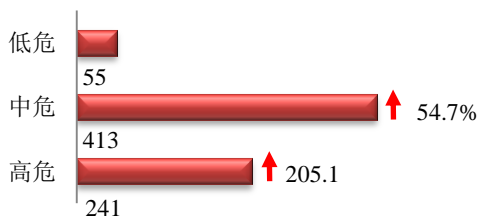
本周境内境内被植入后门的政府网站(GOV类)数量为33个(约占境内1.0%),较上周环比上升50.0%;针对境内网站的仿冒页面涉及域名38个,IP地址33个,平均每个IP地址承载了约2个仿冒页面。

本周我国境内被植入后门网站按类型分布  
(9/2-9/8)

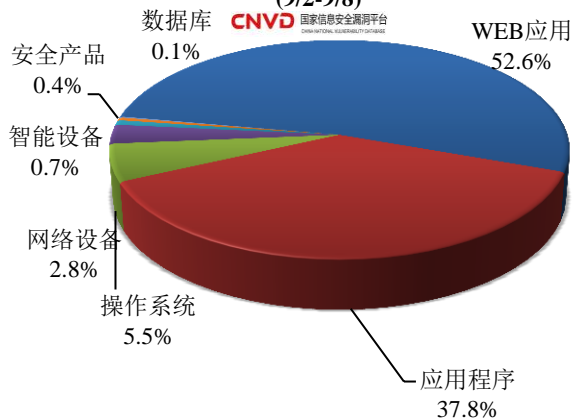


## 本周重要漏洞情况

本周,国家信息安全漏洞共享平台(CNVD)新收录网络安全漏洞709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  
(9/2-9/8)



本周CNVD发布的网络安全漏洞中,WEB应用漏洞占比最高,其次是应用程序漏洞和操作系统。

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

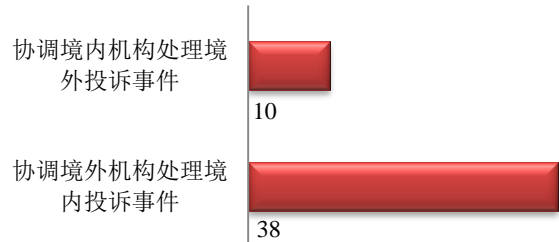
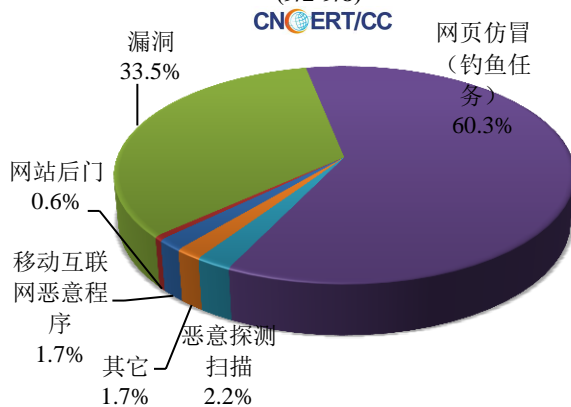
<http://www.cnvd.org.cn/webinfo/list?type=4>

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

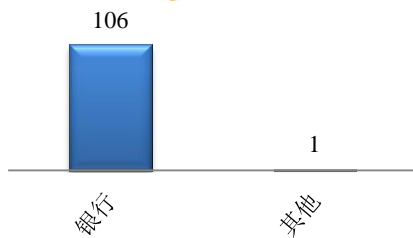
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 179 起，其中跨境网络安全事件 48 起。

本周CNCERT处理的事件数量按类型分布  
(9/2-9/8)

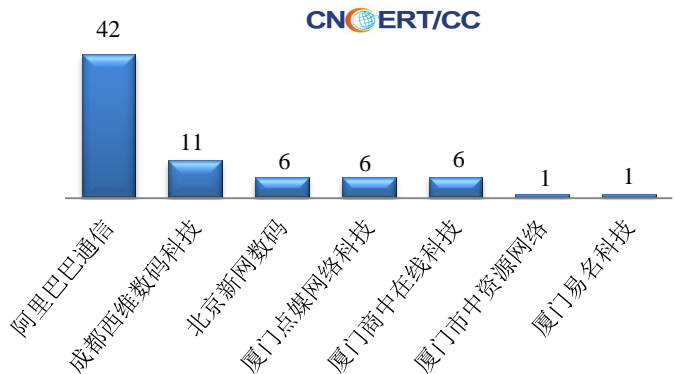


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 107 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 106 起和其他事件 1 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计  
(9/2-9/8)



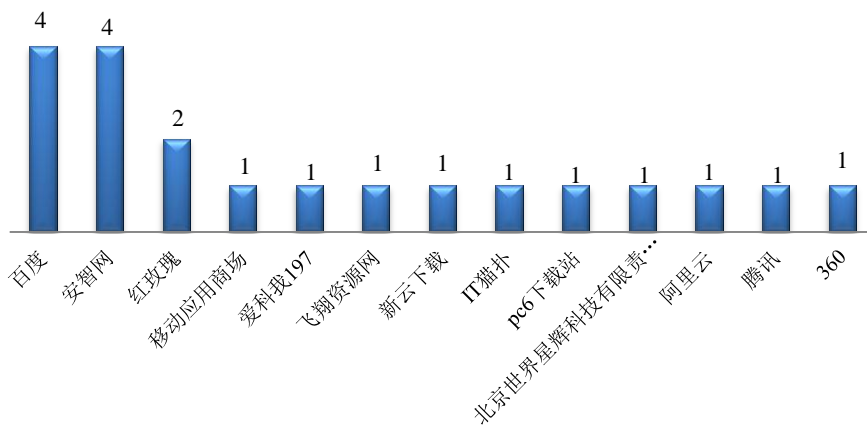
本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (9/2-9/8)



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  
(9/2-9/8)

CNCERT/CC

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 20 个。



## 业界新闻速递

### 1、工信部就“ZAO”App 网络数据安全问题问询约谈陌陌

9月4日工信部网安局消息，9月3日，针对媒体公开报道和用户曝光的“ZAO”App 用户隐私协议不规范，存在数据泄露风险等网络数据安全问题，工业和信息化部网络安全管理局对北京陌陌科技有限公司相关负责人进行了问询约谈，要求其严格按照国家法律法规以及相关主管部门要求，组织开展自查整改，依法依规收集使用用户个人信息，规范协议条款，强化网络数据和用户个人信息安全保护。同时，要进一步加强新技术新业务安全评估，切实采取有效措施，积极防范自有业务平台被利用实施电信网络诈骗等风险隐患。

### 2、IDC：中国网络安全支出未来五年平均增长 25.1%，增速领跑全球

9月2日 IDC 中国官网消息，据 IDC 最新发布的《IDC 全球半年度网络安全支出指南，2018H2》预测，2019 年全球网络安全相关硬件、软件、服务投资将达到 1066.3 亿美元，相比 2018 年增长 9.40%。其中针对中国市场，IDC 预测，2019 年中国网络安全市场总体支出将达到 73.5 亿美元，2019-2023 年预测期内的年 CAGR（复合年均增长率）为 25.1%，增速继续领跑全球网络安全市场。到 2023 年，中国网络安全市场规模将增长至 179.0 亿美元。从行业上来看，政府、通信、金融仍将是中国网络安全市场前三大支出行业，与往期保持一致，占中国总体网络安全市场约六成的比例。

### 3、美国国防部计划利用 AI 进行网络防御

9月4日 Defense one 官网消息，美国国防部新成立的联合人工智能中心（简称 JAIC）正在为美国军方的网络安全数据创建框架，旨在为将来的人工智能（AI）网络防御体系奠定基础。

JAIC 负责人杰克·沙纳罕（Jack Shanahan）表示，该中心将与美国国家安全局、美国网络司令部和数十个网络安全承包商展开合作，共同致力于加速数据收集工作的标准化进程。JAIC 计划创建一个统一的流程来管理、叙述、共享及存储信息，并最终实现使用 AI 监控潜在网络威胁的目标。

#### 4、谷歌 YouTube 因非法收集儿童个人信息被罚 1.7 亿美元

9月4日《华盛顿邮报》消息，美国联邦贸易委员会（FTC）周三称，Alphabet 旗下谷歌公司及其 YouTube 视频服务将支付 1.7 亿美元和解金，以了结有关 YouTube 收集儿童个人信息并因此触犯了联邦法律的指控。

YouTube 被控在未经父母同意的情况下使用“cookies”追踪儿童频道的观众，并借此向这些观众投放了价值数百万美元的靶向广告。除了罚款之外，拟议的和解方案还要求谷歌开发一套识别儿童内容的系统，并通知频道所有者他们有义务先征得家长的同意，随后才能收集儿童信息。。。

### 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：顾笑南

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