国家互联网应急中心

网络安全信息与动态周报

2017 年第 36 期

8 月 28 日-9 月 3 日

CNCERT/CC

本周网络安全基本态势

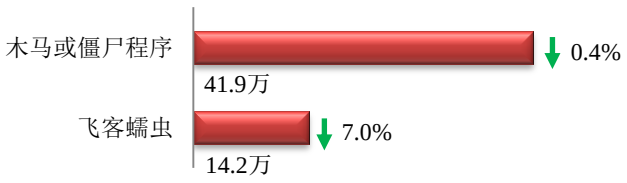
境内感染网络病毒的主机数量	•56.1万	2.2%
境内被篡改网站总数 其中政府网站数量	•2444 •39	11.9% 11.4%
境内被植入后门网站总数 其中政府网站数量	•961 •53	13.3% 18.5%
针对境内网站的仿冒页面数量	•306	5.8%
新增信息安全漏洞数量 其中高危漏洞数量	•348 •108	19.2% 10.2%

v

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

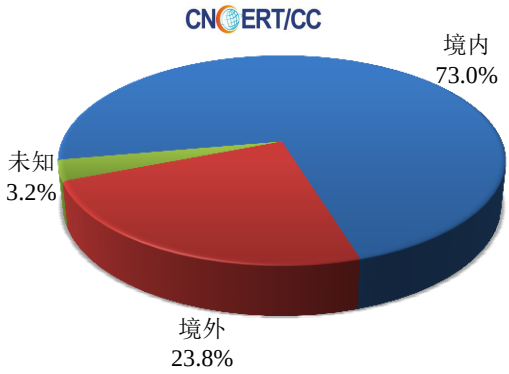
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 56.1 万个，其中包括境内被木马或被僵尸程序控制的主机约 41.9 万以及境内感染飞客（conficker）蠕虫的主机约 14.2 万。

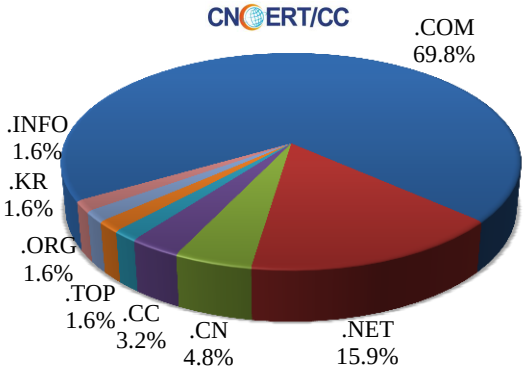


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 63 个，涉及 IP 地址 223 个。在 63 个域名中，有 23.8%为境外注册，且顶级域为.com 的约占 69.8%；在 223 个 IP 中，有约 7.6%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 2 个 IP。

本周放马站点域名注册所属境内外分布
(8/28-9/3)



本周放马站点域名所属顶级域的分布
(8/28-9/3)



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。

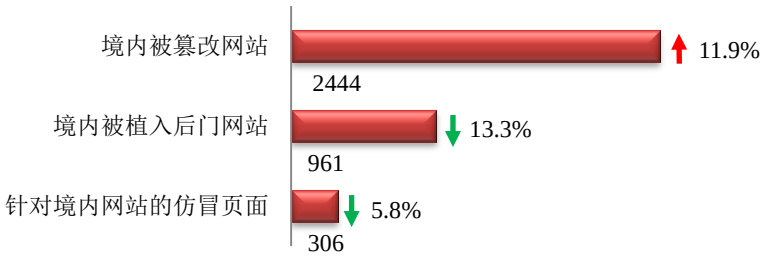
ANVA恶意地址黑名单发布地址

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。

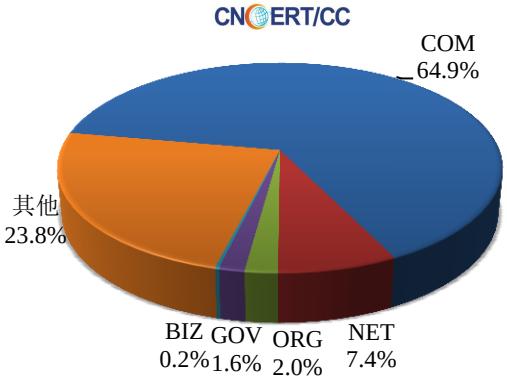
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 2444 个；境内被植入后门的网站数量为 961 个；针对境内网站的仿冒页面数量为 306。

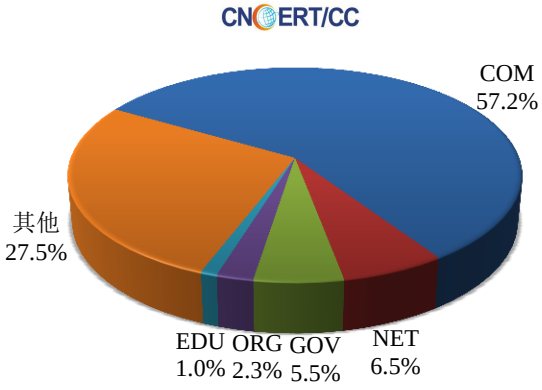


本周境内被篡改政府网站（GOV 类）数量为 39 个（约占境内 1.6%），较上周环比下降了 11.4%；境内被植入后门的政府网站（GOV 类）数量为 53 个（约占境内 5.5%），较上周环比下降了 18.5%；针对境内网站的仿冒页面涉及域名 269 个，IP 地址 126 个，平均每个 IP 地址承载了约 2 个仿冒页面。

本周我国境内被篡改网站按类型分布
(8/28-9/3)

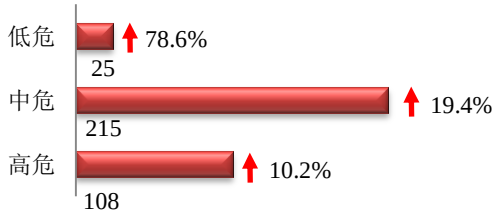


本周我国境内被植入后门网站按类型分布
(8/28-9/3)

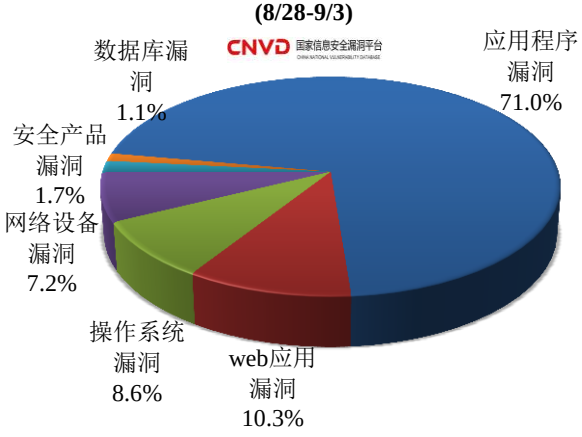


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 348 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
(8/28-9/3)



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

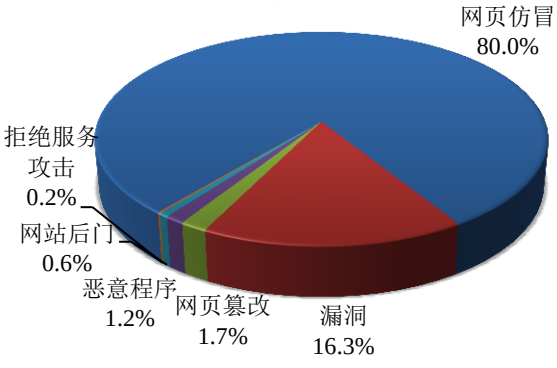
http://www.cnvd.org.cn/webinfo/list?type=4

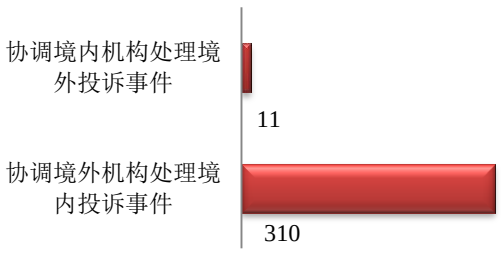
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 645 起，其中跨境网络安全事件 321 起。

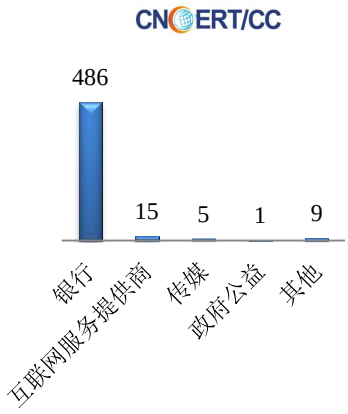
本周CNCERT处理的事件数量按类型分布
(8/28-9/3)



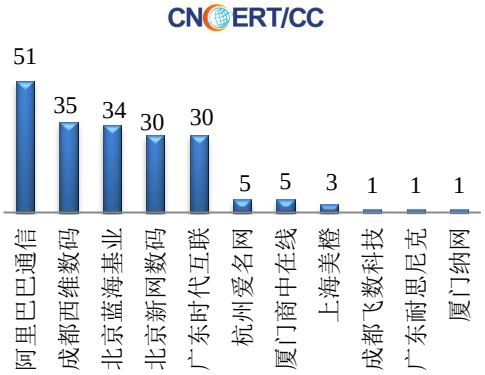


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 516 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 486 起和互联网服务提供商仿冒事件 15 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(8/28-9/3)

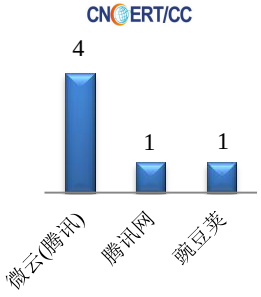


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (8/28-9/3)



本周，CNCERT 协调 3 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 6 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 (8/28-9/3)



业界新闻速递

1、澳大利亚维多利亚州启动新一轮网络安全战略，增强国家政府网络防御体系

HackerNews.cc8 月 29 日消息 澳大利亚维多利亚州政府于 8 月 25 日正式启动新一项五年网络安全战略，旨在增强国家政府网络防御体系并确保国家信息、服务与关键基础设施安全。不过，该战略目前首要保护公民敏感信息免遭丢失、恶意更改或未经授权使用。与此同时，由于政府希望国家服务、系统与基础设施在遭受严重网络攻击时能够迅速得以恢复，因此该战略发布后政府不仅对国家基础设施的威胁采取了全方位应对措施，还强调了公共管理部门的网络安全战略需要根据行业实践进行改进，使之保持一致并适合每个组织风险状况。另

外，维多利亚州政府还希望国家能够将安全与维护功能纳入公民新数字服务项目，旨在提高政府核心基础设施的安全性与可行性。因此，该战略的发布首先要求私营企业与其共享安全信息。知情人士透露，维多利亚州政府将于 9 月在总理府内阁任命一名首席信息安全官员并设立新网络安全办事处，负责监督战略推出与跨政府协调行动。目前，由于该战略的启动，政府机构将被要求向维多利亚州秘书委员会以及国家危机与应变委员会提交一份网络安全季度报告，用于进行正常的国家安全检查。

2、印度政府计划起草网络安全标准法律框架

E 安全 8 月 28 日消息 印度电子信息技术部（Meity）8 月 14 日与政府官员召开内部会议讨论全球网络安全实践、印度制定网络安全标准框架的要求、法律框架的选择、安全测试能力以及设备数据安全状态。会议由联盟法和 IT 部长拉维·香卡·普拉萨德和国家电子 IT 部长乔杜里主持。印度政府计划制定网络安全标准框架。印度政府还可能引入更严格的监管条款。Meity 部长助理阿杰伊·库马尔表示，需综合解决数据问题。库马尔指出，印度希望确保公民权利受到保护，公民数据不被非法窃取，希望确保与国家战略问题相关的任何数据不遭受攻击。目前，诸如《印度标准局法》（BIS Act）、《印度电报法》（Indian Telegraph Act）、《IT 法》等法律提供了法律框架。例如，BIS Act 设立了信息安全和生物识别工作组，并采用其它安全标准。BIS Act 未囊括网络安全。同样，《印度电报法》主要根据电信许可条款和条件讨论安全指南；2008 修订的《IT 法》主要处理计算机资源中的个人敏感数据或信息。知情人士表示，Meity 认为目前已存在相关国际标准，法律框架有必要提出满足安全标准的要求。

3、印度和日本就强化网络安全合作进行对话

E 安全 8 月 28 日消息 印度外交部表示，印度和日本下定决心强化网络空间合作，并重申两国致力于打造一个开放、安全的网络空间，促进经济增长与创新。印度与日本于 8 月 17 日举行第二次网络对话，讨论了两国的网络政策情况、网络威胁与缓解形势、双边合作机制以及在各种国际和地区论坛的合作机会。双方证实，现有国际法普遍适用于网络空间。印度外交部发表声明称，任何国家不得执行或支持通过 ICT（信息通信技术）窃取知识产权，包括商业机密或其它机密商业信息，以达到企业或商业竞争优势的目的。日本外交部外交政策局副局长和负责网络政策的 Masato Otaka 带队参加此次对话，出席的日本代表包括国家网络安全策略与事件预备中心（简称 NISC）、内阁情报与研究办公室、国家警察局和计算机应急响应小组协调中心（简称 JPCERT/CC）。双方同意将于 2018 年举行下一次日印网络对话。

4、比利时欲聘用 200 名网络安全专家确保军方网络安全

E 安全 8 月 31 日消息 比利时网络安全中心（简称 CCB）计划聘用 200 名网络安全专家应对军事和通信领域的网络威胁。比利时网络安全中心按照 2014 年 10 月 10 日颁布的皇家法令成立，经国家首相授权行事。据比利时当地媒体 De Tijd 周二报道，最近几个月，CCB 公布了约 30 个职位空缺。比利时国防部长史蒂文·万德普特透露，网络安全中心计划招聘 200 多名新员工。新聘网络安全专家将负责确保通信和武器系统的网络安全，他们将在爱沙尼亚北约网络合作防御卓越中心（简称 CCDCOE）接受培训。万德普特表示，在遵守现有国际条约和法律的前提下，比利时网络安全中心除了采取网络防御措施，还能在网络空间实施进攻行动。

5、匿名攻击者向 7.11 亿电子邮件账户群发银行木马病毒 Ursnif

HackerNews.cc8 月 31 日消息 据外媒 8 月 29 日报道，法国安全研究人员近期在荷兰的一台“开放且可访问”的垃圾邮件服务器上发现一个庞大的数据库，其中包含逾 7.11 亿电子邮件地址，以及来自全球数百万个 SMTP 登录凭证。调查显示，匿名攻击者主要利用该批电子邮件账户群发银行木马病毒 Ursnif。研究人员经调查发现，通常情况下垃圾邮件主要是为发布广告以获取流量收益，但这次的垃圾邮件群发主要是为了盗取银行账号信息，即邮件冒充各种通知信件或订单确认信息等，诱骗受害者点击链接进入攻击者事先设置的钓鱼网站。与此同时，攻击者还利用该邮件传播木马病毒 Ursnif。目前，研究人员称全球超过 10 万台电脑已感染该病毒。目前，基于安全考虑该事件的研究人员并未发布具体文件信息，而是联系了当地的执法部门迅速获取这些数据，之后将由执法部门继续追查服务器所有者以及背后操纵者真实身份。此外，研究人员强烈建议受影响用户当即更改密码并启用双重身份认证。

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：吕志泉

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158