国家互联网应急中心

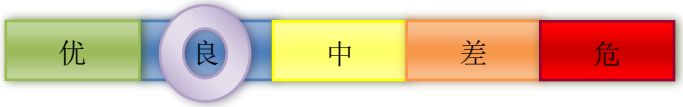
网络安全信息与动态周报

2018 年第 14 期

4 月 2 日-4 月 8 日

CNCERT/CC

本周网络安全基本态势

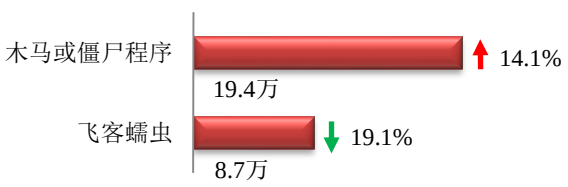


境内感染网络病毒的主机数量	•28.1万	1.2%
境内被篡改网站总数 其中政府网站数量	•1045 •30	40.1% 87.5%
境内被植入后门网站总数 其中政府网站数量	•994 •11	3.7% 21.4%
针对境内网站的仿冒页面数量	•889	16.4%
新增信息安全漏洞数量 其中高危漏洞数量	•165 •44	63.5% 67.2%

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*

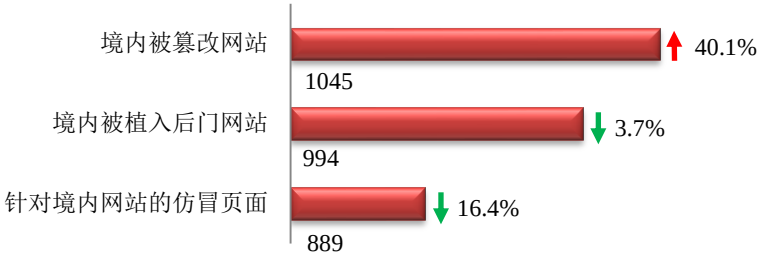
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 28.1 万个，其中包括境内被木马或被僵尸程序控制的主机约 19.4 万以及境内感染飞客（conficker）蠕虫的主机约 8.7 万。



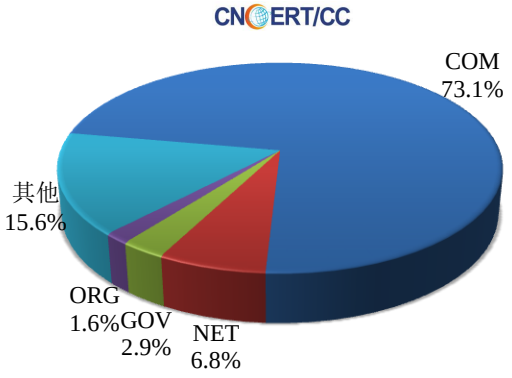
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1045 个；境内被植入后门的网站数量为 994 个；针对境内网站的仿冒页面数量为 889。

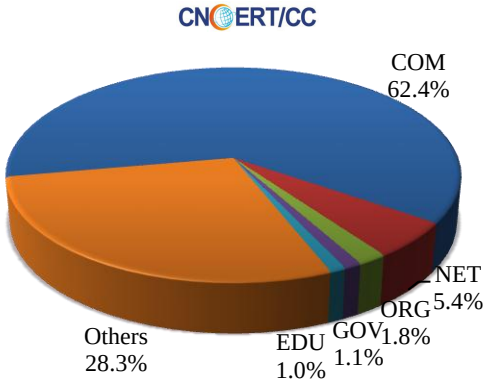


本周境内被篡改政府网站（GOV 类）数量为 30 个（约占境内 2.9%），较上周环比上升了 87.5%；境内被植入后门的政府网站（GOV 类）数量为 11 个（约占境内 1.1%），较上周环比下降了 21.4%；针对境内网站的仿冒页面涉及域名 418 个，IP 地址 146 个，平均每个 IP 地址承载了约 6 个仿冒页面。

本周我国境内被篡改网站按类型分布
(4/2-4/8)

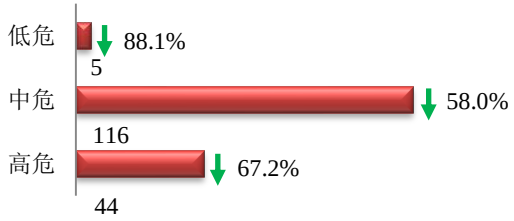


本周我国境内被植入后门网站按类型分布
(4/2-4/8)

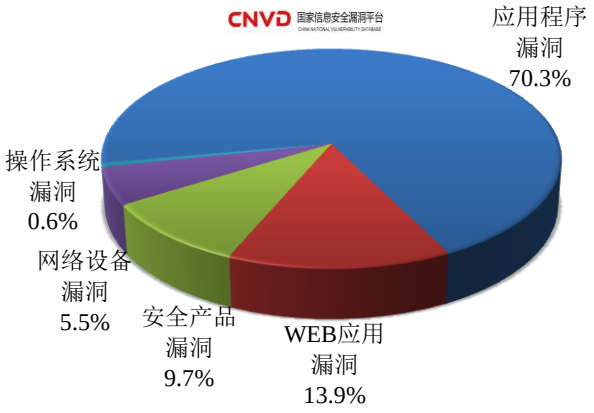


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 165 个，信息安全漏洞威胁整体评价级别为高。



本周CNVD收录漏洞按影响对象类型分布
(4/2-4/8)



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 应用漏洞和安全产品漏洞。

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

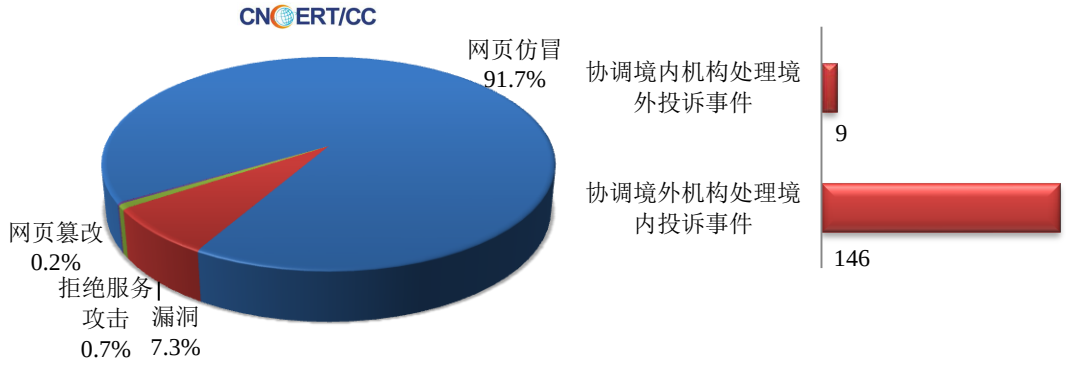
http://www.cnvd.org.cn/webinfo/list?type=4

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

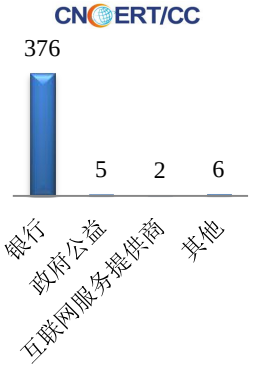
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 424 起，其中跨境网络安全事件 155 起。

本周CNCERT处理的事件数量按类型分布
(4/2-4/8)

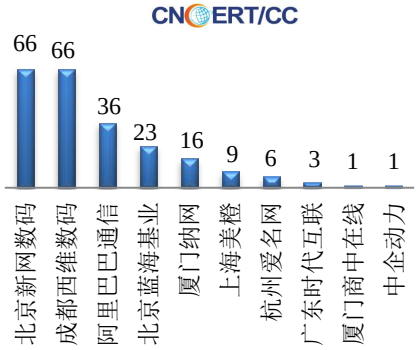


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 389 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 376 起和政府公益仿冒事件 5 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(4/2-4/8)



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 (4/2-4/8)



业界新闻速递

1、公安部拟规定：窃取个人信息不构成犯罪也处罚

央广网 4 月 7 日消息 近日，公安部就《公安机关互联网安全监督检查规定（征求意见稿）》公开征求意见，《规定》拟于近期颁布实施。征求意见稿指出，在国家重大网络安全保卫任务期间，公安机关对与国家重大网络安全保卫任务相关的互联网服务提供者和联网使用单位，可以组织开展专项检查。而互联网服务提供者窃取、非法出售、非法提供个人信息，即使尚不构成犯罪，没有违法所得，也将被处以最高一百万元以下罚金。

2、美网络司令部颁布最新“指挥”战略

E 安全 4 月 2 日消息 美国网络司令部近日发布了一项新的战略——《实现和维护网络空间优势：美国网络司令部指挥愿景》（以下简称“指挥愿景”），该战略涉及了美国网络司令部的目的、方式和手段。该司令部“指挥愿景”的发布，标志着美网络空间领域作战和战略思维的重大变革，也将为全球数字安全和网络环境的稳定发展带去积极影响。美国网络司令部的新战略也涉及了如何防范和遏制他国侵蚀美国在网络空间这一领域绝对优势的相关内容。该新战略指出，在过去十年中网络空间领域的战略背景和作战环境发生了巨大的变化。美国网络司令部此次发布的新战略在这一基础上给出了一个全面的应对方案。新战略的有效实施需要美国政府和学术界大胆运用新思维，以规划出正确的组织结构、制定出高效的决策过程和能力提升路径。这些都为新的网络思维奠定了基础。

3、特朗普签署《澄清境外数据合法使用法案》

E 安全 4 月 8 日消息 特朗普于美国当地时间 2018 年 3 月 23 日签署《澄清境外数据合法使用法案》（又被称为《云法案》 ），这使得美国执法机构更易跨境调取其公民海外信息，FBI 将可凭借一纸传票，收集来自其

他国家的电子邮件和个人信息，从而避开这个国家的隐私保护法和法律制度。然而，隐私保护组织却颇有顾虑。他们担心美国与其他国家签署双边协议交出数据时，数据可能会被他国政府恶意利用。

4、力保东京奥运会 日本警视厅整合相关部门保障网络安全

环球网报 4 月 2 日消息 为力保 2020 年东京奥运会顺利举行，日本警视厅于 4 月 2 日宣布，将下属所有应对黑客攻击及网络犯罪的部门进行整合，为网络安全保障部门开辟专属办公楼。警视厅 2 日举行了新办公楼的开幕仪式。据日本 NHK 电视台报道，日本警视厅此举整合了以往分散在东京各处的 6 个部门、500 余名警察，并将其调动至一处办公。新办公地名为“网络安全大厦”，位于东京文京区，其具体位置不对外公开。

5、伊朗 3500 台路由器遭黑客攻击：字符组成一面美国国旗

新浪网 4 月 8 日消息 “不要干预我们的选举”。当地时间 7 日，黑客侵入了一些国家的计算机系统，在电脑屏幕上留下了这句话，和一面用字符组成的美国国旗。据伊朗国家通讯社（IRNA）4 月 7 日报道，伊朗信息与通信技术部的一份声明显示，全球约有 20 万台路由器交换机受到此次黑客攻击的影响，伊朗约有 3500 台路由器受攻击。此外，一些欧洲国家和印度也受到此次攻击的影响。声明称，此次袭击中，黑客攻击了互联网服务供应商，中断了用户的网络访问。据路透社报道，黑客攻击了思科路由器中的一个漏洞，该公司早些时候发布了警告并更新补丁。但由于伊朗正处于伊历新年假期，一些公司尚未安装补丁。周六晚间，思科公司声明称，上述消息是为客户识别弱点，并排除网络攻击的威胁。3 月 28 日，思科曾发布漏洞修复补丁。

6、芬兰超 13 万公民明文密码及机密信息被泄

E 安全 4 月 8 日消息 根据芬兰媒体 Svenska Yle 的报道，超过 13 万名芬兰公民似乎已经成为了数据泄露事件的最新受害者。而从受害者数量来看，这将是该国有史以来发生的第三大数据泄露事件。芬兰通信管理局（FICORA）于本周五通过自己的网站向所有芬兰公民发出警告称，一个由赫尔辛基新企业中心（“Helsingin Uusyrityskeskus”）负责维护的网站（liiketoimintasuunnitelma[.]com）在本周二遭遇了匿名黑客的攻击，大约有 13 万用户的账户用户名和密码被窃取，同时被窃取的还包括其他一些机密信息。

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：胡俊

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158