国家互联网应急中心

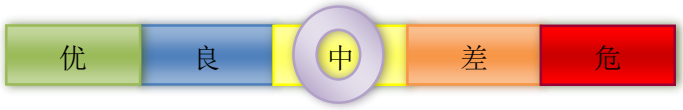
网络安全信息与动态周报

2020 年第 15 期

4 月 6 日-4 月 12 日

CNCERT/CC

本周网络安全基本态势

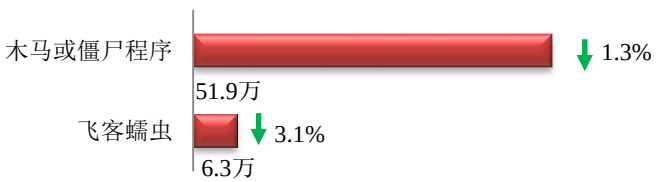


境内感染网络病毒的主机数量	•58.2万	↓1.5%
境内被篡改网站总数 其中政府网站数量	•6860 •20	↓17.2% ↓45.9%
境内被植入后门网站总数 其中政府网站数量	•1445 •7	↓3.5% ↑40.0%
针对境内网站的仿冒页面数量	•94	↓60.2%
新增信息安全漏洞数量 其中高危漏洞数量	•415 •147	↓3.7% ↓29.0%

= 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

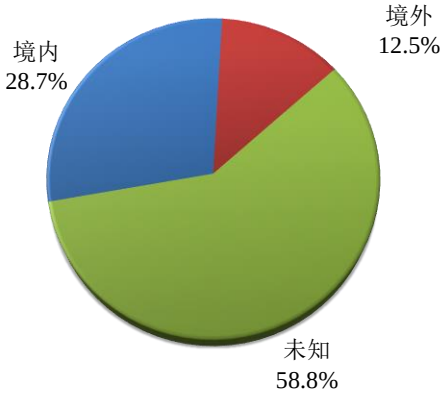
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 58.2 万个，其中包括境内被木马或被僵尸程序控制的主机约 51.9 万以及境内感染飞客（conficker）蠕虫的主机约 6.3 万。

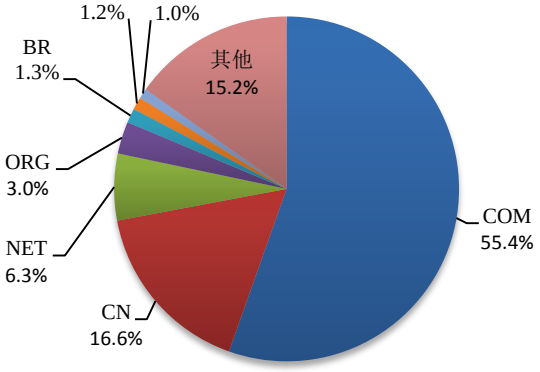


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域 1263 个，涉及 IP 地址 4359 个。在 1263 个域名中，有 12.5%为境外注册，且顶级域为.com 的约占 55.4%；在 4359 个 IP 中，有约 52.4%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 353 个 IP。

本周放马站点域名注册所属境内外分布 (4/6-4/12)



本周放马站点域名所属顶级域的分布 (4/6-4/12)



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。

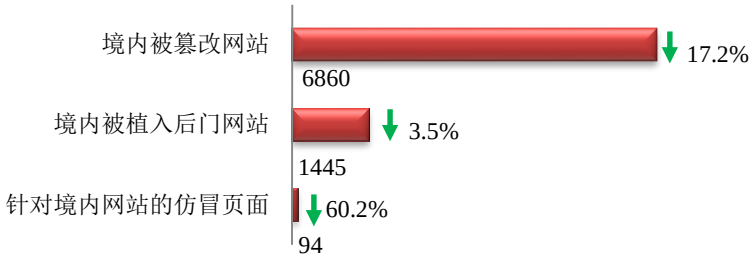
ANVA恶意地址黑名单发布地址

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。

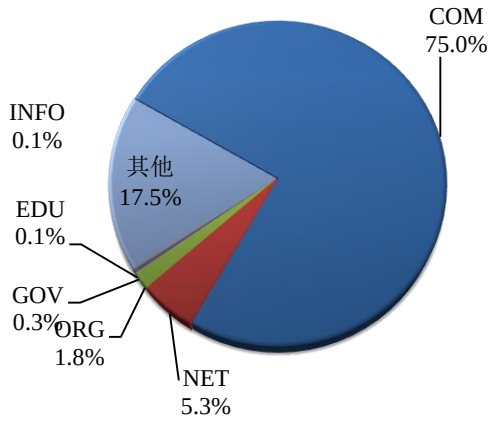
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 6860 个；被植入后门的网站数量为 1445 个；针对境内网站的仿冒页面数量 94 个。

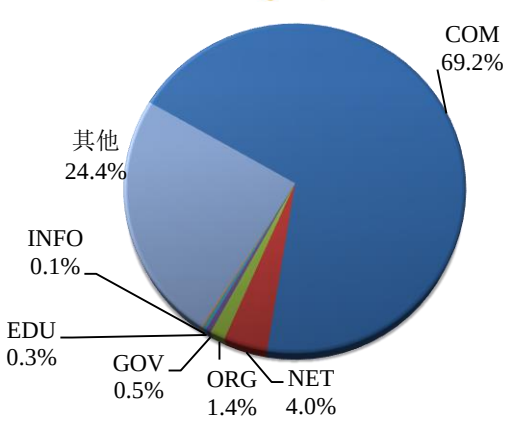


本周境内被篡改政府网站（GOV 类）数量为 20 个（约占境内 0.3%），较上周下降了 45.9%；境内被植入后门的政府网站（GOV 类）数量为 7 个（约占境内 0.5%），较上周上涨了 40.0%。

本周我国境内篡改网站按类型分布
(4/6-4/12)

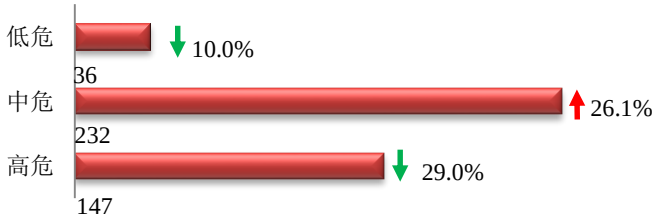


本周我国境内被植入后门网站按类型分类
(4/6-4/12)

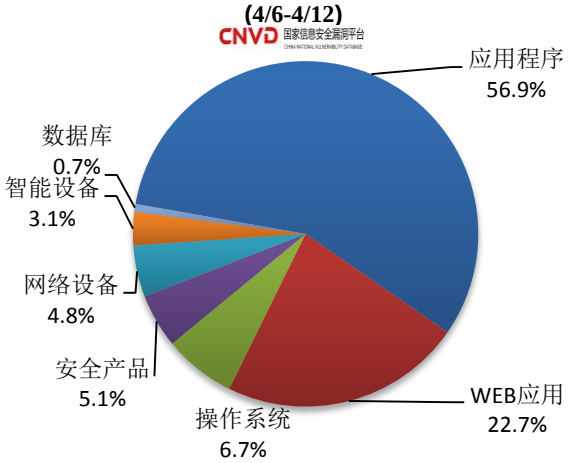


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 415 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
(4/6-4/12)



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

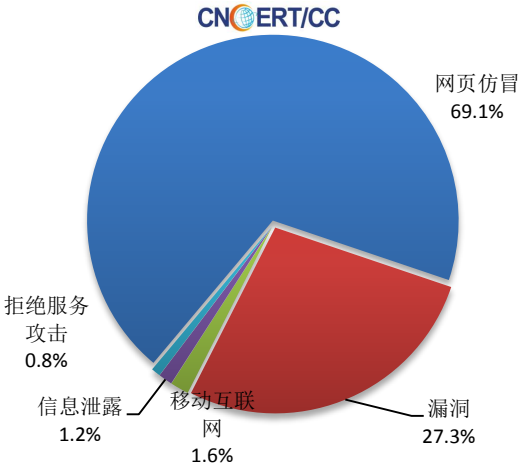
http://www.cnvd.org.cn/webinfo/list?type=4

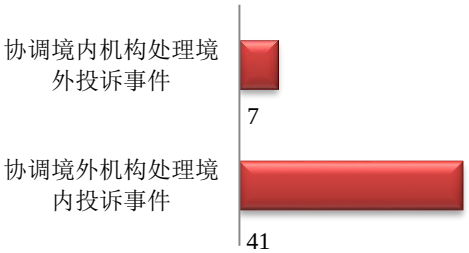
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 249 起，其中跨境网络安全事件 48 起。

本周CNCERT处理的事件数量按类型分布 (4/6-4/12)



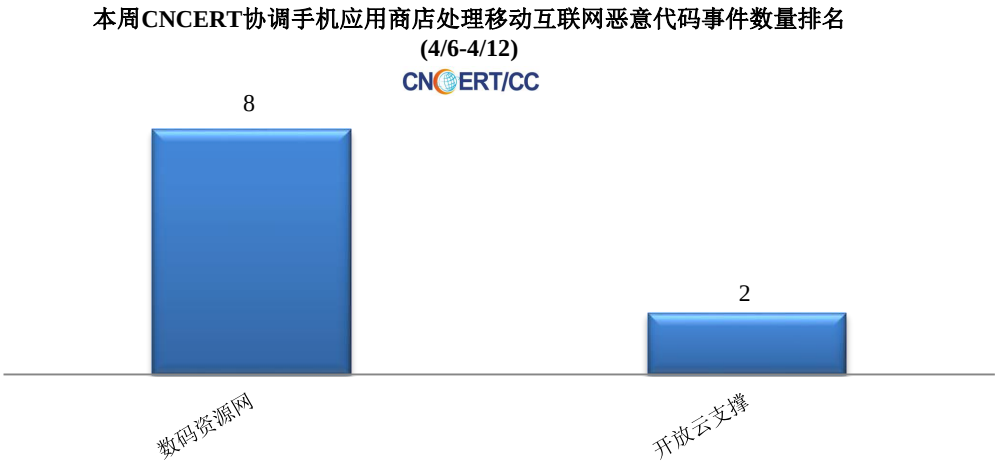


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 172 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包括银行仿冒事件 136 起和电子商务平台 21 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (4/6-4/12)

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 (4/6-4/12)

本周，CNCERT 协调 2 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 10 个。



业界新闻速递

1、 最高检召开“严厉打击网络犯罪 共同防控网络风险”新闻发布会

4 月 8 日，最高人民检察院召开以“严厉打击网络犯罪，共同防控网络风险”为主题的新闻发布会，发布最高检第十八批指导性案例，并回答记者提问。在发布会上，发布了张凯闵等 52 人电信网络诈骗案（检例第 67 号），叶源星、张剑秋提供侵入计算机信息系统程序、谭房妹非法获取计算机信息系统数据案（检例第 68 号），姚晓杰等 11 人破坏计算机信息系统案（检例第 69 号）共 3 个案例，针对每个案例从关键词、要旨、基本案情、指控与证明犯罪、指导意义、相关规定等方面进行详细介绍。

2、 公开征求对《网络数据安全标准体系建设指南》（征求意见稿）的意见

4 月 10 日，工业和信息化部官网消息，为落实《中华人民共和国网络安全法》《全国人民代表大会常务委员会关于加强网络信息保护的决定》《电信和互联网用户个人信息保护规定》等法律法规要求，有效提升电信和互联网行业网络数据安全保护能力，充分发挥标准在保障网络数据安全、推动行业健康有序发展中的引领和支撑作用，助力数字经济高质量发展，有关单位编制完成了《网络数据安全标准体系建设指南》（征求意见稿）及编制说明。为进一步听取社会各界意见，工业和信息化部科技司将相关内容予以公示，公示日期截止 2020 年 5 月 9 日。如有意见或建议，请在公示期间填写《公示意见反馈信息表》并反馈至工业和信息化部科技司。

3、 NASA 称 COVID-19 流行期间恶意攻击数量增加

4 月 7 日，据外媒报道，美国国家航空航天局（NASA）发现，在 COVID-19 大流行期间，黑客针对美国宇航局系统和在家工作人员的恶意活动“显著增加”。NASA 安全运营中心（SOC）制定的缓解工具和措施成功阻止了一波网络攻击，该机构报告称，网络钓鱼攻击的数量增加了一倍，恶意软件攻击呈指数级增长，被屏蔽的恶意网站数量增加了一倍。还观察到越来越多的威胁行为者发送恶意电子邮件，其最终目的是用恶意软件和网络钓鱼敏感信息感染员工，这些信息随后可能被用来访问关键的 NASA 系统和敏感数据。

4、 超 50 万 Zoom 账户信息在暗网被黑客售卖

4 月 13 日，据外媒 Bleepingcomputer 报道，网络安全公司 Cyble 的数字风险评估专家最近发现，一名黑客正在以极其低廉的价格出售被盗的 Zoom 账号，总数 53 万个。除了用来卖的部分，黑客还免费曝光了 290 个账号，这些账号来自佛蒙特大学、科罗拉多大学、佛罗里达大学等多所高校。每个账户被泄露的信息包括邮箱、密码、个人 url 地址，还有 HostKey（作为会议主持人管理会议的 6 位数 PIN 码）。针对 Zoom 事件，美国参议院呼吁联邦贸易委员会对 Zoom 安全事件进行干预，制定视频电话会议软件安全准则。

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：张宇鹏

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315