国家互联网应急中心

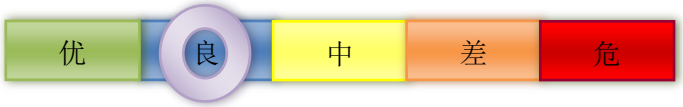
2018 年第 33 期

8 月 13 日-8 月 19 日

网络安全信息与动态周报

CNCERT/CC

本周网络安全基本态势

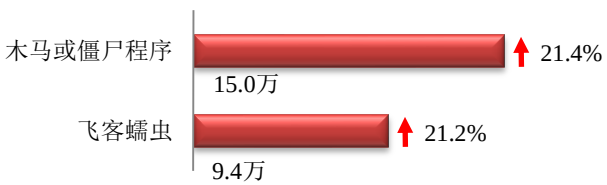


境内感染网络病毒的主机数量	•24.4万	↑ 21.4%
境内被篡改网站总数 其中政府网站数量	•900 •37	↑ 10.2% ↓ 14.0%
境内被植入后门网站总数 其中政府网站数量	•719 •16	↓ 17.4% ↑ 33.3%
针对境内网站的仿冒页面数量	•1018	↓ 30.2%
新增信息安全漏洞数量 其中高危漏洞数量	•274 •107	↑ 28.6% ↑ 62.1%

═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

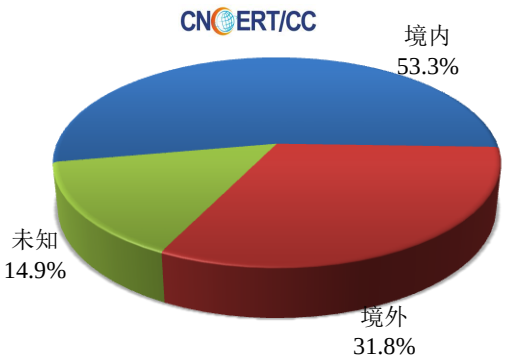
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 24.4 万个，其中包括境内被木马或被僵尸程序控制的主机约 15.0 万以及境内感染飞客（conficker）蠕虫的主机约 9.4 万。

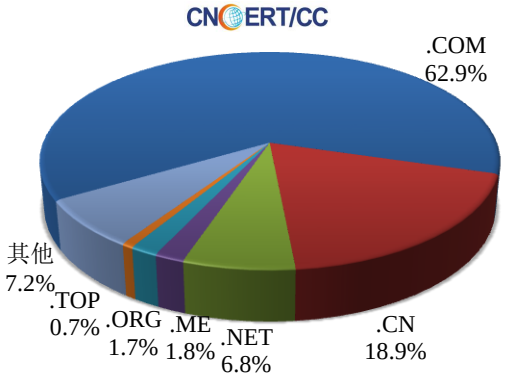


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 824 个，涉及 IP 地址 38858 个。在 824 个域名中，有 31.8%为境外注册，且顶级域为.com 的约占 62.9%；在 38858 个 IP 中，有约 25.2%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 175 个 IP。

本周放马站点域名注册所属境内外分布
(8/13-8/19)



本周放马站点域名所属顶级域的分布
(8/13-8/19)



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。

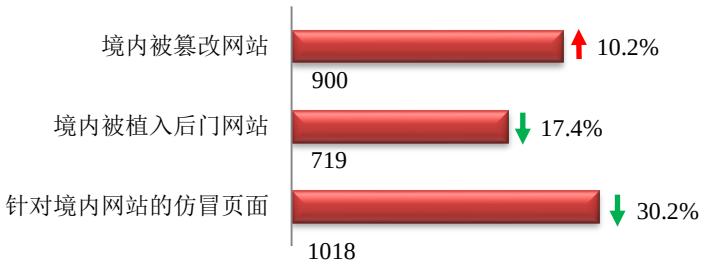
ANVA恶意地址黑名单发布地址

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。

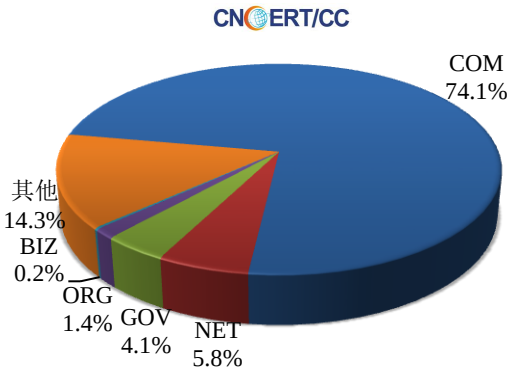
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 900 个；境内被植入后门的网站数量为 719 个；针对境内网站的仿冒页面数量为 1018。

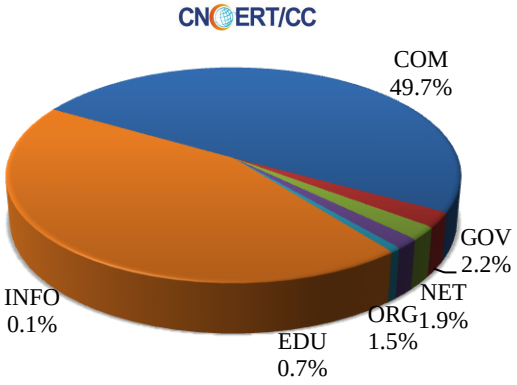


本周境内被篡改政府网站（GOV 类）数量为 37 个（约占境内 4.1%），较上周环比下降了 14.0%；境内被植入后门的政府网站（GOV 类）数量为 16 个（约占境内 2.2%），较上周环比上升了 33.3%；针对境内网站的仿冒页面涉及域名 475 个，IP 地址 151 个，平均每个 IP 地址承载了约 7 个仿冒页面。

本周我国境内被篡改网站按类型分布
(8/13-8/19)

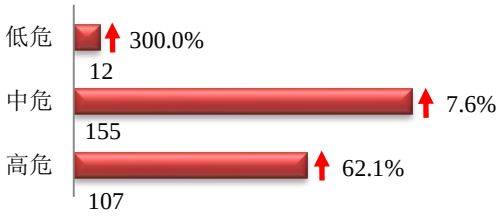


本周我国境内被植入后门网站按类型分布
(8/13-8/19)

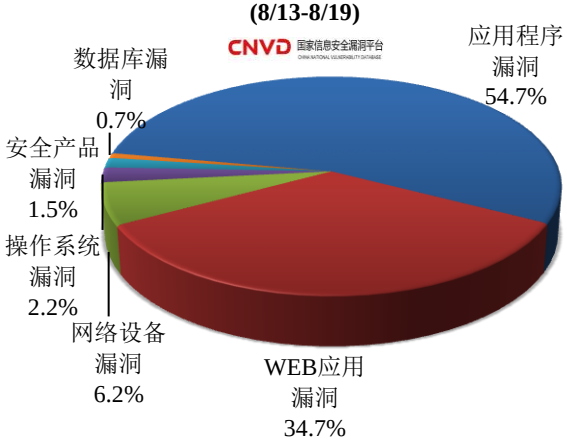


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 274 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
(8/13-8/19)



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 应用漏洞和网络设备漏洞。

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

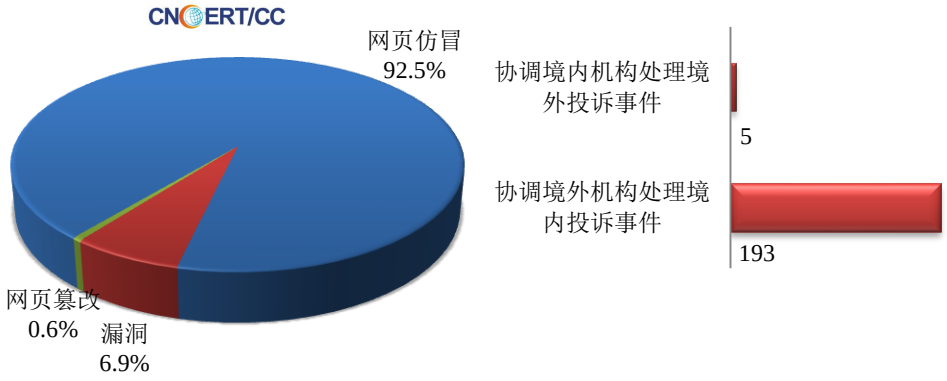
http://www.cnvd.org.cn/webinfo/list?type=4

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

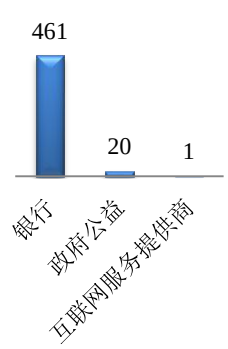
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 523 起，其中跨境网络安全事件 198 起。

本周CNCERT处理的事件数量按类型分布 (8/13-8/19)

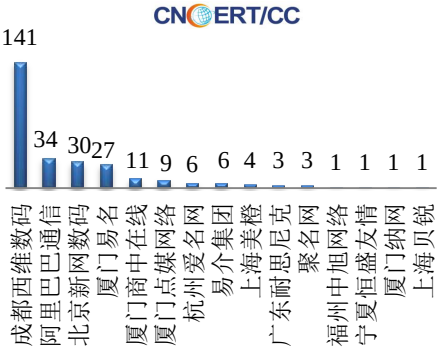


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 482 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 461 起和政府公益仿冒事件 20 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(8/13-8/19)

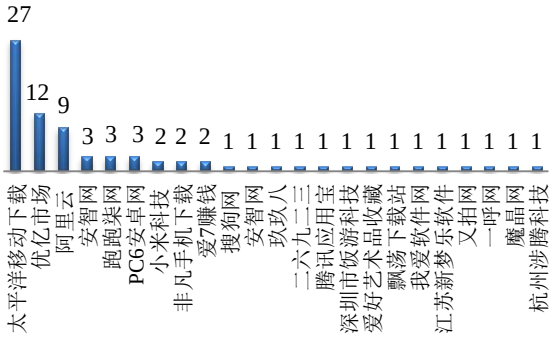


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (8/13-8/19)



本周，CNCERT 协调 23 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 77 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
(8/13-8/19)



业界新闻速递

1、特朗普推翻奥巴马政令 放松美国实施网络攻击限制

新浪网 8 月 16 日消息 知情人士透露，美国总统特朗普（Donald Trump）推翻了奥巴马（Barack Obama）时代的一项政策令，该政令规定了美国政府如何以及何时能够部署网络武器打击其对手，特朗普此举旨在放松对此类行动的限制。特朗普周三签署一项行政令，推翻了被称为“总统 20 号政令”（Presidential Policy Directive 20）的机密规则，这一政令制定了一个复杂的跨部门流程，美国在使用网络攻击（尤其是针对外国对手）之前必须遵循这一流程。尽管上述政令属于机密，但其内容 2013 年因前情报承包商雇员斯诺登（Edward Snowden）的披露而被公众知晓。特朗普前任奥巴马 2012 年签署了该政令。

2、以色列将启动计划加强网络安全产业发展

新华网 8 月 15 日消息 以色列创新局日前发表声明说，该机构将联合以色列经济和工业部、国家网络局在未来三年内启动一项发展计划，投资 9000 万新谢克尔（约合 2443 万美元）加强国家网络安全产业发展。据悉，该计划主要包括对有全球影响力的以色列技术、有突破性研发潜力的以色列网络安全公司提供资金支持等。以色列经济和工业部长埃利·科亨表示，该计划旨在保持国家在创新方面的领先地位和在网络安全行业的全球领导力。以色列国家网络局局长伊加尔·昂纳说，网络安全是高科技产业发展的重要引擎，该计划不仅致力于解决网络行业的挑战，还着眼于未来发展，有助于保持以色列在全球网络产业中的技术创新优势。

3、澳大利亚开始讨论向加密设备引入后门的法案

cnBeta.COM8 月 14 日消息 澳大利亚议会从本周开始讨论向加密设备引入后门的法案。法案的细节没有公开，根据此前公布的法案会议摘要，该法案落实措施解决加密设备和通信对国家安全和执法调查的影响，为政府机构和私营企业合作提供一个框架，让执法能适应日益复杂的网络环境。法案要求本国企业和外国企业为政

府提供更多帮助。虽然一直否认，澳大利亚政府系统通过在加密设备和通信植入后门来实现对加密设备和通信的访问。如果没有后门，设备制造商和运营商也无法破解端对端加密。

4、印度银行遭黑客入侵，被盗取 94 亿卢比，12 亿转移到了香港

E 安全 8 月 15 日消息 在最近一次重大的网络攻击中，黑客通过入侵印度浦那“宇宙银行”的 ATM 交换机服务器窃取了 94 亿卢比，黑客窃取了多个 Visa 和 Rupay 借记卡所有者的详细信息。这些信息被用于执行大约 12,000 笔交易，价值 78 亿卢比，同样，在该国境内其它区域进行了 2,800 笔交易，其中 80 万卢比被清除。在另一笔交易中，资金被发送到位于香港的汉森银行。该交易是以名为 ALM Trading Limited 的公司名义进行的。这位受益人获得了 12 亿卢比。印度银行被盗总金额约为 94 亿卢比（约为 9 亿人民币）。宇宙银行的主席 Milind Kale 表示，“这是从加拿大完成的入侵；印度储备银行和税收团队正在调查此事。”

5、全美第二大互联网服务供应商 Comcast 意外暴露 2650 万用户个人信息

黑客视界 8 月 14 日消息 据发现安全漏洞的安全研究员瑞恩•史蒂文森（Ryan Stevenson）称，Comcast Xfinity 无意中暴露了超过 2650 万名用户的家庭住址和社会安全号码。隶属于这家全美第二大互联网服务提供商的在线客户门户网站上被发现存在两个此前未被报告的漏洞，这使得即使是不具备太多专业技能的黑客也可以很容易地访问这些敏感信息。在 BuzzFeed News 向 Comcast 报告了这项调查结果之后，该公司对漏洞进行了修复。虽然，Comcast 目前表示尚未发现任何滥用漏洞的行为，但相关的审查仍在进行中。

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：周彧

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158