,,

国家互联网应急中心

网络安全信息与动态周报

2020 年第 26 期

6 月 22 日-6 月 28 日

CNCERT/CC

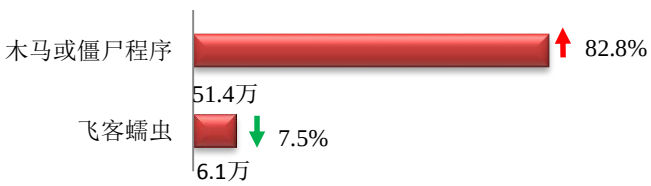
本周网络安全基本态势

境内感染网络病毒的主机数量	•57.5万	↑ 65.4%
境内被篡改网站总数 其中政府网站数量	•6181 •21	↓ 26.9% ↓ 25.0%
境内被植入后门网站总数 其中政府网站数量	•1464 •1	↑ 0.6% ↓ 80.0%
针对境内网站的仿冒页面数量	•719	↓ 9.3%
新增信息安全漏洞数量 其中高危漏洞数量	•259 •104	↓ 46.4% ↓ 17.5%

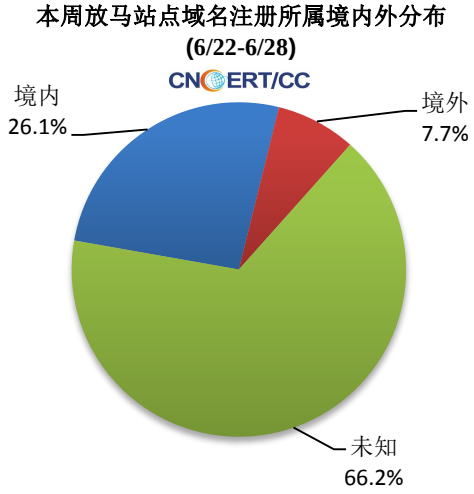
= 表示数量与上周相同　↑ 表示数量较上周环比增加　↓ 表示数量较上周环比减少

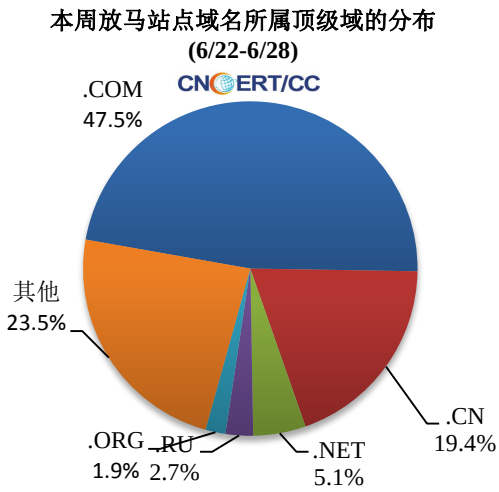
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 57.5 万个，其中包括境内被木马或被僵尸程序控制的主机约 51.4 万以及境内感染飞客（conficker）蠕虫的主机约 6.1 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 2481 个，涉及 IP 地址 4889 个。在 2481 个域名中，有 7.7%为境外注册，且顶级域为.com 的约占 47.5%；在 4889 个 IP 中，有约 58.4%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 483 个 IP。





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。

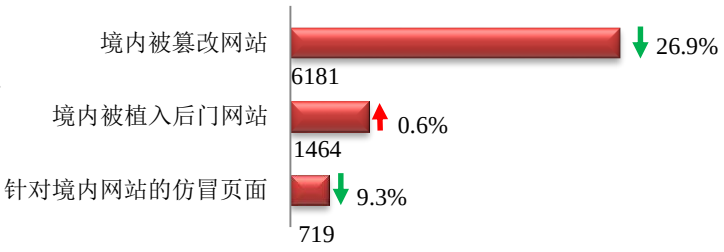
ANVA网络安全威胁信息共享平台

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

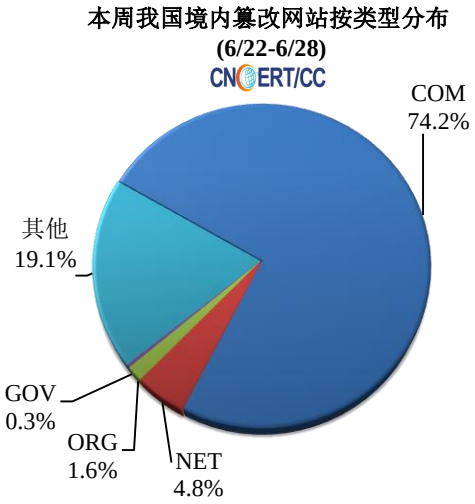
中国反网络病毒联盟（Anti Network-Virus Alliance of China，缩写 ANVA）是由 CNCERT 发起并组织运作的行业联盟。

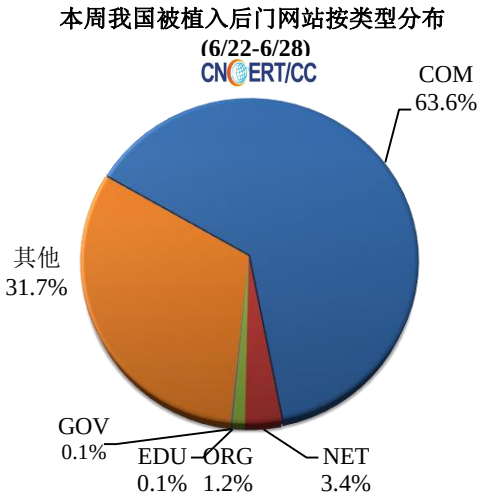
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 6181 个；被植入后门的网站数量为 1464 个；针对境内网站的仿冒页面数量 719 个。



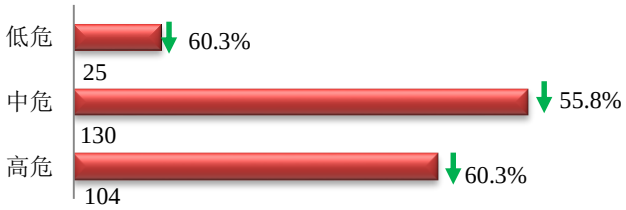
本周境内被篡改政府网站（GOV 类）数量为 21 个（约占境内 0.3%），较上周下降了 25.0%；境内被植入后门的政府网站（GOV 类）数量为 1 个（约占境内 0.1%），较上周下降了 80.0%。

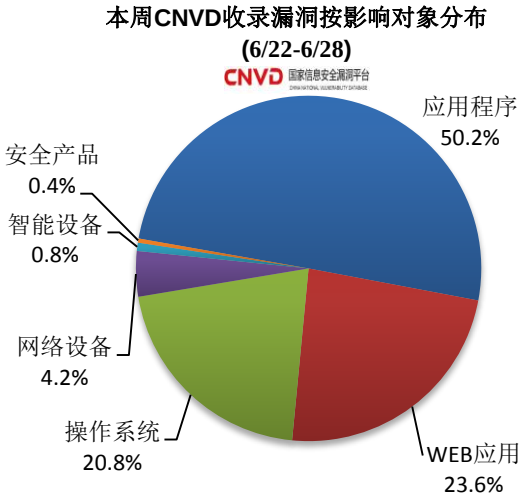




本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 259 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

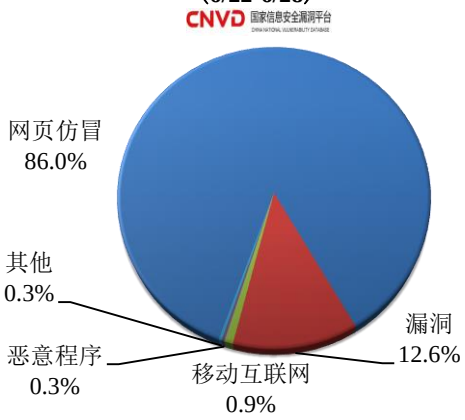
http://www.cnvd.org.cn/webinfo/list?type=4

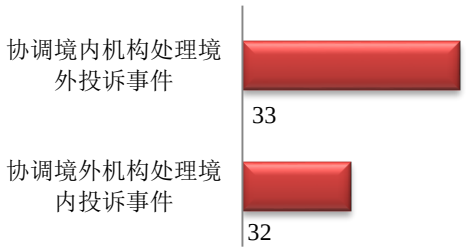
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信企业、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 342 起，其中跨境网络安全事件 65 起。

本周CNCERT处理的事件数量按类型分布
(6/22-6/28)

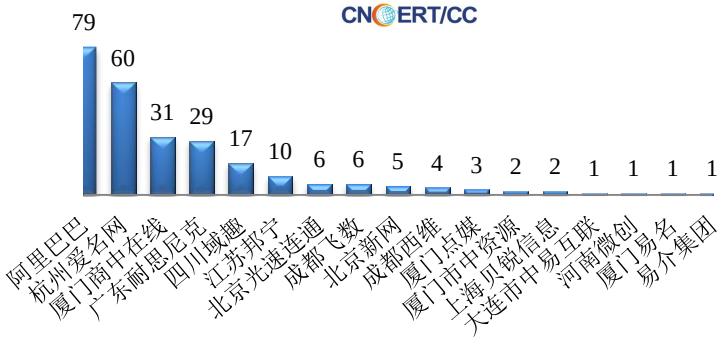




本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 294 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，包括银行仿冒事件 138 起、电子商务平台 76 起和其他事件 80 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计
(6/22-6/28)

本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (6/22-6/28)



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 2 个。

业界新闻速递

1、 数据安全法草案初次提请全国人大常委会审议

6 月 28 日，数据安全法草案初次提请十三届全国人大常委会第二十次会议审议。数据安全已成为事关国家安全与经济社会发展的重大问题。草案按照总体国家安全观的要求，确立数据安全保护管理各项基本制度，提升国家数据安全保障能力，有效应对数据这一非传统领域的国家安全风险与挑战，切实维护国家主权、安全和发展利益。草案坚持安全与发展并重，规定支持、促进数据安全与发展的措施，提升数据安全治理和数据开发利用水平，促进以数据为关键要素的数字经济发展。此外，草案立足数据安全工作实际，着力解决数据安全领域突出问题，落实数据活动主体的安全保护义务与责任，切实维护公民、组织的合法权益。适应电子政务发展的需要，建立政务数据安全管理制度和开放利用规则，大力推进政务数据资源开放和开发利用。

2、 9 款约会社交 App 云泄露数十万用户 845GB 敏感数据

6 月 23 日，据外媒报道，9 家流行约会软件曝光了 845 GB 的露骨照片和聊天隐私等信息，预计泄露了数十万用户的隐私数据。此前安全研究人员在扫描开放的互联网时，偶然发现了一组公开可访问的亚马逊网络服务“数据存储库”。每一个都包含了来自不同约会应用软件的数据信息，这些应用包括 3somes、Cougary、Gay Daddy Bear、 Xpal、BBW 约会、casual alx、SugarD 和 GHunt 等。研究人员总共找到了 845GB 和近 250 万份记录，可能代表了数十万用户的数据。据悉，这些被泄露的信息特别敏感，其中包括露

骨照片和录音，同时研究人员还发现了来自其他平台的私人聊天截图和付款收据，这些数据都是用户在应用内发送的。

3、 研究人员发现网上公开约 8 万台打印机的互联网打印协议端口

6 月 23 日，据外媒报道，来自 Shadowserver Foundation 的安全研究人员在发布的一份报告中，警告那些将打印机暴露在网络上的公司。Shadowserver 专家表示，他们专门在网络上扫描了具有互联网打印协议（IPP）功能的打印机，这些打印机在没有受到防火墙保护的情况下仍处于暴露状态，并允许攻击者通过“获取打印机属性”功能查询本地详细信息。专家们称平均每天约有 80000 台打印机通过 IPP 端口在网上曝光。这个数字大约是当前在线连接的所有支持 IPP 的打印机的八分之一。

关于国家互联网应急中心（CNCERT）

国家互联网应急中心是国家计算机网络应急技术处理协调中心的简称（英文简称为 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，是一个非政府非盈利的网络安全技术协调组织，主要任务是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展中国互联网上网络安全事件的预防、发现、预警和协调处置等工作，以维护中国公共互联网环境的安全、保障基础信息网络和网上重要信息系统的安全运行。目前，CNCERT 在我国大陆 31 个省、自治区、直辖市设有分中心。

同时，CNCERT 积极开展国际合作，是中国处理网络安全事件的对外窗口。CNCERT 是国际著名网络安全合作组织 FIRST 正式成员，也是 APCERT 的发起人之一，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，CNCERT 已与 78 个国家和地区的 260 个组织建立了“CNCERT 国际合作伙伴”关系。CNCERT 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：刘立伟

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315