国家互联网应急中心

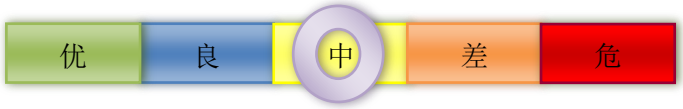
网络安全信息与动态周报

2020 年第 35 期

8 月 24 日-8 月 30 日

CNCERT/CC

本周网络安全基本态势

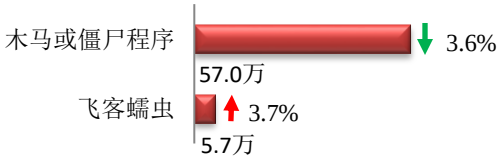


境内感染网络病毒的主机数量	•62.7万	3.0%
境内被篡改网站总数 其中政府网站数量	•2710 •6	23.6% 60.0%
境内被植入后门网站总数 其中政府网站数量	•1173 •4	14.1% 33.3%
针对境内网站的仿冒页面数量	•9678	38.3%
新增信息安全漏洞数量 其中高危漏洞数量	•673 •289	76.6% 114.1%

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*

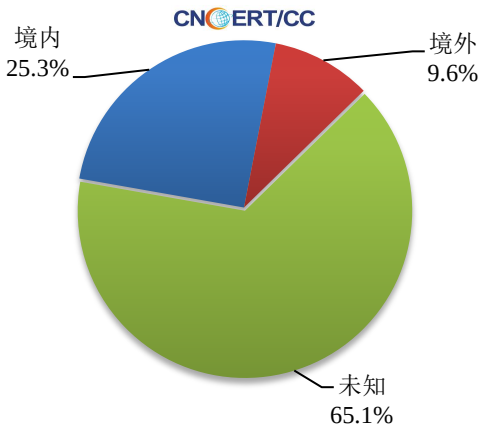
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 62.7 万个，其中包括境内被木马或被僵尸程序控制的主机约 57.0 万以及境内感染飞客（conficker）蠕虫的主机约 5.7 万。

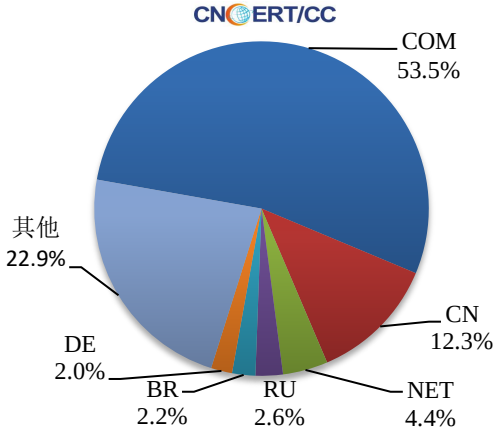


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 1515 个，涉及 IP 地址 4563 个。在 1515 个域名中，有 9.6%为境外注册，且顶级域为.com 的约占 53.5%；在 4563 个 IP 中，有约 61.4%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 231 个 IP。

本周放马站点域名注册所属境内外分布
(8/24-8/30)



本周放马站点域名注册所属顶级域分布
(8/24-8/30)



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。

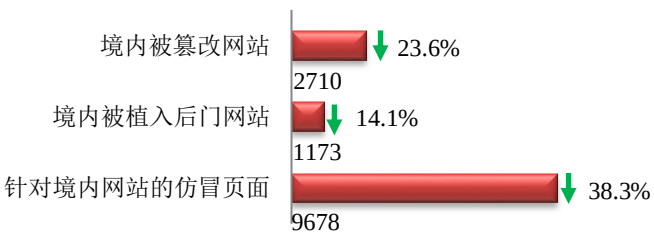
ANVA网络安全威胁信息共享平台

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。

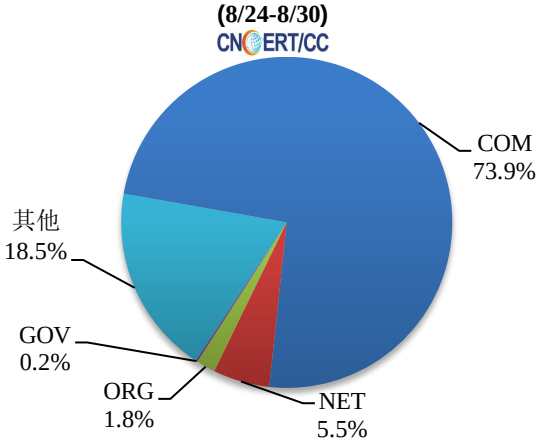
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 2710 个；被植入后门的网站数量为 1173 个；针对境内网站的仿冒页面数量 9678 个。

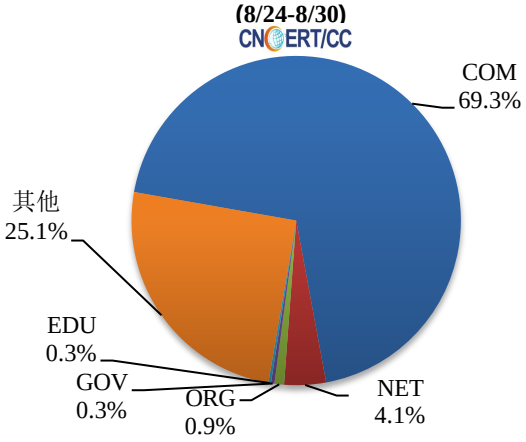


本周境内被篡改政府网站（GOV 类）数量为 6 个（约占境内 0.2%），较上周下降了 60.0%；境内被植入后门的政府网站（GOV 类）数量为 4 个（约占境内 0.3%），较上周上涨了 33.3%。

本周我国境内篡改网站按类型分布
(8/24-8/30)

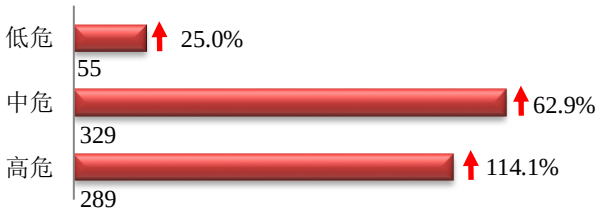


本周我国境内被植入后门网站按类型分布
(8/24-8/30)

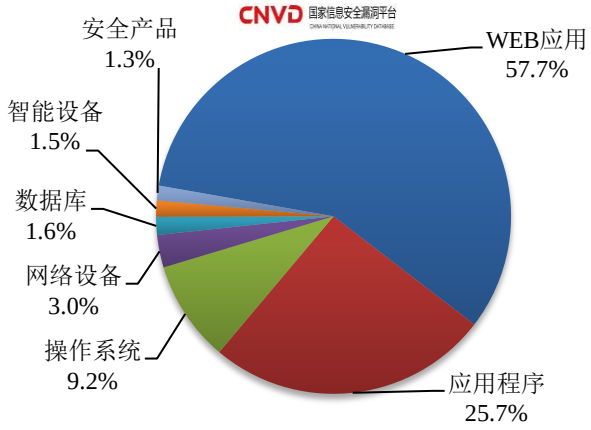


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 673 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
(8/24-8/30)



本周 CNVD 发布的网络安全漏洞中，WEB 应用漏洞占比最高，其次是应用程序和操作系统。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

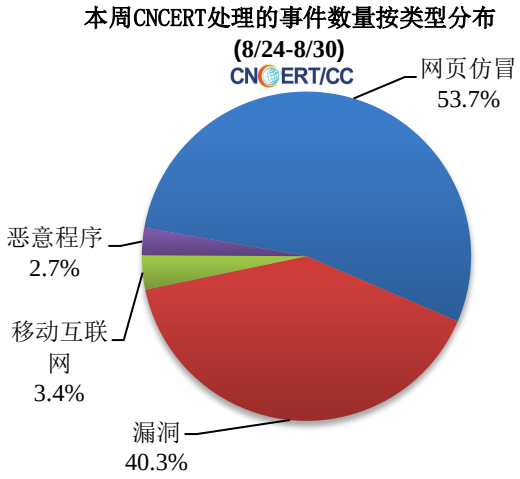
CNVD漏洞周报发布地址

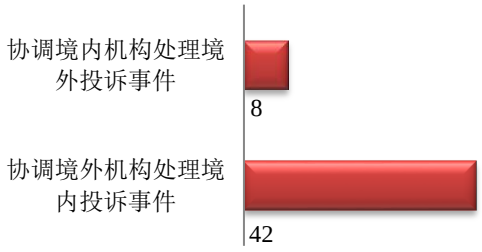
http://www.cnvd.org.cn/webinfo/list?type=4

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。

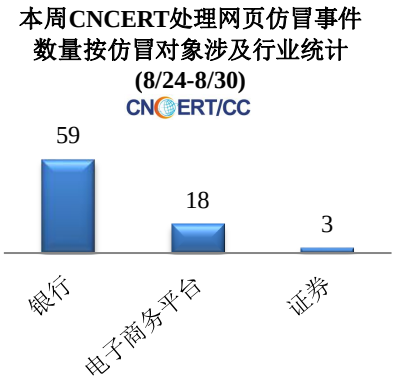
本周事件处理情况

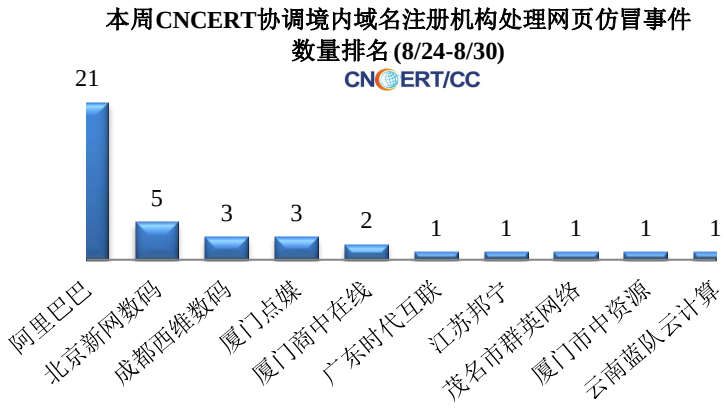
本周，CNCERT 协调基础电信企业、云服务商、域名注册服务机构、应用商店、各省分中心以及国际合作组织共处理了网络安全事件 149 起，其中跨境网络安全事件 50 起。



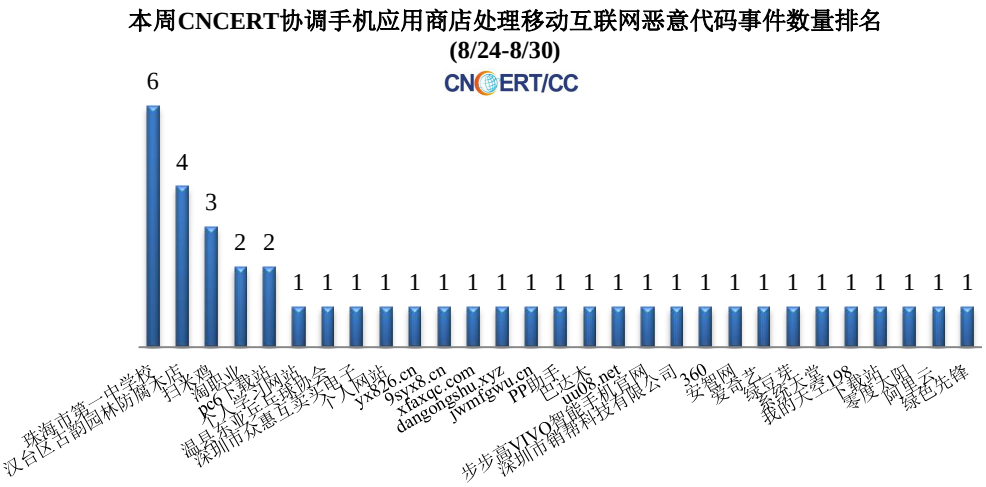


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 80 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，包括银行仿冒事件 59 起、电子商务平台 18 起和证券事件 3 起。





本周，CNCERT 协调 29 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 41 个。



业界新闻速递

1、 警惕 Gafgyt 僵尸网络攻击国内 Linux 服务器及 IOT 设备

8 月 26 日，据腾讯安全威胁情报中心公众号消息，检测到有境外 IP 针对国内 Linux 服务器的远程命令注入攻击。黑客通过批量扫描 80、5555、60001 端口来发现易受攻击的 Linux 服务器、android 设备以及监控摄像头设备并利用 ZeroShell 远程代码执行漏洞（CVE-2019-12725）、bash shell 漏洞、JAWS Webserver 未授权 shell 命令执行漏洞进行攻击，攻击成功后下载 Gafgyt 家族木马。Gafgyt 是一种流行的僵尸网络程序，被认为是 Mirai 的前身，其源代码在 2015 年初被部分泄露。Gafgyt 主要通过 telent 弱口令以及命令注入漏洞等方式进行攻击传播，通过感染基于 Linux 的 IoT 设备（包括基于 Linux 系统的路由器、智能摄像头等设备）来发起 DDoS 攻击，攻击类型以 UDP、TCP 和 HTTP 攻击为主。

2、 新西兰证券交易所遭遇 DDoS 攻击被迫中断交易

8 月 27 日消息，据 CNBC 报道，当地时间 8 月 27 日上午，新西兰证券交易所（NZX）再次发生崩溃，交易所股价和指数报价无法获取，这已经是该交易所连续第三天发生崩溃。交易所在公告中表示，由于系统连接问题，新西兰证交所确认在上午 11:10 开始暂停部分市场交易。新西兰证券交易所 8 月 25 日和 26 日多次遭受分布式拒绝服务（DDoS）攻击，被迫短时中断交易。其网站和市场公告平台也受到影响。DDoS 攻击是最简单的网络攻击形式之一，它在短时间内发起大量请求，耗尽服务器的资源，无法响应正常的访

问，造成网站实质下线。新西兰证交所表示，目前正与网络服务商合作，调查问题的根源。

3、 黑客组织利用 Autodesk 3Ds Max 恶意软件攻击全球企业

8 月 26 日，据外媒报道，安全公司 Bitdefender 发现一个新型黑客组织正在利用隐藏在恶意 3Ds Max 插件中的恶意软件攻击全球企业。3Ds Max 是一款由 Autodesk 开发的 3D 计算机图形应用程序，通常用于工程、建筑、游戏或软件公司。这个恶意插件名为“PhysXPluginMfx”，实则上是 MAXScript 攻击的一个变种。Bitdefender 公司发布报告称，该插件的目的实际上是部署后门，以便查找受感染计算机中的敏感文件并窃取重要文档。该公司还指出调查并确认该黑客组织至少攻击了一个国际建筑和视频制作公司。目前，Autodesk 已经发出了一份与这次入侵有关的通知，建议 3ds Max 的用户尽快安装最新版的 Autodesk 3ds Max 2021-2015SP1 安全工具来找出并且删除 PhysXPluginMfx 插件。

4、 在不安全的服务器上暴露了 3.5 亿个解密的电子邮件地址

8 月 27 日，据外媒报道，CyberNews 研究小组发现了一个不安全的数据库，该存储桶由一个身份不明的方拥有，其中包含价值 7 千兆字节的未加密文件，其中包括 350,000,000 串唯一的电子邮件地址。大量电子邮件被留在一个可公开访问的 Amazon AWS 服务器上，允许任何人下载和访问数据。2020 年平均每天有 700 万条记录被曝光。该存储桶位于美国，托管在 Amazon S3 服务器上，已经暴露了至少 18 个月。任何人都可以下载并访问 CSV 文件，无需任何类型的许可。目前，亚马逊已关闭了相关的服务器。

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：朱天

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315