国家互联网应急中心

网络安全信息与动态周报

2018 年第 21 期

5 月 21 日-5 月 27 日

CNCERT/CC

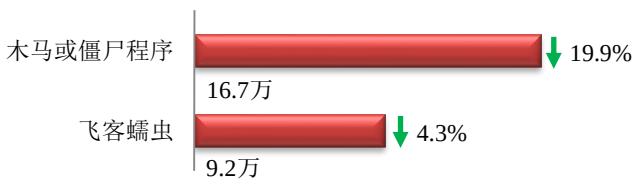
本周网络安全基本态势

境内感染网络病毒的主机数量	•25.9万	15.0%
境内被篡改网站总数 其中政府网站数量	•993 •31	3.9% 3.1%
境内被植入后门网站总数 其中政府网站数量	•824 •37	10.6% 48.0%
针对境内网站的仿冒页面数量	•1947	159.6%
新增信息安全漏洞数量 其中高危漏洞数量	•335 •115	5.1% 22.8%

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*

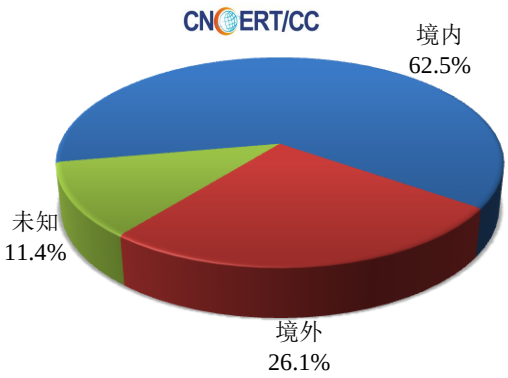
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 25.9 万个，其中包括境内被木马或被僵尸程序控制的主机约 16.7 万以及境内感染飞客（conficker）蠕虫的主机约 9.2 万。

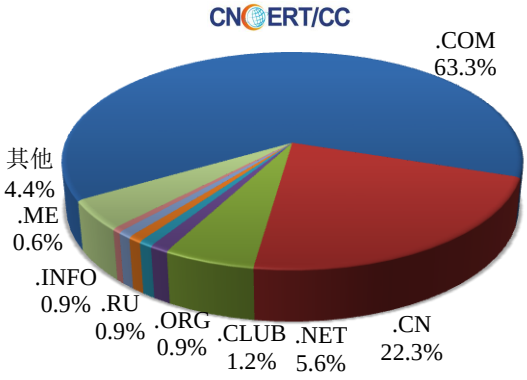


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 341 个，涉及 IP 地址 56971 个。在 341 个域名中，有 26.1%为境外注册，且顶级域为.com 的约占 63.3%；在 56971 个 IP 中，有约 67.3%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 116 个 IP。

本周放马站点域名注册所属境内外分布
(5/21-5/27)



本周放马站点域名所属顶级域的分布
(5/21-5/27)



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。

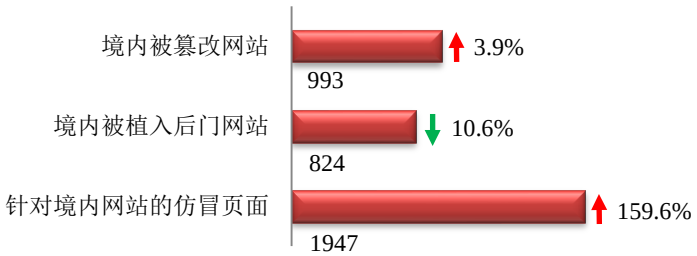
ANVA恶意地址黑名单发布地址

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。

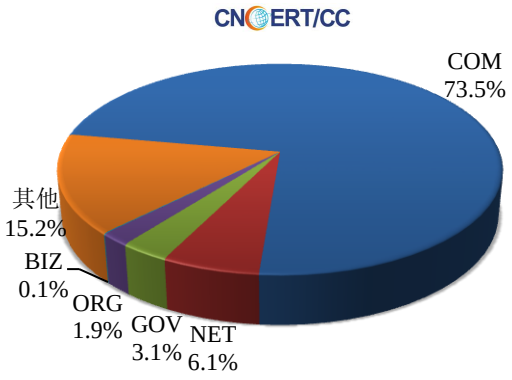
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 993 个；境内被植入后门的网站数量为 824 个；针对境内网站的仿冒页面数量为 1947。

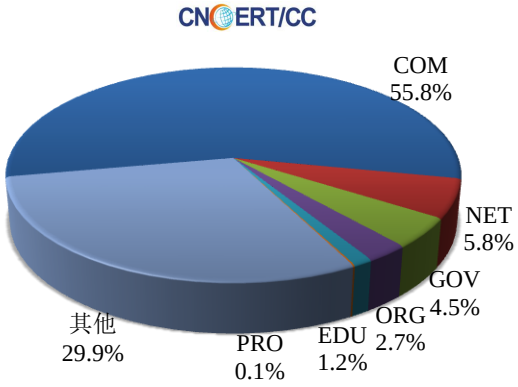


本周境内被篡改政府网站（GOV 类）数量为 31 个（约占境内 3.1%），较上周环比下降了 3.1%；境内被植入后门的政府网站（GOV 类）数量为 37 个（约占境内 4.5%），较上周环比上升了 48.0%；针对境内网站的仿冒页面涉及域名 362 个，IP 地址 187 个，平均每个 IP 地址承载了约 10 个仿冒页面。

本周我国境内被篡改网站按类型分布
(5/21-5/27)

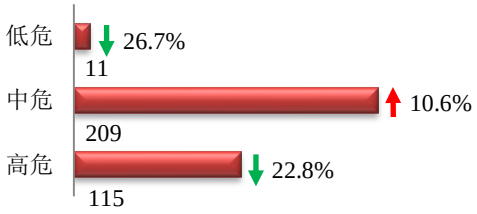


本周我国境内被植入后门网站按类型分布
(5/21-5/27)

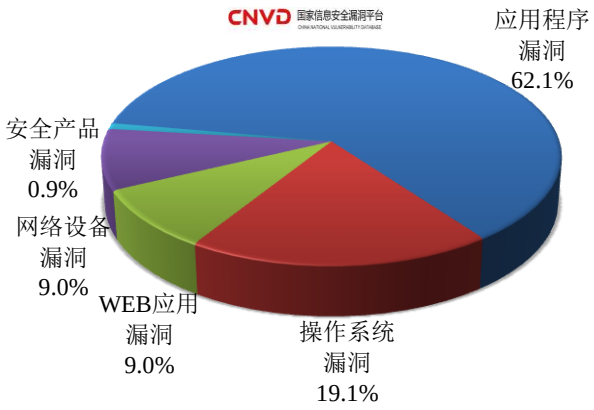


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 335 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
(5/21-5/27)



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

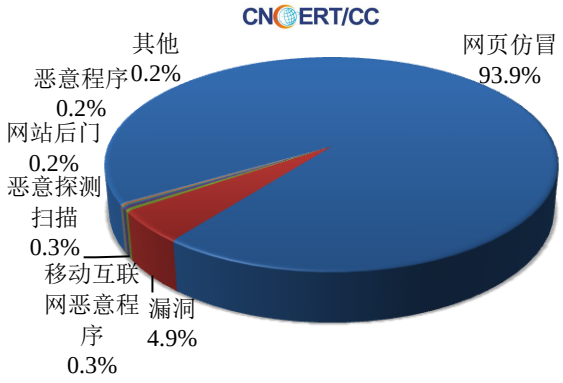
http://www.cnvd.org.cn/webinfo/list?type=4

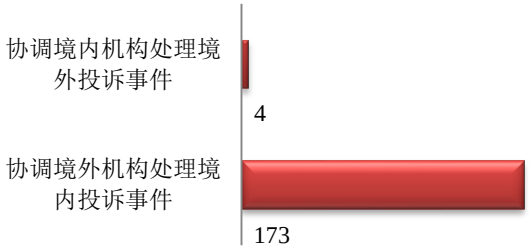
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 595 起，其中跨境网络安全事件 177 起。

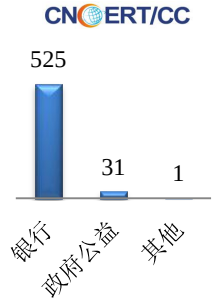
本周CNCERT处理的事件数量按类型分布 (5/21-5/27)



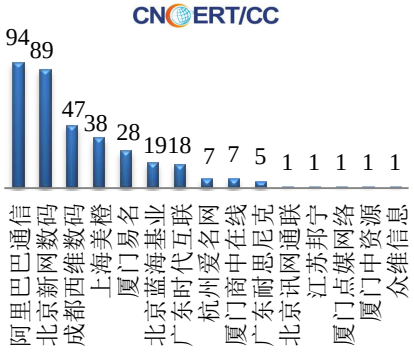


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 557 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 525 起和政府公益仿冒事件 31 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(5/21-5/27)



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 (5/21-5/27)



本周，CNCERT 协调 1 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 1 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
(5/21-5/27)

业界新闻速递

1、网络安全管理局组织召开 2018 年工业互联网安全检查评估工作部署会议

工信部网站 5 月 23 日消息 为深入贯彻落实《关于深化“互联网+先进制造业”发展工业互联网的指导意见》，督促企业切实提升工业互联网安全保障水平，依据《网络安全法》有关规定及工业和信息化部相关职责，部网络安全管理局组织开展了2018年工业互联网安全检查评估工作，并于2018年5月23日召开了工作部署会，全面启动工业互联网安全检查评估工作。会议主要介绍了本次检查评估工作的背景情况、整体安排、主要内容及实施方式，并对专业检查评估机构及被检查企业提出了要求。部网络安全管理局委托 5 家专业检查评估机构对工业企业、工业平台及工业 APP 开展安全检查评估，首批检查涉及 16 家企业。会议要求各单位统一思想，高度重视，全力做好安全检查评估工作。此次检查评估重在了解重点行业、重点领域工业互联网平台、企业、应用等安全情况，掌握我国工业互联网安全现状。专业检查评估机构要认真负责，突出重点，查找薄弱环节，发现工业互联网重点平台、企业、应用的主要风险隐患，督促企业及时整改。工业企业、平台企业应做好配合协调，确保检查评估工作顺利实施。通过检查评估，逐步探索形成“以查促建、以查促管、以查促改、以查促防”的长效工作机制，为下一步构建工业互联网安全保障体系奠定良好基础。

2、工信部加快构建工业互联网安全保障体系

新华网 5 月 25 日消息 工信部网络安全管理局副局长梁斌在 5 月 24 日于北京召开的中国工业信息安全大会上表示，工信部正在加快构建工业互联网安全保障体系，目前已初步形成以健全制度机制、建设技术手段、促进产业发展、强化人才培育四大领域为基本内容的体系架构。梁斌介绍，下一步，工信部将从以下五方面推进我国工业互联网安全保障工作：加强工作指导。加快出台工业互联网安全指导性文件，明确不同主体的安全责任和义务，同步建立健全安全管理制度。发挥标准规范引导作用，编制工业互联网安全系列标准建设指南；建设安全技术保障体系。建设国家、地方、企业三级协同的安全技术保障体系，包括国家工业互联网安全技术保

障平台、安全基础资源库、提升工业互联网安全综合管理和保障能力；建立安全检查机制。近日已全面启动针对工业互联网平台企业、工业企业、工业 APP 和联网设备的安全检查评估，督促企业加强自身安全防护；强化工业互联网数据安全保护。建立工业互联网全产业链数据安全管理体系，明确相关主体的保护责任和具体要求，建立工业数据分级分类管理制度，加强数据安全监督检查；推进工业互联网安全产业发展。组织开展工业互联网安全试点示范。依托国家网络安全产业园等形式，发挥市场主体作用，培育几个有代表性的工业互联网安全龙头企业。

3、美国能源部发布“五年计划”保护网络安全

E 安全 5 月 23 日消息 当地时间 5 月 14 日,美国能源部发布了长达 52 页的美国《能源行业网络安全多年计划》，为美国能源部网络安全、能源安全和应急响应办公室（CESER）勾画了一个“综合战略”，确定了美国能源部未来五年力图实现的目标和计划，以及实现这些目标和计划将采取的相应举措，以降低网络事件给美国能源带来的风险。美国能源部在这份计划中提出了降低网络风险的综合战略，主要涉及两个方面的任务：通过与合作伙伴合作，加强美国当今的能源输送系统安全，以解决日益严峻的威胁并持续改进安全状况；推出颠覆性解决方案，从而在未来开发出具备安全性、弹性和自我防御功能的能源系统。这项综合网络战略设定了三个目标：加强美国能源行业的网络安全防范工作，通过信息共享和态势感知加强当前能源输送系统的安全性；协调网络事件响应和恢复工作；加速颠覆性解决方案的研发与示范（RD&D）工作，以创建更安全、更具弹性的能源系统。

4、美网络司令部 133 支网络任务部队全部实现全面作战能力

E 安全 5 月 21 日消息 当地时间 2018 年 5 月 17 日，美国国防部网络司令部官员称，美网络司令部下的 133 支网络任务部队（CMF，包括陆军 41 支，海军 40 支，空军 39 支，海军陆战队 13 支）已全部实现全面作战能力。美国网络司令部提前实现全面作战能力，证明军方实现了其此前的承诺，即国家网络部队经过充分训练和武装后具备保卫国家网络空间安全的能力。为了达到全面的作战能力，各小组必须满足一系列严格的标准，包括认可的行动理念以及获得高比例的培训、资质和认证的人员。作为认证过程的一部分，训练各小组成员必须要在模拟的真实环境下完成任务以通过这项专项训练。美国网络司令部的官员们强调，虽然实现全面作战能力具有里程碑式的意义，但未来仍有很多工作要做。现在，准备执行任务及持续优化任务成果已转变为工作重点。随着网络任务部队的建立，美军正在快速将这股新生力量转换为可持续的战备力量。

5、欧洲议会颁布 GDPR 法案将生效 助推网络安全保险市场

新浪网 5 月 21 日消息 5 月 21 日消息，欧洲议会颁布的《一般数据保护法案》（General Data Protection Regulation（GDPR））将于 2018 年 5 月 25 日在欧盟各国正式生效。该法案把可以直接或间接识别到的某一个个体的任何信息都视为个人信息，包括了从姓名、照片、身份证号、邮箱地址、银行账户、健康记录到网络用户名、位置定位、社交媒体发布的信息、计算机 IP 地址等各个方面，堪称目前世界范围内最宽泛的个人信息定义。作为一部用来保护欧盟公民个人隐私和数据安全的新法案，其颁布使得欧盟对于数据保护的监管达到了前所未有的高度。GDPR 不仅适用于在欧盟国家注册的组织机构， 也同样适用于任何在欧盟以外地区注册但为欧盟地区提供商品和服务， 并监控个人行为和数据信息的组织机构。对于任何持有和处理欧盟国家公民个人信息

的公司无论其公司所在地，皆受该法案管辖。

6、英国政府将出台“网络安全法”以规范互联网

HackerNews.cc5 月 22 日消息 根据英国政府发布的新闻稿，“约 60%的人”表示他们在网上目击了不适当或有害的内容，“40%的人”表示他们经历过网络暴力。英国数字国务部长马特·汉考克（Matt Hancock）认为互联网的“狂野西部”本质是危险的，需要加强监管。因此，该国将出台新的网络安全法律来保护用户。在上述新闻稿中，英国政府表示即将出台的立法将旨在保护儿童不受利用，防止网络欺凌，并停止在线恐怖主义。英国政府今年晚些时候将出版一份关于即将出台的立法的白皮书。

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：李世淙

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158