国家互联网应急中心

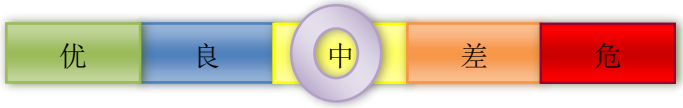
网络安全信息与动态周报

2020 年第 22 期

5 月 25 日-5 月 31 日

CNCERT/CC

本周网络安全基本态势

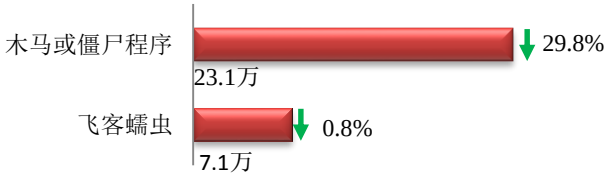


境内感染网络病毒的主机数量	•30.2万	↓ 24.7%
境内被篡改网站总数 其中政府网站数量	•8217 •24	↑ 6.7% ↓ 22.6%
境内被植入后门网站总数 其中政府网站数量	•1654 •6	↓ 8.0% =
针对境内网站的仿冒页面数量	•633	↑ 33.0%
新增信息安全漏洞数量 其中高危漏洞数量	•312 •92	↑ 8.0% ↓ 30.3%

= 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

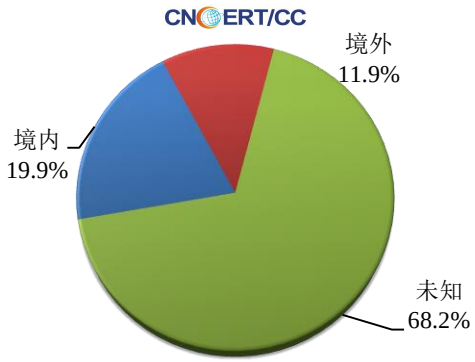
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 30.2 万个，其中包括境内被木马或被僵尸程序控制的主机约 23.1 万以及境内感染飞客（conficker）蠕虫的主机约 7.1 万。

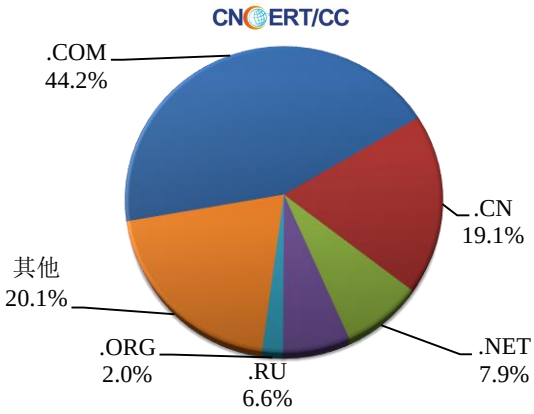


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域 782 个，涉及 IP 地址 3539 个。在 782 个域名中，有 11.9%为境外注册，且顶级域为.com 的约占 44.2%；在 3539 个 IP 中，有约 65.7%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 369 个 IP。

本周放马站点域名注册所属境内外分布
(5/25-5/31)



本周放马站点域名所属顶级域的分布
(5/25-5/31)



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。

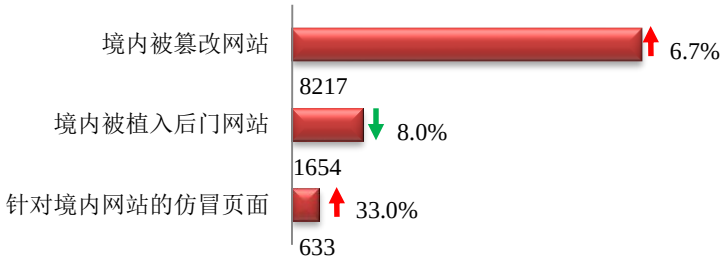
ANVA网络安全威胁信息共享平台

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。

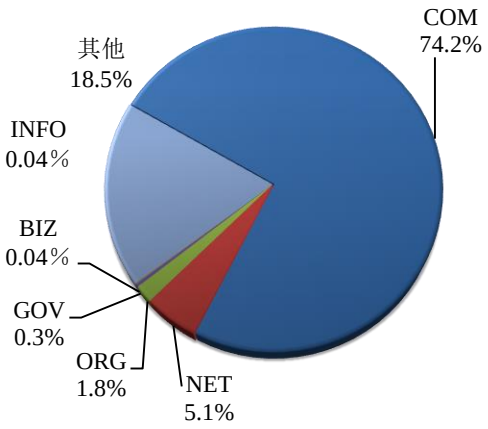
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 8217 个；被植入后门的网站数量为 1654 个；针对境内网站的仿冒页面数量 633 个。

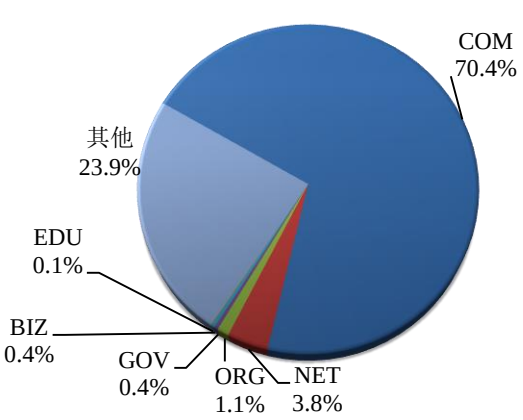


本周境内被篡改政府网站（GOV 类）数量为 24 个（约占境内 0.3%），较上周下降了 22.6%；境内被植入后门的政府网站（GOV 类）数量为 6 个（约占境内 0.3%），与上周持平。

本周我国境内篡改网站按类型分布
(5/25-5/31)

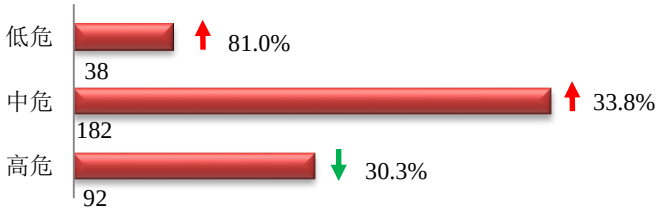


本周我国境内被植入后门网站按类型分类
(5/25-5/31)

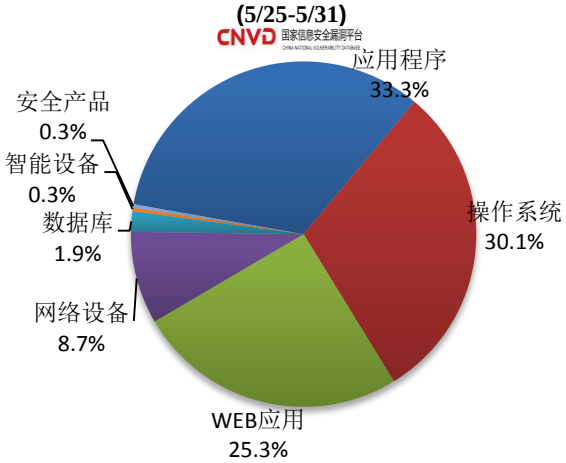


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 312 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
(5/25-5/31)



本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是操作系统和 WEB 应用。

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

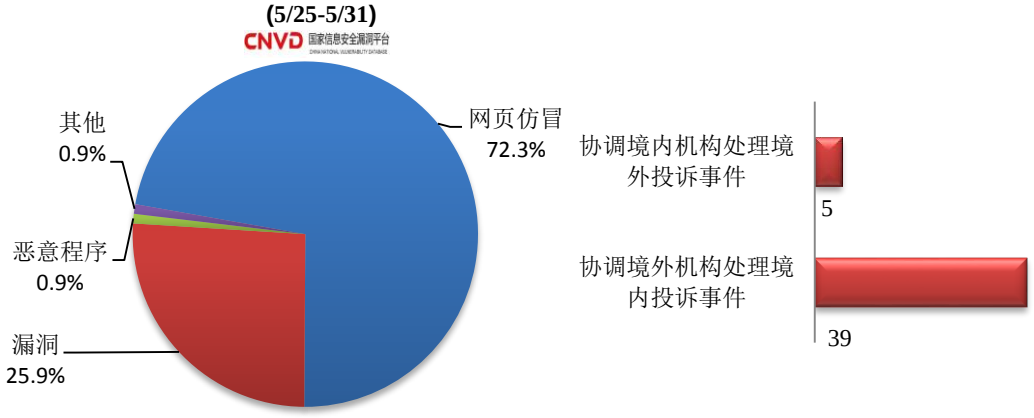
http://www.cnvd.org.cn/webinfo/list?type=4

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

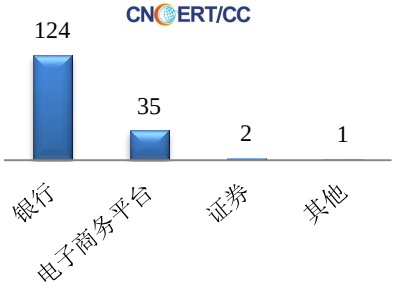
本周，CNCERT 协调基础电信企业、云服务商、域名注册服务机构、应用商店、各省分中心以及国际合作组织共处理了网络安全事件 224 起，其中跨境网络安全事件 44 起。

本周CNCERT处理的事件数量按类型分布
(5/25-5/31)

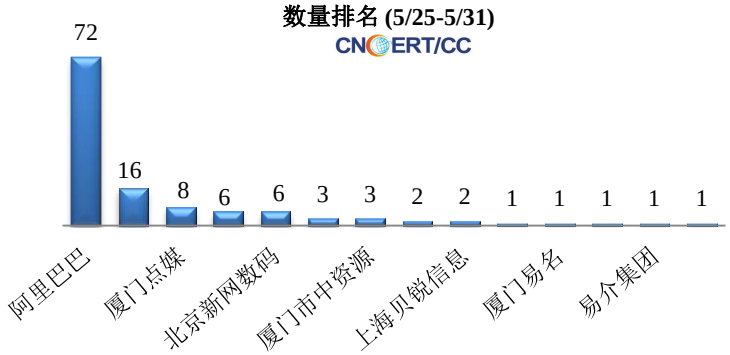


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 162 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，包括银行仿冒事件 124 起、电子商务平台 35 起、证券 2 起和其他事件 1 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计
(5/25-5/31)



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 (5/25-5/31)



本周，CNCERT 协调 3 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 47 个。

业界新闻速递

1、 APP 违法违规收集使用个人信息专项治理报告（2019）发布

5 月 25 日，APP 专项治理工作组发布《App 违法违规收集使用个人信息专项治理报告（2019）》。2019 年 1 月，中央网信办、工业和信息化部、公安部、市场监管总局四部门联合发布《关于开展 APP 违法违规收集使用个人信息专项治理的公告》，在全国范围组织开展 APP 违法违规收集使用个人信息专项治理，并成立 APP 违法违规收集使用个人信息专项治理工作组。一年来，专项治理工作成效显著，《APP 违法违规收集使用个人信息行为认定方法》《个人信息安全规范》等标准规范相继出台完善，用户规模大、与生活关系密切、问题反映集中的千余款 APP 经深度评估后进行了有效整改，无隐私政策、强制索权、无注销渠道等问题明显改善，APP 运营者履行个人信息保护责任义务的能力和水平明显提升，全社会关注和重视个人信息安全的氛围基本形成。

《APP 违法违规收集使用个人信息专 项治理报告（2019）》介绍了治理工作开展情况，包括技术规范制定、举报信息受理、专业机构检测评估、问题督促整改及处置，以及四部门全面推进深化治理等；报告引用多方数据，客观分析了个人信息保护相关突出问题、企业能力、民众意识、社会影响等方面的发展变化趋势，展示了治理工作成效。最后，在总结 2019 年治理工作经验的基础上，就持续开展治理工作，培育良好移动互联网生态，提出了具体建议。

2、 泰国移动运营商泄露 83 亿互联网记录

5 月 25 日，据外媒报道，研究人员发现泰国移动运营商 AIS 子公司控制的一个

ElasticSearch 数据库可公开访问，数据库包含大约 83 亿记录，容量约为 4.7 TB，每 24 小时增加 2 亿记录。该数据库无需密码即可访问，包括 DNS 查询和 Netflow 数据。AIS 是泰国最大的 GSM 移动运营商，用户约有 4000 万。此次可公开访问的数据库由其子公司 Advanced Wireless Network (AWN)控制。随后，安全研究人员将这个 bug 报告给了 AIS 和泰国国家计算机紧急应急小组 ThaiCERT，之后 AIS 关闭数据库，停止其他用户任意访问。

3、 英国廉价航空公司 easyJet 数据泄露 将面临 180 亿英镑巨额诉讼

5 月 26 日，据外媒 ZDNet 报道，由于受到最近披露的数据泄露事件影响，英国廉价航空公司 easyJet 将面临代表客户的 180 亿英镑集体诉讼。 该诉讼旨在确保每个受影响的客户获得最高 2000 英镑的赔偿。 据悉，此前 easyJet 于 5 月 19 日公开表示，属于 900 万客户的信息可能已经受到网络攻击遭泄露，其中还包括超过 2200 条信用卡记录。此次事件归咎于“高度复杂”的攻击形式，攻击者设法访问系统的财务信息以及电子邮件地址和旅行详细信息。目前，EasyJet 仍在联系受影响的用户。

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：楼书逸

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315