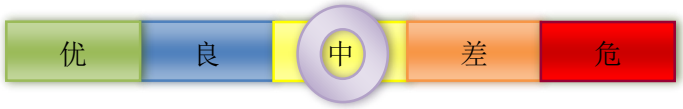
国家互联网应急中心

2020 年第 44 期

10 月 26 日-11 月 1 日

网络安全信息与动态周报

本周网络安全基本态势

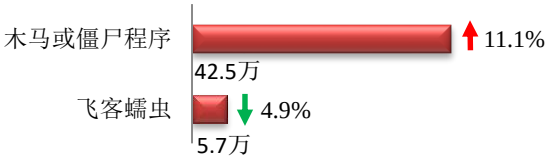


境内感染网络病毒的主机数量	•48.2万	8.9%
境内被篡改网站总数 其中政府网站数量	•4539 •26	23.5% 7.1%
境内被植入后门网站总数 其中政府网站数量	•583 •2	32.4% 100.0%
针对境内网站的仿冒页面数量	•594	60.4%
新增信息安全漏洞数量 其中高危漏洞数量	•418 •137	30.0% 41.7%

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*

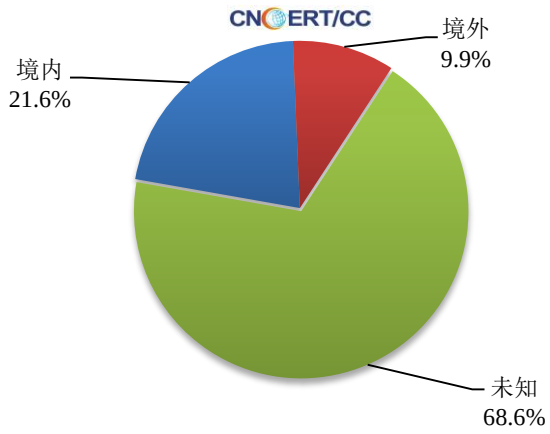
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 48.2 万个，其中包括境内被木马或被僵尸程序控制的主机约 42.5 万以及境内感染飞客（conficker）蠕虫的主机约 5.7 万。

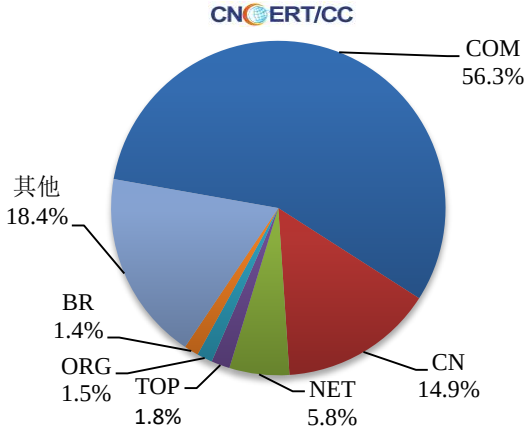


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 1002 个，涉及 IP 地址 5201 个。在 1002 个域名中，有 9.9%为境外注册，且顶级域为.com 的约占 56.3%；在 5201 个 IP 中，有约 20.4%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 376 个 IP。

本周放马站点域名注册所属境内外分布
(10/26-11/01)



本周放马站点域名注册所属顶级域分布
(10/26-11/01)



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。

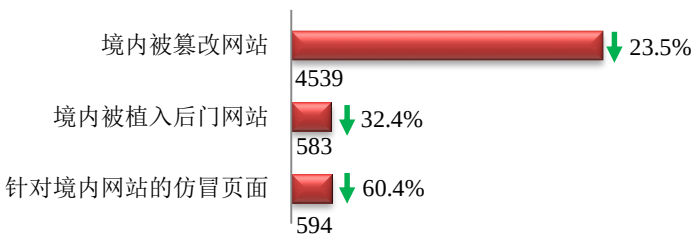
ANVA网络安全威胁信息共享平台

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。

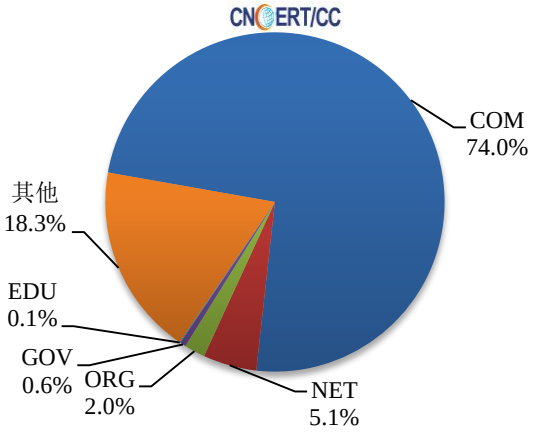
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 4539 个；被植入后门的网站数量为 583 个；针对境内网站的仿冒页面数量 594 个的仿冒页面。

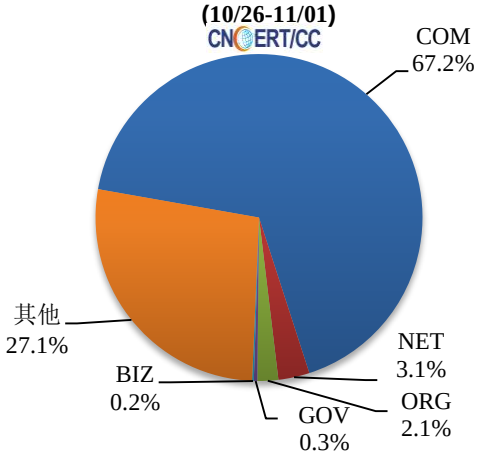


本周境内被篡改政府网站（GOV 类）数量为 26 个（约占境内 0.6%），较上周下降了 7.1%；境内被植入后门的政府网站（GOV 类）数量为 2 个（约占境内 0.3%），较上周上涨了 100.0%。

本周我国境内篡改网站按类型分布
(10/26-11/01)

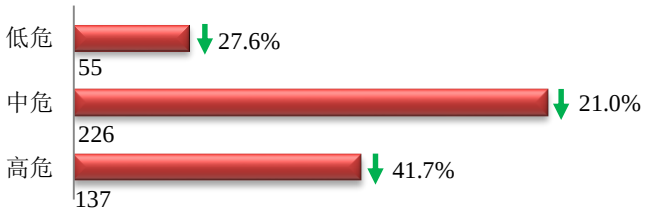


本周我国境内被植入后门网站按类型分布
(10/26-11/01)

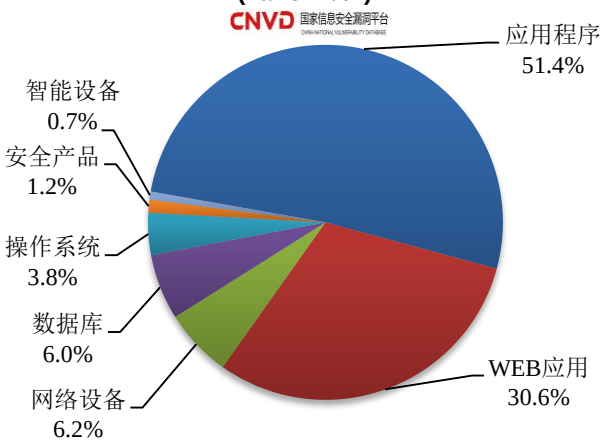


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 418 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
(10/26-11/01)



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。

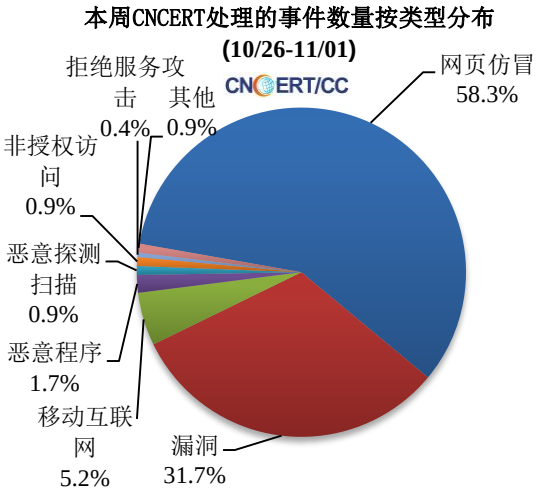
CNVD漏洞周报发布地址

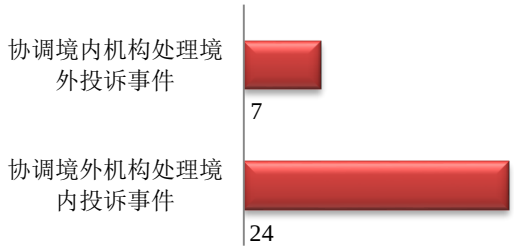
http://www.cnvd.org.cn/webinfo/list?type=4

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。

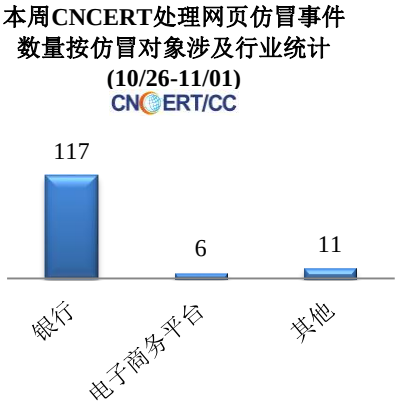
本周事件处理情况

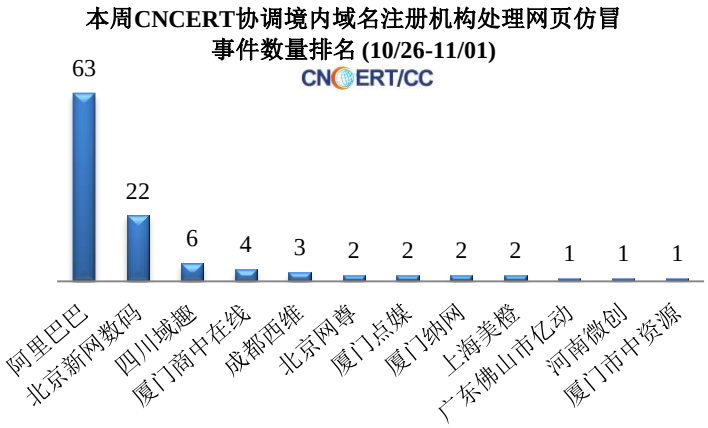
本周，CNCERT 协调基础电信企业、云服务商、域名注册服务机构、应用商店、各省分中心以及国际合作组织共处理了网络安全事件 230 起，其中跨境网络安全事件 31 起。



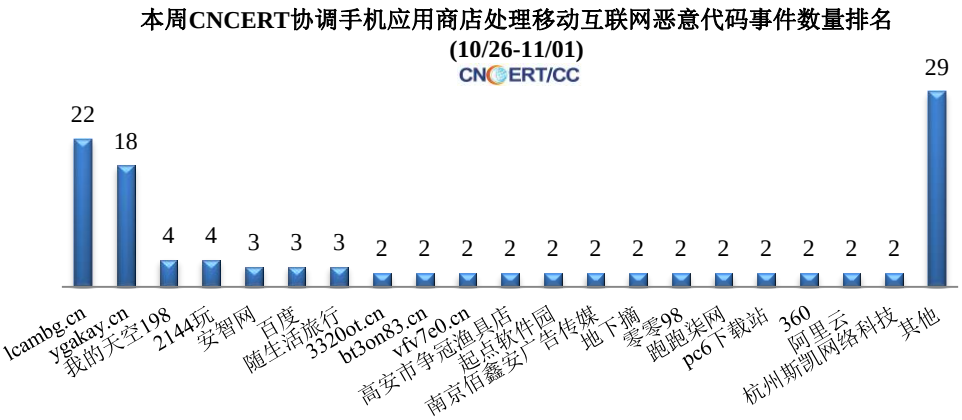


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 134 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，包括银行仿冒事件 117 起、电子商务平台 6 起以及其他事件 11 起。





本周，CNCERT 协调 49 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 112 个。



业界新闻速递

1. 大量 Office 365 用户受到来自 Microsoft Teams 网络钓鱼攻击

10 月 24 日，据 securityaffairs 网站消息，安全研究人员报告说，已经有多达 5 万名 Office 365 用户受到了某网络钓鱼活动的攻击，这些活动伪装成来自 Microsoft Teams 的自动邮件，诱饵邮件会向用户显示“错过聊天信息”，从而窃取 Office 365 用户的登录凭证。安全报告显示，钓鱼邮件冒充 Microsoft Teams 的自动邮件，以窃取用户的登录凭证。在钓鱼邮件正文中有三个链接，单击其中的任何一个都将进入一个仿照 Microsoft 登录页面设计的假网站。钓鱼网页提示收件人输入他们的电子邮箱和密码。

2. 以色列智能灌溉系统遭遇网络攻击

10 月 26 日，据 ZDNet 网站消息，近日，以色列安全研究公司 Security Joes 发现，全球 100 多个地方安装的 Mottech Water Management 公司的智能灌溉系统没有更改出厂默认密码，这意味着任何人都可以通过网络访问并篡改其中的农作物、树木、城市及建筑群灌溉系统。一旦攻击者找到这些可公开访问的联网灌溉系统，攻击者只需要输入默认的管理员用户名并按下回车键，即可直接访问智能灌溉控制面板，也能够暂停和终止灌溉操作、更改设置、控制泵水量及压力，甚至删除用户以锁定灌溉系统。目前，研究人员已向以色列 CERT、受影响的公司以及智能灌溉系统供应商 Mottech Water Management 发出警报。

3. Oracle WebLogic Server console 高危漏洞预警

10 月 30 日，据中国内参网站消息，Oracle 发布了 10 月漏洞补丁更新公告，修复了多个 WebLogic Server 相关的高危漏洞。其中 WebLogic console 存在远程代码执行漏洞，漏洞编号：CVE-2020-14882，

攻击者可通过 WebLogic Server HTTP Console 接口，实现未授权的远程代码执行攻击，从而获得目标系统管理权限。该漏洞 POC 已在互联网公开，且无需身份验证即可触发该漏洞，漏洞风险较大，建议受影响用户及时下载补丁程序并安装更新，做好资产自查以及预防工作，以免遭受黑客攻击。

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：王小群

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315