国家互联网应急中心

网络安全信息与动态周报

2021 年第 22 期

5 月 24 日-5 月 30 日

CNCERT/CC

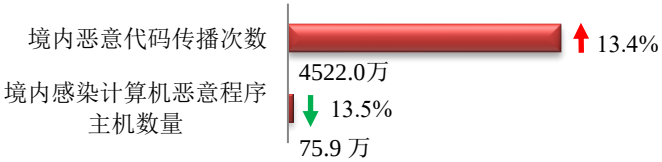
本周网络安全基本态势

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	•4522.0万 •75.9万	↑13.4% ↓13.5%
境内被篡改网站总数 其中政府网站数量	•1170 •3	↑10.5% =
境内被植入后门网站总数 其中政府网站数量	•1339 •9	↑4.2% ↑80.0%
针对境内网站的仿冒页面数量	•465	↑35.2%
新增信息安全漏洞数量 其中高危漏洞数量	•604 •143	↑4.0% ↑19.2%

= 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

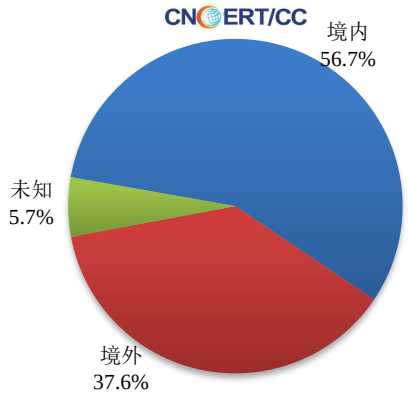
本周网络病毒活动情况

境内计算机恶意程序传播次数约为 4522.0 万次，境内感染计算机恶意程序主机数量约为 75.9 万个。

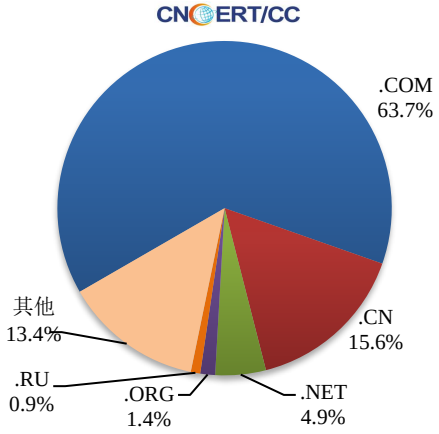


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 1539 个，涉及 IP 地址 7542 个。在 1539 个域名中，有 37.6%为境外注册，且顶级域为.com 的约占 63.7%；在 7542 个 IP 中，有约 32.2% 位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 281 个。

本周放马站点域名注册所属境内外分布
(5/24-5/30)



本周放马站点域名注册所属顶级域分布
(5/24-5/30)



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。

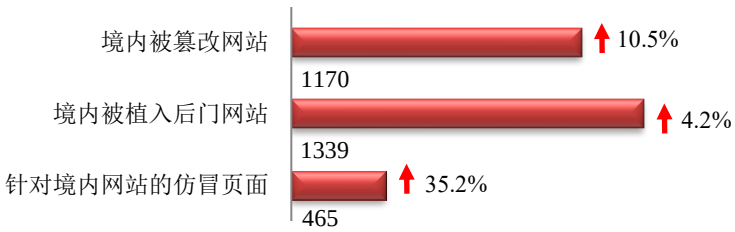
ANVA网络安全威胁信息共享平台

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。

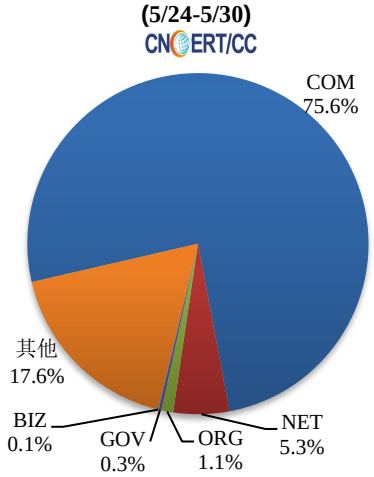
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 1170 个；被植入后门的网站数量为 1339 个；针对境内网站的仿冒页面数量为 465 个。

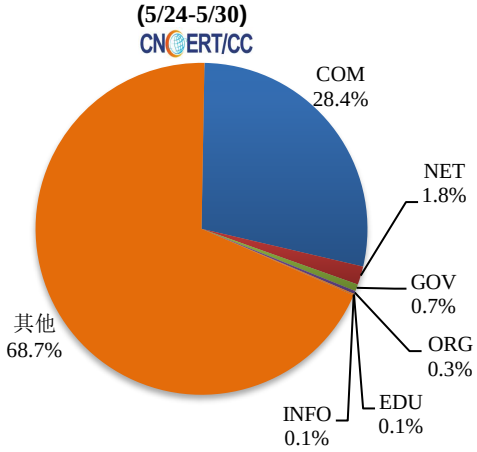


本周境内被篡改政府网站（GOV 类）数量为 3 个（约占境内 0.3%），与上周持平；境内被植入后门的政府网站（GOV 类）数量为 5 个（约占境内 0.7%），与上周相比上升了 80.0%。

本周我国境内篡改网站按类型分布
(5/24-5/30)

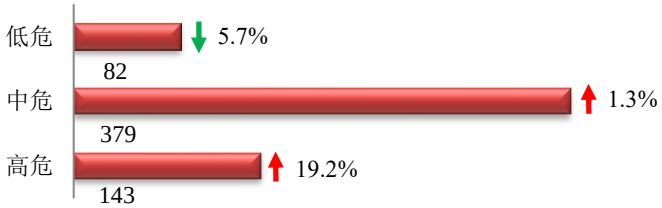


本周我国境内被植入后门网站按类型分布
(5/24-5/30)

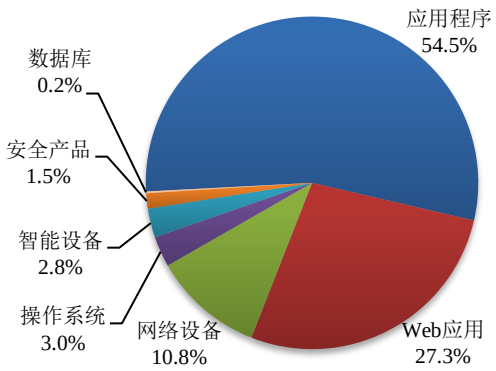


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 604 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
(5/24-5/30）



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。

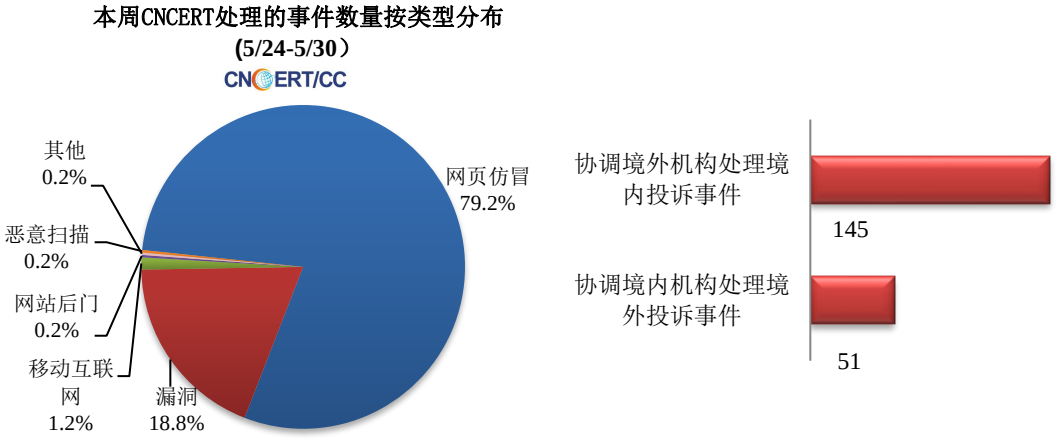
CNVD漏洞周报发布地址

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

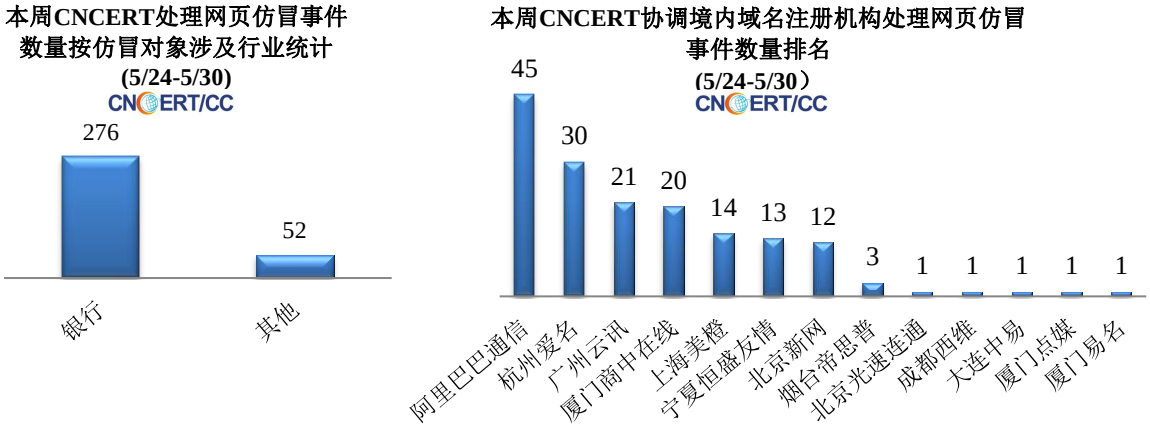
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信企业、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

本周事件处理情况

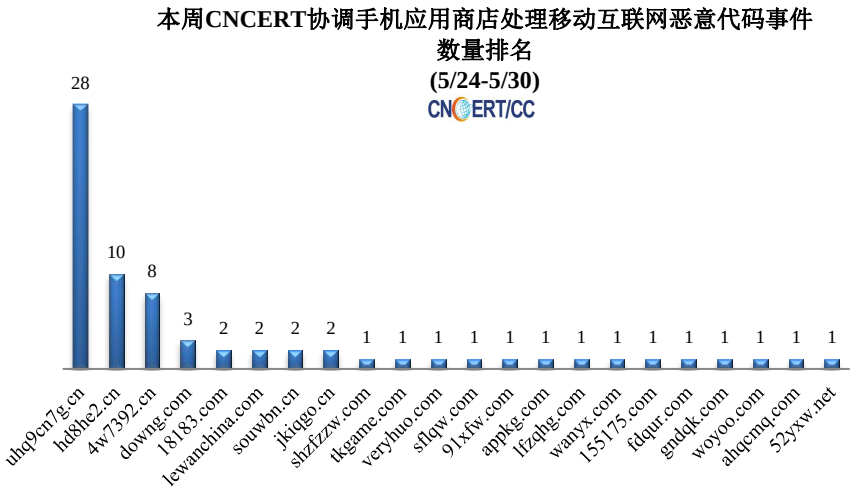
本周，CNCERT 协调云服务商、域名注册服务机构、应用商店、各省分中心以及国际合作组织共处理了网络安全事件 414 起，其中跨境网络安全事件 196 起。



本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理 328 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 276 起，其他事件 52 起。



本周，CNCERT 协调 22 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 71 个。



业界新闻速递

1. CNCERT 发布《2020 年我国互联网网络安全态势综述》

2021 年 5 月 26 日，国家互联网应急中心（CNCERT）正式发布《2020 年我国互联网网络安全态势综述》报告（以下简称“2020 年态势报告”）。为全面反映我国网络安全的整体态势，CNCERT 自 2010 年以来，每年发布前一年度网络安全态势情况综述，至今已连续发布 12 年，对我国党政机关、行业企业及社会了解我国网络安全形势，提高网络安全意识，做好网络安全工作提供了有力参考。2020 年态势报告以 CNCERT 宏观网络安全监测数据与工作实践为基础，综合各类安全威胁、事件信息，网络安全事件应急处置以及网络安全威胁治理实践等内容。报告主要分为三个部分：一是总结 2020 年我国互联网网络安全状况。报告总结了我国在网络安全法律法规建设完善、网络威胁治理等所取得的重要成果。重点从 APT 攻击、数据安全、安全漏洞、恶意程序、网络反诈、工业控制系统安全等六个方面对全年突出的网络安全状况特点进行了梳理。二是预测 2021 年网络安全热点。报告提出六点预测，认为 APT 攻击威胁、个人信息保护、供应链安全、关键信息基础设施安全、远程协作安全风险、大数据安全等将成为 2021 年网络安全领域值得关注的热点。三是梳理网络安全监测数据。报告从攻击来源、攻击对象、攻击规模等维度，通过丰富的宏观安全监测数据统计分析，对恶意程序、安全漏洞、拒绝服务攻击、网站安全、云平台安全、工业控制系统安全、区块链安全等七个方面进行了梳理。

2. 关于 VMware vCenter Server 存在远程代码执行漏洞的安全公告

2021 年 5 月 26 日，据国家信息安全漏洞共享平台（CNVD）消息，CNVD 收录了 VMware vCenter Server 远程代码执行漏洞（CNVD-2021-37150，对应 CVE-2021-21985）。攻击者利用该漏洞，可在

未授权的情况下远程执行代码。目前，漏洞相关细节尚未公开，VMware 公司已发布新版本修复漏洞。CNVD 建议广大用户尽快更新至最新版本。

3. 四部委发布《全国一体化大数据中心协同创新体系算力枢纽实施方案》的通知

2021 年 5 月 26 日，据国家发展和改革委员会网站消息，根据《关于加快构建全国一体化大数据中心协同创新体系的指导意见》（发改高技〔2020〕1922 号）部署要求，为加快推动数据中心绿色高质量发展，建设全国算力枢纽体系，国家发展改革委会同中央网信办、工业化和信息化部和国家能源局研究制定了《全国一体化大数据中心协同创新体系算力枢纽实施方案》。具体方案内容请访问相关部委网站浏览或下载。

4. CNCERT 发布 2021 年第一季度 DDoS 攻击资源分析报告

2021 年 5 月 27 日，国家互联网应急中心（CNCERT）发布《2021 年第一季度我国 DDoS 攻击资源分析报告》，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。本季度重点关注情况包括：一是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，最多位于吉林省、河南省和山东省，按归属运营商统计，联通占比最大。二是本季度参与攻击的活跃境内肉鸡中，按省份统计最多位于江苏省、安徽省和浙江省；按归属运营商统计，电信占比最大。三是本季度被利用参与 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、和湖南省；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浙江省、河北省和湖北省；数量最多的归属运营商是电信。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。四是本季度转发伪造跨域攻击流量的路由器中，位于上海市、四川省和北京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、福建省和广东省的路由器数量最多。

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：常霞

网址： www.cert.org.cn

Email：cncert_report@cert.org.cn

电话： 010-82990315