国家互联网应急中心

2018 年第 19 期

5 月 7 日-5 月 13 日

网络安全信息与动态周报

本周网络安全基本态势

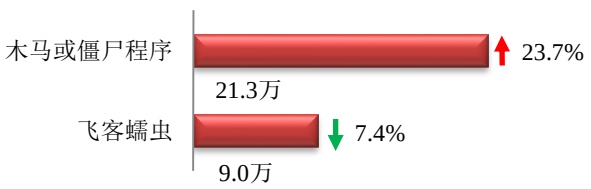
优 | 良 | 中 | 差 | 危

境内感染网络病毒的主机数量	•30.3万	↑ 12.5%
境内被篡改网站总数 其中政府网站数量	•1092 •33	↑ 5.0% ↓ 5.7%
境内被植入后门网站总数 其中政府网站数量	•942 •28	↑ 13.4% ↑ 33.3%
针对境内网站的仿冒页面数量	•1430	↓ 9.4%
新增信息安全漏洞数量 其中高危漏洞数量	•260 •62	↑ 6.6% ↓ 21.5%

═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

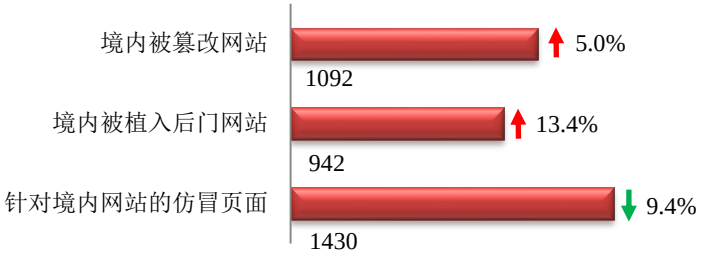
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 30.3 万个，其中包括境内被木马或被僵尸程序控制的主机约 21.3 万以及境内感染飞客（conficker）蠕虫的主机约 9.0 万。



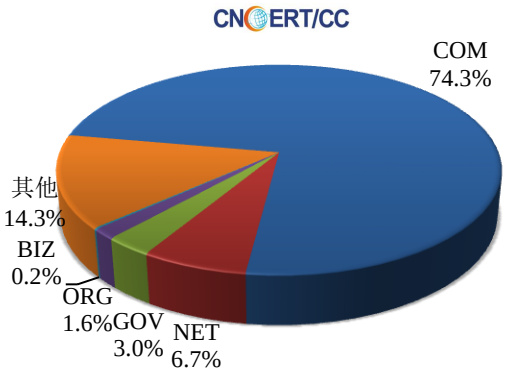
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1092 个；境内被植入后门的网站数量为 942 个；针对境内网站的仿冒页面数量为 1430。

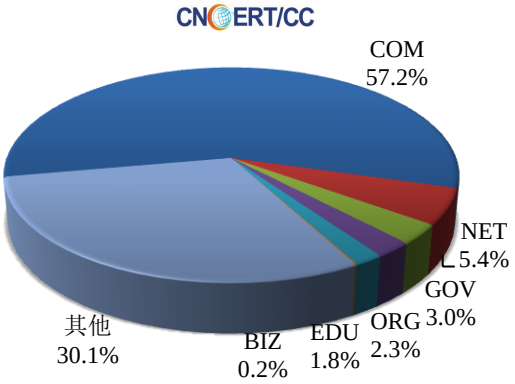


本周境内被篡改政府网站（GOV 类）数量为 33 个（约占境内 3.0%），较上周环比下降了 5.7%；境内被植入后门的政府网站（GOV 类）数量为 28 个（约占境内 3.0%），较上周环比下降了 33.3%；针对境内网站的仿冒页面涉及域名 540 个，IP 地址 282 个，平均每个 IP 地址承载了约 5 个仿冒页面。

本周我国境内被篡改网站按类型分布
(5/7-5/13)

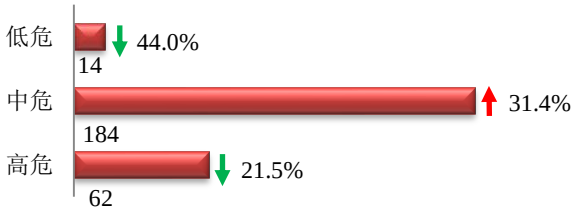


本周我国境内被植入后门网站按类型分布
(5/7-5/13)

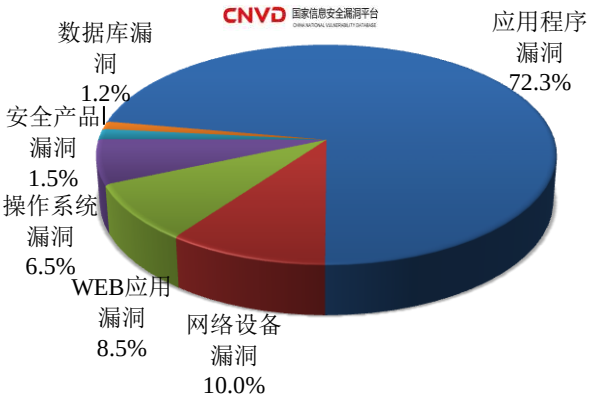


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 260 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
(5/7-5/13)



本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是网络设备漏洞和 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

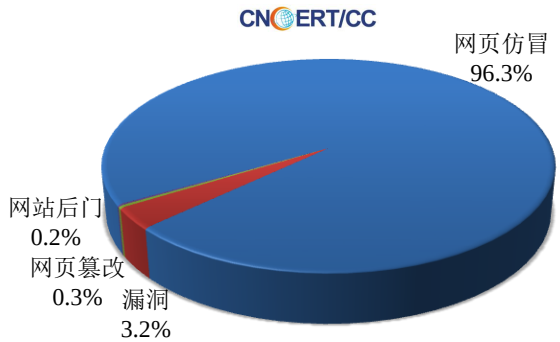
http://www.cnvd.org.cn/webinfo/list?type=4

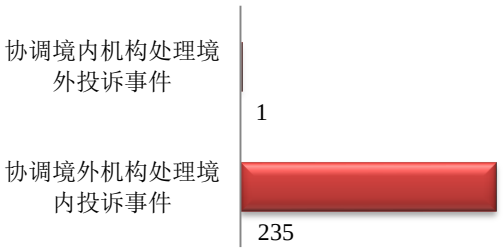
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 1031 起，其中跨境网络安全事件 236 起。

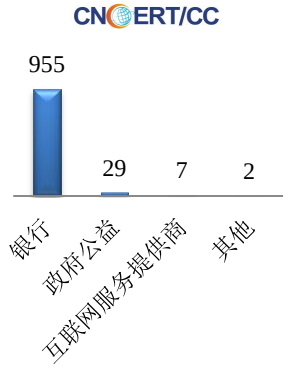
本周CNCERT处理的事件数量按类型分布
(5/7-5/13)



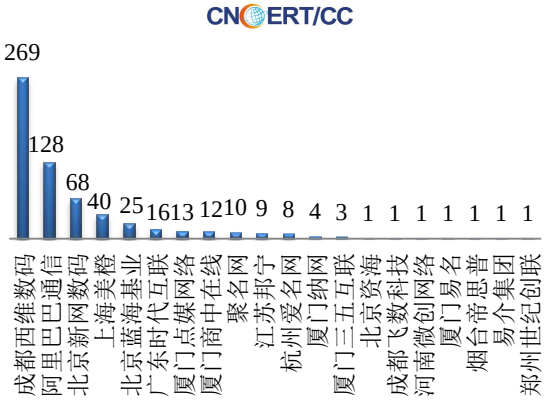


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 993 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 955 起和政府公益仿冒事件 29 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(5/7-5/13)

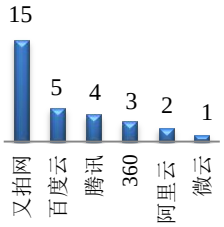


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (5/7-5/13)



本周，CNCERT 协调 6 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 30 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 (5/7-5/13)



业界新闻速递

1、工信部六措施落实 IPV6 规模部署行动计划

新华网 5 月 9 日消息 近日，为贯彻落实中共中央办公厅、国务院办公厅印发的《推进互联网协议第六版（IPv6）规模部署行动计划》（厅字〔2017〕47 号，以下简称《行动计划》），加快网络基础设施和应用基础设施升级步伐，促进下一代互联网与经济社会各领域的融合创新，工信部发布了关于贯彻落实《行动计划》的通知。据了解，工信部将从六方面组织实施工作，包括：实施 LTE 网络端到端 IPv6 改造；加快固定网络基础设施 IPv6 改造；推进应用基础设施 IPv6 改造；开展政府网站 IPv6 改造与工业互联网 IPv6 应用；强化 IPv6 网络安全保障；落实配套保障措施。按通知要求，2018 年是涉及工信部相关 IPV6 任务的重要时间节点。通知明确，到 2018 年

末，基础电信企业完成全国范围 LTE 核心网、接入网、承载网、业务运营支撑系统等 IPv6 改造并开启 IPv6 业务承载功能，为移动终端用户数据业务分配 IPv6 地址，提供端到端的 IPv6 访问通道；移动互联网 IPv6 用户规模不少于 5000 万户（基础电信企业已分配 IPv6 地址且一年内有 IPv6 上网记录的用户）；完成北京、上海、广州、郑州、成都的互联网骨干直联点 IPv6 改造，开通 IPv6 网间互联带宽不少于 1Tbps。此外，通知还表示，工信部将成立 IPv6 督查工作专家组，研究制定推进 IPv6 规模部署相关任务完成情况的考核标准，并将定期组织开展专项督查工作，就 LTE 网络 IPv6 端到端贯通、固定网络基础设施改造、应用基础设施改造、强化网络安全保障等重点任务进行分项考核。

2、美网络司令部“网络整合中心”落成

E 安全 5 月 10 日消息 当地时间 2018 年 5 月 4 日，美国国家安全局（NSA）和网络司令部（USCYBERCOM）的领导为网络整合中心（Integrated Cyber Center，简称 ICC）落成剪彩，负责整合美国及盟国网络行动的联合作战中心正式竣工。网络整合中心（ICC）是美国联邦政府为美国间谍和网络战士打击外国网络威胁配备的新物理基础设施，该中心位于美国马里兰州米德堡（NSA 总部所在地）。ICC 将更好地同步和协调 NSA、网络司令部、美国其它政府机构及其盟国伙伴之间的网络行动，以消除分歧。该中心将于 2018 年 8 月全面运作。美国高级官员希望 ICC 能有效帮助 NSA 与美国网络司令部轻松协调相关网络工作。美国打造 ICC 的目标是集中组织不同机构和军事部门的代表，加强跨政府合作。ICC 的主要任务之一是，当政府机构在网络行动上出现意见分歧时，ICC 将负责协调，解决分歧。

3、美国白宫成立人工智能特别委员会

新浪网 5 月 11 日消息 北京时间 5 月 11 日凌晨消息，本周四，美国白宫举办了一场由人工智能领域的专家参与的科技峰会，在次会议上，白宫科技政策办公室副主任迈克尔·克拉希欧斯（Michael Kratsios）宣布将组建人工智能特别委员会，该委员会由各政府部门人工智能领域的领先研究者组成。人工智能特别委员会（Select Committee on Artificial Intelligence）将由国家科学与技术委员会（National Science and Technology Council）管理，将主要负责向白宫提供政府层面的有关人工智能研究与发展方面的建议，同时将帮助政府、私企、和独立研究者建立合作伙伴关系。该人工智能特别委员会也将服从 OSTP 的领导，同时，还将与国家自然基金和美国国防部下属研究机构国防部高等研究计划局（Defense Advanced Research Projects Agency，DARPA）进行协作。为了促成一个政府全部门的讨论，该委员会成员还将包括来自国家安全局、联邦首席信息办公室、和管理与预算办公室的官员。

4、欧盟“关键基础设施”NIS 指令 5 月 10 日正式生效

E 安全 5 月 11 日消息 欧盟网络与信息系统（NIS）指令于当地时间 2018 年 5 月 10 日起正式生效。此项面向欧盟范围内的新法令有望提高关键基础设施相关组织的 IT 安全性，同时亦将约束各搜索引擎、在线市场以及其它对现代经济拥有关键性影响的组织机构。NIS 指令侧重于保障欧盟国家电力、交通以及医疗卫生等领域关键基础设施的安全性，其力图通过加强网络防御能力以提升此类服务的安全性与弹性。NIS 指令将覆盖一切被认定对欧盟国家基础设施拥有重要影响的组织机构，例如各在线市场、搜索引擎以及关键基础设施供应商。根据英国国家网络安全中心（NCSC）官网上公布的信息，此项指令要求各欧盟成员国建立国家网络安全战略、

计算机安全事件应急小组（CSIRT）和国家 NIS 主管部门。各欧盟国家之间亦应开展合作，旨在共享与网络攻击相关的信息。此外，各国还必须确定关键组织或“基础服务运营商（OES）”名单。这些 OES 必须采取适当的安全措施以管理其网络与信息系统风险，同时就出现的严重安全事件向相关国家主管部门进行通报。在英国，OES 名单可能涵盖饮用水供应商，数字基础设施卫生部门，空运、海运、公路运输以及铁路运输系统，云服务，网上市场以及搜索引擎等领域，亦将充分保护金融与民用核能等行业免受网络攻击影响。

5、巴基斯坦数百万公民信息网上公开售卖，售价 1 美元

E 安全 5 月 9 日消息 根据巴基斯坦“Techjuice”网站在本周一（5 月 7 日）发表的一篇文章来看，数百万巴基斯坦公民的个人敏感信息正在不同的社交媒体平台上被出售，而这些信息在巴基斯坦国内网站上的售价仅为 100 卢比，即 1 美元。在 2017 年 8 月，一家当地媒体报道，旁遮普省信息技术委员会（PITB）意外暴露了成千上万巴基斯坦公民的个人敏感信息，这些数据由 CNIC（巴基斯坦国家身份证号码）和其他个人文件的扫描件组成。根据 PITB 在当时的说法，数据泄露是由于一个应用程序漏洞导致的，而这个漏洞已经被修复，但并没有对泄露的数据进行置评。而现在，也就是在该事件发生的 9 个月之后，PITB 再次被推向了舆论的风口浪尖。因为有很多人开始怀疑，通过 PITB 网站泄露的数据正在被公开出售。不仅如此，被出售的数据还包括由巴基斯坦国家数据库和注册局（National Database and Registration Authority，NADRA）持有的个人和家庭数据、警方追踪的犯罪记录、由电信公司记录的通话数据以及其他一些由政府机构持有或私营公司持有的数据，而这些数据泄露的根源似乎都与 PITB 的应用程序漏洞有关。根据 TechJuice 从两个独立实体收到的报告和证据来看，这些敏感信息具体包括：CNIC 信息，短信和通话记录，NADRA 家谱数据，犯罪记录，租赁酒店及酒店游客信息，短信诈骗服务，已注册移动用户的离线数据库。

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：李挺

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158