国家互联网应急中心

2021 年第 33 期

8 月 9 日-8 月 15 日

网络安全信息与动态周报

CNCERT/CC

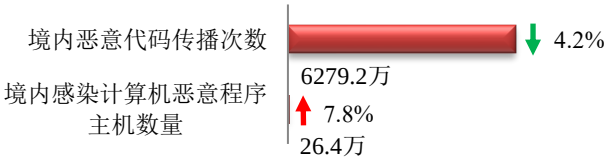
本周网络安全基本态势

境内计算机恶意程序传播次数 境内感染计算机恶意程序主机数量	•6297.2万 •26.4 万	↓ 4.2% ↑ 7.8%
境内被篡改网站总数 其中政府网站数量	•2509 •4	↓ 13.1% ↓ 71.4%
境内被植入后门网站总数 其中政府网站数量	•961 •4	↑ 1.5% ↓ 20.0%
针对境内网站的仿冒页面数量	•212	↓ 10.9%
新增信息安全漏洞数量 其中高危漏洞数量	•603 •135	↑ 46.0% ↑ 27.4%

= 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

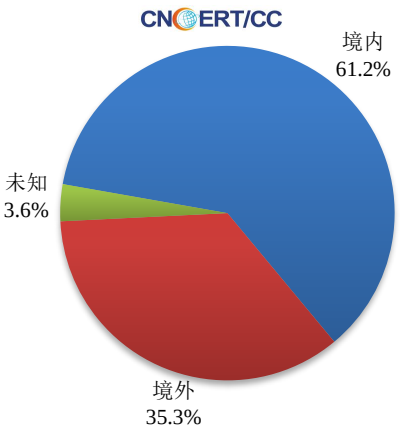
本周网络病毒活动情况

境内计算机恶意程序传播次数约为 6279.2 万次，境内感染计算机恶意程序主机数量约为 26.4 万个。

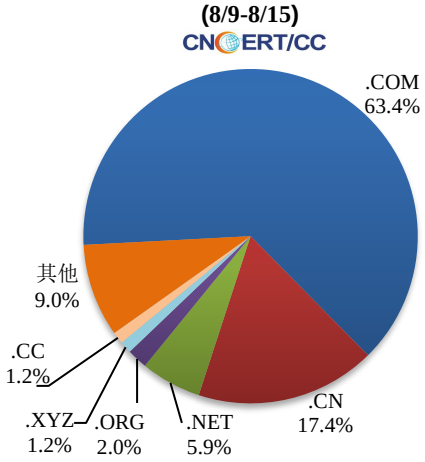


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 2079 个，涉及 IP 地址 9500 个。在 2079 个域名中，有 35.3%为境外注册，且顶级域为.com 的约占 63.4%；在 9500 个 IP 中，有约 70.0%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 292 个。

本周放马站点域名注册所属境内外分布
(8/9-8/15)



本周放马站点域名注册所属顶级域分布
(8/9-8/15)



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。

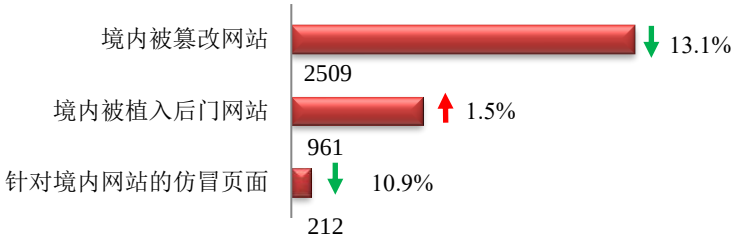
ANVA网络安全威胁信息共享平台

https://share.anva.org.cn/web/publicity/listurl

中国反网络病毒联盟（Anti Network-Virus Alliance of China，缩写 ANVA）是由 CNCERT 发起并组织运作的行业联盟。

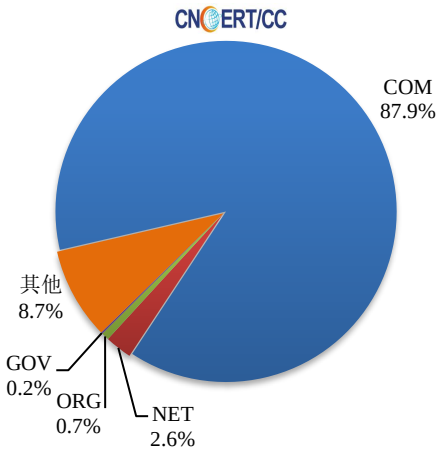
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 2509 个；被植入后门的网站数量为 961 个；针对境内网站的仿冒页面数量为 212 个。

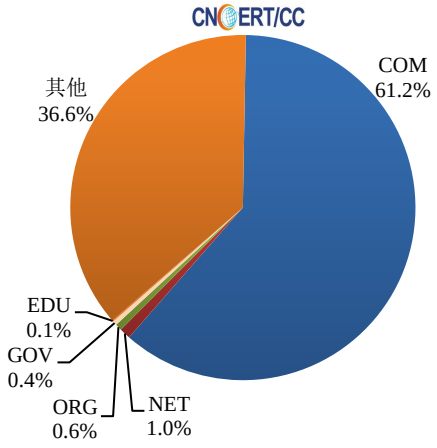


本周境内被篡改政府网站（GOV 类）数量为 4 个（约占境内 0.2%），与上周相比下降 71.4%；境内被植入后门的政府网站（GOV 类）数量为 4 个（约占境内 0.4%），与上周相比下降 20.0%。

本周我国境内篡改网站按类型分布
(8/9-8/15)

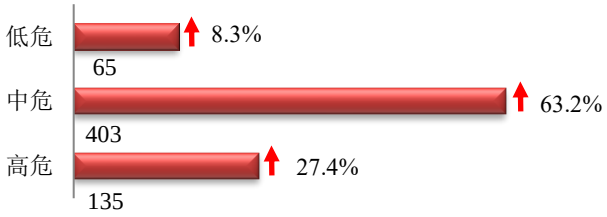


本周我国境内被植入后门网站按类型分布
(8/9-8/15)

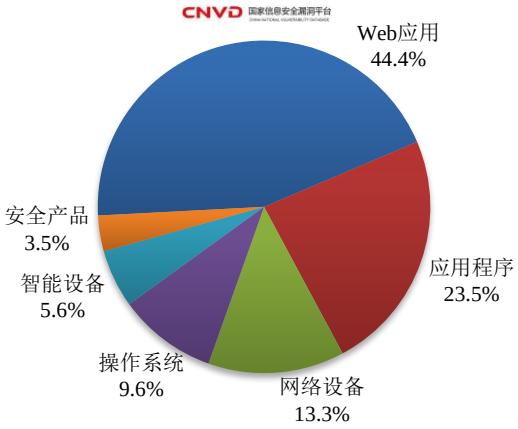


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 603 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分布
(8/9-8/15）



本周 CNVD 发布的网络安全漏洞中，Web 应用占比最高，其次是应用程序和网络设备。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

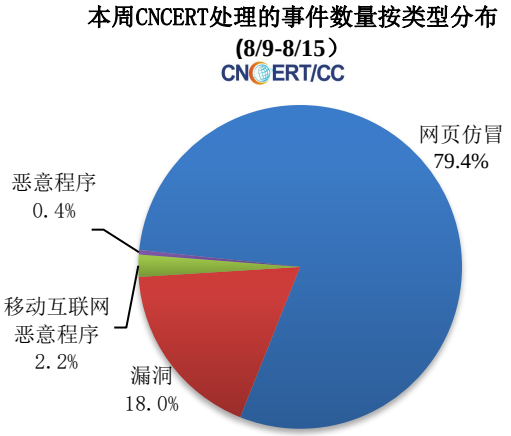
CNVD漏洞周报发布地址

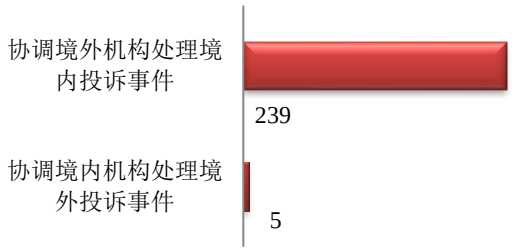
http://www.cnvd.org.cn/webinfo/list?type=4

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、基础电信企业、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。

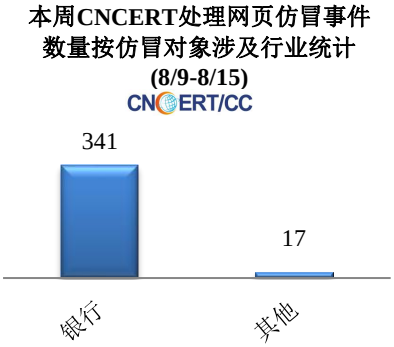
本周事件处理情况

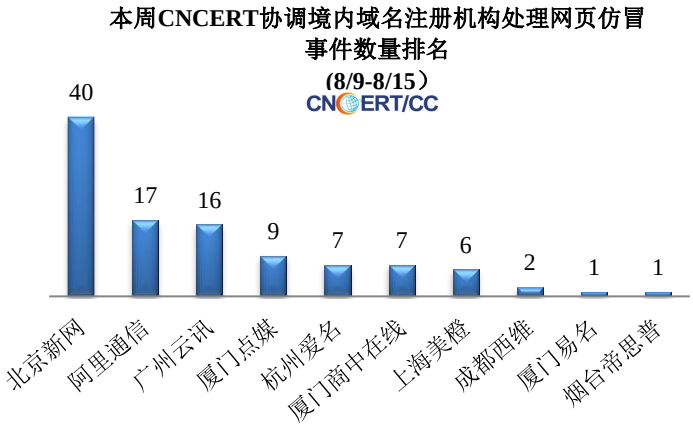
本周，CNCERT 协调云服务商、域名注册服务机构、应用商店、各省分中心以及国际合作组织共处理了网络安全事件 451 起，其中跨境网络安全事件 244 起。



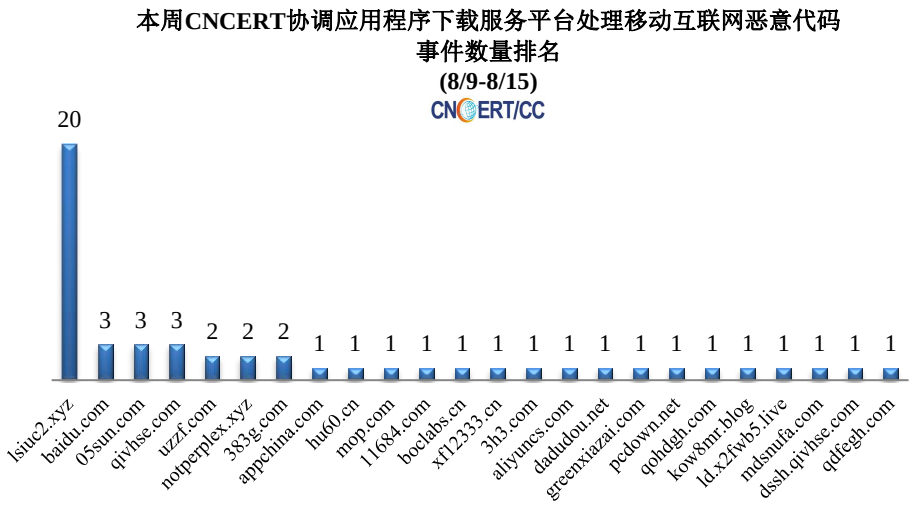


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理 358 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，银行仿冒事件 341 起，其他事件 17 起。





本周，CNCERT 协调 24 个提供恶意移动应用程序下载服务的平台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 52 个。



业界新闻速递

1. 国家网信办会同有关部门深入推进摄像头偷窥等黑产集中治理工作

2021 年 8 月 9 日，据中国网信网消息，今年 5 月以来，国家网信办会同工业和信息化部等相关政府部门深入推进摄像头偷窥等黑产集中治理工作，对人民群众反应强烈的非法利用摄像头偷窥个人隐私画面、交易隐私视频、传授偷窥偷拍技术等侵害公民个人隐私行为进行集中治理。国家网信办指导各地网信办督促各类平台清理相关违规有害信息 2.2 万余条，处置平台账号 4000 余个、群组 132 个，下架违规产品 1600 余件。其中，百度、腾讯、UC 等重点网站平台，清理有害信息 8000 余条、处置违规账号 134 个；京东、淘宝、闲鱼等电商平台，下架违规宣传或违规售卖摄像设备 1600 余件、处置违规账号 3700 余个、清理违规信息 1.2 万余条。对存在隐私视频信息泄露隐患的 14 家视频监控 APP 厂商进行了约谈，并督促其完成整改。工业和信息化部组织各省、自治区、直辖市通信管理局、专业机构、基础电信企业，以及 18 个重点视频监控云平台、摄像头生产企业代表，召开全国电视电话会议，部署摄像头网络安全集中整治工作；组织开展智能音视频采集设备应用安全、网络安全、数据安全等有关标准宣传普及，督促摄像头生产企业对照安全标准开展自查自纠，组织检测机构进入 5 家摄像头生产企业开展现场巡查和产品抽检；组织对 18 家具有行业代表性的视频监控云平台开展检查，发现处置 SQL 注入、越权操作等一批高危漏洞；全面排查联网摄像头存在的安全隐患，发现 4 万多个弱口令、未授权访问、远程命令执行等摄像头漏洞，取证并处置 500 余个。

2. CNCERT 发布 2021 年第二季度我国 DDoS 攻击资源季度分析报告

2021 年 8 月 10 日，CNCERT 发布 2021 年第二季度我国 DDoS 攻击资源季度分析报告。本报告围绕互联网环境威胁治理问题，基于 CNCERT 监测的 DDoS 攻击事件数据进行抽样分析，重点对“DDoS 攻击是从哪些网络资源上发起的”这个问题进行分析。本季度的重点关注情况为：本季度利用肉鸡发起攻击的活跃控制端中，境外控制端按国家和地区统计，最多位于美国、德国 和荷兰；境内控制端按省份统计，最多位于江苏省、浙江省和福建省，按归属运营商统计，电信占比最大。本季度参与攻击的活跃境内肉鸡中，按省份统计最多位于广东省、辽宁省和福建省；按归属运营商统计，电信占比最大。本季度被利用参与 Memcached 反射攻击的活跃境内反射服务器中，按省份统计排名前三名的省份是广东省、山东省、和四川省；数量最多的归属运营商是电信。被利用参与 NTP 反射攻击的活跃境内反射服务器中，按省份统计排名前三名的省份是河北省、浙江省和河南省；数量最多的归属运营商是联通。被利用参与 SSDP 反射攻击的活跃境内反射服务器中，按省份统计排名前三名的省份是浙江省、广东省和辽宁省；数量最多的归属运营商是电信。本季度转发伪造跨域攻击流量的路由器中，位于广东省、四川省和上海市的路由器数量最多。本季度转发伪造本地攻击流量的路由器中，位于江苏省、河南省和浙江省的路由器数量最多。

3. 全国人大法工委：个人信息保护法草案（三次审议稿）拟作六方面修改

2021 年 8 月 13 日，据中国人大网消息，13 日上午，全国人大常委会法制工作委员会举行记者会，发言人臧铁伟介绍立法工作有关情况并回答记者提问。据介绍，十三届全国人大常委会第三十次会议将于 8 月 17 日至 20 日在北京举行。根据各方面意见，提请本次常委会会议审议的个人信息保护法草案（三次审议稿）拟作如下主要修改：一是，我国宪法规定，国家尊重和保障人权，公民的人格尊严不受侵犯，公民的通信自由和通信秘密受法律保护。制定实施本法对于保障公民的人格尊严和其他权益具有重要意义。据此，拟在草案第一条中增加规定“根据宪法”制定本法。二是，进一步完善个人信息处理规则，特别是对应用程序（APP）过度收集个人信息、“大数据杀熟”等作出有针对性规范。三是，将不满十四周岁未成年人的个人信息作为敏感个人信息，并要求个人信息处理者对此制定专门的个人信息处理规则。四是，完善个人信息跨境提供的规则，对按照我国缔结或者参加的国际条约、协定向境外提供个人信息、对转移到境外的个人信息的保护不应低于我国的保护标准等作出规定。五是，增加个人信息可携带权的规定，完善死者个人信息保护的规定。六是，对完善个人信息保护投诉、举报工作机制及违法处理个人信息涉嫌犯罪案件的移送提出明确要求。

关于国家互联网应急中心（CNCERT）

国家计算机网络应急技术处理协调中心（英文简称 CNCERT/CC），成立于 2001 年 8 月，为非政府非盈利的网络安全技术中心，是中国计算机网络应急处理体系中的牵头单位。作为国家级应急中心，CNCERT/CC 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，运行和管理国家信息安全漏洞共享平台（CNVD），维护公共互联网安全，保障关键信息基础设施的安全运行。

CNCERT/CC 在中国大陆 31 个省、自治区、直辖市设有分支机构，并通过组织网络安全企业、学校、社会组织和研究机构，协调骨干网络运营单位、域名服务机构和其他应急组织等，构建中国互联网安全应急体系，共同处理各类互联网重大网络安全事件。CNCERT/CC 积极发挥行业联动合力，发起成立了中国反网络病毒联盟（ANVA）和中国互联网网络安全威胁治理联盟（CCTGA）。

同时，CNCERT/CC 积极开展网络安全国际合作，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 2020 年，已与 78 个国家和地区的 265 个组织建立了“CNCERT/CC 国际合作伙伴”关系。CNCERT/CC 是国际应急响应与安全组织 FIRST 的正式成员，以及亚太计算机应急组织 APCERT 的发起者之一，还积极参加亚太经合组织、国际电联、上合组织、东盟、金砖等政府层面国际和区域组织的网络安全相关工作。

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：吕利锋

网址： www.cert.org.cn

Email：cncert_report@cert.org.cn

电话： 010-82990315