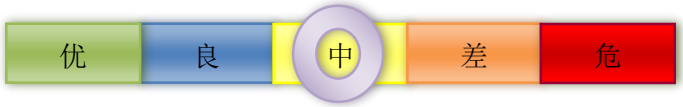
国家互联网应急中心

2020 年第 39 期
9 月 21 日-9 月 27 日

网络安全信息与动态周报

本周网络安全基本态势

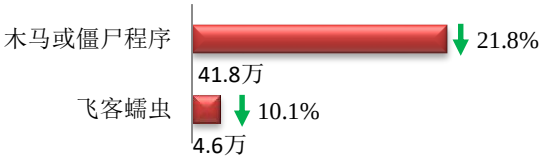


境内感染网络病毒的主机数量	•46.4万	20.7%
境内被篡改网站总数 其中政府网站数量	•3467 •15	3.4% 28.6%
境内被植入后门网站总数 其中政府网站数量	•775 •5	34.4% 37.5%
针对境内网站的仿冒页面数量	•6770	47.9%
新增信息安全漏洞数量 其中高危漏洞数量	•369 •68	6.6% 27.7%

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*

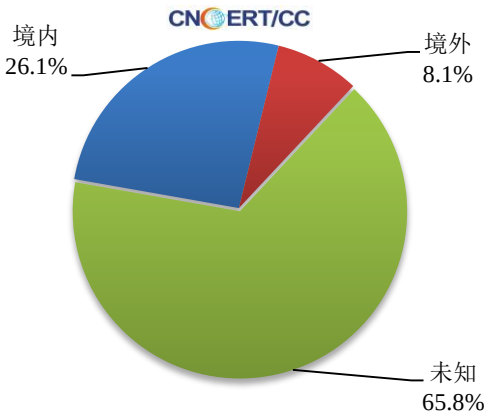
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 46.4 万个，其中包括境内被木马或被僵尸程序控制的主机约 41.8 万以及境内感染飞客（conficker）蠕虫的主机约 4.6 万。

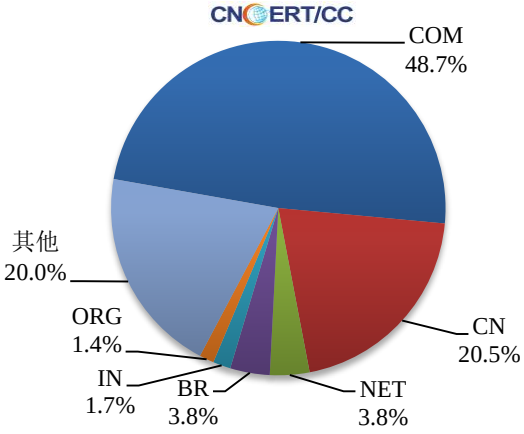


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 994 个，涉及 IP 地址 2447 个。在 994 个域名中，有 8.1%为境外注册，且顶级域为.com 的约占 48.7%；在 2447 个 IP 中，有约 59.2%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 62 个 IP。

本周放马站点域名注册所属境内外分布
(9/21-9/27)



本周放马站点域名注册所属顶级域分布
(9/21-9/27)



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。

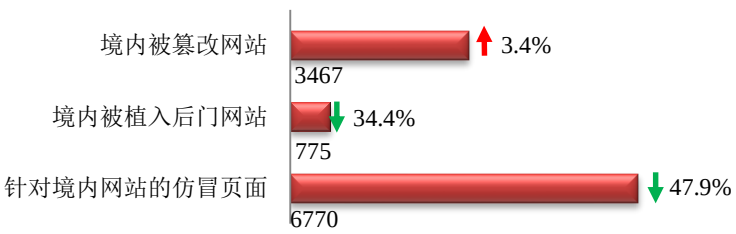
ANVA网络安全威胁信息共享平台

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。

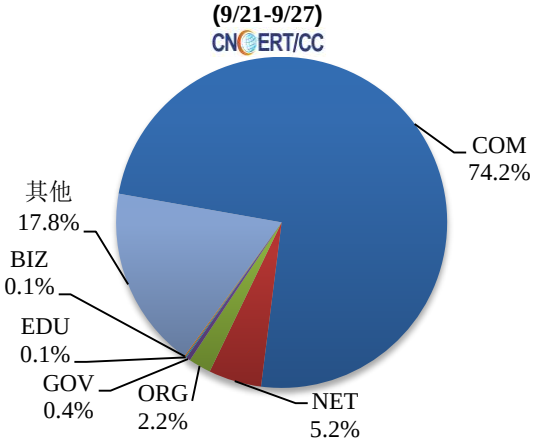
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 3467 个；被植入后门的网站数量为 775 个；针对境内网站的仿冒页面数量 6770 个的仿冒页面。

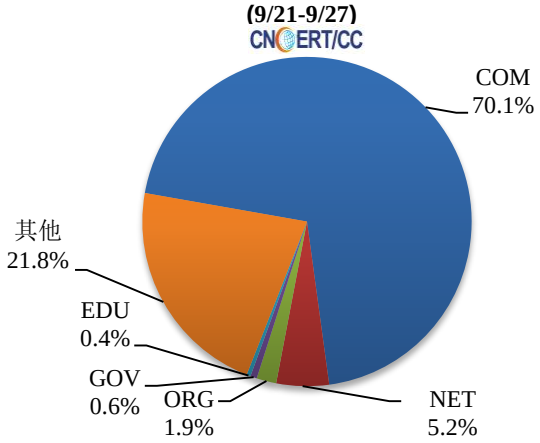


本周境内被篡改政府网站（GOV 类）数量为 15 个（约占境内 0.4%），较上周下降了 28.6%；境内被植入后门的政府网站（GOV 类）数量为 5 个（约占境内 0.6%），较上周下降了 37.5%。

本周我国境内篡改网站按类型分布
(9/21-9/27)

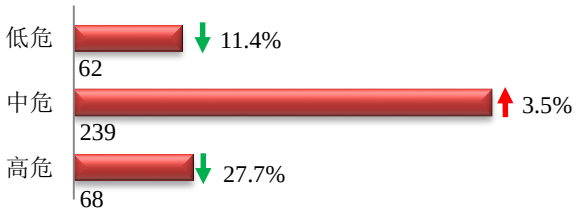


本周我国境内被植入后门网站按类型分布
(9/21-9/27)

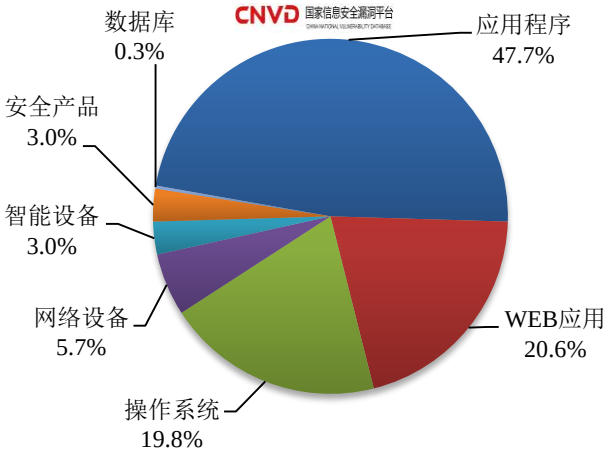


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 369 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
(9/21-9/27)



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。

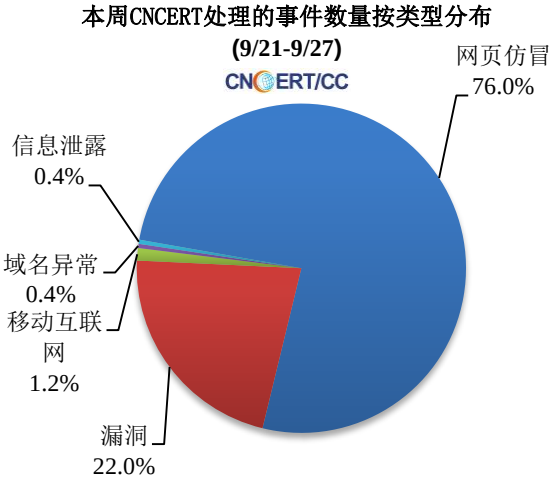
CNVD漏洞周报发布地址

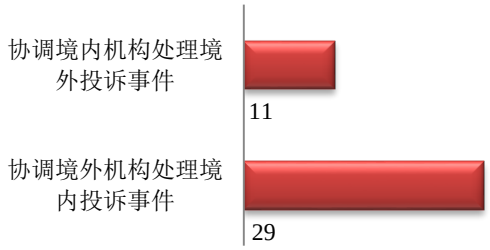
http://www.cnvd.org.cn/webinfo/list?type=4

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。

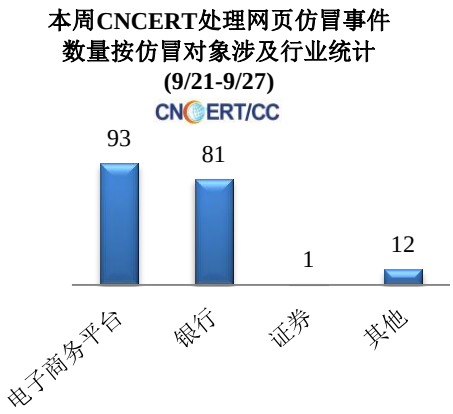
本周事件处理情况

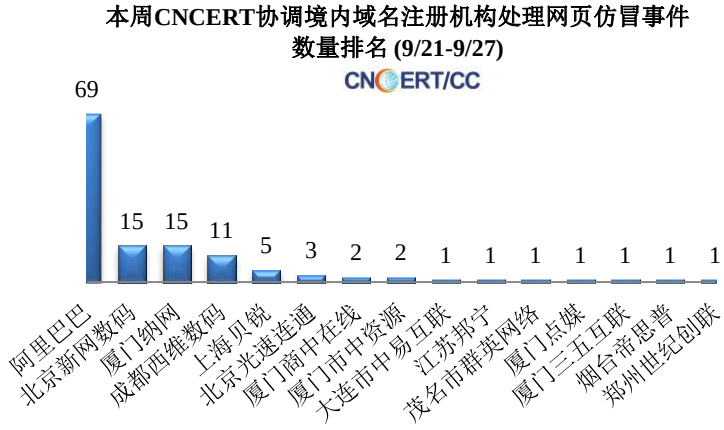
本周，CNCERT 协调基础电信企业、云服务商、域名注册服务机构、应用商店、各省分中心以及国际合作组织共处理了网络安全事件 246 起，其中跨境网络安全事件 40 起。



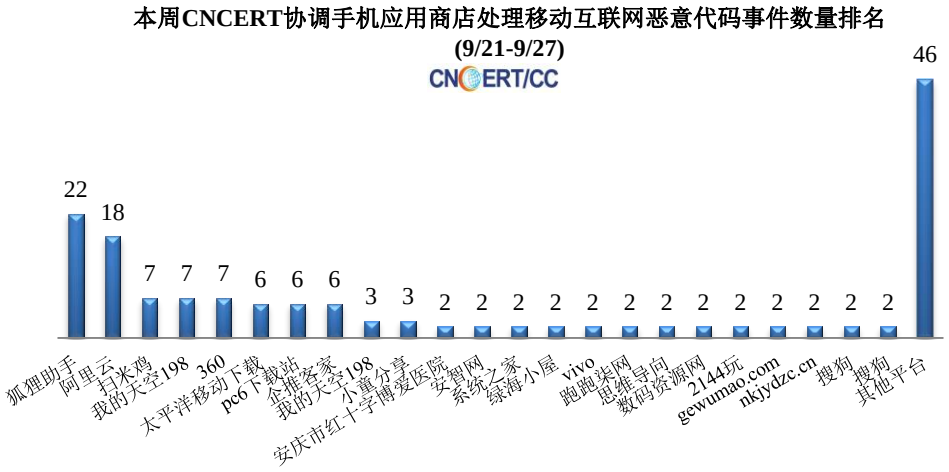


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 187 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，包括电子商务平台 93 起、银行仿冒事件 81 起、证券 1 起和其他事件 12 起。





本周，CNCERT 协调 69 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 157 个。



业界新闻速递

1、 CNCERT 发布《2020 年上半年我国互联网网络安全监测数据分析报告》

为全面反映 2020 年上半年我国互联网网络安全状况，CNCERT 对上半年监测数据进行了梳理，9 月 27 日发布了《2020 年上半年我国互联网网络安全监测数据分析报告》。报告从恶意程序、安全漏洞、拒绝服务攻击、网站安全、云平台安全、工业控制系统安全六个方面对我国 2020 年上半年网络安全监测数据情况，对攻击来源、攻击对象、攻击规模等进行了详细梳理，以及时反映我国网络安全整体情况。

2、 微软 Bing 应用数据库遭泄露 多达 1 亿条搜索记录被截取

9 月 27 日，据外媒报道，WizCase 专家在互联网上搜索敞开的数据库或服务器时发现了一个不受保护的 Elasticsearch 服务器，其中包含了与微软旗下 Bing 移动应用程序用户相关的 TB 级数据。该数据库中的身份验证被移除，其内容暴露给互联网上的所有人。暴露的 6.5 TB 服务器每天接收多达 200G 的数据。WizCase 指出，Bing 移动应用软件仅在谷歌 Play 上就有超过 1000 万的下载量，每天记录数百万次搜索。微软称目前已解决了配置不当问题。

3、 黑客从 KuCoin 交易所窃取超过 1.5 亿美元的加密货币

9 月 27 日，据外媒报道，新加坡加密货币交易所 KuCoin 今天披露了一次大规模黑客攻击。该公司在其网站上发布的一份声明中证实，一名黑客侵入了其系统，并清空了其

热钱包中的所有资金。KuCoin 加密货币交易使用热钱包作为他们的临时存储系统，来存储目前在平台上交换的资产，它们被用来推动转换操作和资金转移。KuCoin 表示，黑客成功盗取了比特币资产、erc -20 代币以及其他类型的代币。根据用户追踪被盗资金的 Etherium 地址，目前估计损失最小为 1.5 亿美元。

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：温森浩

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315