国家互联网应急中心

网络安全信息与动态周报

2018 年第 4 期

1 月 22 日-1 月 28 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	•25.2万	↑ 5.5%
境内被篡改网站总数 其中政府网站数量	•867 •0	↓ 64.4% ↓ 100.0%
境内被植入后门网站总数 其中政府网站数量	•812 •17	↓ 10.6% ↓ 54.1%
针对境内网站的仿冒页面数量	•384	↑ 15.3%
新增信息安全漏洞数量 其中高危漏洞数量	•241 •109	↓ 41.2% ↓ 14.8%

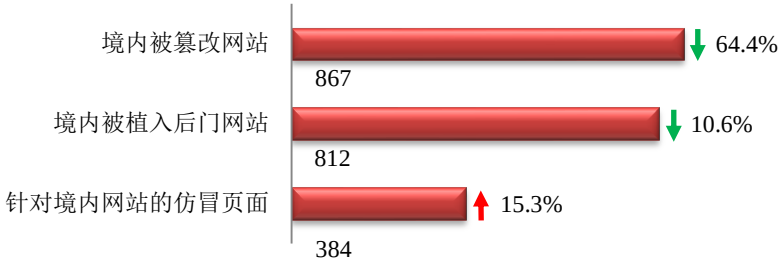
═表示数量与上周相同　↑表示数量较上周环比增加　↓表示数量较上周环比减少

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 25.2 万个，其中包括境内被木马或被僵尸程序控制的主机约 13.8 万以及境内感染飞客（conficker）蠕虫的主机约 11.4 万。

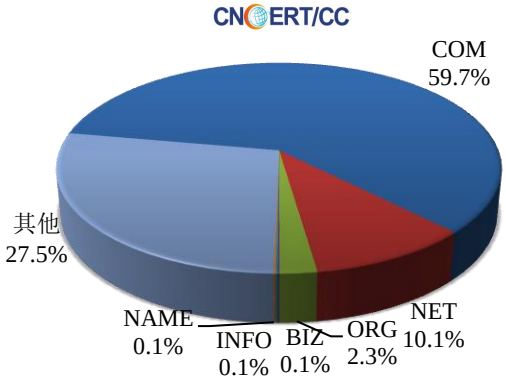
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 867 个；境内被植入后门的网站数量为 812 个；针对境内网站的仿冒页面数量为 384。

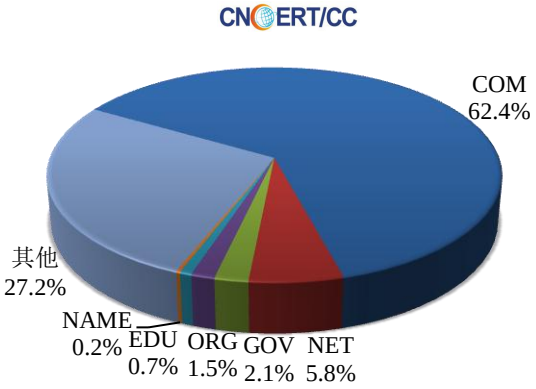


本周境内被植入后门的政府网站（GOV 类）数量为 17 个（约占境内 2.1%），较上周环比下降了 54.1%；针对境内网站的仿冒页面涉及域名 305 个，IP 地址 134 个，平均每个 IP 地址承载了约 3 个仿冒页面。

本周我国境内被篡改网站按类型分布
(1/22-1/28)

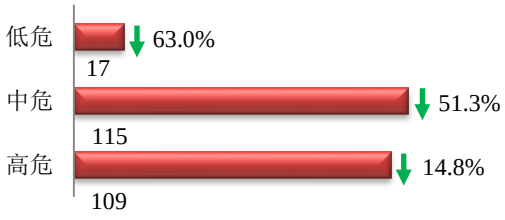


本周我国境内被植入后门网站按类型分布
(1/22-1/28)

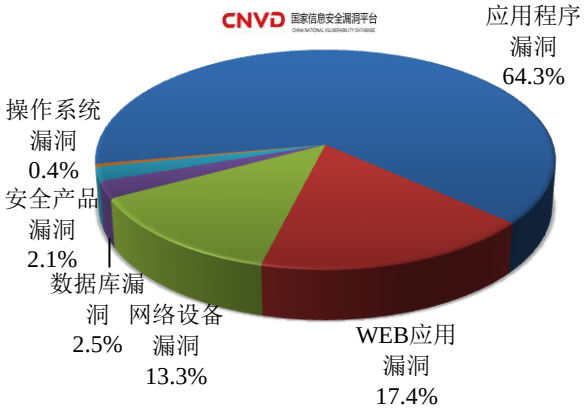


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 241 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
(1/22-1/28)



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 应用漏洞和网络设备漏洞。

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

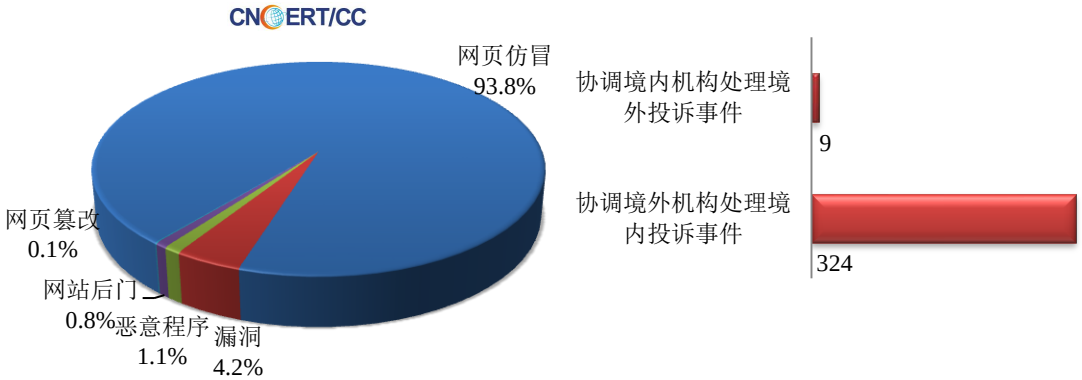
http://www.cnvd.org.cn/webinfo/list?type=4

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

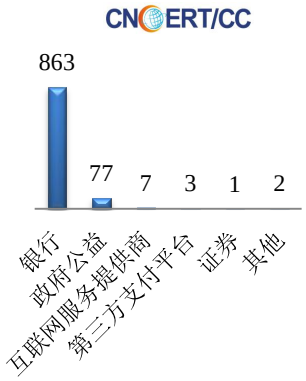
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 1016 起，其中跨境网络安全事件 333 起。

本周CNCERT处理的事件数量按类型分布
(1/22-1/28)

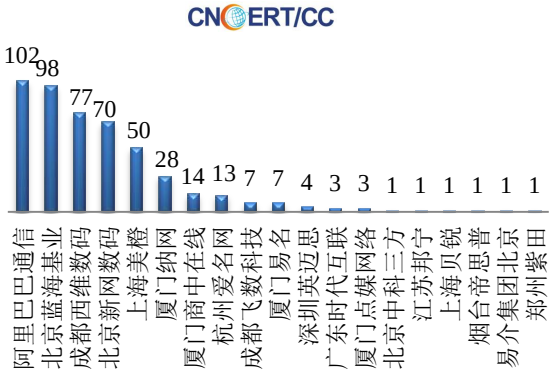


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 953 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 863 起和政府公益仿冒事件 77 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(1/22-1/28)

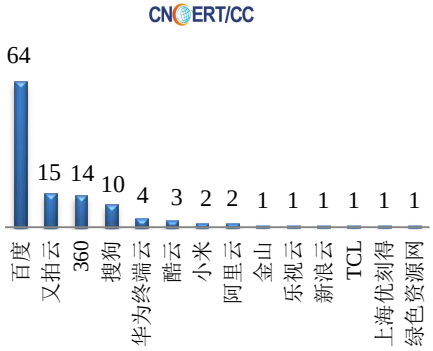


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (1/22-1/28)



本周，CNCERT 协调 14 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 120 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 (1/22-1/28)



业界新闻速递

1、全球网络安全中心正式成立

E 安全 1 月 26 日消息 各国政府及企业每年在网络攻击威胁应对领域的投入已增长至 4450 亿美元（约合人民币 2.85 万亿元），由第 48 届达沃斯世界经济论坛（WEF）牵头的全球网络安全中心于 2018 年 1 月 23 日正式成立。这一全新机构旨在提升网络弹性，同时建立起一套独立的最佳实践库，并将针对不同攻击场景提供指导性意见。根据世界经济论坛总裁阿洛伊斯·齐韦吉在新闻发布会上所言，该中心将常设于日内瓦，并计划于 2018 年 3 月正式开始运作。该中心还将帮助“网络发达”区域制定新的战略，用以保护各类关键基础设施。此

外，物联网（IoT）与联网设备的兴起亦成为企业特别担心的一类挑战，人们普遍认为其会造成更严重的网络安全问题。网络安全全球中心将自主管理。世界经济论坛发言人格奥尔·施密特 向公众介绍称，中心的运营将依赖成员资助，论坛本身将领投数百万瑞士法郎。

2、废除网络中立规则后 全美超 750 个社区用区域自建方案替代 ISP 服务

cnBeta.COM1 月 26 日消息 距离美国联邦通信委员会（FCC）废除网络中立规则已经过去一个多月时间，FCC 最终将互联网的未来交给了互联网服务供应商（ISP）手中，这将扼杀网络的开放性。据 Motherboard 网站报道，美国许多社区为了掌握自己的宽带服务质量，自建 ISP 宽带网络方案已经如雨后春笋般席卷美国。美国非营利性组织地方自立协会（Institute for Local Self-Reliance，ILSR）最新调查研究表明全美境内已经有超 750 个社区通过自建宽带网络、市营宽带、电力公司网络取代网络供应商。

3、挪威医疗卫生机构计算机系统遭到入侵，超过 290 万居民信息或将泄露

HackerNews.cc1 月 23 日消息 据外媒报道，位于挪威东南部地区的医疗卫生机构 Health South-East RHF 于 1 月 8 日表示其计算机系统遭到不明人士入侵，可能会影响到约 290 万人（占挪威人口的 56%）的医疗数据。目前相关专家认为该起入侵事件或属境外国家发起的网络间谍活动的涉猎范畴，并表示已采取紧急措施来消除威胁。根据挪威卫生安全部门 HelseCERT 透露，他们检测到来自 Health South-East RHF 的异常流量，从而发现了入侵行为。研究人员认为在地下网络犯罪中，医疗数据是一种有价值的商品，恶意人士可以将这些数据用于进一步的攻击。专家和政府代表认为，Health South-East RHF 遭受的数据泄露可能是由于境外国家发起的网络间谍活动造成的，因为这些发起者对收集与政府、军方、情报人员和政客有关的数据极为感兴趣。

4、新型僵尸网络 HNS 不断增长，已感染逾 2 万物联网设备

HackerNews.cc1 月 27 日消息 外媒 1 月 25 日消息，一个名为 Hide'N Seek(HNS)的新僵尸网络正在世界各地不断增长，对物联网设备造成重大影响（截至目前为止，受感染的物联网设备数量已达 2 万）。据研究人员介绍，HNS 僵尸网络使用定制的点对点通信来诱捕新的物联网设备并构建其基础设施，目前 HNS 主要是针对不安全的物联网设备，尤其是 IP 摄像机。Bitdefender 的安全研究人员发现 HNS 僵尸网络于 2018 年 1 月 10 日首次出现，和其他与 Mirai 有关的物联网（IoT）僵尸网络并不相同。因为 HNS 有着不同的起源，且不共享其源代码。事实上，Bitdefender 高级电子威胁分析师 Bogdan Botezatu 认为 HNS 与 Hajime 僵尸网络更为相似。目前 Bitdefender 的研究人员尚未发现 HNS 僵尸网络具有 DDoS 功能，这意味着 HNS 将被部署为一个代理网络。另外，研究人员透露 HNS 僵尸网络仍然不断变化中，可能会被应用于多种攻击场景。

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。截止 2016 年，CNCERT 与 69 个国家和地区的 185 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：徐原

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158