国家互联网应急中心

网络安全信息与动态周报

2021 年第 41 期

10 月 4 日-10 月 10 日

CNCERT/CC

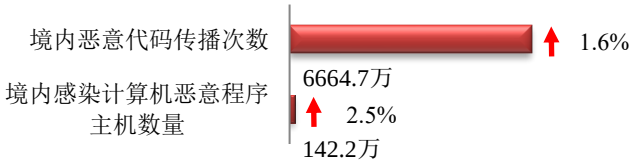
本周网络安全基本态势

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	• 6664.7万 • 142.2万	↑ ↑	1.6% 2.5%
境内被篡改网站总数 其中政府网站数量	• 4084 • 23	↑ =	9.0%
境内被植入后门网站总数 其中政府网站数量	• 1260 • 0	↑ ↓	11.4% 100.0%
针对境内网站的仿冒页面数量	• 44	↓	77.1%
新增信息安全漏洞数量 其中高危漏洞数量	• 265 • 80	↓ ↓	35.7% 1.2%

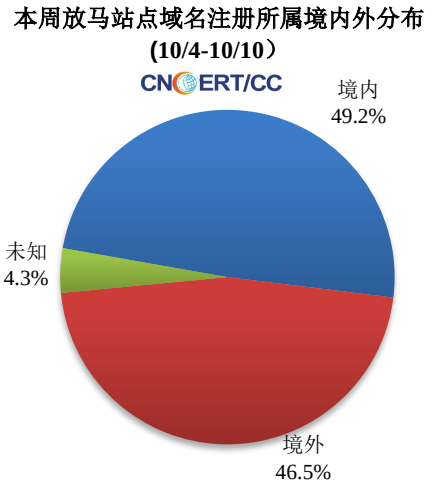
= 表示数量与上周相同　↑ 表示数量较上周环比增加　↓ 表示数量较上周环比减少

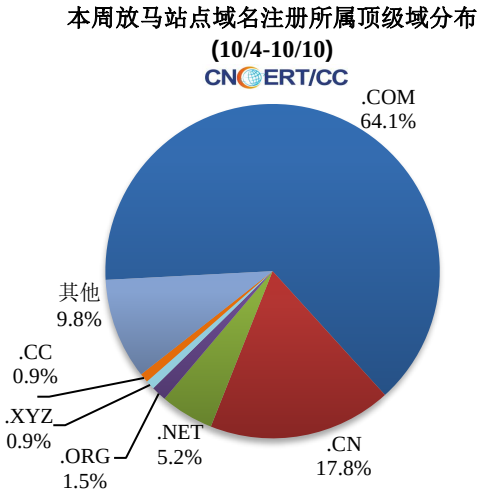
本周网络病毒活动情况

境内计算机恶意程序传播次数约为 6664.7 万次，境内感染计算机恶意程序主机数量约为 142.2 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 1025 个，涉及 IP 地址 4008 个。在 1025 个域名中，有 46.5%为境外注册，且顶级域为.com 的约占 64.1%；在 4008 个 IP 中，有约 25.7%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 388 个。





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。

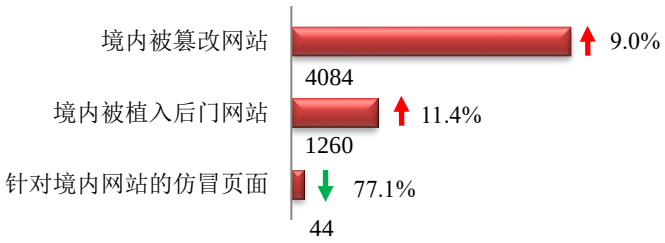
ANVA网络安全威胁信息共享平台

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。

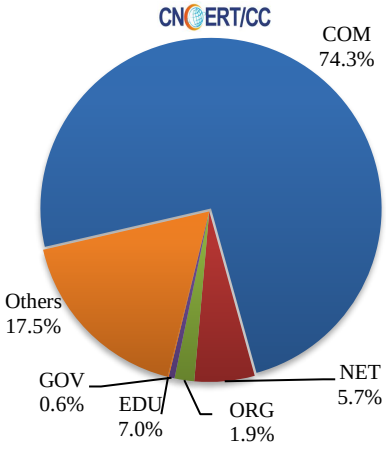
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 4084 个；被植入后门的网站数量为 1260 个；针对境内网站的仿冒页面数量为 44 个。

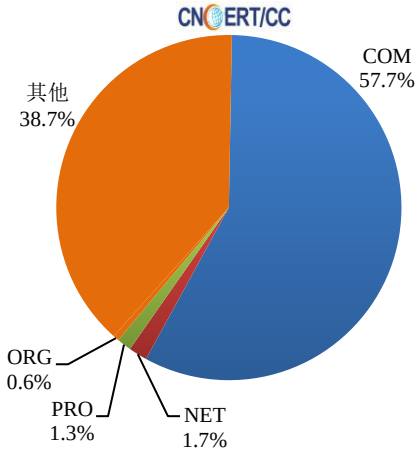


本周境内被篡改政府网站（GOV 类）数量为 23 个（约占境内 0.6%），与上周相比持平；境内被植入后门的政府网站（GOV 类）数量为 0 个，与上周相比下降 100.0%。

本周我国境内篡改网站按类型分布
(10/4-10/10)

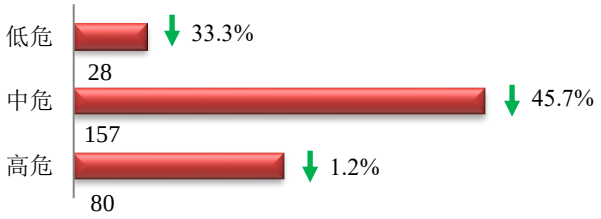


本周我国境内被植入后门网站按类型分布
(10/4-10/10)

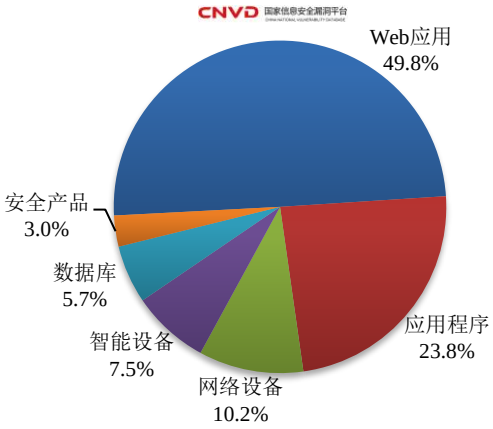


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 265 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
(10/4-10/10）



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。

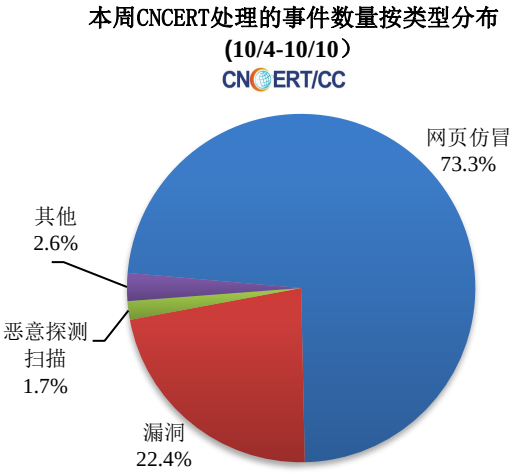
CNVD漏洞周报发布地址

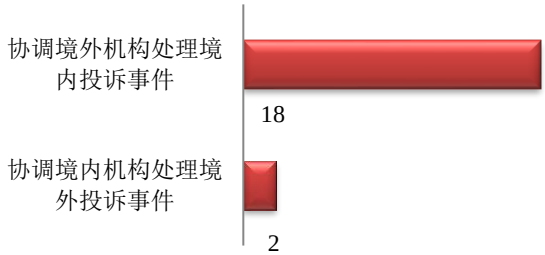
http://www.cnvd.org.cn/webinfo/list?type=4

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。

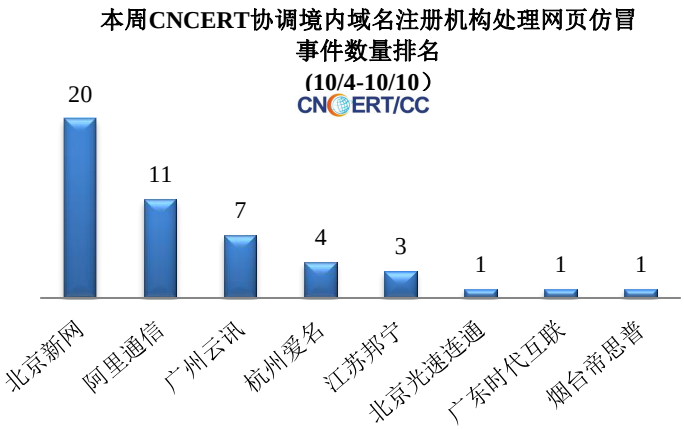
本周事件处理情况

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 116 起，其中跨境网络安全事件 20 起。

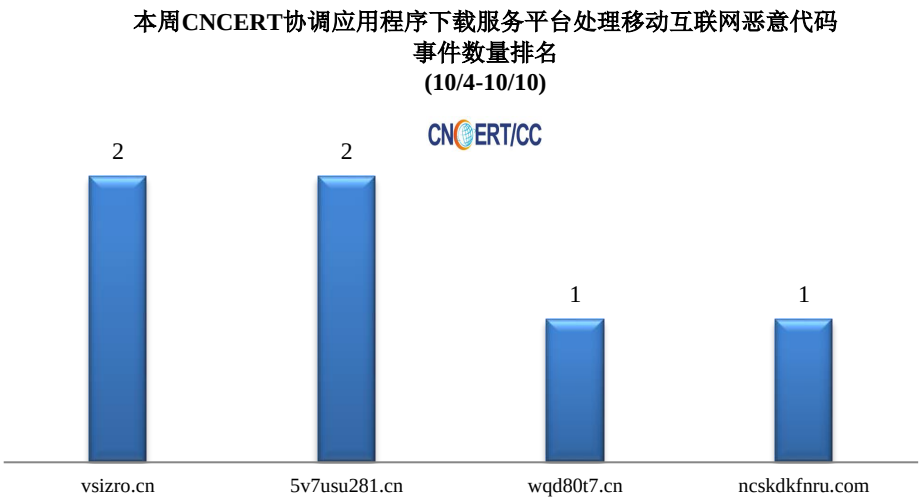




本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理 242 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，银行仿冒事件 85 起。



本周， CNCERT 协调 4 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 6 个。



业界新闻速递

1. CNCERT/CC 连任 APCERT 副主席

2021 年 9 月 29 日，国家计算机网络应急技术处理协调中心（CNCERT/CC）参加了亚太地区计算机应急响应组织（APCERT）举办的 APCERT2021 年全体成员线上大会，第三次成功竞选连任 2021-2022 年度 APCERT 副主席。本次 APCERT2021 年全体成员线上大会议程包括 APCERT 工作组会议、指导委员会委员选举、主席和副主席选举、2021 年应急演练报告、APCERT2022 年年会申办、APCERT 奖励计划介绍等。我中心作为 APCERT 副主席和信息共享组负责人，介绍了近一年来的工作情况及下一年的工作计划。会议进行了新一届指导委员会的选举，中国 CNCERT/CC、日本 JPCERT/CC、马来西亚 Cybersecurity Malaysia、韩国 KrCERT/CC、澳大利亚 ACSC、斯里兰卡 Sri Lanka CERT|CC、中国台北 TWNCERT 成为新一届 APCERT 指导委员会委员。随后，七个现任指导委员会委员召开内部会议选举产生 2021-2022 年度 APCERT 主席和副主席，马来西亚 Cybersecurity Malaysia 连任主席，CNCERT/CC 连任副主席。会议还宣布 APCERT2022 年年会的主办方为斯里兰卡 Sri Lanka CERT|CC,计划于 2022 年 9 月底或 10 月初举行。APCERT 成立于 2003 年，是亚太地区计算机应急响应组织的联盟。APCERT 现有成员 32 个，来自中国、澳大利亚、日本、韩国、马来西亚等 23 个经济体，其目标是通过国际合作建立亚太地区安全、干净、可信的网络空间。

2. CNCERT 参加东盟举办的网络安全应急演练

2021 年 10 月 5 日，CNCERT 作为对话伙伴国，受邀参加了东盟方组织的 2021 年东盟和对话伙伴国网络安全应急演练，这是 CNCERT 连续第十五次参加该项演练。此次演练的主题是“针对企业供应链攻击的应急响应”。演练背景是 A 软件服务商因为网站服务器存在漏洞被攻击组织上传了恶意的软件更新包，继而导致使用其软件服务的 B 公司遭受攻击，进而造成其用户的文件被勒索软件加密。演练过程中，CNCERT 按照事件处置流程，组织对接收的投诉事件进行调查分析，模拟协调其他国家 CERT 组织进行事件处置，发布预警信息以提高公众防范意识。演练期间，CNCERT 还邀请了多家国家级网络安全应急服务支撑单位的技术专家共同参与，通过模拟演练有效强化了我国内应急处理体系的建设，提高了共同应对突发网络安全事件的技术分析和协调处置能力。此次演练有效检验了各国 CERT 组织在网络安全事件处置方面的应急响应技术和能力，增强了东盟与伙伴国在共同维护网络安全方面的合作。共有来自 15 个国家（包括东盟十个国家和中国、印度、韩国、日本和澳大利亚五个伙伴国）的 18 个 CERT 组织参加了此次演练。

3. 2021 年国家网络安全宣传周网络安全博览会在西安举行

据中国网信网消息，10 月 8 日，由中央网信办、陕西省人民政府指导，西安市人民政府主办，西安市委网信办、西安市大数据局、国家工业信息安全发展研究中心承办的 2021 年国家网络安全宣传周网络安全博览会（以下简称“博览会”）在西安国际会展中心举办。本届博览会以“网络安全为人民，网络安全靠人民”为主题，重点展示党的十八大以来网络安全领域重大成就，展示网络安全前沿技术、新型产品，以及示范应用。博览会由线下展和线上数字化展会两部分组成。线下展于 10 月 8 日起在西安国际会展中心举办，展览面积约 1.6 万平米，共 70 余家单位、企业参展。线上数字化展会于 10 月 11 日至未来一年，在国家网络安全宣传周官网上展示。

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：贾子骁

网址： www.cert.org.cn

Email：cncert_report@cert.org.cn

电话： 010-82990315