国家互联网应急中心

网络安全信息与动态周报

2020 年第 41 期

10 月 5 日-10 月 11 日

CNCERT/CC

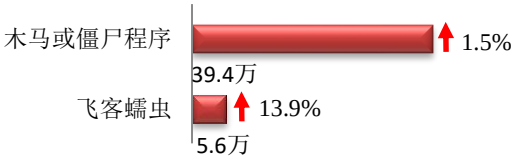
本周网络安全基本态势

境内感染网络病毒的主机数量	•45.0万	2.9%
境内被篡改网站总数 其中政府网站数量	•5170 •21	13.5% 23.5%
境内被植入后门网站总数 其中政府网站数量	•618 •0	11.5%
针对境内网站的仿冒页面数量	•455	20.5%
新增信息安全漏洞数量 其中高危漏洞数量	•169 •44	= =

= 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

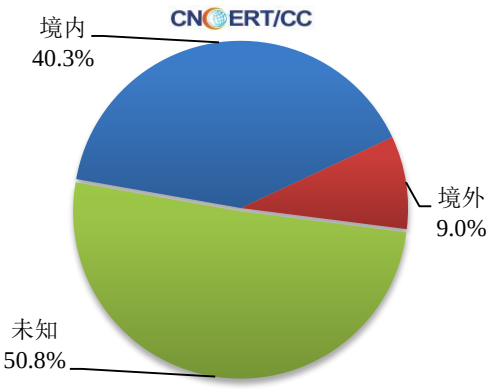
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 45.0 万个，其中包括境内被木马或被僵尸程序控制的主机约 39.4 万以及境内感染飞客（conficker）蠕虫的主机约 5.6 万。

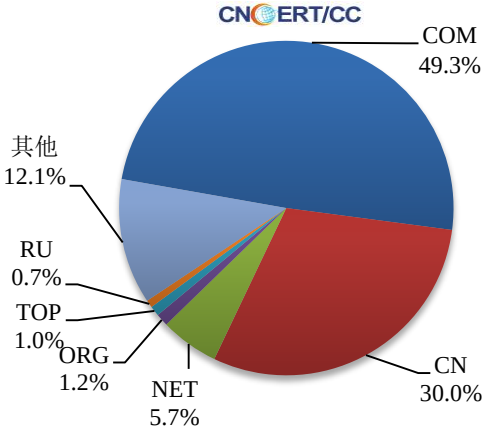


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 1237 个，涉及 IP 地址 15016 个。在 1237 个域名中，有 9.0%为境外注册，且顶级域为.com 的约占 49.3%；在 15016 个 IP 中，有约 14.4%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 640 个 IP。

本周放马站点域名注册所属境内外分布 (10/5-10/11)



本周放马站点域名注册所属顶级域分布 (10/5-10/11)



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。

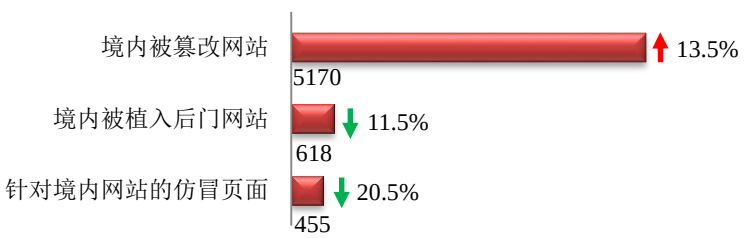
ANVA网络安全威胁信息共享平台

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

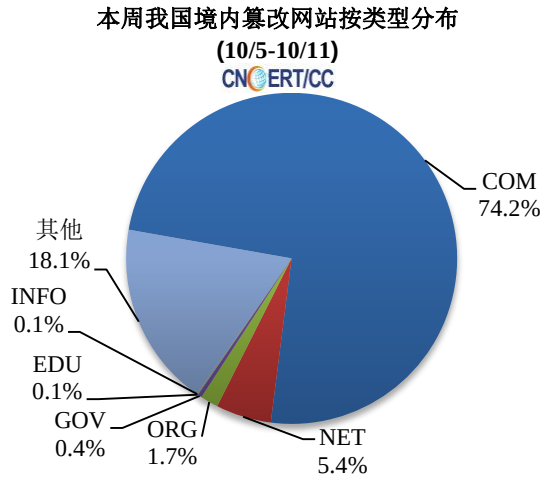
中国反网络病毒联盟（Anti Network-Virus Alliance of China，缩写 ANVA）是由 CNCERT 发起并组织运作的行业联盟。

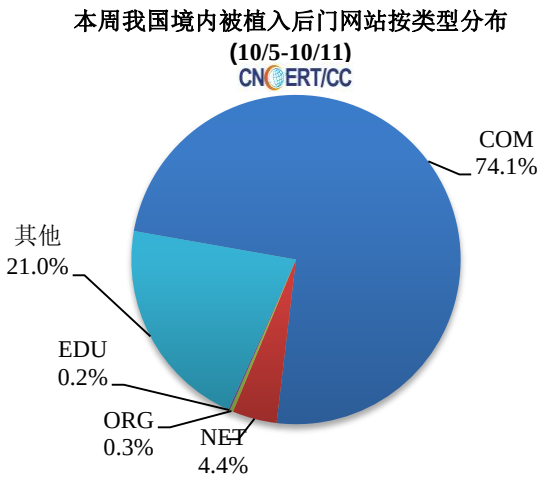
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 5170 个；被植入后门的网站数量为 618 个；针对境内网站的仿冒页面数量 455 个的仿冒页面。



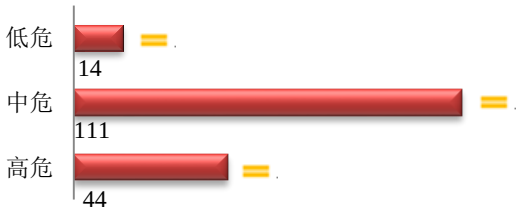
本周境内被篡改政府网站（GOV 类）数量为 21 个（约占境内 0.4%），较上周上涨了 23.5%；境内被植入后门的政府网站（GOV 类）数量为 0 个。

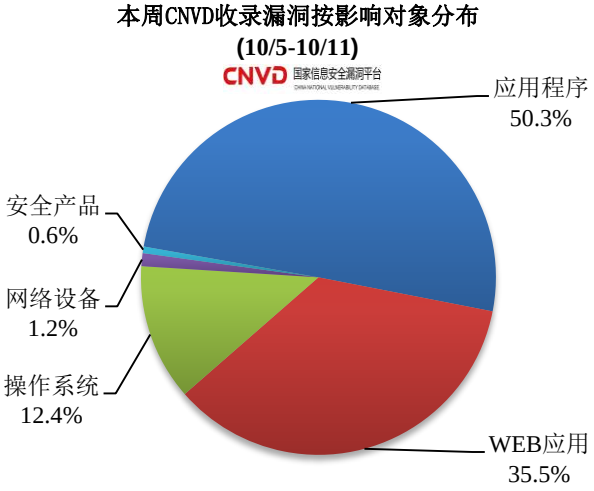




本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 169 个，信息安全漏洞威胁整体评价级别为中。





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。

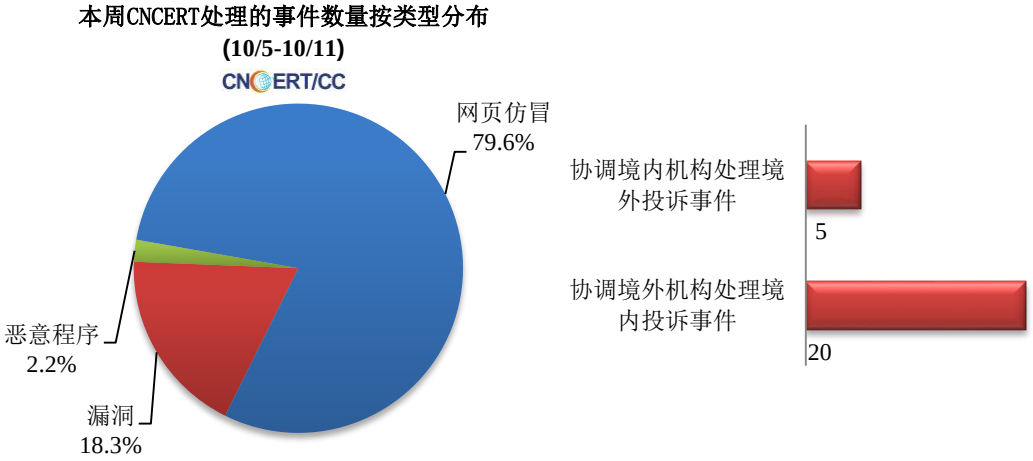
CNVD漏洞周报发布地址

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

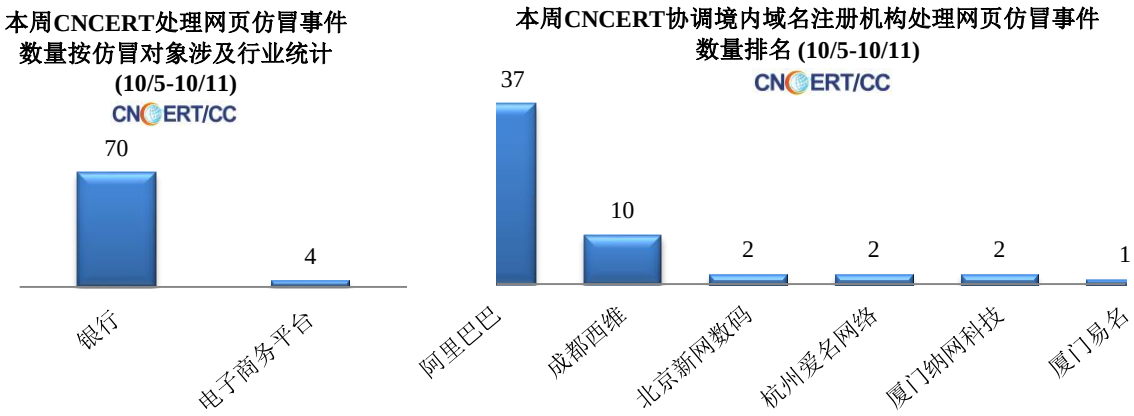
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信企业、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

本周事件处理情况

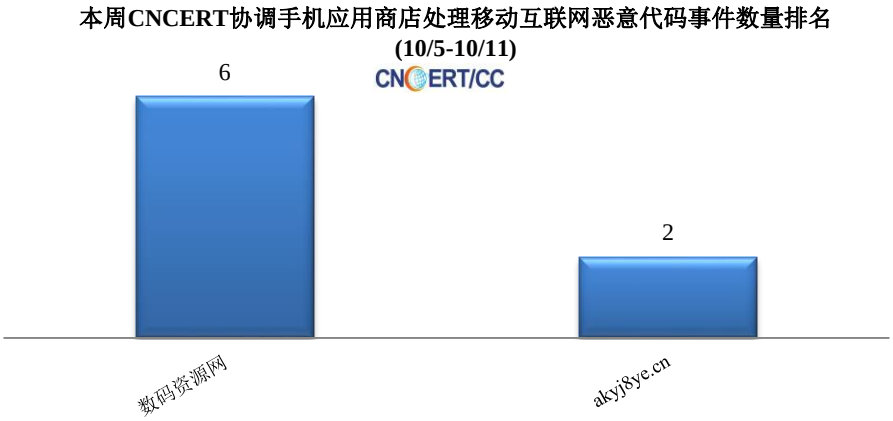
本周，CNCERT 协调基础电信企业、云服务商、域名注册服务机构、应用商店、各省分中心以及国际合作组织共处理了网络安全事件 93 起，其中跨境网络安全事件 25 起。



本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 74 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，包括银行仿冒事件 70 起和电子商务平台 4 起。



本周，CNCERT 协调 2 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 8 个。



业界新闻速递

1、 CNCERT 参加东盟举办的网络安全应急演练

2020 年 10 月 7 日，CNCERT 作为东盟对话伙伴方，参加了 2020 年度东盟国家组织开展的网络安全应急演练，这是 CNCERT 连续第十四次参加该项演练。

此次演练的主题是“利用疫情开展的恶意软件活动”。演练以某医院服务邮箱账号遭受黑客组织攻击，被仿冒进行网络欺诈，向医院病人发邮件欺骗其提供个人敏感信息为背景，需要参演组织通过综合分析了解整个事件过程，找到存在问题和提供解决方案。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，协调其他国家相关组织和 CERT 部门进行事件处置，并指导相关部门进行修复和防范。

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保障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。

2、 APEC-TEL 第 61 次会议网络安全与繁荣指导组线上会议顺利召开

2020 年 10 月 9 日，亚太经合组织电信工作组（APEC-TEL）第 61 次会议网络安全与繁荣指导组（SPSG）会议在网上顺利召开，国家计算机网络应急技术处理协调中心（CNCERT/CC）的徐原作为网络安全与繁荣指导组召集人主持了本次会议。同时，

CNCERT/CC 作为中国网络安全技术中心和应急处理体系的牵头单位，支撑 APEC-TEL 中国代表团圆满完成了任期四年的网络安全与繁荣指导组副召集人和召集人工作，提高了我方在网络安全领域的国际地位和影响力。

本次网络安全与繁荣指导组线上会议讨论了 APEC-TEL2020 年至 2025 年战略行动计划文稿，听取了组内正在执行项目和新申请项目的介绍，探讨了指导组召集人提名等事务。另外，澳大利亚、中国、中国台北和世界互联网协会的代表还分享了本经济体或组织关于网络安全的最新发展和活动情况。后续，CNCERT/CC 将代表网络安全与繁荣指导组在 APEC-TEL 第 61 次会议全会上汇报指导组的工作和会议情况。

自 2016 年 10 月起，CNCERT/CC 徐原担任网络安全与繁荣指导组的副召集人，任期两年（APEC-TEL 第 54 至 57 次会议）。2018 年 9 月正式就任召集人，任期两年（APEC-TEL 第 58 至 61 次会议）。CNCERT/CC 支撑完成了主持网络安全与繁荣指导组会议，领导组内各经济体代表做好指导组发展计划和框架、战略计划执行、审核项目等工作，并应邀在指导组项目研讨会上致辞，参加 APEC 电信工作组和数字经济组联合会议等，提高了我方在网络安全领域的影响力。同时还牵头起草 APEC-TEL2020 年至 2025 年战略行动计划文稿网络安全部分，深入参与 APEC 保障数字经济框架文稿修改，增强了我方在网络安全领域的话语权。期间，CNCERT/CC 还申请了 APEC 自筹资金项目“物联网安全研讨会”，并在 2018 年 APEC-TEL 第 57 次会议上成功组织举办研讨会，得到了 APEC-TEL 各经济体的热切关注和一致好评。

3、 全球软件巨头 Software AG 遭勒索攻击

10 月 7 日，据外媒报道，名为“Clop”的勒索团伙攻陷了全球最大的软件公司之一 Software AG 的内部网络、加密文件并要求支付 2000 多万美元才提供解密密钥。谈判失败后，该团伙在暗网网站上公开了 Software AG 公司的数据，包括员工的护照和身份证扫描件、员工邮件、金融文档和公司内网目录。高达 2000 多万美元的勒索金是迄今为止见到的最高勒索金之一。目前这家德国技术巨头公司的服务尚未恢复正常。

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 2019 年，已与 78 个国家和地区的 260 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