国家互联网应急中心

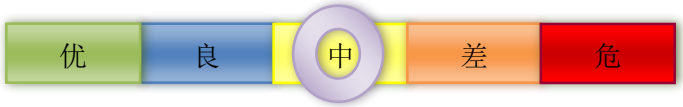
2020 年第 34 期

8 月 17 日-8 月 23 日

网络安全信息与动态周报

CNCERT/CC

本周网络安全基本态势

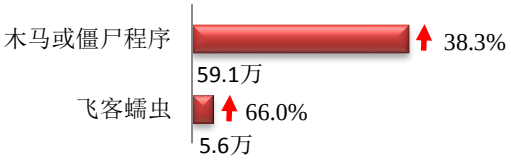


境内感染网络病毒的主机数量	•64.7万	↑ 40.3%
境内被篡改网站总数 其中政府网站数量	•3548 •15	↓ 10.6% ↓ 16.7%
境内被植入后门网站总数 其中政府网站数量	•1366 •3	↓ 6.5% ↓ 50.0%
针对境内网站的仿冒页面数量	•15693	↓ 11.9%
新增信息安全漏洞数量 其中高危漏洞数量	•381 •135	↑ 26.6% ↑ 8.9%

= 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

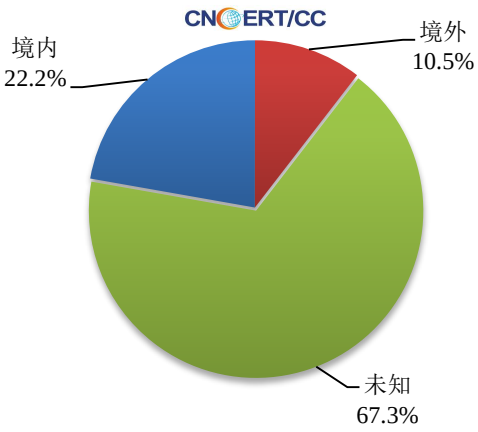
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 64.7 万个，其中包括境内被木马或被僵尸程序控制的主机约 59.1 万以及境内感染飞客（conficker）蠕虫的主机约 5.6 万。

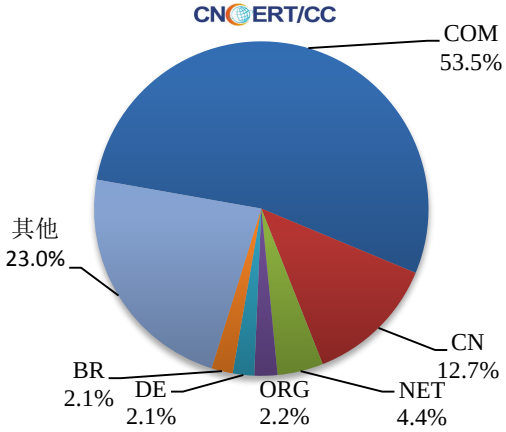


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 2325 个，涉及 IP 地址 6324 个。在 2325 个域名中，有 10.5%为境外注册，且顶级域为.com 的约占 53.5%；在 6324 个 IP 中，有约 66.7%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 285 个 IP。

本周放马站点域名注册所属境内外分布
(8/17-8/23)



本周放马站点域名注册所属顶级域分布
(8/17-8/23)



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。

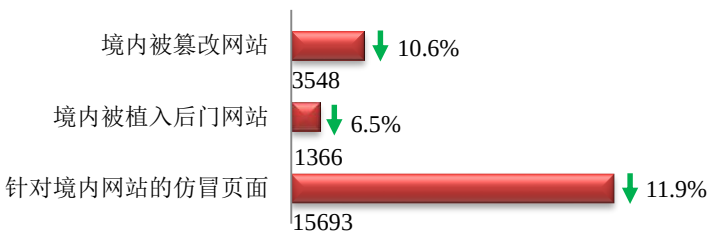
ANVA网络安全威胁信息共享平台

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

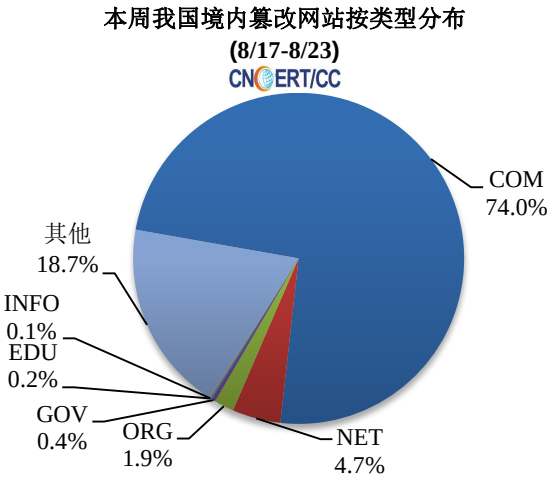
中国反网络病毒联盟（Anti Network-Virus Alliance of China，缩写 ANVA）是由 CNCERT 发起并组织运作的行业联盟。

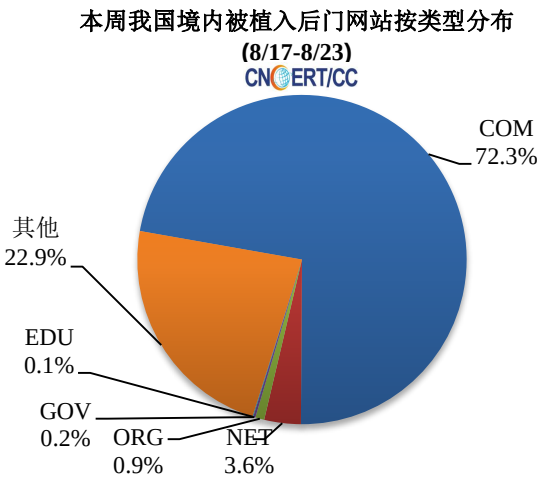
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 3548 个；被植入后门的网站数量为 1366 个；针对境内网站的仿冒页面数量 15693 个。



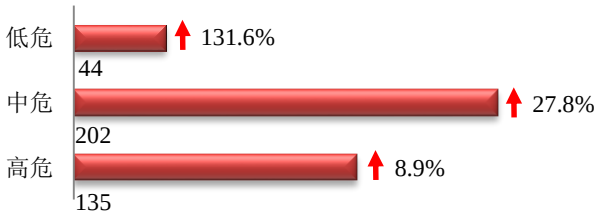
本周境内被篡改政府网站（GOV 类）数量为 15 个（约占境内 0.4%），较上周下降了 16.7%；境内被植入后门的政府网站（GOV 类）数量为 3 个（约占境内 0.2%），较上周下降了 50.0%。

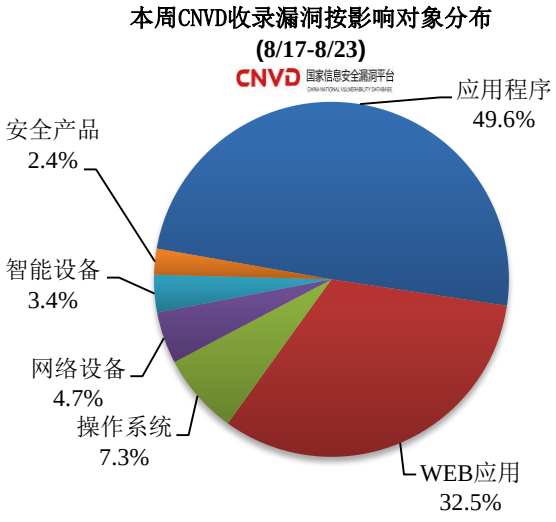




本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 381 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。

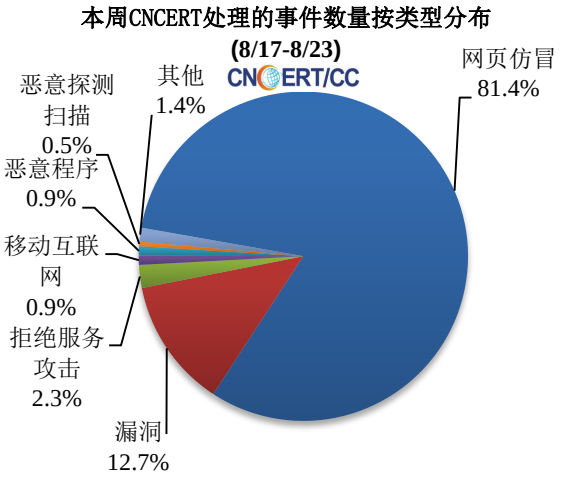
CNVD漏洞周报发布地址

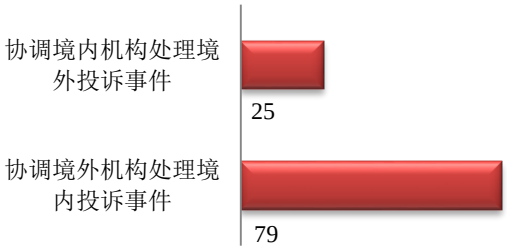
http://www.cnvd.org.cn/webinfo/list?type=4

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。

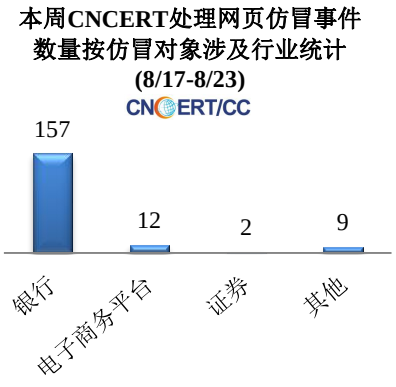
本周事件处理情况

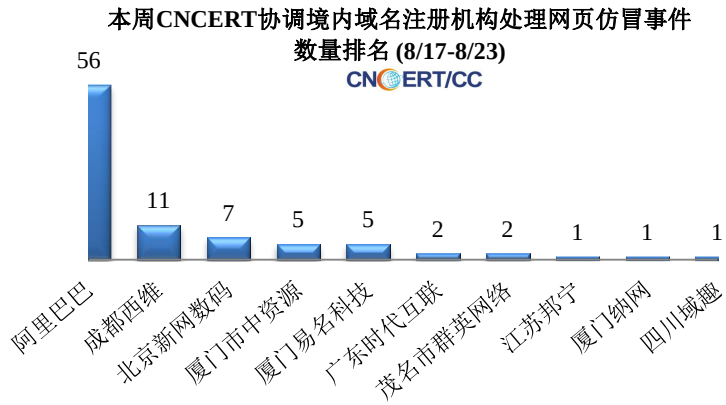
本周，CNCERT 协调基础电信企业、云服务商、域名注册服务机构、应用商店、各省分中心以及国际合作组织共处理了网络安全事件 221 起，其中跨境网络安全事件 104 起。



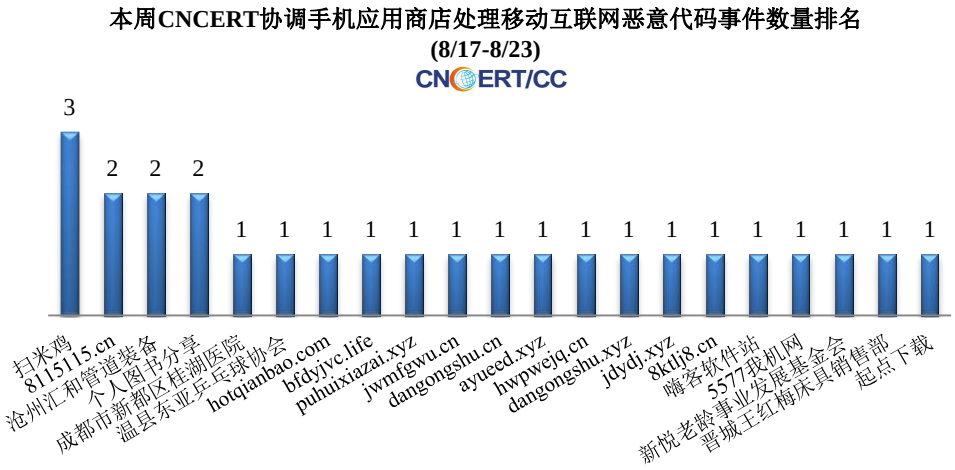


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 180 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，包括银行仿冒事件 157 起、电子商务平台 12 起、证券 2 起和其他事件 9 起。





本周，CNCERT 协调 21 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 26 个。



业界新闻速递

1、 工信部通报下架 8 款侵害用户权益 APP

8 月 19 日，工信部网站发布关于下架侵害用户权益 App 名单的通报.通报显示，7 月 24 日，工信部通报了 58 家存在侵害用户权益行为 APP 企业的名单。截至目前，尚有 8 款 APP 未按要求限时完成整改，依相关法规，工信部组织对上述 APP 进行下架处理。工信部表示，相关应用商店应在本通报发布后，立即组织对名单中应用软件进行下架处理。

2、 全球最大邮轮运营商嘉年华公司遭遇勒索软件攻击

8 月 17 日，据“ZDNet”网站消息，当日，全球最大的游轮运营商嘉年华公司披露了一个系统安全漏洞，并承认 8 月 15 日遭遇勒索软件攻击。攻击者“访问并加密了公司某品牌部分信息技术系统”，并下载了相关文件。目前，该公司已就此事通知了执法部门，并与法律顾问和事故应对专业人员进行了接触。尽管可能面对潜在的诉讼，但预计事件不会对公司“业务、运营或财务业绩”产生实质性影响。嘉年华并未透露事件具体细节，比如加密其网络的勒索软件名称，或者受影响的内部网络或品牌。

3、 FritzFrog 僵尸网络正通过 SSH 感染 Linux 服务

8 月 20 日，据 Freebuf 网站消息，研究人员发现了一个名为 FritzFrog 的先进的 P2P 僵尸网络，该僵尸网络自 2020 年 1 月以来一直积极地瞄准全球的 SSH 服务器，其中，北美、中国、韩国是重灾区。据悉，该僵尸网络用 Golang 语言编写，具有可蠕虫功能，主

要瞄准政府、教育和金融部门的实体。作为一种模块化、多线程、无文件的 SSH Internet 蠕虫，FritzFrog 通过破坏公共 IP 地址来发展 P2P 僵尸网络。此外，为了避免被检测，FritzFro 的进程是以 ifconfig 和 nginx 名称运行，然后侦听端口 1234 以等待命令。攻击者通过 SSH 连接到受感染的计算机，然后在计算机上运行一个 netcat 客户端，再将其连接到恶意软件的服务器。最后，通过 SSH 发送的 ant 命令将用作 netcat 的输入，并重定向到恶意软件。根据专家的说法，该僵尸网络自 1 月 9 日以来一直处于活跃状态，已累计使用 20 种不同版本的恶意软件二进制文件进行了 13000 次攻击。

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：李志辉

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315