国家互联网应急中心

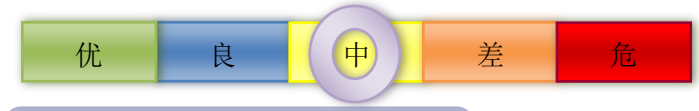
网络安全信息与动态周报

2021 年第 14 期

3 月 29 日-4 月 4 日

CNCERT/CC

本周网络安全基本态势

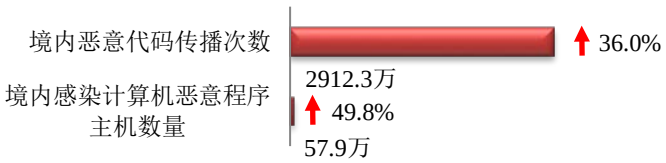


境内计算机恶意程序传播次数 境内感染计算机恶意程序主机数量	•2912.3万 •57.9万	↑ 36.0% ↑ 49.8%
境内被篡改网站总数 其中政府网站数量	•3163 •13	↓ 1.1% =
境内被植入后门网站总数 其中政府网站数量	•509 •3	↓ 9.6% ↓ 66.7%
针对境内网站的仿冒页面数量	•1878	↑ 91.2%
新增信息安全漏洞数量 其中高危漏洞数量	•700 •141	↓ 2.6% ↓ 15.1%

= 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

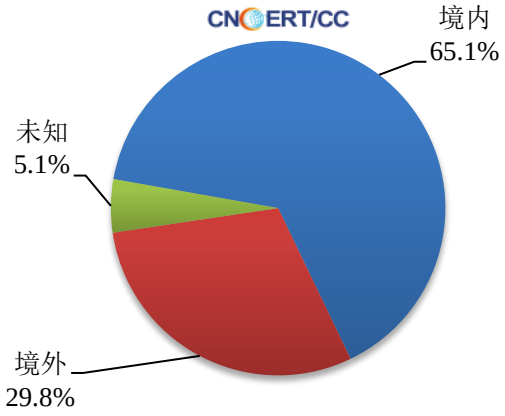
本周网络病毒活动情况

境内计算机恶意程序传播次数约为 2912.3 万次，境内感染计算机恶意程序主机数量约为 57.9 万个。

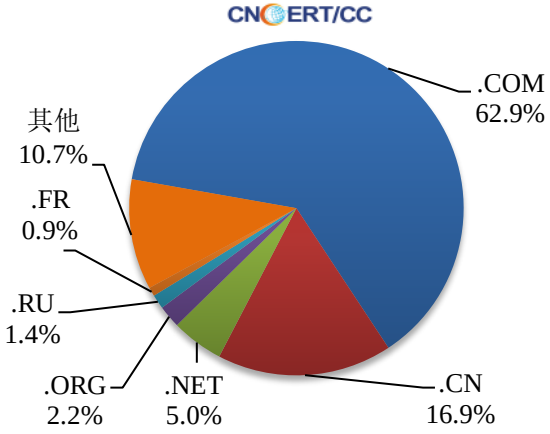


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 2105 个，涉及 IP 地址 6015 个。在 2105 个域名中，有 29.8%为境外注册，且顶级域为.com 的约占 62.9%；在 6015 个 IP 中，有约 50.1%于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 437 个。

本周放马站点域名注册所属境内外分布
(3/29-4/4)



本周放马站点域名注册所属顶级域分布
(3/29-4/4)



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。

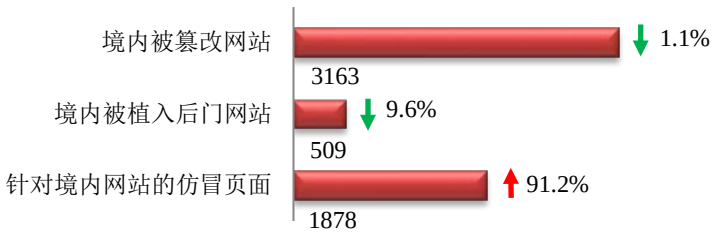
ANVA网络安全威胁信息共享平台

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。

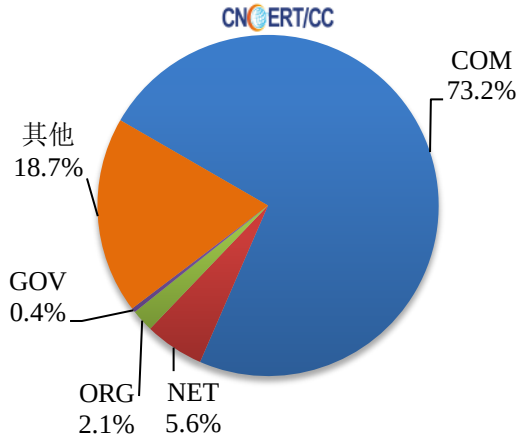
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 3163 个；被植入后门的网站数量为 509 个；针对境内网站的仿冒页面数量为 1878 个。

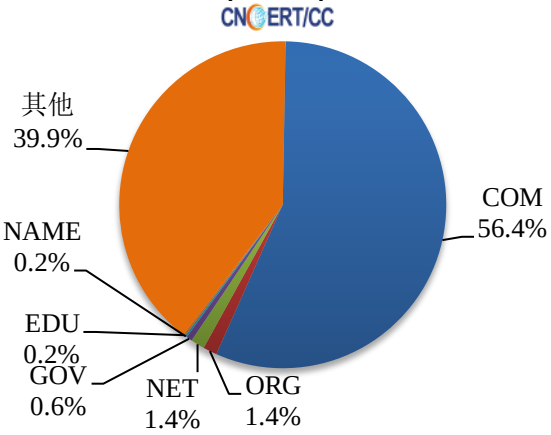


本周境内被篡改政府网站（GOV 类）数量为 13 个（约占境内 0.4%），与上周持平；境内被植入后门的政府网站（GOV 类）数量为 3 个。

本周我国境内篡改网站按类型分布
(3/29-4/4)

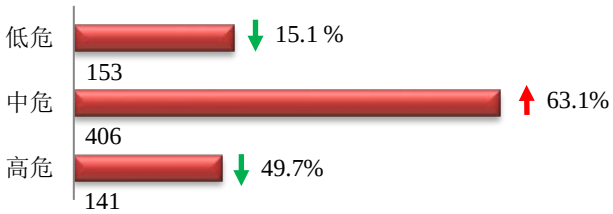


本周我国境内被植入后门网站按类型分布
(3/29-4/4)

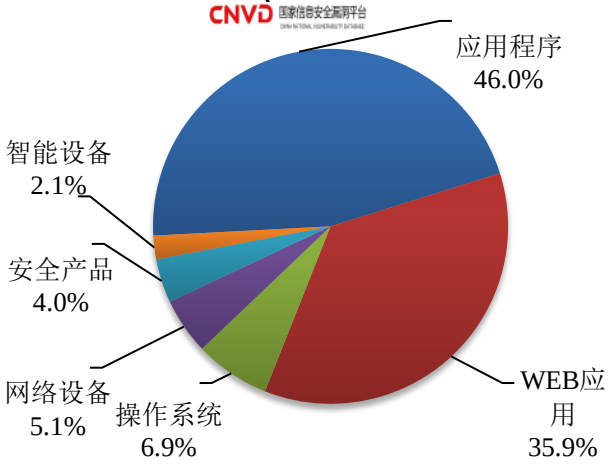


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 700 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
(3/29-4/4)



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

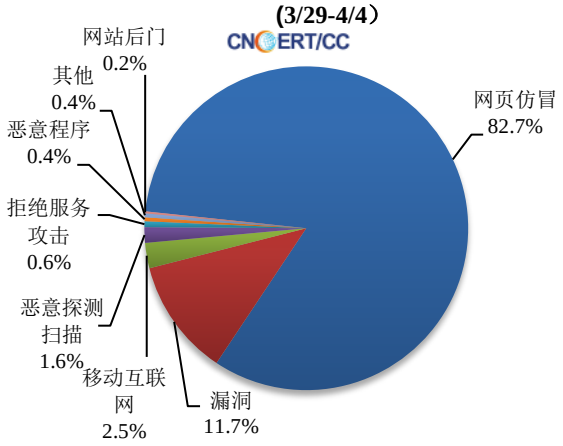
http://www.cnvd.org.cn/webinfo/list?type=4

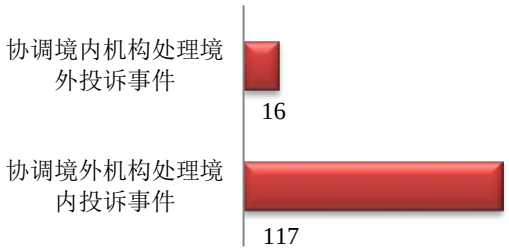
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信企业、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 514 起，其中跨境网络安全事件 133 起。

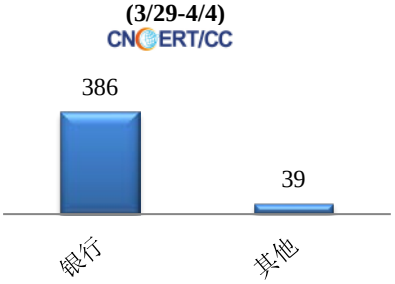
本周CNCERT处理的事件数量按类型分布 (3/29-4/4）



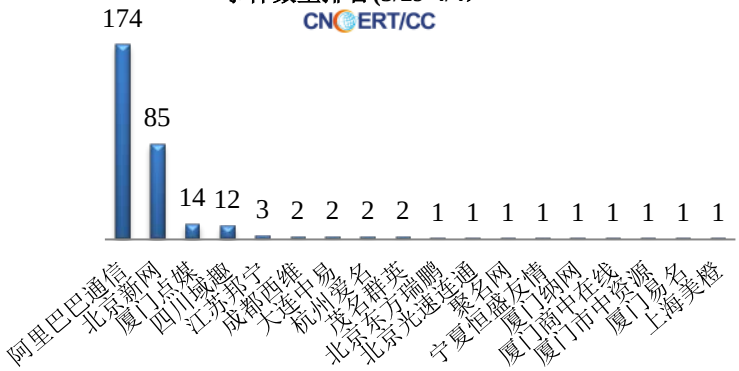


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理 425 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，银行仿冒事件 386 起，其他事件 39 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (3/29-4/4)

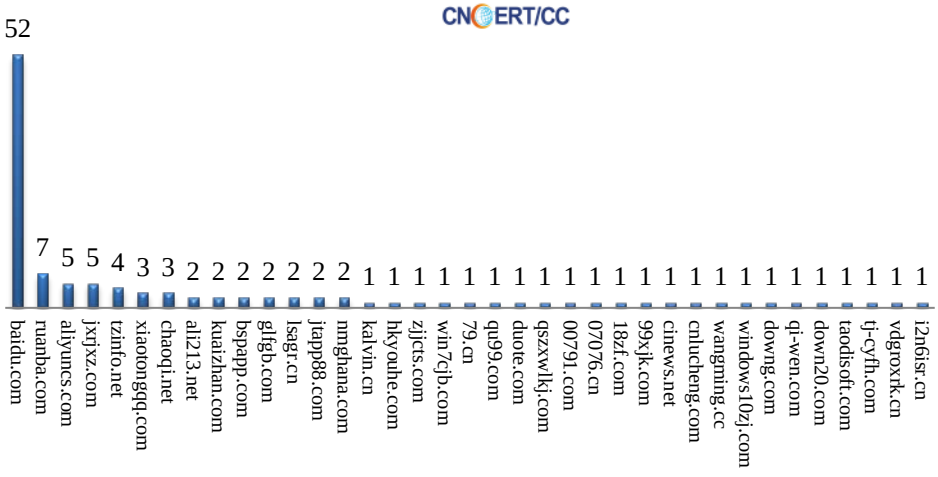


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (3/29-4/4）



本周，CNCERT 协调 37 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 116 个。

本周CNCERT协调手机应用商店处理移动互联网恶意代码事件数量排名
(3/29-4/4)



业界新闻速递

1. CNCERT 发布《2020 年虚假小额贷款类网络诈骗的态势情况分析报告》

2021 年 3 月 30 日，据 CNCERT 官网消息，CNCERT 发布了《2020 年虚假小额贷款类网络诈骗的态势情况分析报告》。虚假小额贷款诈骗是一类互联网上流行的网络诈骗。其典型的诈骗套路为：诈骗分子通过泄露的用户个人信息，拨打受害人电话或发送诈骗短信，以“提供无抵押、无担保”的快速贷款为诱饵，骗取受害人交纳风险保证金，或以需证明还款能力为借口诱使受害人转账，从而获取经济利益。这种诈骗方式往往会要求受骗人多次转账打款，受骗人一但生疑，诈骗分子则消失不见。大量网民难以分辨贷款的真实性，从而受骗上当。

长期以来，CNCERT 在对此类流行的网络诈骗行为进行监测分析的过程中，积累了相关数据，并开展了受害用户预警及案件分析支撑等工作。主要发现为：一是抽样监测发现 3461 个诈骗服务器上共承载 19420 个虚假小额贷款类诈骗网站/APP。位于中国香港的诈骗服务器数量最多，有 1986 个，占所有监测发现的诈骗服务器数量的 57.4%，其次是美国，有 322 个，占比为 9.3%；二是抽样监测发现 7909820 个用户注册或登录了此类虚假贷款网站或 APP，其中提交了个人敏感身份信息的深度受害用户占所有提交个人信息的受害用户的 11.3%，且年龄在 20-30 岁之间的受害用户最多，占到了 41.8%，男性人数更是占到了深度受害用户人数的 78.3%。

2. 中国同阿盟发表《中阿数据安全合作倡议》

2021 年 3 月 29 日，据新华社消息，外交部副部长马朝旭 29 日同阿拉伯国家联盟首席助理秘书长扎齐举行中阿数据安全视频会议，双方签署并发表《中阿数据安全合作倡议》。双方高度评价

中阿双边关系发展。马朝旭表示，去年中阿合作论坛第九届部长级会议成功举行，习近平主席向会议致贺信，为中阿政治关系发展开启了新篇章。中方愿同阿方一道，为中阿战略伙伴关系注入新内涵，携手打造志同道合、发展繁荣的中阿命运共同体。

双方一致认为，在当前数字经济迅猛发展、数据和网络安全风险突出背景下，达成《中阿数据安全合作倡议》具有重要特殊意义，标志着双方数字领域战略互信和务实合作进入新阶段。双方愿以此为契机不断深化合作，共同推动全球数字治理和国际规则制定。

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：李明

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315