国家互联网应急中心

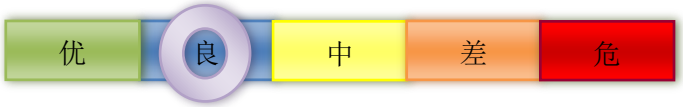
2018 年第 17 期

4 月 23 日-4 月 29 日

网络安全信息与动态周报

CNCERT/CC

本周网络安全基本态势

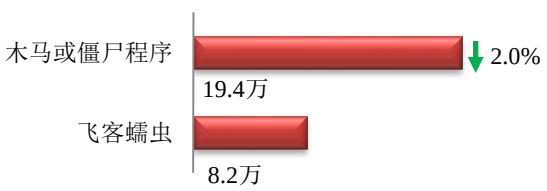


境内感染网络病毒的主机数量	•27.6万	
境内被篡改网站总数 其中政府网站数量	•978 •23	↓22.7% ↓30.3%
境内被植入后门网站总数 其中政府网站数量	•1046 •18	↓19.2% ↓50.0%
针对境内网站的仿冒页面数量	•821	↓2.5%
新增信息安全漏洞数量 其中高危漏洞数量	•400 •136	↑61.3% ↑70.0%

=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

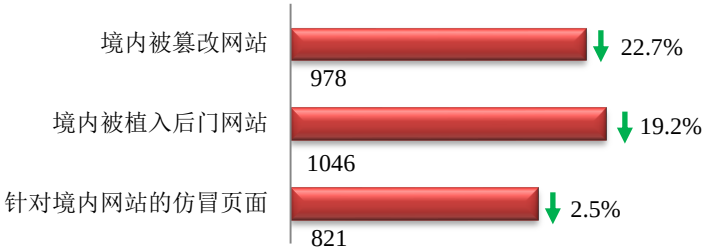
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 27.6 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 8.2 万。



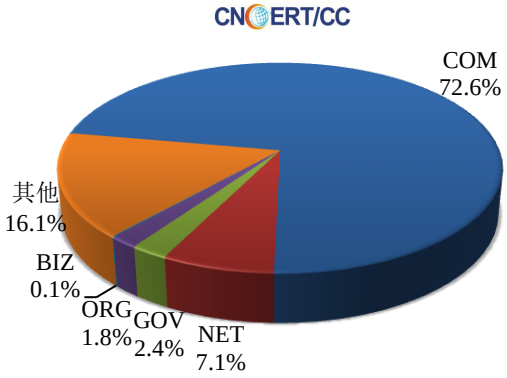
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 978 个；境内被植入后门的网站数量为 1046 个；针对境内网站的仿冒页面数量为 821。

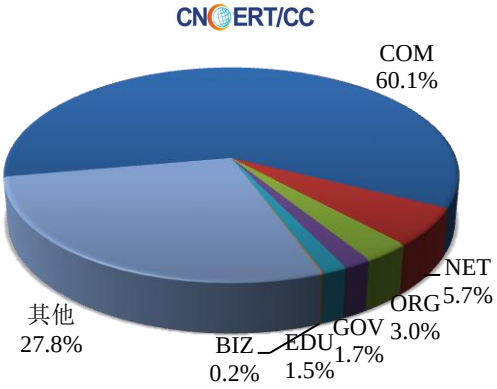


本周境内被篡改政府网站（GOV 类）数量为 23 个（约占境内 2.4%），较上周环比下降了 30.3%；境内被植入后门的政府网站（GOV 类）数量为 18 个（约占境内 1.7%），较上周环比下降了 50.0%；针对境内网站的仿冒页面涉及域名 372 个，IP 地址 136 个，平均每个 IP 地址承载了约 6 个仿冒页面。

本周我国境内被篡改网站按类型分布
(4/23-4/29)

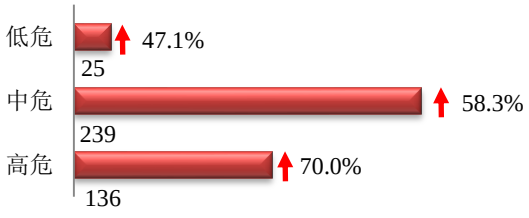


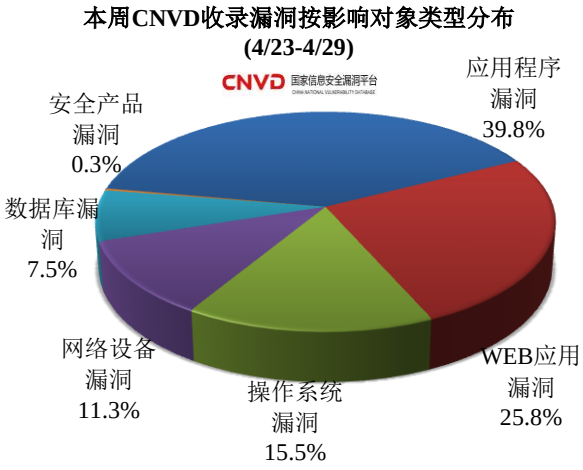
本周我国境内被植入后门网站按类型分布
(4/23-4/29)



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 400 个，信息安全漏洞威胁整体评价级别为中。





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 应用漏洞和操作系统漏洞。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

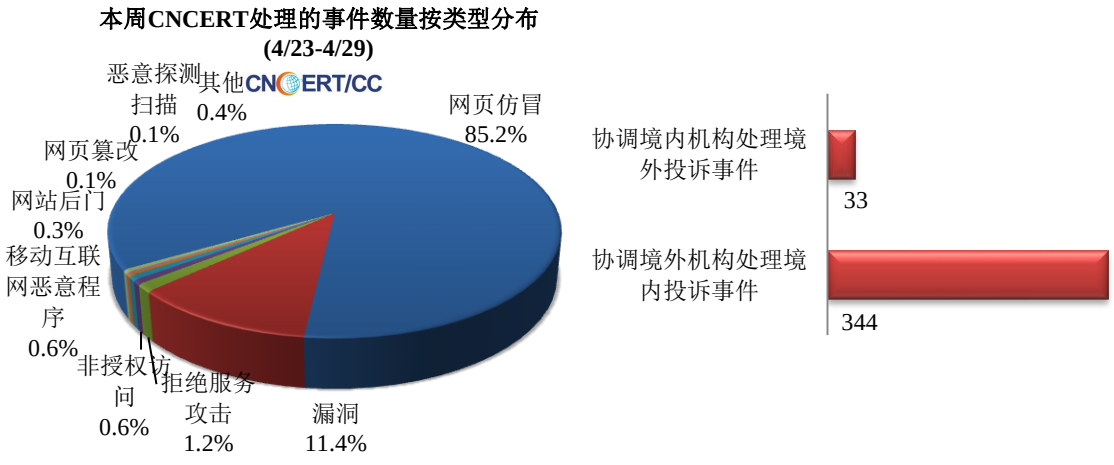
CNVD漏洞周报发布地址

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。

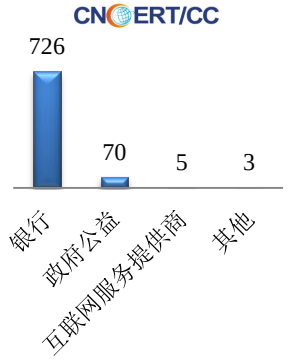
本周事件处理情况

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 944 起，其中跨境网络安全事件 377 起。

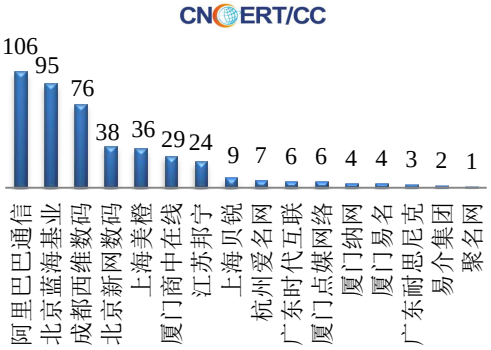


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 804 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 726 起和政府公益仿冒事件 70 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(4/23-4/29)

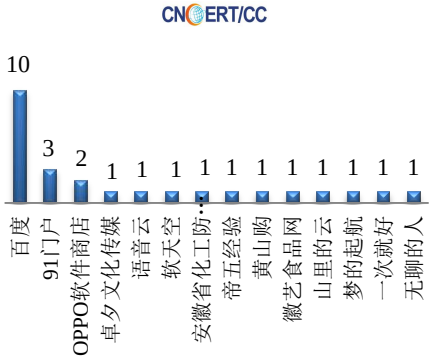


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (4/23-4/29)



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 26 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 (4/23-4/29)



业界新闻速递

1、第五届首都网络安全日于 4 月 27 日开幕

新浪网 4 月 27 日消息 在北京市委、市政府的领导下，市委网信办、市公安局主办的第五届首都网络安全日于 4 月 27 日在北京展览馆盛大开幕。本届活动以“新时代网络安全”主论坛为引领，融合北京国际互联网科技博览会、新时代网络安全系列高峰论坛、网络安全技术大赛、“净网 2018”主题宣传等系列特色活动，全程自 26 日至 28 日共计 3 天。大会主论坛以启迪•未来——“新时代的网络安全”为主题，于 4 月 27 日上午在北京展览馆 7 号馆举行。论坛演讲嘉宾包括来自美国、俄罗斯、以色列等国家的世界知名专家、政界高层、学界泰斗和商界精英，分享了全球互联网+时代背景下人工智能技术为网络安全领域带来的新思路、新技术、新手

段，破局当下网络安全存在的威胁与挑战。系列分论坛从人工智能、云计算、数据保护、区块链等技术角度及空间安全战略、关键信息基础设施等级保护、未知威胁防控策略等战略制定的角度，全方位对网络安全的现状做出了分析，对未来发展趋势展开了深入探讨。

2、英国政府承诺提供资金用于帮助各英联邦国家提升网络安全水平

E 安全 4 月 25 日消息 英国政府已经承诺提供 1500 万英镑（约合人民币 1.33 亿元）资金，用于帮助各英联邦国家提升网络安全水平，这笔资金还将用于应对在全球范围内造成安全威胁的各犯罪集团以及敌对国家实体，其中亦涵盖英国本土。在 2018 年 4 月举行的英国联邦政府首脑会议（简称 CHOGM）上，53 个英联邦国家的首脑已签署一份网络声明《英联邦网络宣言》，这将成为世界上规模最大且地域多样化的政府间网络安全合作承诺。英国政府在公布这一消息时同时指出，其支持其它各国建立网络应变能力的举措，将有助于防止犯罪分子及敌对国家实体发动针对各类目标的网络攻击活动。这份《英联邦网络宣言》首次提出在整个英联邦范围内以自由开放方式保障互联网安全这一共同愿景，以帮助各成员国提升自身网络安全水平，同时加强合作以打击那些试图破坏其国家价值观、安全甚至是选举完整性的恶意行为者。这笔 1500 万英镑的资金还将帮助各英联邦国家预防并应对可能对政府、企业及公民造成影响的网络安全风险。

3、欧洲刑警组织宣布关闭出售 DDoS 网络攻击的网站 Webstresser.org

cnBeta.COM4 月 26 日消息 据外媒报道，当地时间周三上午，欧洲刑警组织宣布关闭了 Webstresser.org——一个明码标价出售 DDoS 网络攻击的网站。据欧洲刑警披露，该网站总共有 13.6 多万名用户，截止到 4 月前总共发起了 400 万起网络攻击。欧洲刑警称，Webstreeser 曾是全球最大的 DDoS 服务供应商，在这个网站被捣毁之前它曾攻击过银行、警察局、政府以及游戏网站。去年 7 月，英国最大的 7 家银行就遭到了来自 Webstresser 的网络攻击并最终迫使整个系统关闭造成数十万美元的经济损失。据《福布斯》披露，美国人是最主要的攻击对象和客户。除了捣毁网站，警方还逮捕了该网站在英国、克罗地亚、加拿大以及塞尔维亚的四名管理者，另外位于荷兰、意大利、西班牙、澳大利亚等高级客户也被逮捕，而该网站设立在荷兰、美国、德国的基础设施也已被查封。

4、印度某政府网站发生数据泄露事件

E 安全 4 月 25 日消息 据印度媒体 Medianama 的报道，安全研究员 Srinivas Kodali 在本周一报告了一起数据泄露事件，受影响的是一个隶属印度安得拉邦的政府网站。由于泄露的敏感性，Kodali 决定暂时不会公布该网站的名称，直到数据得到安全保护。根据 Kodali 的描述，遭泄露的数据包括 Aadhaar 号码、银行分行、IFSC 代码和帐号、姓名、地址、身份证号码、手机号码、配给卡号码、职业、宗教信仰和种姓信息。通过 Kodali 提供的屏幕截图，我们还可以看出，该网站存储有大量与个人信息相关的数据。而其提供的工具允许通过输入关键词来进行搜索，并会在结果返回列表中罗列出所有与之相关的信息。Kodali 强调，具备生成这种列表的能力意味着这种泄露并不“轻微”，这些信息完全可以被用来锁定某个单一的个人。另外，这个数据库是公开可用的，并且允许任何人在未经授权的情况下访问。MediaNama 与 Kodali 进行了交谈，他表示，仍然没有办法向政府和 UIDAI 报告这些数据泄露。在他发布了有关数据泄露的消息后，有人从数据库中屏蔽了 Aadhaar 数据。然而，剩余的其他所有数据仍可被公开访问。

5、乌克兰能源和煤炭工业部网站遭黑客攻击

新华网 4 月 26 日消息 乌克兰能源和煤炭工业部网站 4 月 24 日遭黑客攻击。网站瘫痪，主页被锁定为要求支付赎金的页面。路透社报道，乌克兰能源和煤炭工业部网站受到勒索软件攻击，主页留下要求支付比特币赎金的英文信息，以此换取解锁文件。乌克兰网络警察部门发言人尤利娅·克维特科说，就已知信息而言，能源和煤炭工业部受到攻击是一起孤立事件，不构成大规模网络攻击。乌克兰政府的其他部门和机构网站没有遭遇类似状况。路透社援引克维特科的话报道："这起事件并非大规模攻击。如果必要，我们会随时反应并施以援手。"

6、迪拜打车巨头公司 Careem Networks 遭遇网络攻击，导致 1400 万乘客的信息失窃

腾讯网 4 月 24 日消息 据外媒报道，迪拜打车巨头 Careem Networks 周一宣布，公司在今年 1 月遭遇了一次网络攻击，导致 1400 万乘客的信息失窃。Careem 是 Uber 在中东地区最主要的竞争对手。该公司在一份声明中表示，公司已经获悉，一个用于存储客户和司机帐户信息的计算机系统在今年 1 月 14 日被黑客攻破。它说，虽然没有证据表明在外部第三方服务器上保存的密码或信用卡信息被泄露，但是现在可以肯定的是，1400 万用户的姓名、电子邮箱地址、手机号和旅行数据已经被泄露了。该公司发言人表示，在攻击发生的时候，该公司在中东地区的 78 个城市运营，其平台拥有 1400 万用户和 55.8 万司机。攻击发生后注册的新用户没有受到影响。

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：吕利锋

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158