国家互联网应急中心

2022 年第 23 期

5 月 30 日-6 月 5 日

网络安全信息与动态周报

CNCERT/CC

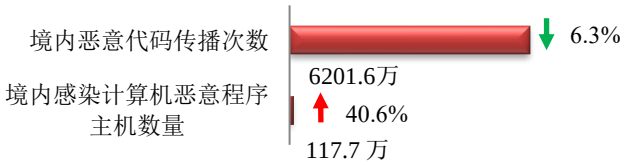
本周网络安全基本态势

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	• 6201.6万 • 117.7万	↓ 6.3% ↑ 40.6%
境内被篡改网站总数 其中政府网站数量	• 661 • 0	↓ 58.8%
境内被植入后门网站总数 其中政府网站数量	• 507 • 1	↑ 64.1%
针对境内网站的仿冒页面数量	• 2328	↑ 21.4%
新增信息安全漏洞数量 其中高危漏洞数量	• 589 • 219	↑ 28.0% ↑ 32.7%

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

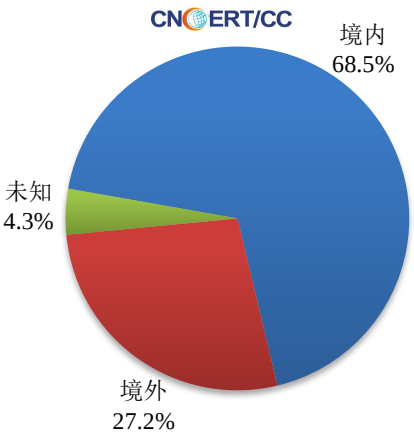
本周网络病毒活动情况

境内计算机恶意程序传播次数约为 6201.6 万次，境内感染计算机恶意程序主机数量约为 117.7 万个。

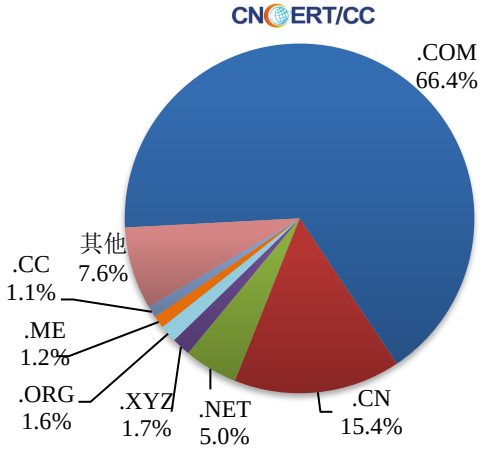


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 8691 个，涉及 IP 地址 27057 个。在 8691 个域名中，有 27.2%为境外注册，且顶级域为.com 的约占 66.4%；在 27057 个 IP 中，有约 90.7%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 442 个。

本周放马站点域名注册所属境内外分布
(5/30-6/5）



本周放马站点域名注册所属顶级域分布
(5/30-6/5)



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。

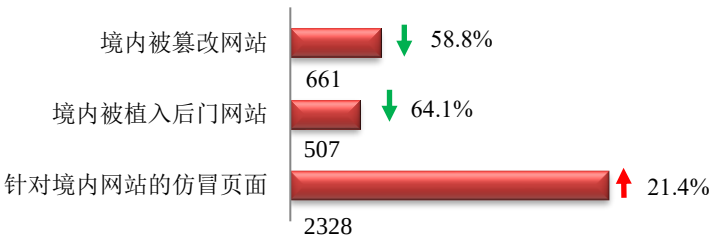
ANVA网络安全威胁信息共享平台

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。

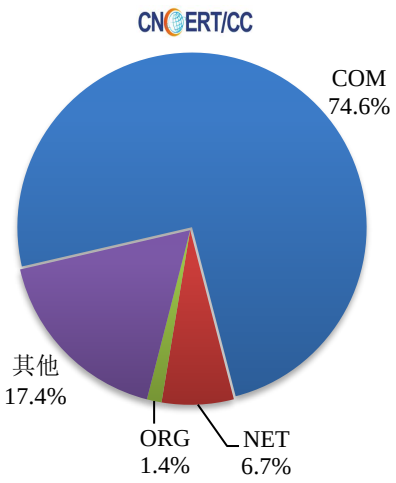
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 661 个；被植入后门的网站数量为 507 个；针对境内网站的仿冒页面数量 2328 个。

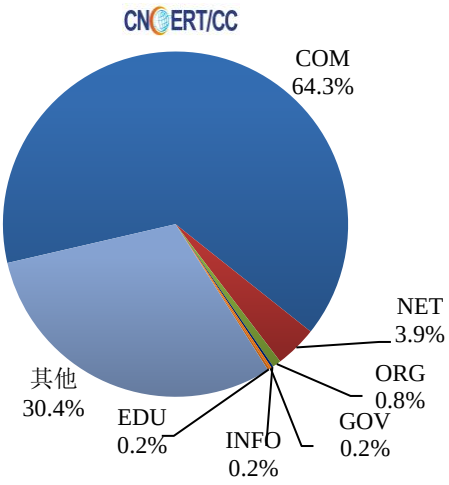


本周境内被篡改政府网站（GOV 类）数量为 0 个；境内被植入后门的政府网站（GOV 类）数量为 1 个，约占境内 0.2%。

本周我国境内篡改网站按类型分布
(5/30-6/5)

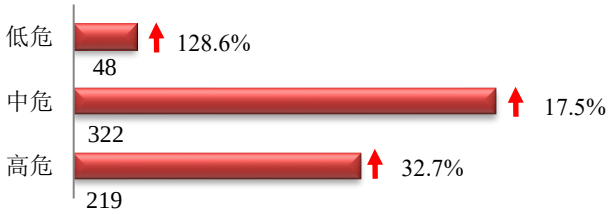


本周我国境内被植入后门网站按类型分布
(5/30-6/5)

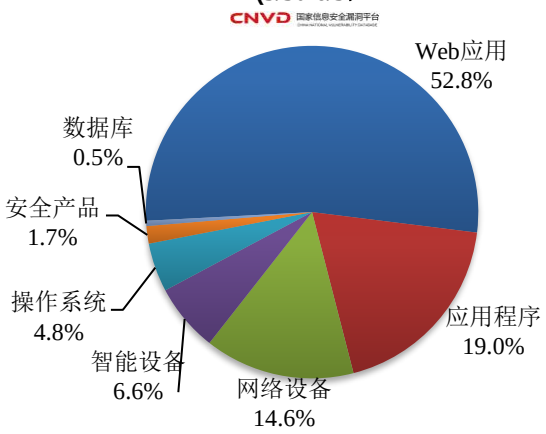


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 589 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
(5/30-6/5）



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。

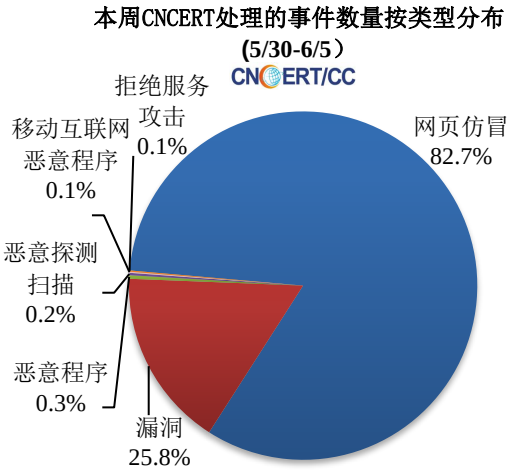
CNVD漏洞周报发布地址

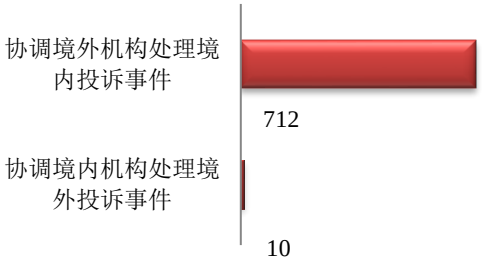
http://www.cnvd.org.cn/webinfo/list?type=4

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。

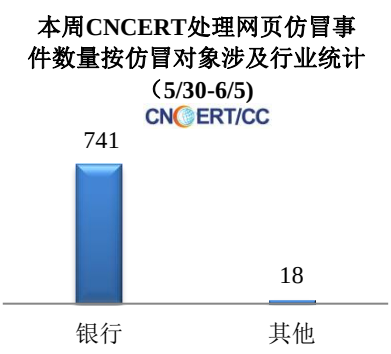
本周事件处理情况

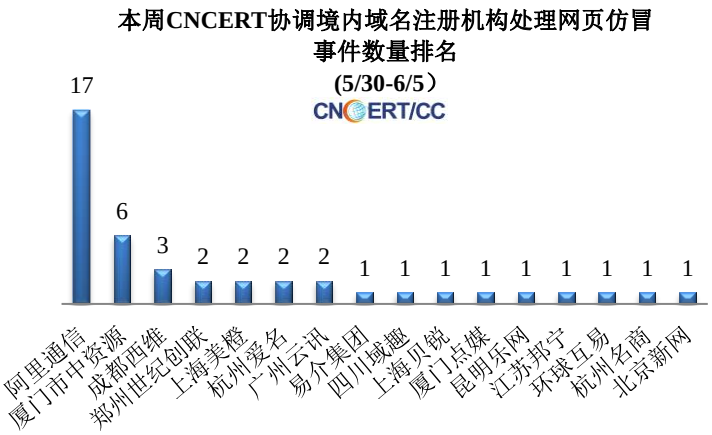
本周，CNCERT 协调云服务商、域名注册服务机构、应用商店、各省分中心以及国际合作组织共处理网络安全事件 918 起，其中跨境网络安全事件 722 起。



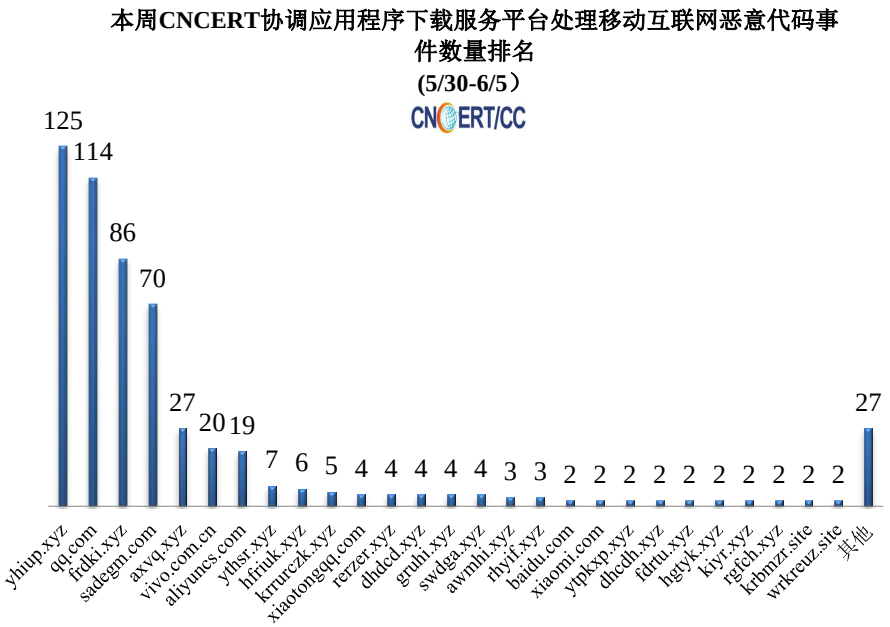


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理 759 起页仿冒投诉事件。根据仿冒对象涉及行业划分，银行仿冒事件 741 起，其他事件 18 起。





本周， CNCERT 协调 54 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 552 个。



业界新闻速递

1. 关于 Mirai 变种僵尸网络大规模传播的风险提示

5 月 31 日，据 CNCERT 官网消息，近期，CNCERT 和奇安信公司共同监测发现一个新的且在互联网上快速传播的 DDoS 僵尸网络，通过跟踪监测发现其每日上线境内肉鸡数（以 IP 数计算）最多已超过 2 万、且每日会针对多个攻击目标发起攻击，给网络空间带来较大威胁。该僵尸网络为 Mirai 变种，包括针对 mips、arm、x86 等 CPU 架构的样本，在近 2 个月的时间中，我们捕获的该 Mirai 变种样本至少迭代过 4 个版本，通信协议都与 Mirai 基本一致，传播方式当前主要为 Telnet 口令爆破，历史上曾利用 Nday 漏洞进行传播。请广大用户强化风险意识，加强安全防范，避免不必要的经济损失，主要建议包括：1、及时修复相关系统漏洞。2、不使用弱密码或默认密码，定期更换密码。当发现主机感染僵尸木马程序后，立即核实主机受控情况和入侵途径，并对受害主机进行清理。

2. 关于微软支持诊断工具 MSDT 存在远程代码执行漏洞的安全公告

5 月 31 日，据国家信息安全漏洞共享平台（CNVD）网站消息，CNVD 收录了微软支持诊断工具远程代码执行漏洞（CNVD-2022-42150，对应 CVE-2022-30190）。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，漏洞利用代码已公开，且已出现在野利用的情况。微软公司已发布漏洞缓解指南，CNVD 建议受影响用户谨慎访问来历不明的 Office 文档，同时及时采取漏洞临时缓解措施，并密切关注后续的补丁更新情况。

3. 关于 Confluence 存在远程代码执行漏洞的安全公告

6 月 3 日，据国家信息安全漏洞共享平台（CNVD）网站消息， CNVD 收录了 Confluence 远程代码执行漏洞（CNVD-2022-43094，对应 CVE-2022-26134）。未经身份验证的攻击者利用该漏洞可在目标服务器执行任意代码。目前，Atlassian 公司已发布漏洞缓解建议，暂未发布修复补丁。CNVD 建议受影响的单位和用户按照厂商公告，及时采取漏洞临时缓解措施，并密切关注后续的补丁更新情况。

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 2021 年，已与 81 个国家和地区的 274 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：朱芸茜

网址： www.cert.org.cn

Email：cncert_report@cert.org.cn

电话： 010-82990315