国家互联网应急中心

2019 年第 23 期
6 月 3 日-6 月 9 日

网络安全信息与动态周报

本周网络安全基本态势

境内感染网络病毒的主机数量	•21.2万	↑ 2.2%
境内被篡改网站总数 其中政府网站数量	•2209 •3	↓ 66.6% ↓ 76.9%
境内被植入后门网站总数[1] 其中政府网站数量	•3654 •50	↓ 10.3% ↑ 47.1%
针对境内网站的仿冒页面数量	•9185	↑ 406.6%
新增信息安全漏洞数量 其中高危漏洞数量	•171 •54	↓ 41.6% ↓ 44.3%

═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

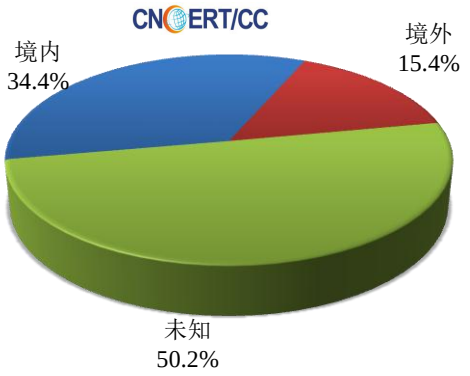
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 21.2 万个，其中包括境内被木马或被僵尸程序控制的主机约 12.4 万以及境内感染飞客（conficker）蠕虫的主机约 8.8 万。

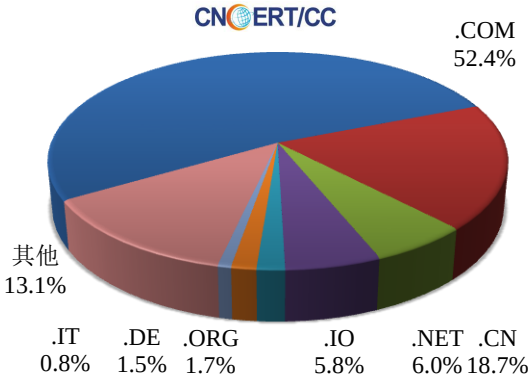
[1]本期境内被植入后门总数受监测数据范围扩大影响，波动较大

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 2706 个，涉及 IP 地址 4134 个。在 2706 个域名中，有 15.4%为境外注册，且顶级域为.com 的约占 52.4%；在 3396 个 IP 中，有约 49.9%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 500 个 IP。

本周放马站点域名注册所属境内外分布
(6/3-6/9)



本周放马站点域名所属顶级域的分布
(6/3-6/9)



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。

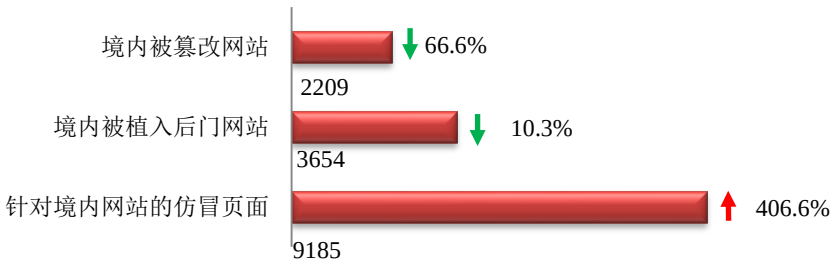
ANVA恶意地址黑名单发布地址

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。

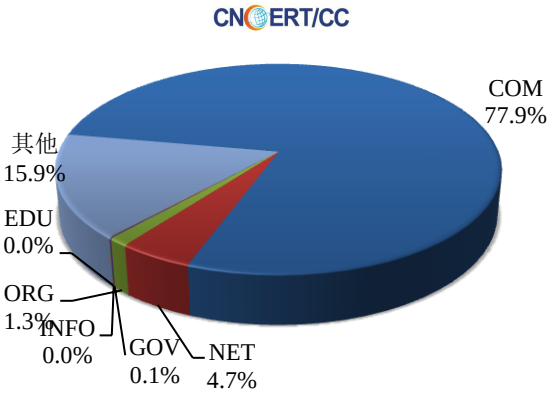
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 2209 个；境内被植入后门的网站数量为 3654 个；针对境内网站的仿冒页面数量 9185 个。

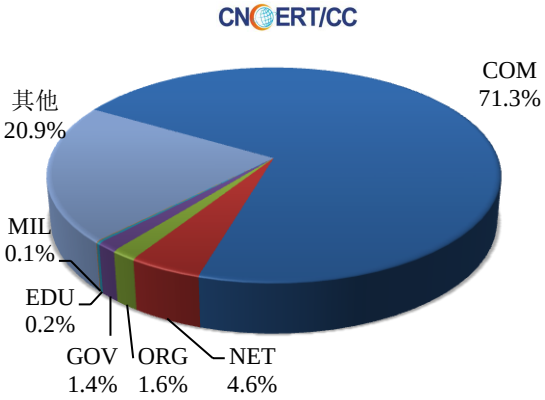


本周境内被篡改政府网站（GOV 类）数量为 3 个（约占境内 0.1%），较上周环比下降 76.9%；境内被植入后门的政府网站（GOV 类）数量为 50 个（约占境内 1.4%），较上周环比上升 47.1%；针对境内网站的仿冒页面涉及域名 937 个，IP 地址 755 个，平均每个 IP 地址承载了约 12 个仿冒页面。

本周我国境内被篡改网站按类型分布
(6/3-6/9)

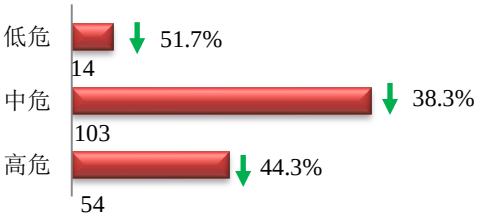


本周我国境内被植入后门网站按类型分布
(6/3-6/9)

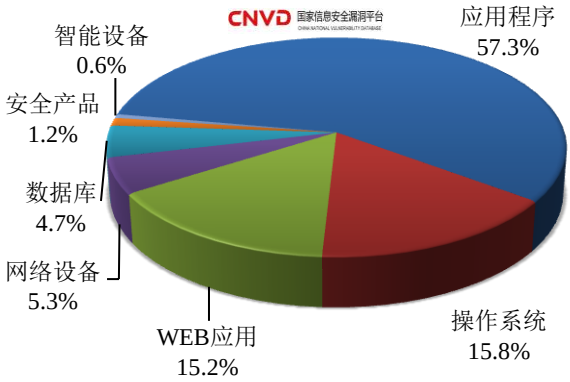


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 171 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类型分布
(6/3-6/9)



本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是操作系统漏洞和 WEB 应用漏洞。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

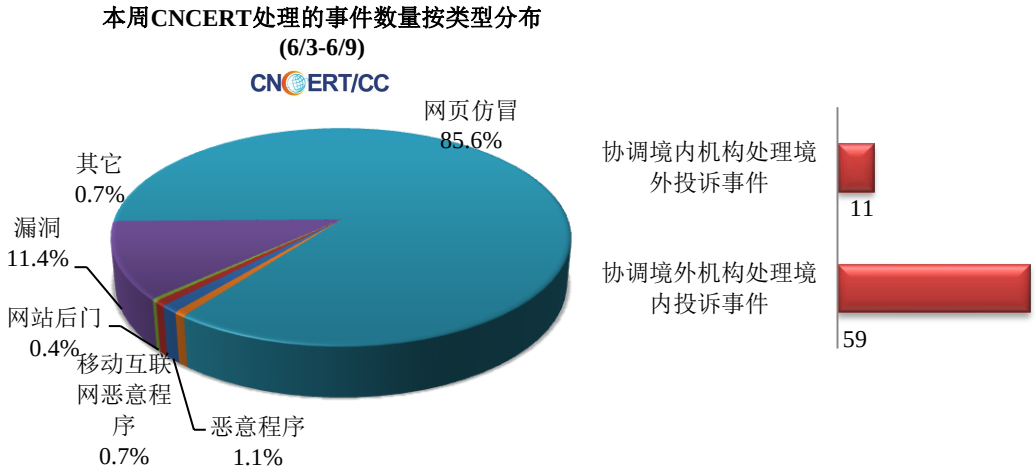
CNVD漏洞周报发布地址

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

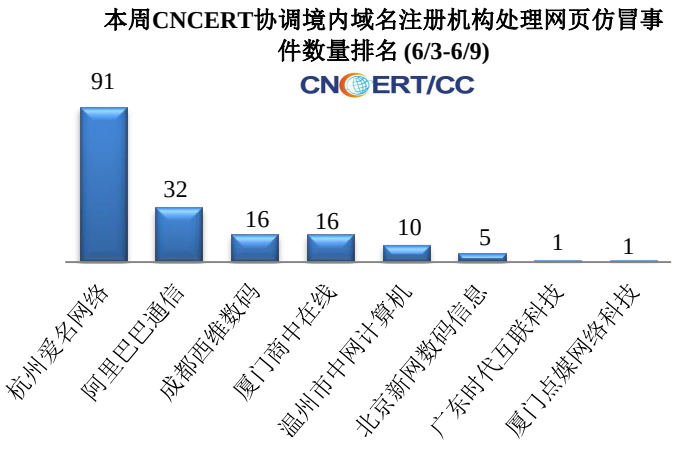
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 271 起，其中跨境网络安全事件 70 起。

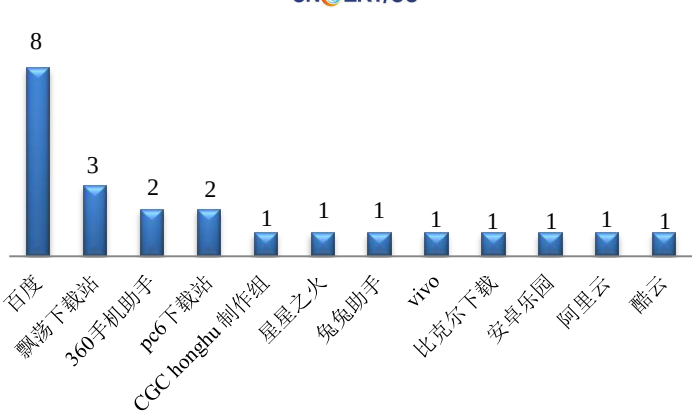


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 232 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 227 起和互联网移动供应商仿冒事件 2 起。



本周，CNCERT 协调 12 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 23 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
(6/3-6/9)



业界新闻速递

1、 工业和信息化部向四家企业颁发 5G 牌照

工业和信息化部 6 月 6 日消息，依中国电信集团有限公司、中国移动通信集团有限公司、中国联合网络通信集团有限公司、中国广播电视网络有限公司申请，工业和信息化部经履行法定程序，于 2019 年 6 月 6 日向四家企业颁发了基础电信业务经营许可证，批准四家企业经营“第五代数字蜂窝移动通信业务”。工业和信息化部部长苗圩同志出席颁证会并颁发许可证。工业和信息化部党组成员、总工程师张峰同志主持会议，国家发展改革委相关负责同志及中国电信、中国移动、中国联通、中国广电、中国铁塔主要负责同志出席会议。

2、欧盟发布非个人数据自由流动指南

中国外交部官网 6 月 4 日消息 据欧盟官网消息，欧委会 5 月 29 日发布非个人数据自由流动指南，配套欧盟 5 月 28 日在成员国适用的非个人数据自由流动条例使用。指南旨在帮助用户，特别是中小企业了解非个人数据自由流动条例与通用数据保护条例（GDPR）之间的相互关系，如数据集由个人和非个人数据组成的情况等。非个人数据自由流动指南指南提供了企业处理个人和非个人数据组成的数据集时应用规则的实际案例，阐释了个人和非个人数据的概念，包括混合数据集等；罗列了两条例中数据自由流动的原则和防止数据本地化的规定，涵盖了非个人数据自由流动条例规定的数据可携带性概念。此外，该指南还包括两条例规定的自律要求。

3. 美国两个医疗数据库遭入侵，超 2000 万患者信息受影响

搜狐新闻 6 月 7 日消息 据外媒报道，包括医疗患者和支付信息的数据库遭到黑客攻击，这些被盗的数据由美国医学收集机构（AMCA）代表血液检测公司 LabCorp 和医疗检测巨头 Quest Diagnostics 维护。6.4 日，LabCorp 向美国证券贸易委员会提交了一份文件，称其包括 770 万名患者的数据库被黑客入侵。这个数据库储存了患者姓名、生日、地址、电话号码及所欠或支付的金额。此外，大约 20 万包含信用卡或银行账户信息的条目已被黑客窃取。

4、澳大利亚顶尖大学的系统遭黑客入侵

腾讯新闻 6 月 5 日消息 黑客于 2018 年年底侵入澳大利亚国立大学网络防御系统，获取了一些敏感数据。系统中的姓名、地址、出生日期、电话号码、个人电子邮件地址和紧急联系方式、税号、工资单信息、银行帐户详细信息和护照详细信息等信息遭泄露，甚至学术记录也被黑客访问。部分数据可追溯到 19 年前。由于澳大利亚国立大学的许多毕业生后来担任政府高级职位，数据泄露事件可能产生较为严重的影响，黑客可了解在不同政府部门工作的人员信息。澳大利亚网络情报机构表示，目前正在调查中。

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 2017 年，CNCERT 与 72 个国家和地区的 211 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：韩志辉

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315