国家互联网应急中心

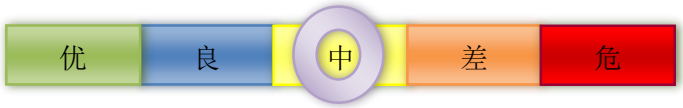
网络安全信息与动态周报

2020 年第 16 期

4 月 13 日-4 月 19 日

CNCERT/CC

本周网络安全基本态势

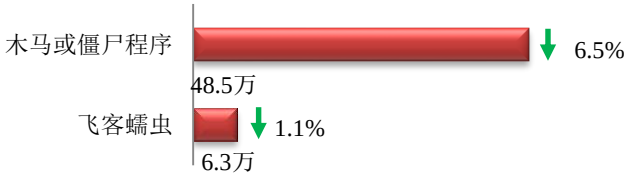


境内感染网络病毒的主机数量	•54.8万	↓ 5.9%
境内被篡改网站总数 其中政府网站数量	•7715 •29	↑ 12.5% ↑ 45.0%
境内被植入后门网站总数 其中政府网站数量	•1466 •9	↑ 1.5% ↑ 28.6%
针对境内网站的仿冒页面数量	•197	↑ 109.6%
新增信息安全漏洞数量 其中高危漏洞数量	•419 •204	↑ 1.0% ↑ 38.8%

= 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

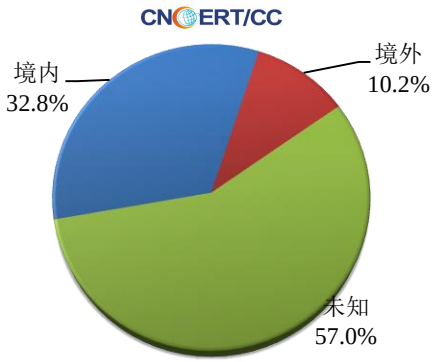
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 54.8 万个，其中包括境内被木马或被僵尸程序控制的主机约 48.5 万以及境内感染飞客（conficker）蠕虫的主机约 6.3 万。

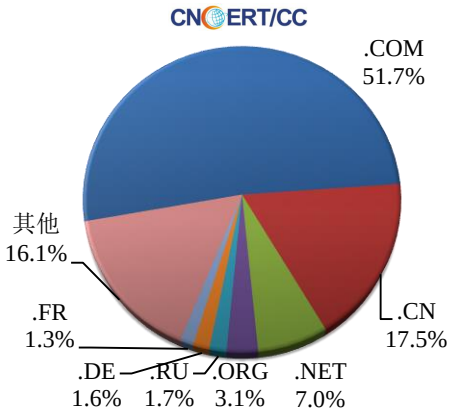


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域 1357 个，涉及 IP 地址 5730 个。在 1357 个域名中，有 10.2%为境外注册，且顶级域为.com 的约占 51.7%；在 5730 个 IP 中，有约 52.3%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 608 个 IP。

本周放马站点域名注册所属境内外分布
(4/13-4/19)



本周放马站点域名所属顶级域的分布
(4/13-4/19)



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。

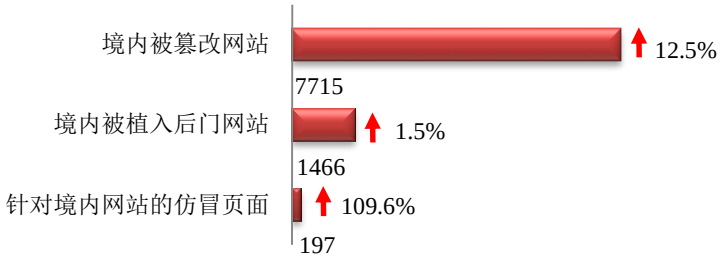
ANVA恶意地址黑名单发布地址

http://www.anva.org.cn/virusAddress/listBlack

中国反网络病毒联盟（Anti Network-Virus Alliance of China，缩写 ANVA）是由中国互联网协会网络与信息安全工作委员会发起、CNCERT 具体组织运作的行业联盟。

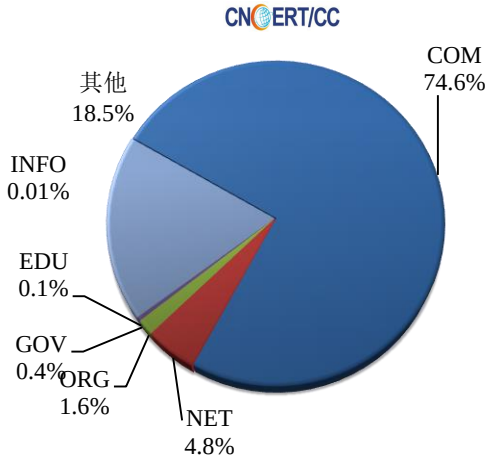
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 7715 个；被植入后门的网站数量为 1466 个；针对境内网站的仿冒页面数量 197 个。

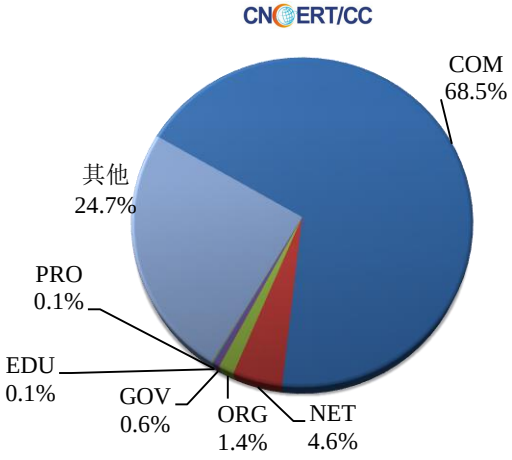


本周境内被篡改政府网站（GOV 类）数量为 29 个（约占境内 0.4%），较上周上涨了 45.0%；境内被植入后门的政府网站（GOV 类）数量为 9 个（约占境内 0.6%），较上周上涨了 28.6%。

本周我国境内篡改网站按类型分布
(4/13-4/19)

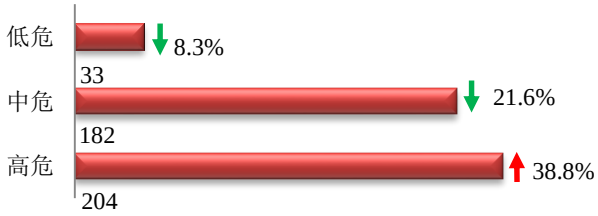


本周我国境内被植入后门网站按类型分类
(4/13-4/19)

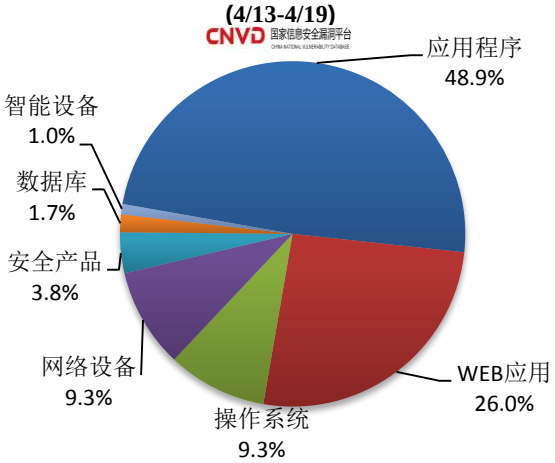


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 419 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
(4/13-4/19)



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、操作系统和网络设备。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

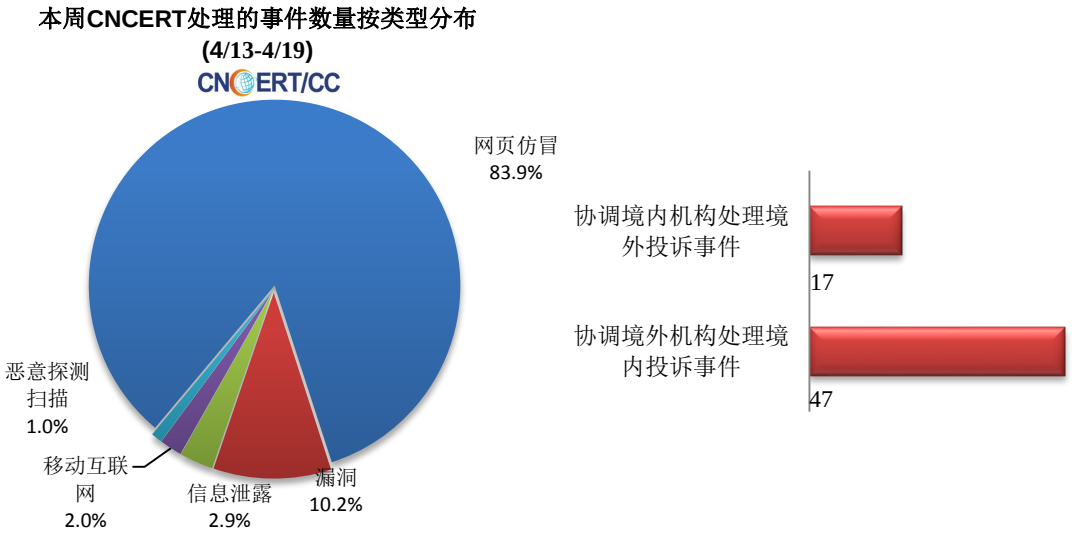
CNVD漏洞周报发布地址

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

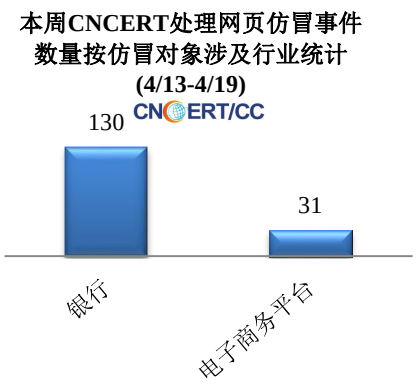
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

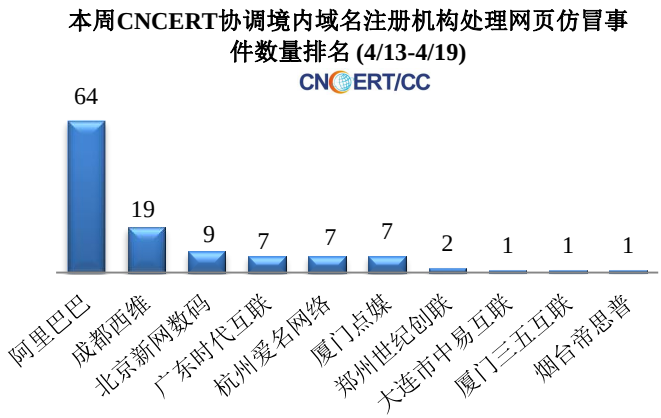
本周事件处理情况

本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 208 起，其中跨境网络安全事件 64 起。

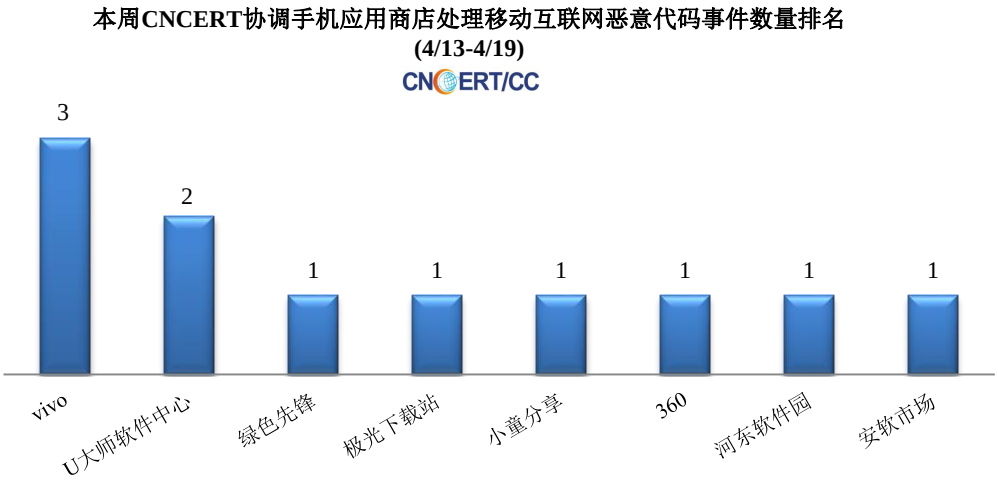


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 172 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包括银行仿冒事件 130 起和电子商务平台 31 起。





本周，CNCERT 协调 8 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 11 个。



业界新闻速递

1、 跨部委打击危害公民个人信息和数据安全违法犯罪长效机制成立

4 月 14 日，为持续保持对侵犯公民个人信息违法犯罪的高压严打态势，从源头上治理公民个人信息被泄露、隐私被侵犯的安全隐患，促进、提高行政机关、企事业单位对公民个人信息和数据安全的保护能力，形成源头治理、综合治理、系统治理的工作格局，公安部与中央网信办牵头，建立打击危害公民个人信息和数据安全违法犯罪长效机制。机制成员单位包括公安部、中央网信办、最高人民法院、最高人民检察院、工业和信息化部、国家市场监督管理总局等。针对公民个人信息泄露事件频发、侵犯公民个人信息违法犯罪活动突出等问题，各部门依托该机制，紧密围绕危害公民个人信息和数据安全的隐患，充分发挥职能优势，严厉惩治犯罪，加强法律指导，突出联合整治，加强行业监管，加强宣传教育引导，构建保护公民个人信息和数据安全的社会综合治理体系。

2、 商务部、中央网信办、工业和信息化部联合发布公告认定 12 家国家数字服务出口基地

4 月 16 日，商务部会同中央网信办、工业和信息化部联合发布公告，认定了中关村软件园等 12 个园区为国家数字服务出口基地。目前，数字技术的广泛应用在全球抗击新冠肺炎疫情的斗争中发挥了重要作用，在线办公、在线教育、云签约、5G 等新模式新业态蓬勃发展。建设国家数字服务出口基地，有利于加快数字贸易发展和数字技术应用，培育贸易新业态新模式，实现服务贸易高质量发展。下一步，商务部将会同中央网信办、工业和信息化部认真贯彻落实《中共中央 国务院关于推进贸易高质量发展的指导意见》

关于“推进数字服务出口基地建设”的要求，组织各基地所在省市制定基地建设的实施方案，研究出台具体支持政策，加快服务出口数字化转型，培育数字服务出口新主体，积极推动数字服务行业扩大对外开放，将基地打造成我国发展数字贸易的重要载体和数字服务出口的集聚区。

3、 荷兰警方一周内关闭 15 项 DDoS 租用服务

4 月 15 日，“E 安全”网站消息，荷兰警方表示，他们在一周内成功取缔了 15 家 DDoS 租用服务提供商，这是他们打击在线 DDoS 服务供应商最成功的行动之一。荷兰当局表示，此次行动是在欧洲刑警组织、国际刑警组织、联邦调查局、网络托管供应商和域名注册商共同支持下进行的，这是过去六个月中荷兰警方第二次对 DDoS 出租服务进行的打击。但是，荷兰当局没有发布这 15 种 DDoS 服务的名称。荷兰警方在发布的新闻稿中表示，据统计，荷兰中部的网络犯罪团队使用了创新的方法来检测此类助推器。因此警方通过采取预防措施让 DDos 系统和黑客域名下线等方式，尽可能地保护人们免受 DDoS 攻击。

4、 德国政府可能在 COVID-19 网络钓鱼攻击中已损失数千万欧元

4 月 18 日，据外媒 ZDNet 报道，德国西部北莱茵威斯特法伦州政府在未能建立安全的网站分发冠状病毒紧急援助资金后遭遇钓鱼攻击，损失了数千万欧元。据悉，网络犯罪分子创建了北威州经济事务部官方网站副本，随后他们使用电子邮件活动分发了指向该虚假网站的链接，吸引用户后并在用户注册时收集详细信息。随后，黑客代表真实用户向政府提出援助请求，但他们替换了要汇入资金的银行帐户。据了解，此次黑客行动从 3 月中旬持续到了 4 月 9 日，事件被发现后，北威州政府立刻暂停向用户付款并关闭了其网站。

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 与 76 个国家和地区的 233 个组织建立了“CNCERT 国际合作伙伴”关系。

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：雷君

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315