国家互联网应急中心

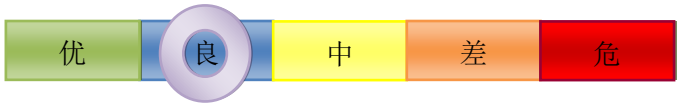
网络安全信息与动态周报

2017 年第 38 期

9 月 11 日-9 月 17 日

CNCERT/CC

本周网络安全基本态势

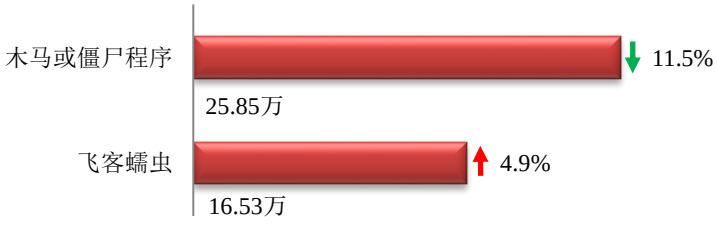


境内感染网络病毒的主机数量	•42.38万	5.7%
境内被篡改网站总数 其中政府网站数量	•2,066 •53	17.8% 3.6%
境内被植入后门网站总数 其中政府网站数量	•917 •54	20.2% 63.6%
针对境内网站的仿冒页面数量	•297	21.4%
新增信息安全漏洞数量 其中高危漏洞数量	•450 •178	34.3% 89.4%

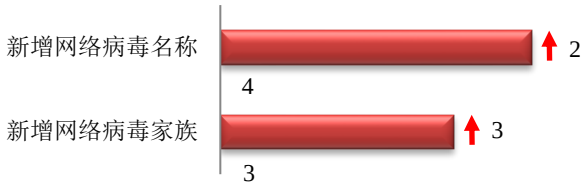
表示数量与上周相同 *表示数量较上周环比增加* *表示数量较上周环比减少*

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 42.38 万个，其中包括境内被木马或被僵尸程序控制的主机约 25.85 万以及境内感染飞客（conficker）蠕虫的主机约 16.53 万。

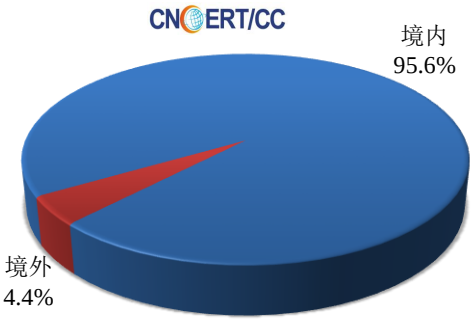


本周 CNCERT 捕获的新增网络病毒文件，按网络病毒名称统计新增 4 个，按网络病毒家族统计新增 3 个。

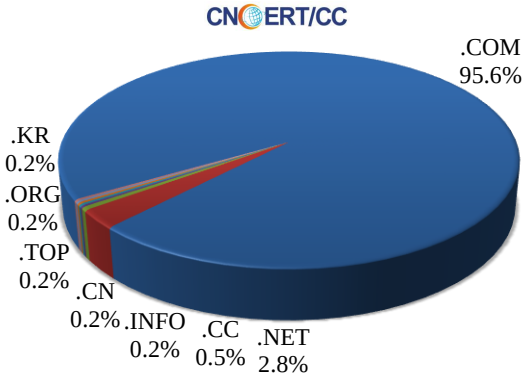


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 435 个，涉及 IP 地址 410 个。在 435 个域名中，有 4.4%为境外注册，且顶级域为.com 的约占 95.6%；在 410 个 IP 中，有约 2.4%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 4 个 IP。

本周放马站点域名注册所属境内外分布
(9/11-9/17)



本周放马站点域名所属顶级域的分布
(9/11-9/17)



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。

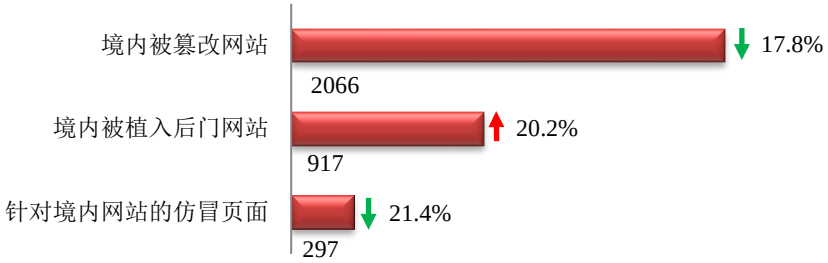
ANVA恶意地址黑名单发布地址

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。

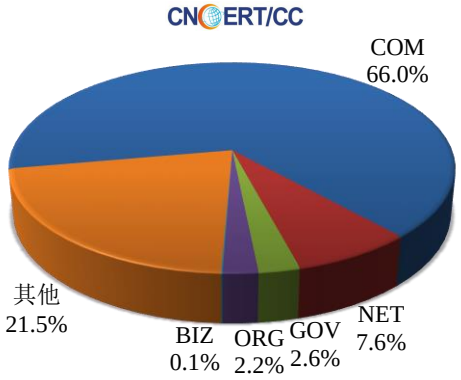
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 2066 个；境内被植入后门的网站数量为 917 个；针对境内网站的仿冒页面数量为 297。

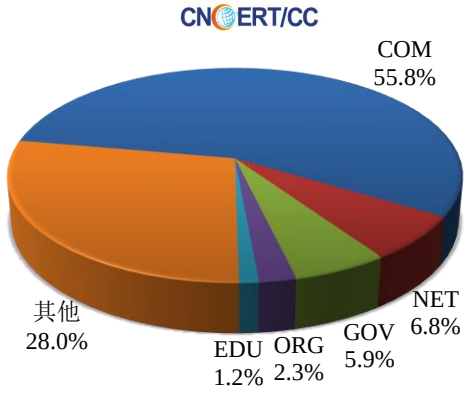


本周境内被篡改政府网站（GOV 类）数量为 53 个（约占境内 2.6%），较上周环比下降了 3.6%；境内被植入后门的政府网站（GOV 类）数量为 54 个（约占境内 5.9%），较上周环比上升了 63.6%；针对境内网站的仿冒页面涉及域名 257 个，IP 地址 122 个，平均每个 IP 地址承载了约 2 个仿冒页面。

本周我国境内被篡改网站按类型分布
(9/11-9/17)

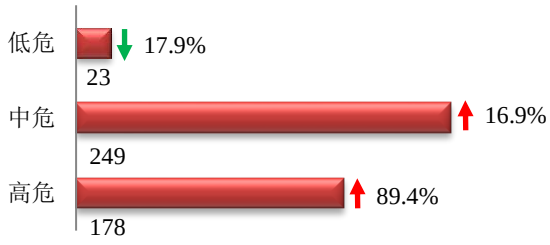


本周我国境内被植入后门网站按类型分布
(9/11-9/17)

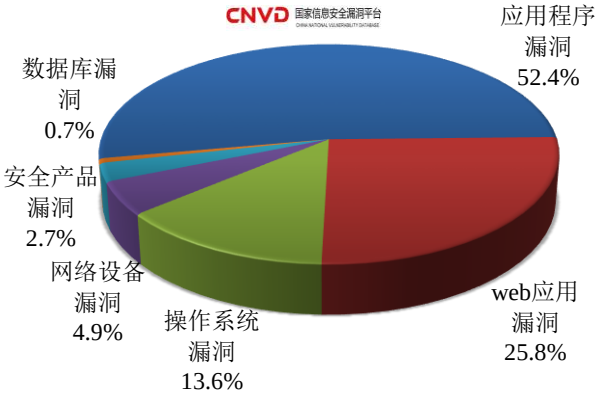


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 450 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
(9/11-9/17)



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

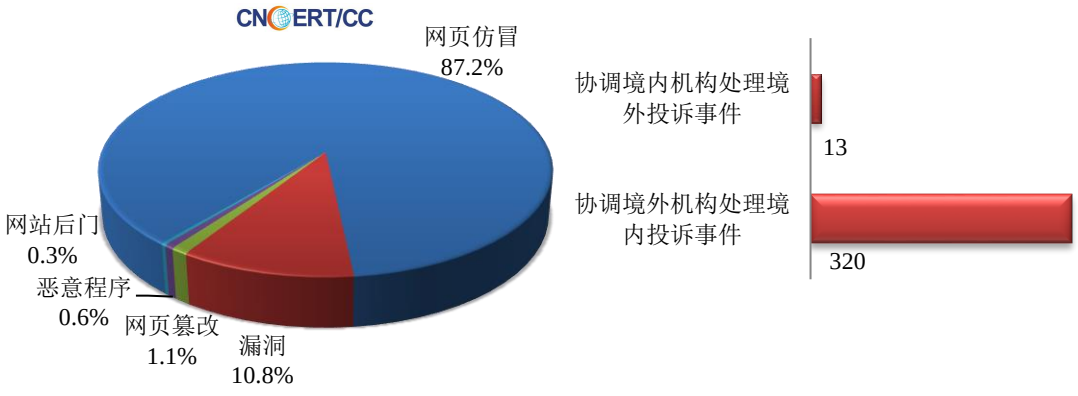
http://www.cnvd.org.cn/webinfo/list?type=4

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

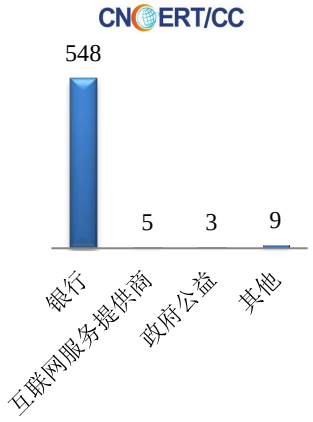
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 648 起，其中跨境网络安全事件 333 起。

本周CNCERT处理的事件数量按类型分布
(9/11-9/17)

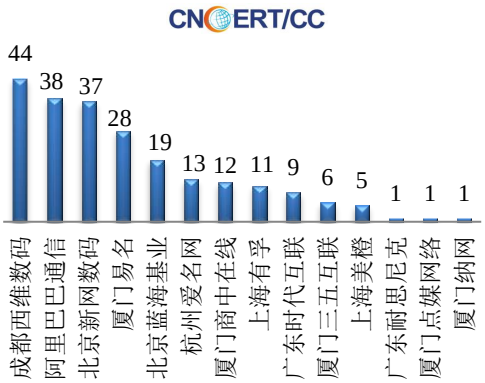


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 565 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 548 起和互联网服务提供商仿冒事件 5 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(9/11-9/17)

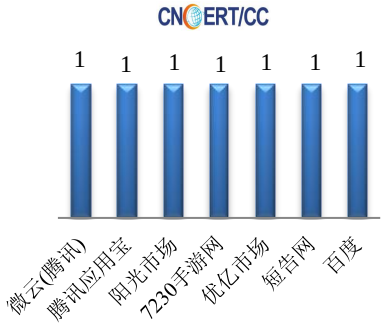


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (9/11-9/17)



本周，CNCERT 协调 7 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 7 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 (9/11-9/17)



业界新闻速递

1、工信部发布《公共互联网网络安全威胁监测与处置办法》

中国网 9 月 15 日消息 记者 9 月 14 日从工信部获悉，工信部制定印发《公共互联网网络安全威胁监测与处置办法》，对公共互联网上存在或传播的、可能或已经对公众造成危害的网络资源、恶意程序、安全隐患或安全事件监测处置，并建立网络安全威胁信息共享平台，集成合力维护网络安全。工信部提出，公共互联网网络安全威胁既包括被用于实施网络攻击的恶意 I P地址、恶意域名、恶意电子信息、恶意程序等，也包括网络服务和产品中存在的安全隐患以及网络安全事件。这些一旦被发现认定，将采取停止服务、屏蔽、清除、通报等

措施。工信部提出建立网络安全威胁信息共享平台，统一汇集、存储、分析、通报、发布网络安全威胁信息，制定相关接口规范，与相关单位网络安全监测平台实现对接。工信部网络安全管理局局长赵志国表示，工信部将完善危险监测处置、数据保护、新技术、新业务安全评估等政策，最大限度消除安全隐患，制止攻击行为，避免危害发生。《公共互联网网络安全威胁监测与处置办法》自 2018 年 1 月 1 日起实施。

2、2017 国家网络安全宣传周 9 月 16 日在上海开幕

人民网 9 月 16 日消息 2017 年国家网络安全宣传周 9 月 16 日在沪开幕。本次活动于 9 月 16 日至 24 日在全国范围内统一举行，主题是“网络安全为人民，网络安全靠人民”，由中央宣传部、中央网信办、教育部、工业和信息化部、公安部、中国人民银行、新闻出版广电总局、全国总工会、共青团中央等九部门共同举办。国家层面举办网络安全宣传周，到今年已是第四届；与往年相比，今年宣传周期间不但会举办网络安全博览会，而且还新增了网络安全成就展。昨天，中央网信办网络安全协调局相关处室负责人在回答记者提问时介绍，2017 网络安全博览会暨网络安全成就展是 2017 国家网络安全宣传周一项重要内容，该活动由中央网信办、上海市人民政府指导，上海市委网信办主办，国家工业信息安全发展研究中心、上海市信息安全行业协会承办，将于 9 月 17 日-9 月 20 日在国家会展中心（上海）7.2 馆举行。为让广大人民群众了解五年来国家网络安全取得的成就，今年专门设立了网络安全成就展，成就展由中央网信办、教育部、工信部、公安部、人民银行、国家密码局、共青团中央等部门共同设计，集中展示国家网络安全顶层设计、技术产业、保障能力、人才培养、宣传教育等方面取得的显著成就。

3、东盟各国专家冀与中国携手应对网络信息安全挑战

中新网 9 月 12 日消息 第七届中国-东盟工程项目合作与发展论坛暨第四届中国-东盟网络信息安全研讨会 9 月 12 日在南宁举行，东盟多国专家增进交流与共识，并期待中国-东盟携手应对网络信息安全挑战。中国国际科技交流中心主任陈剑表示，在“一带一路”倡议下，中国—东盟聚焦工程项目合作以及信息安全，具有更广阔的发展前景。特别是工程项目合作中的人才培养问题以及工程标准的相互认证问题。“中国国际科技交流中心愿意推动这方面的资源对接，为发展注入活力。”缅甸工程委员会主席 Charlie Than 称，他们已制定了旨在提升工程师认证和教育的路线图，还包括与中国科学技术协会合作。本届论坛由广西科学技术协会和中国—东盟博览会秘书处联合主办，以“工业控制与信息安全”为主题，与会专家围绕工业控制系统信息安全问题、网络空间防御问题、关键信息基础设施与工控安全问题、工业控制系统信息安全等级保护问题、智慧城市建设面临的信息安全挑战问题等进行深入而广泛的交流和探讨。

4、美国能源部投资了五千万美金提升重要能源设施的安全性

E 安全 9 月 17 日消息 美国能源部（DOE）表示要向 DOE 国家实验室投资五千万美金（约合人民币 3.27 亿元）支持早期研究和下一代工具与技术的开发以提升国家重要能源设施的安全弹性，这些设施包括电网，石油和天然气设施。能源部长 Rick Perry 认为，一个有弹性的，可靠的又安全的电网对国家安全，经济以及美国每天依赖的重要服务至关重要。哈维和厄玛飓风肆虐过后，受灾社区需要全天候的支持，而持续增强和提升供电系统以保障灾后重建也变得更为迫切。通过利用国家实验室及其合作伙伴的世界级创新发明，这笔投资才会让我们的电力部门具备更符合实际需求的功能，从而真正提升国家重要能源设施的弹性和安全性。该电力系统

必须持续更新才能解决各类挑战，例如恶劣的天气和网络威胁，各种类型的供电，消费者参与电力市场的能力，物联网的增长，电力设施的老化。美国国家能源部还发布了 20 个网络安全项目，这些项目都将研发创新型、可扩展和具有成本效益网络安全方案提升国家电网，石油和天然气设施的可靠性和弹性。这些技术有望被美国能源供应部门广泛采纳，因为它们易于被资产拥有者和运营者接受，从而满足能源部门在成本效益方面的需求。

5、俄罗斯联邦安全局 FSB 或负责国家网络攻击响应系统

E 安全 9 月 12 日消息 俄罗斯法律信息网站上周五发布一份草案文件指出，俄罗斯联邦安全局（简称 FSB）可能会负责国家的网络攻击检测与管理系统。这份草案包含一项重要提议：修正总统针对俄罗斯数字资源而建立网络攻击检测、防御和消除影响颁布的法令。这项法令最初于 2013 年 1 月 15 日由俄罗斯总统宣布。一旦草案提议的修订被通过，俄罗斯联邦安全局将负责维护该系统。该文件明确了俄罗斯联邦安全局的相关管理职责及责任。今年 7 月，俄罗斯议会上院通过了一揽子政府法案，以保护关键信息基础设施免遭网络攻击，法案最终成为法律，明确关键基础设施包括政府数字系统和电信网络、国防行业技术流程自动化控制系统、医疗保健、交通、通信、金融、能源、核、航空航天等行业。法律同时规定，创建恶意软件，并对关键基础设施造成严重损害者可能会被判处长达 10 年的监禁。这项法律将于 2018 年 1 月正式实施。

6、土耳其计划出台国家网络安全新战略

新华网 9 月 13 日消息 土耳其交通、航运和信息部部长艾哈迈德·阿尔斯兰日前表示，政府正在计划出台新的国家网络安全战略和行动计划。据当地媒体 12 日报道，阿尔斯兰说，此举旨在应对当今来自国内外的网络安全威胁、打击网络犯罪、防范黑客攻击。该计划包括 5 个战略目标、41 项行动主题和 167 个具体步骤。土耳其官方网络安全机构网络安全委员会已召开 4 次会议，为这项战略计划的起草酝酿做准备。据介绍，土耳其成立了国家计算机紧急情况应对中心，以协调国有和私营企业在打击网络犯罪领域的合作，共同采取行动。未来政府将公布新的有关法规，强制企业聘请全职的网络安全专家应对可能的网络威胁，未能采取相关网络防范措施的企业可能将面临政府罚款。土耳其还将成立一个封闭的虚拟网络，确保国家机构内部数据信息传输交换的安全。土耳其信息和通信技术委员会将在国家网络安全工作中发挥更加积极有效的作用。政府还将成立一个由 1000 名专业人士组成的专家团队来开展国家网络安全工作。阿尔斯兰说，交通、航运和信息部计划在今年内举行一次网络安全演练，测试并评估土耳其应对国内网络安全威胁的防范能力，明年将开展针对国际网络威胁的演练和测试。为提高公众对网络安全的意识，土耳其政府还准备建立一个公众互动平台，提供有关网络安全的在线模拟训练。

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：马莉雅

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158