国家互联网应急中心

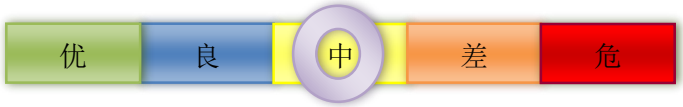
网络安全信息与动态周报

2020 年第 30 期

7 月 20 日-7 月 26 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	•45.5万	↓ 5.7%
境内被篡改网站总数 其中政府网站数量	•4964 •18	↓ 7.8% ↓ 5.3%
境内被植入后门网站总数 其中政府网站数量	•1229 •3	↓ 10.1% =
针对境内网站的仿冒页面数量	•1198	↑ 51.3%
新增信息安全漏洞数量 其中高危漏洞数量	•481 •147	↑ 43.2% ↑ 10.5%

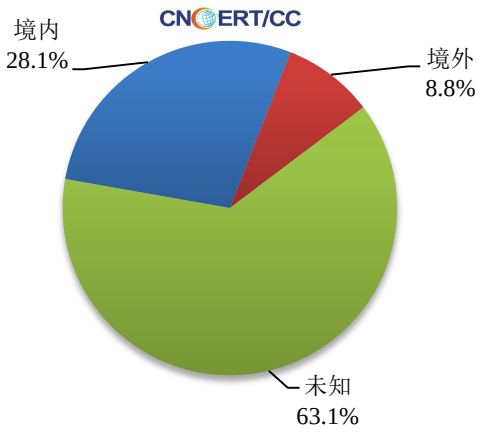
= 表示数量与上周相同　↑ 表示数量较上周环比增加　↓ 表示数量较上周环比减少

本周网络病毒活动情况

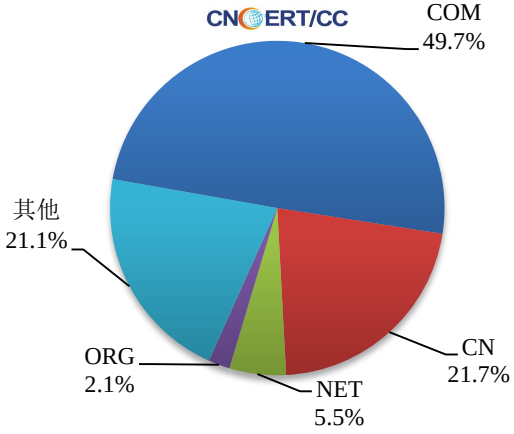
本周境内被木马或僵尸程序控制的主机约 45.5 万个。

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 1922 个，涉及 IP 地址 4732 个。在 1922 个域名中，有 8.8%为境外注册，且顶级域为.com 的约占 49.7%；在 4732 个 IP 中，有约 67.5%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 411 个 IP。

本周放马站点域名注册所属境内外分布 (7/20-7/26)



本周放马站点域名注册所属顶级域分布 (7/20-7/26)



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。

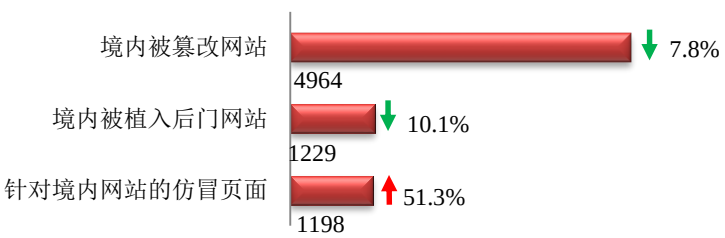
ANVA网络安全威胁信息共享平台

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。

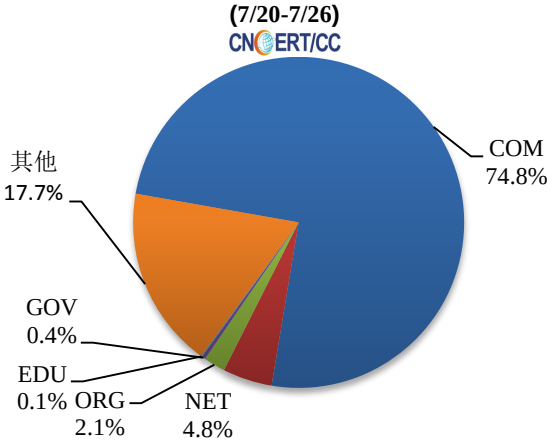
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 4964 个；被植入后门的网站数量为 1229 个；针对境内网站的仿冒页面数量 1198 个。

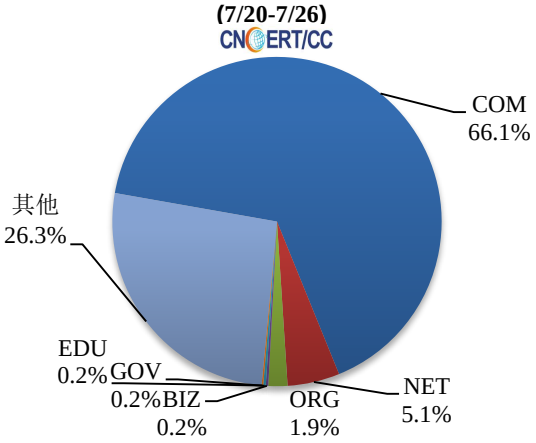


本周境内被篡改政府网站（GOV 类）数量为 18 个（约占境内 0.4%），较上周下降了 5.3%；境内被植入后门的政府网站（GOV 类）数量为 3 个（约占境内 0.2%）。

本周我国境内篡改网站按类型分布
(7/20-7/26)

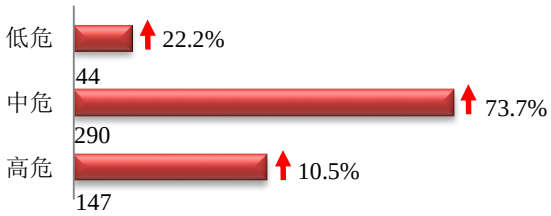


本周我国境内被植入后门网站按类型分布
(7/20-7/26)

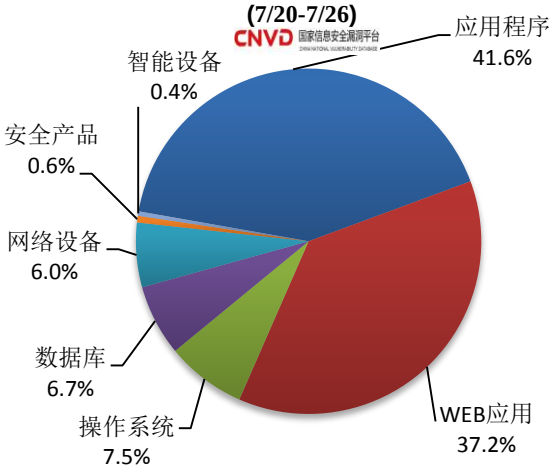


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 481 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
(7/20-7/26)



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

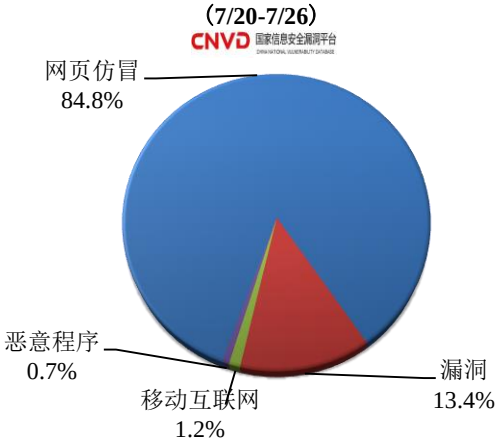
http://www.cnvd.org.cn/webinfo/list?type=4

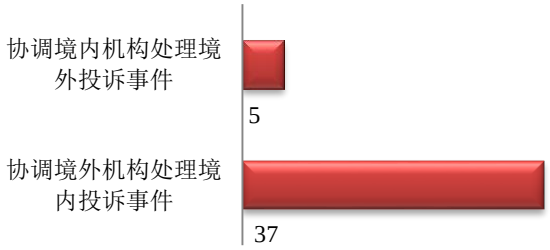
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信企业、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 434 起，其中跨境网络安全事件 42 起。

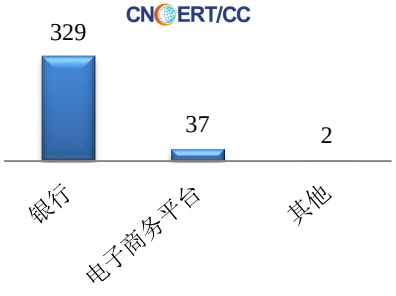
本周CNCERT处理的事件数量按类型分布
（7/20-7/26）



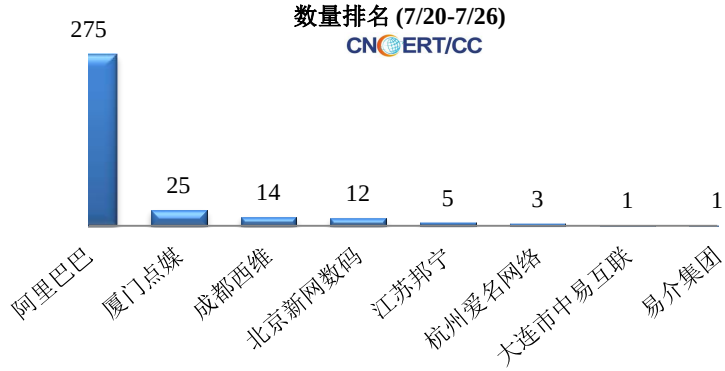


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 368 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，包括银行仿冒事件 329 起、电子商务平台 37 起和其他事件 2 起。

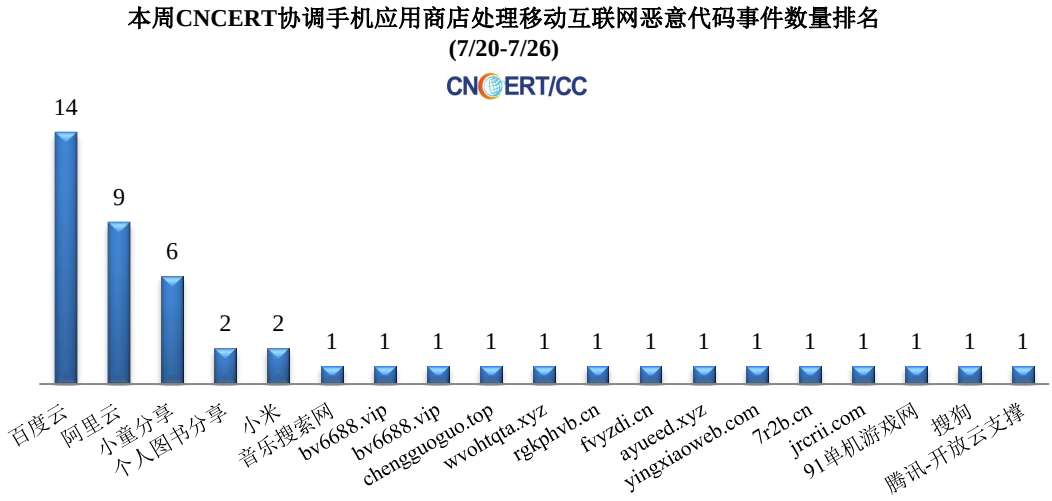
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (7/20-7/26)



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 (7/20-7/26)



本周，CNCERT 协调 19 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、 四部门联合启动 2020 年 App 违法违规收集使用个人信息治理工作

7 月 25 日，中国网信网消息，为进一步贯彻落实党中央部署，坚持网络安全为人民、网络安全靠人民、保障个人信息安全，维护公民在网络空间的合法权益，中央网信办、工业和信息化部、公安部、国家市场监管总局四部门 7 月 22 日在京召开会议，启动 2020 年 App 违法违规收集使用个人信息治理工作。会议总结了 2019 年中央网信办、工业和信息化部、公安部、国家市场监管总局联合开展 App 违法违规收集使用个人信息专项治理工作取得的积极进展。会议还指出，当前 App 数量已超 500 万款，违法违规收集使用个人信息问题还未根本解决，2020 年治理工作将在去年基础上，进一步加大整治工作力度，突出问题导向、强化标准规范支撑、加强责任追究，持续委托 App 治理工作组重点开展以下几方面工作：一是制定发布 SDK、手机操作系统个人信息安全评估要点，持续受理并处理公众对违法违规收集使用个人信息行为的线索举报和问题反映，对用户规模大、问题反映集中的 App、SDK、小程序等进行深度评估。二是针对面部特征等生物特征信息收集使用不规范，App 后台自启动、关联启动、私自调用权限上传个人信息，录音、拍照等敏感权限滥用等社会反映强烈的重点问题，开展专题研究和深度检测。三是对违法违规收集使用个人信息行为加大发现力度、曝光力度、处罚力度。根据情节、后果严重程度，依法依规予以约谈、警告、下架、罚款等处罚，对违法违规行为形成有效震慑。四是制定出台 App 收集使用个人信息行为应用商店审核管理指南，指导督促应用商店切实做好 App 上线前的安全审核，把严入口关。五是发布免费技术工具，指导中小企业开展个人信

息收集使用行为自评估，防范排查个人信息安全风险隐患，提升中小企业个人信息收集使用活动的合法合规性。六是推进 App 个人信息安全认证工作，有序开展认证证书和标识发放，建立持续动态的认证跟踪机制。七是加强个人信息安全评估培训，推动个人信息安全评估工作的规范化；加大力度开展个人信息保护宣传教育，扩大个人信息保护知识、技能传播的普及面。

2、 关于侵害用户权益行为的 APP 通报（2020 年第三批）

7 月 24 日，工信部官网消息，依据《网络安全法》《电信条例》《电信和互联网用户个人信息保护规定》等法律法规，工业和信息化部近期组织第三方检测机构对手机应用软件进行检查，督促存在问题的企业进行整改。截至目前，尚有 58 款 APP 未完成整改。上述 APP 应在 7 月 30 日前完成整改落实工作，逾期不整改的，工业和信息化部将依法依规组织开展相关处置工作。

此次检测中，部分移动应用分发平台管理主体责任缺位，未严格落实工业和信息化部《移动智能终端应用软件预置和分发管理暂行规定》（工信部信管〔2016〕407 号）要求，对上架 APP 审核把关不严，7 月 22 日，已对相关企业进行了集中约谈，后续对问题突出、有令不行、整改不彻底的企业依法严厉处置。

3、 信安标委发布《网络安全标准实践指南—移动互联网应用程序（App）收集使用个人信息自评估指南》

7 月 25 日，信安标委网站消息，为落实《网络安全法》相关要求，围绕中央网信办、工信部、公安部、市场监管总局联合制定的《App 违法违规收集使用个人信息行为认定方法》，基于 App 专项治理工作组发布的《App 违法违规收集使用个人信息自评估指南》，信安标委秘书处组织编制了《网络安全标准实践指南—移动互联网应用程序（App）收集使用个人信息自评估指南》该《实践指南》归纳总结了 App 收集使用个人信息的六项评估点，供 App 运营者自评估参考使用，小程序、快应用等运营者也可参考其中的适用条款进行自评估。

4、 7 个 VPN 服务导致 1.2TB 用户数据泄露

7 月 21 日，据外媒报道，vpnMentor 专家报告称，最近 7 个虚拟专用网（VPN）将 1.2TB 的私人用户数据暴露在网上。这 7 个应用程序使服务器不受安全保护，从而暴露了私人用户的数据，供任何人查看。这些服务器包含超过 2000 万虚拟专用网络用户的个人识别

信息（PII）数据，包括用户的电子邮件和家庭地址、明文密码和 IP 地址，以及用户的互联网活动日志。

5、 阿根廷电信公司被黑并遭勒索 750 万美元

7 月 23 日，CertiK 公众号消息，阿根廷电信公司“Telecom SA”遭勒索软件攻击。勒索软件针对性地攻击了工作人员计算机上的 OneDrive 和 Office365 等 Windows 硬件，用户的座机、手机及互联网服务并未受到影响。据消息，在确认勒索软件对公司进行攻击之前，部分员工发现公司的 VPN 无法访问，且其用于访问 Personal，Arnet，Telecom 和 Fibertel 数据库的 Siebel 系统运行失常。根据这一情况，有猜测认为当时的黑客攻击可能已经通过电子邮件作为附件传输给了某位员工。Telecom 技术团队立即建议运营商与服务器断开连接，不要打开任何此类文件或电子邮件。据黑客称，目前所有被攻击的文件都已被攻击者用代码锁定，Telecom 公司必须用门罗币支付高达 750 万美元的赎金，而如果在 48 小时之内黑客未收到赎金，则赎金将增加一倍达到 1500 万美元。

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：李明

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315