国家互联网应急中心

网络安全信息与动态周报

2021 年第 9 期

2 月 22 日-2 月 28 日

CNCERT/CC

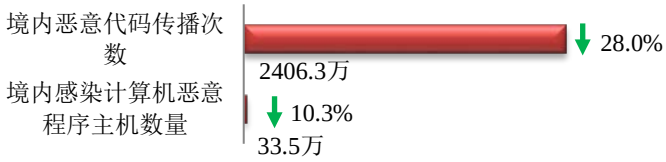
本周网络安全基本态势

境内计算机恶意程序传播次数 境内感染计算机恶意程序主机数量	•2406.3万 •33.5万	↓ 28.0% ↓ 10.3%
境内被篡改网站总数 其中政府网站数量	•4357 •22	↑ 26.3% ↑ 46.7%
境内被植入后门网站总数 其中政府网站数量	•518 •2	↓ 58.7% ↑ 200%
针对境内网站的仿冒页面数量	•226	↑ 189.7%
新增信息安全漏洞数量 其中高危漏洞数量	•502 •205	↑ 202.4% ↑ 206.0%

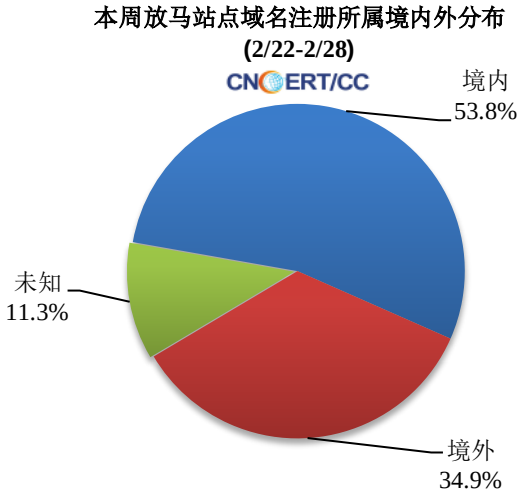
表示数量与上周相同　表示数量较上周环比增加　表示数量较上周环比减少

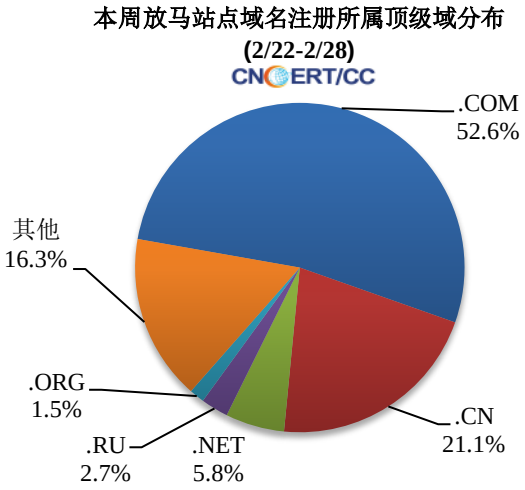
本周网络病毒活动情况

境内计算机恶意程序传播次数约为 2406.3 万次，境内感染计算机恶意程序主机数量约为 33.5 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名 743 个，涉及 IP 地址 3328 个。在 743 个域名中，有 11.6%为境外注册，且顶级域为.com 的约占 52.6%；在 3328 个 IP 中，有约 17.8%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 417 个 IP。





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。

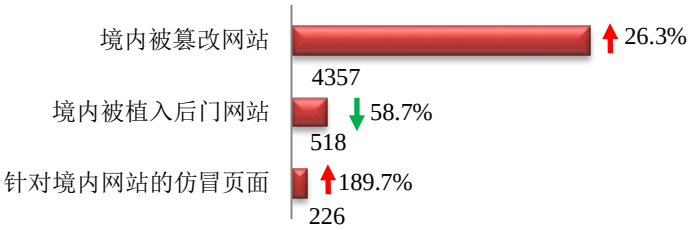
ANVA网络安全威胁信息共享平台

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。

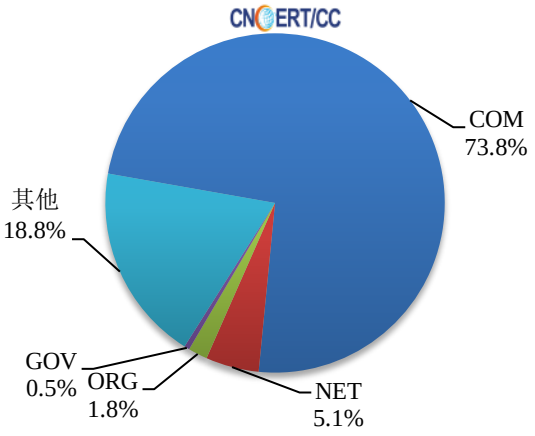
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 4357 个；被植入后门的网站数量为 518 个；针对境内网站的仿冒页面数量为 226 个。

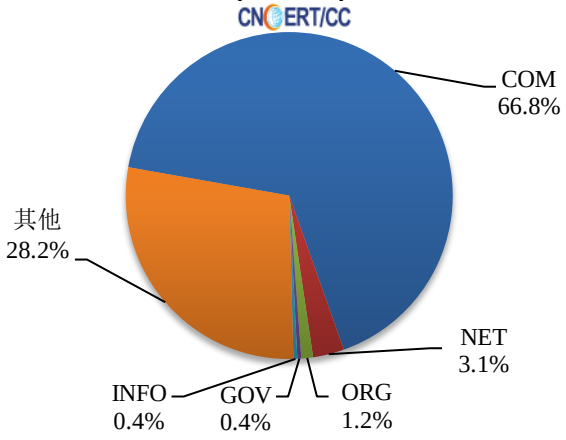


本周境内被篡改政府网站（GOV 类）数量为 22 个（约占境内 0.5%），较上周上升了 46.7%；境内被植入后门的政府网站（GOV 类）数量为 2 个。

本周我国境内篡改网站按类型分布
(2/22-2/28)

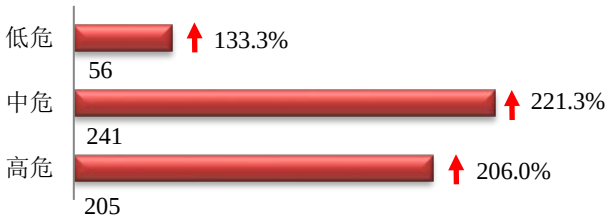


本周我国境内被植入后门网站按类型分布
(2/22-2/28)

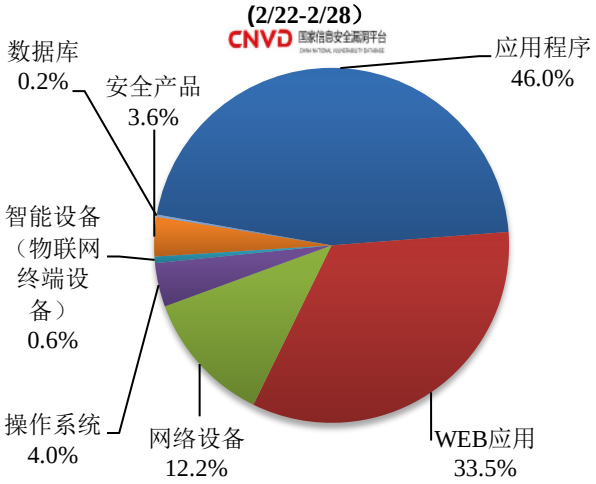


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 502 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
(2/22-2/28)



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 应用和网络设备。

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

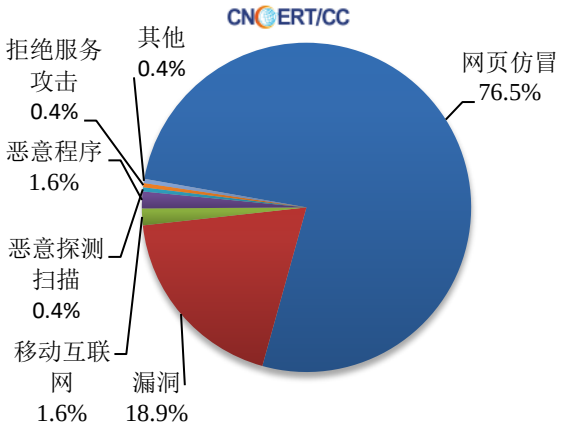
http://www.cnvd.org.cn/webinfo/list?type=4

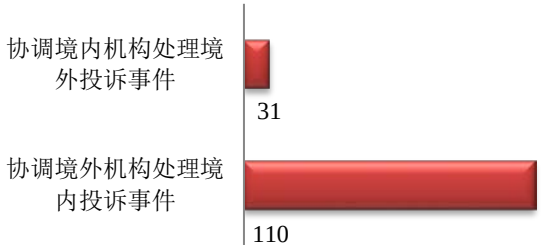
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信企业、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 243 起，其中跨境网络安全事件 141 起。

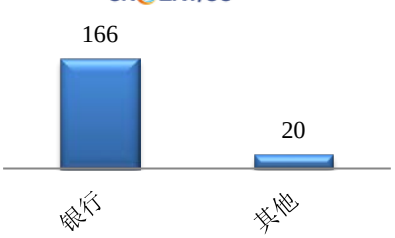
本周CNCERT处理的事件数量按类型分布
(2/22-2/28）



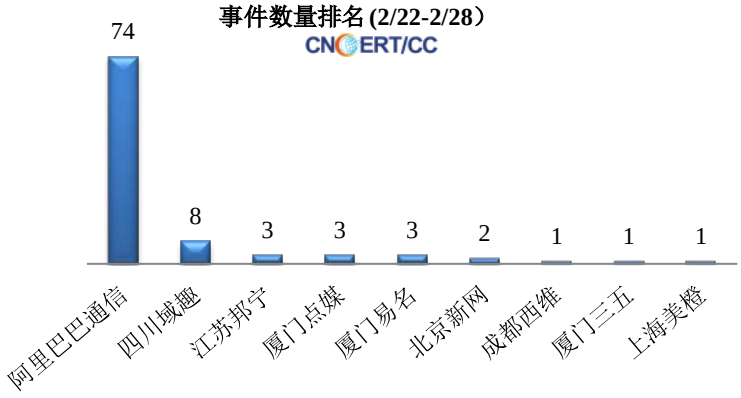


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理 186 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，银行仿冒事件 166 起，其他事件 20 起。

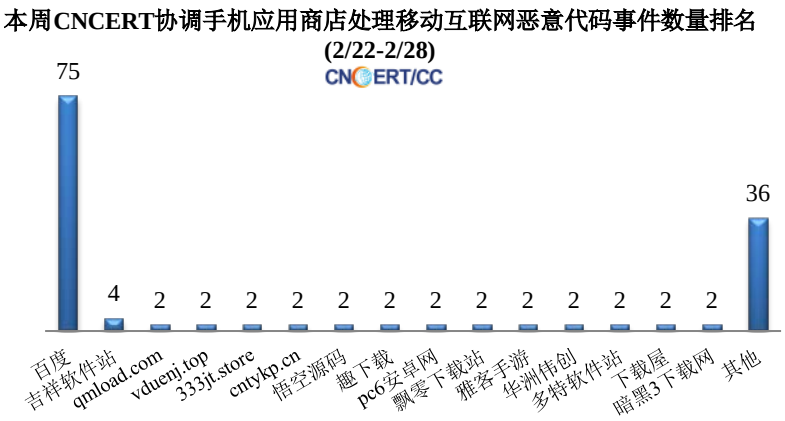
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (2/22-2/28)



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 (2/22-2/28）



本周，CNCERT 协调 46 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 141 个。



业界新闻速递

1. 拜登签署行政命令，要求对供应链进行安全审查

2 月 24 日，据美国白宫网站消息，美国总统拜登签署了一项行政命令，指示联邦机构对包括信息技术在内的各行业供应链安全风险进行审查，解决美国供应链的脆弱性和风险问题。

具体而言，该行政令指示国防、公共卫生、信息和通信技术、能源、交通以及农产品和食品生产行业进行供应链风险评估，并在一年内提交商业/国土安全联合报告。该行政命令的一个重要目标是解决各关键进口物品（如电池和药品）的短缺问题，但同时也包括了对信息和通信技术领域的强制性审查。审查的一个重要理由是希望减少依赖海外制造的半导体。

2. CNVD 发布 VMware 多款产品存在远程代码执行漏洞的安全公告

2 月 24 日，国家信息安全漏洞共享平台（CNVD）收录了 VMware vCenter Server 远程代码执行漏洞（CNVD-2021-12322，对应 CVE-2021-21972）、VMware ESXi OpenSLP 堆溢出漏洞（CNVD-2021-12321，对应 CVE-2021-21974）。攻击者利用上述漏洞，可在未授权的情况下远程执行代码。目前，部分漏洞细节和利用代码已公开。

根据 VMware 公司发布的漏洞安全公告，VMware 多个组件存在远程代码执行、堆溢出漏洞和信息泄露漏洞的高危漏洞。1）VMware vCenter Server 远程代码执行漏洞。未经身份验证的攻击者利用该漏洞，通过向目标主机的 443 端口发送恶意构造请求，写入后门文件，进而在 vCenterServer 的操作系统上实现远程代码执行。2）VMware ESXi OpenSLP 堆溢出漏洞。与 ESXi 宿主机处于同一网段、未经身份验证的攻击者利用该漏洞，通过向目标主机的 427 端口发送恶意构造请求，触发 OpenSLP 服务基于堆的缓冲区溢出，导致远程代码执行。

经综合技术研判，上述漏洞的威胁程度高，范围广，CNVD 对上述漏洞的综合评级为“高危”。目前，VMware 公司已发布新版本修复上述漏洞，CNVD 建议用户立即升级至最新版本。

3. 全国信安标委发布征求《信息安全技术 网络音视频服务数据安全指南》等 3 项国家标准（征求意见稿）意见

2 月 24 日，据全国全国信息安全标准化技术委员会网站消息，全国信息安全标准化技术委员会归口的《信息安全技术 网络音视频服务数据安全指南》等 3 项国家标准（清单见附件）现已形成标准征求意见稿。

根据《全国信息安全标准化技术委员会标准制修订工作程序》要求，现将该 3 项国家标准（征求意见稿）面向社会公开征求意见。标准相关材料已发布在信安标委网站（网址：https://www.tc260.org.cn/front/bzzqyjList.html?start=0&length=10）。如有意见或建议请于 2021 年 4 月 24 日 24:00 前反馈秘书处。

关于国家互联网应急中心（CNCERT）

国家计算机网络应急技术处理协调中心（英文简称 CNCERT/CC），成立于 2001 年 8 月，为非政府非盈利的网络安全技术中心，是中国计算机网络应急处理体系中的牵头单位。作为国家级应急中心，CNCERT/CC 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，运行和管理国家信息安全漏洞共享平台（CNVD），维护公共互联网安全，保障关键信息基础设施的安全运行。

CNCERT/CC 在中国大陆 31 个省、自治区、直辖市设有分支机构，并通过组织网络安全企业、学校、社会组织和研究机构，协调骨干网络运营单位、域名服务机构和其他应急组织等，构建中国互联网安全应急体系，共同处理各类互联网重大网络安全事件。CNCERT/CC 积极发挥行业联动合力，发起成立了中国反网络病毒联盟（ANVA）和中国互联网网络安全威胁治理联盟（CCTGA）。

同时，CNCERT/CC 积极开展网络安全国际合作，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 2020 年，已与 78 个国家和地区的 265 个组织建立了“CNCERT/CC 国际合作伙伴”关系。CNCERT/CC 是国际应急响应与安全组织 FIRST 的正式成员，以及亚太计算机应急组织 APCERT 的发起者之一，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：贾世琳

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315