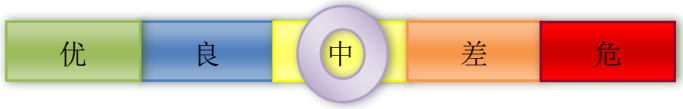
国家互联网应急中心

2020 年第 42 期
10 月 12 日-10 月 18 日

网络安全信息与动态周报

本周网络安全基本态势

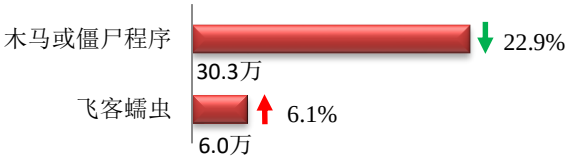


境内感染网络病毒的主机数量	•36.3万	19.2%
境内被篡改网站总数 其中政府网站数量	•4769 •32	7.8% 52.4%
境内被植入后门网站总数 其中政府网站数量	•621 •1	0.5%
针对境内网站的仿冒页面数量	•1911	320.0%
新增信息安全漏洞数量 其中高危漏洞数量	•372 •124	120.1% 181.8%

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*

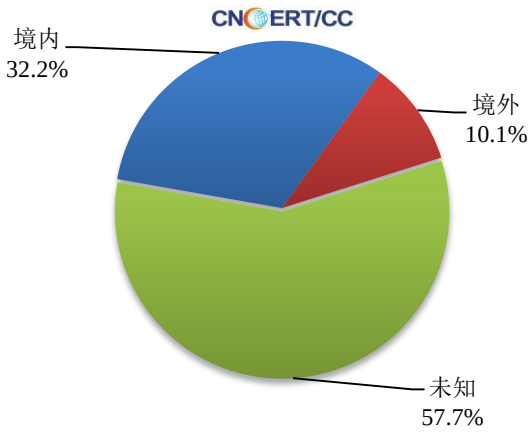
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 36.3 万个，其中包括境内被木马或被僵尸程序控制的主机约 30.3 万以及境内感染飞客（conficker）蠕虫的主机约 6.0 万。

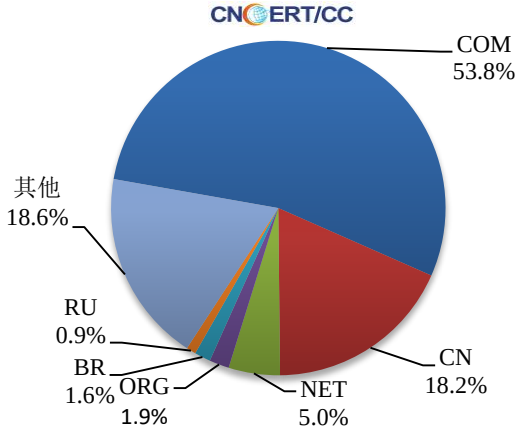


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 1410 个，涉及 IP 地址 10657 个。在 1410 个域名中，有 10.1%为境外注册，且顶级域为.com 的约占 53.8%；在 10657 个 IP 中，有约 24.7%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 656 个 IP。

本周放马站点域名注册所属境内外分布
(10/12-10/18)



本周放马站点域名注册所属顶级域分布
(10/12-10/18)



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。

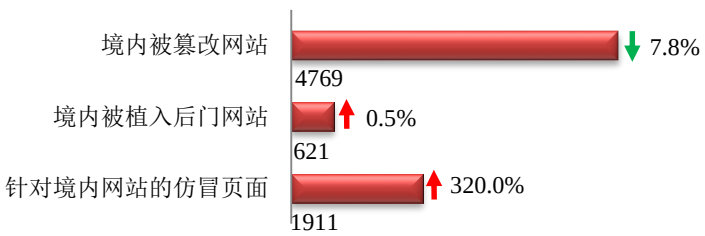
ANVA网络安全威胁信息共享平台

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

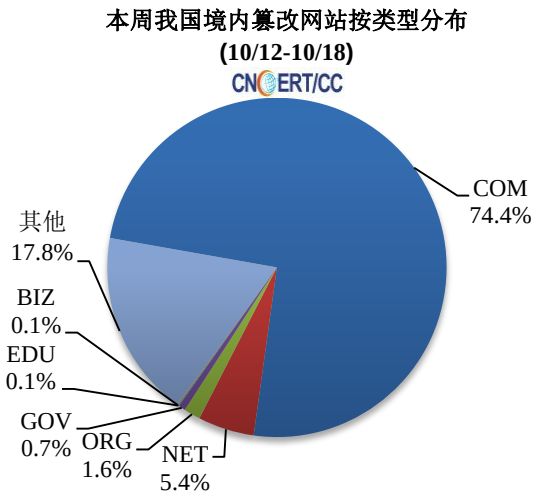
中国反网络病毒联盟（Anti Network-Virus Alliance of China，缩写 ANVA）是由 CNCERT 发起并组织运作的行业联盟。

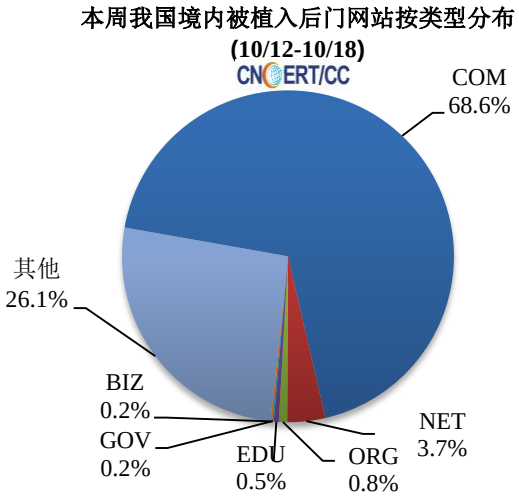
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 4769 个；被植入后门的网站数量为 621 个；针对境内网站的仿冒页面数量 1911 个的仿冒页面。



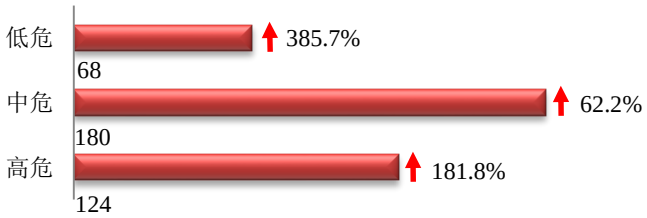
本周境内被篡改政府网站（GOV 类）数量为 32 个（约占境内 0.7%），较上周上涨了 52.4%；境内被植入后门的政府网站（GOV 类）数量为 1 个。

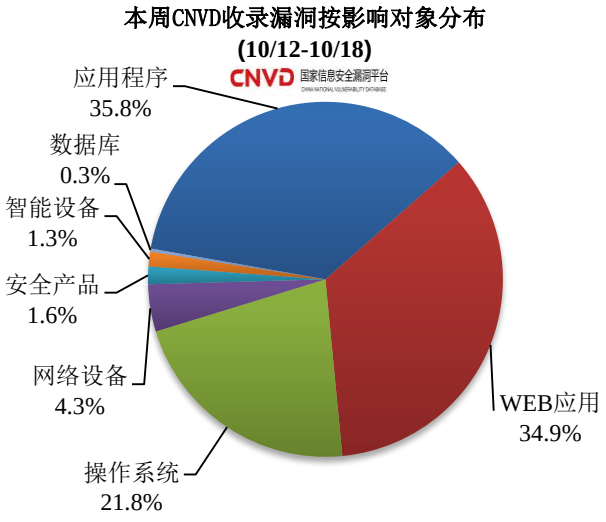




本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 372 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。

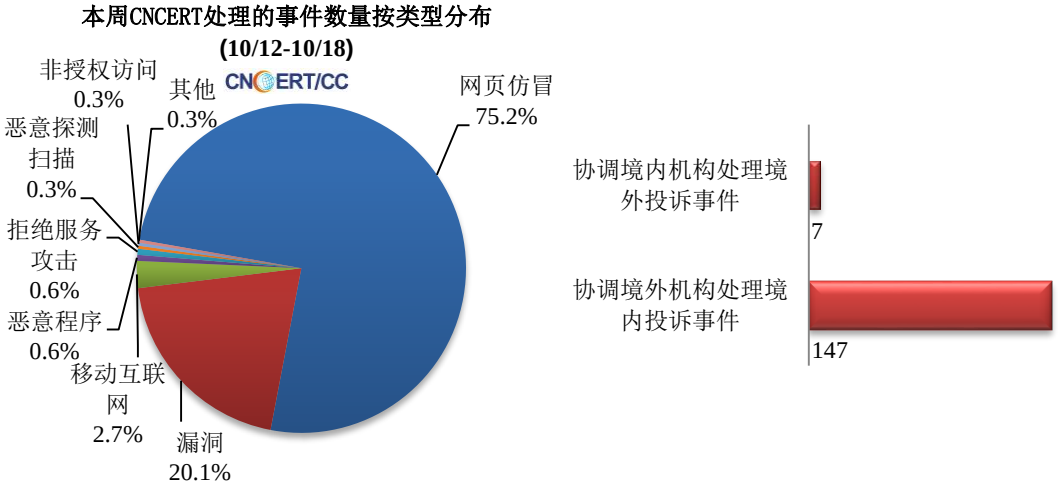
CNVD漏洞周报发布地址

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

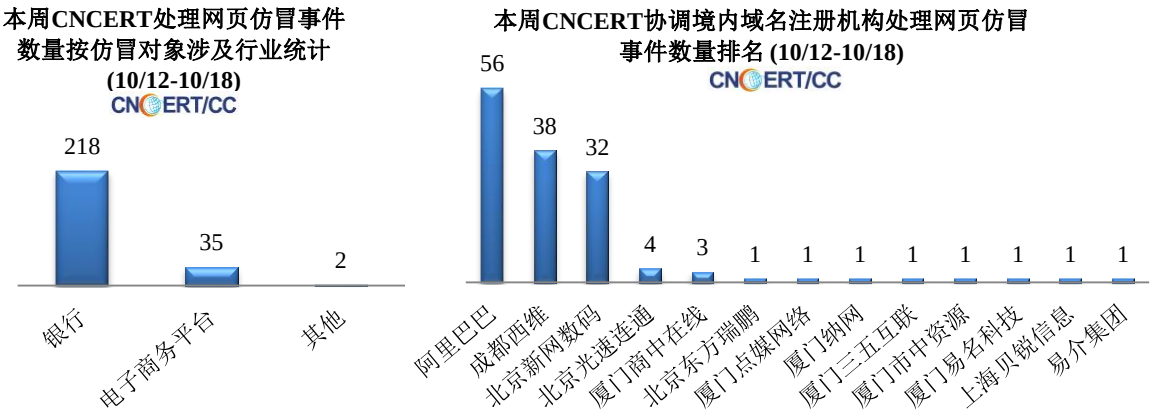
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信企业、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

本周事件处理情况

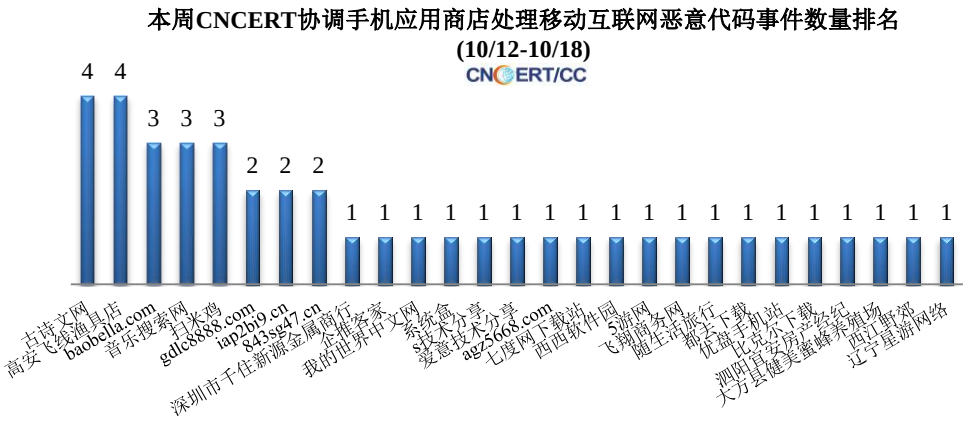
本周，CNCERT 协调基础电信企业、云服务商、域名注册服务机构、应用商店、各省分中心以及国际合作组织共处理了网络安全事件 339 起，其中跨境网络安全事件 154 起。



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 255 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 218 起、电子商务平台 35 起以及其他事件 2 起。



本周，CNCERT 协调 27 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 42 个。



业界新闻速递

1. 我国立法加强个人信息保护 收集用户数据要事前告知取得同意

10 月 13 日，新华社北京电，近年来，随着大数据等技术的发展，一些网络平台擅自收集用户数据等行为，让群众反映强烈。13 日首次提请全国人大常委会会议审议的个人信息保护法草案，确立以“告知——同意”为核心的个人信息处理一系列规则，有望为破解这些问题提供法律依据。报道显示，草案规定，处理个人信息应当在事先充分告知的前提下取得个人同意，并且个人有权撤回同意；重要事项发生变更的应当重新取得个人同意；不得以个人不同意为由拒绝提供产品或者服务。个人信息处理者在处理个人信息前，应当以显著方式、清晰易懂的语言将个人信息处理者的身份、联系方式，个人信息的处理目的、处理方式，处理的个人信息种类、保存期限，个人行使本法规定权利的方式和程序等事项向个人告知。此外，报道还称，一些平台还利用收集的大数据向用户推送个性化广告。草案对此明确，利用个人信息进行自动化决策，应当保证决策的透明度和处理结果的公平合理。个人认为自动化决策对其权益造成重大影响的，有权要求个人信息处理者予以说明，并有权拒绝个人信息处理者仅通过自动化决策的方式作出决定。通过自动化决策方式进行商业营销、信息推送，应当同时提供不针对其个人特征的选项。

2. Linux 内核曝严重蓝牙漏洞，影响多个版本

10 月 15 日，Freebuf 网站消息，谷歌安全研究人员在 Linux 内核中发现了一组蓝牙漏洞（BleedingTooth），该漏洞可能允许攻击者进行零点击攻击，运行任意代码或访问敏感信息。BleedingTooth 漏洞分别被命名为 CVE-2020-12351，CVE-2020-12352 和 CVE-2020-24490。其中最严重的漏洞是基于堆的类型混淆漏洞（CVE-2020-12351），被评为高危漏洞。据悉，漏洞存在于 BlueZ 中，软件栈默认情况下为 Linux 实现了所有蓝牙核心协议和层。除 Linux 笔记本电脑外，它还用于许多消费或工业物联网设备。受害者蓝牙覆盖范围内的远程攻击者都可以通过目标设备的 bd 地址来利用此漏

洞。攻击者能够通过发送恶意的 L2CAP 数据包来触发漏洞，导致拒绝服务，甚至执行具有内核特权的任意代码。

3. 希腊电信公司遭黑客攻击 数百万个电话数据被窃取

10 月 16 日，中新网电，据欧联网援引欧联通讯社报道，希腊最大电信公司 Cosmote15 日向媒体通报，该公司上个月发生了一起重大的数据泄露事件，数以百万计希腊民众的电话以及信息数据被窃取，其中甚至包括总理和政府高级官员的通信数据。据报道，此前，Cosmote 公司数据库遭到不明身份黑客的网络攻击。黑客窃取了 2020 年 9 月 1 日至 5 日期间的数百万个电话和短信的资料，包括固定电话、移动电话、移动网络等。根据 Cosmote 发布的公告显示，该公司在对其系统进行检查时，发现有一个未经授权的操作，从公司大数据系统中导出带有呼叫详细信息的文件。数据中包含电话号码、通话日期和时间、基站坐标等。但这些文件中不包含通话和聊天信息内容、用户姓名和地址、密码、信用卡或银行帐户信息等个人资料。

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：郭晶

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315