国家互联网应急中心

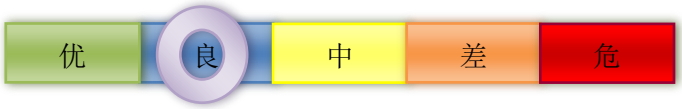
网络安全信息与动态周报

2019 年第 14 期

4 月 1 日-4 月 7 日

CNCERT/CC

本周网络安全基本态势

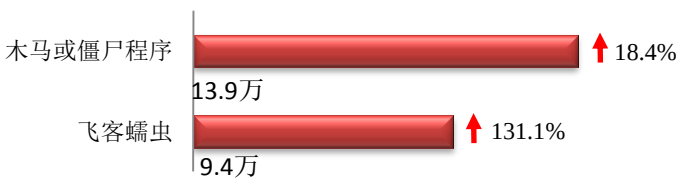


境内感染网络病毒的主机数量	• 23.3万	↑ 47.5%
境内被篡改网站总数 其中政府网站数量	• 464 • 34	↓ 11.8% ↑ 30.8%
境内被植入后门网站总数 其中政府网站数量	• 854 • 7	↑ 34.9% ↑ 133.3%
针对境内网站的仿冒页面数量	• 2257	↓ 14.8%
新增信息安全漏洞数量 其中高危漏洞数量	• 180 • 71	↓ 33.1% ↓ 23.7%

═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

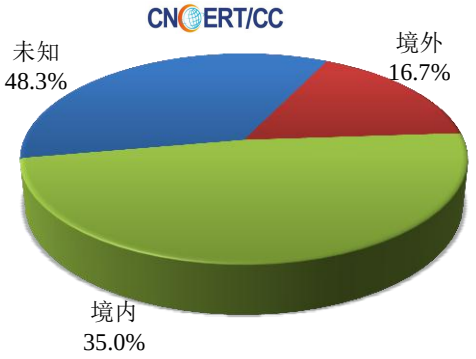
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 23.3 万个，其中包括境内被木马或被僵尸程序控制的主机约 13.9 万以及境内感染飞客（conficker）蠕虫的主机约 9.4 万。

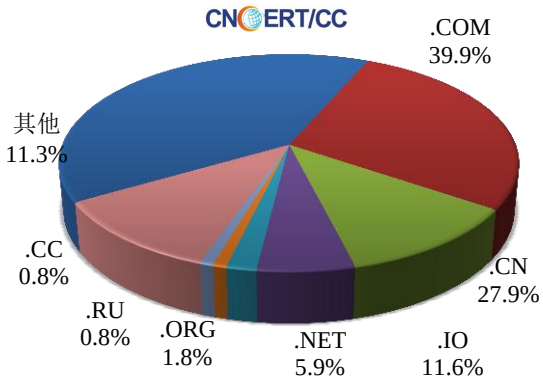


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 2309 个，涉及 IP 地址 3573 个。在 2309 个域名中，有 16.7%为境外注册，且顶级域为.com 的约占 39.9%；在 3573 个 IP 中，有约 32.3%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 323 个 IP。

本周放马站点域名注册所属境内外分布
(4/1-4/7)



本周放马站点域名所属顶级域的分布
(4/1-4/7)



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。

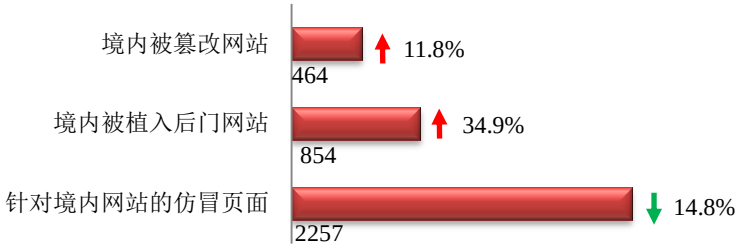
ANVA恶意地址黑名单发布地址

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。

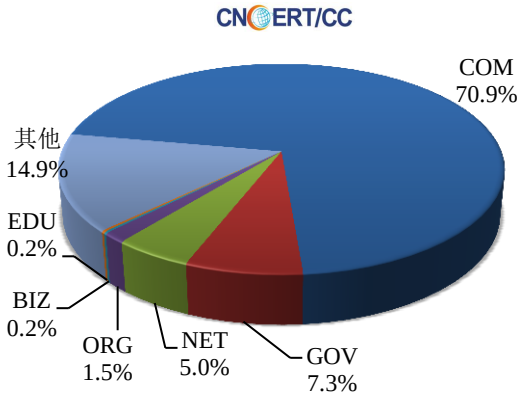
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 464 个；境内被植入后门的网站数量为 854 个；针对境内网站的仿冒页面数量 2257 个。

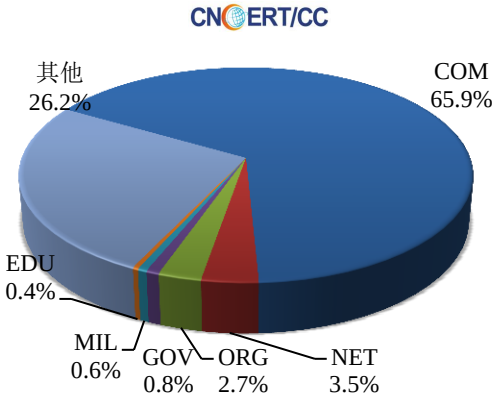


本周境内被篡改政府网站（GOV 类）数量为 34 个（约占境内 7.3%），较上周环比上升了 30.8%；境内被植入后门的政府网站（GOV 类）数量为 7 个（约占境内 0.8%），较上周环比上升了 133.3%；针对境内网站的仿冒页面涉及域名 707 个，IP 地址 387 个，平均每个 IP 地址承载了约 6 个仿冒页面。

本周我国境内被篡改网站按类型分布
(4/1-4/7)

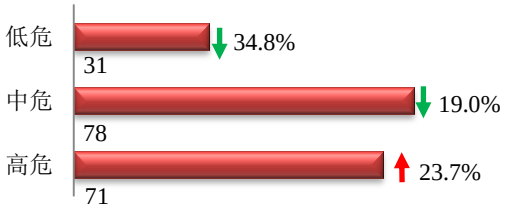


本周我国境内被植入后门网站按类型分布
(4/1-4/7)

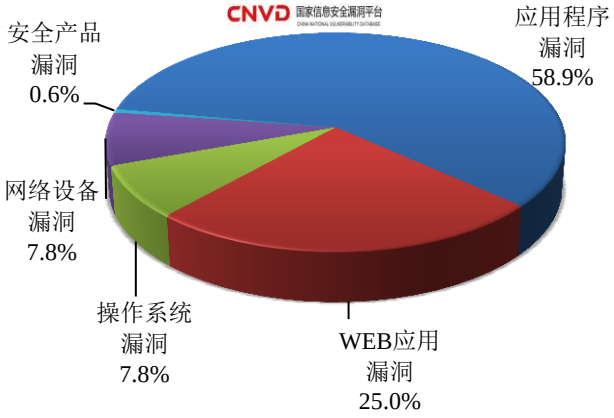


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 180 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
(4/1-4/7)



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

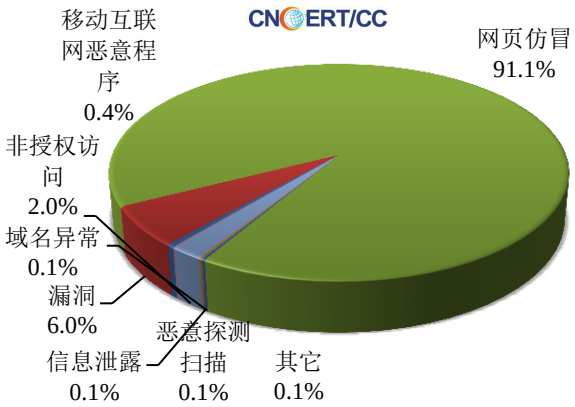
http://www.cnvd.org.cn/webinfo/list?type=4

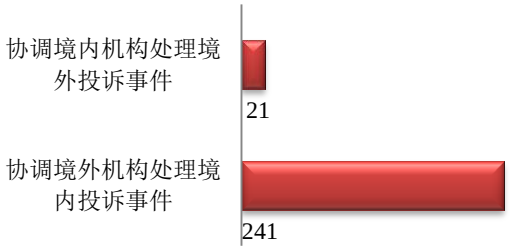
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 704 起，其中跨境网络安全事件 262 起。

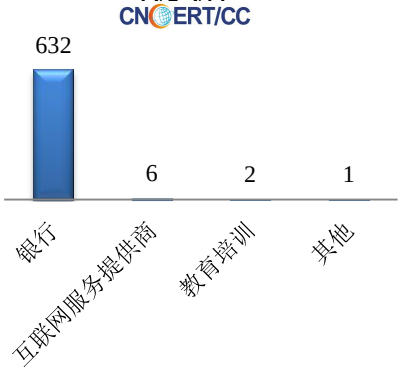
本周CNCERT处理的事件数量按类型分布 (4/1-4/7)



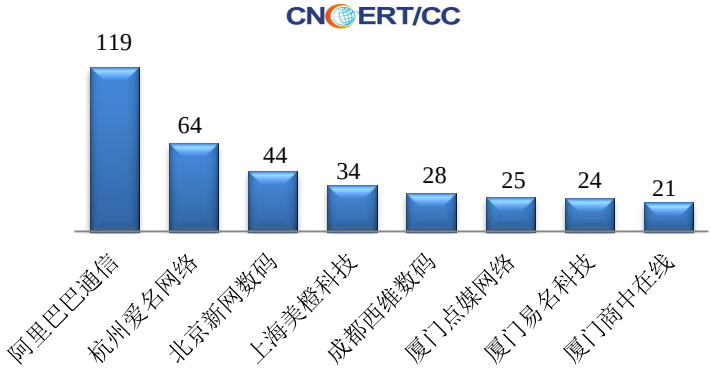


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 641 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 632 起和互联网服务提供商事件 6 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (4/1-4/7)

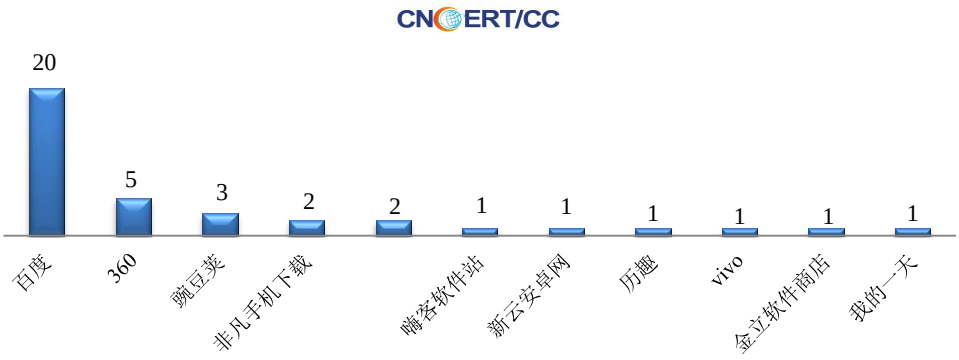


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (4/1-4/7)



本周，CNCERT 协调 11 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 38 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 (4/1-4/7)



业界新闻速递

1、英国收紧社交媒体审查

HackerNews4 月 8 日消息，英国政府在网络安全方面将继续采取强硬立场，近期将会成立全球首家专门负责社交媒体公司的独立监管机构。对于没有达到要求的公司不仅要面临巨额的罚款，而且公司的高管负责人因工作疏忽需要承担个人责任。英国内政部（Home Office）、英国文化、传媒和体育部（Department for Digital, Culture, Media and Sport）近日联合发布了旨在使互联网变得更加安全的新措施。英国政府正式发布了期待已久的白皮书，并有望引入了全新的监管机构来集中化管理社交媒体。新成立的监管机构的任务是指导和协助社交媒体公司解决一系列在线安全问题，其中包括：煽动暴力和传播暴力内容（包括恐怖主义内容）；鼓励自残或自杀；虚假信息和假新闻的传播；网络欺凌；儿童访问不适当的材料；儿童剥削和虐待内容。

2、澳大利亚通过新法律：社交媒体出现暴力内容将受惩罚

新浪科技 4 月 4 日消息，澳大利亚本通过了一项新法律，社交媒体如果没有在自己的平台上做好暴力内容移除工作，他们将会遭受巨额罚款，甚至高管有可能遭遇牢狱之灾。这项法律让澳大利亚站在了全球行动的前线，目前许多国家都在对 Facebook 和 YouTube 等平台进行监管，要求他们对自己平台上的内容负责。这项法律认定，社交媒体上的暴力内容属于违法内容，任何与公布袭击、谋杀、强奸或绑架相关的视频都属于违法内容。社交媒体企业如果没有“迅速有效”地移除这些内容，企业将会面临高额罚款，最高金额为该公司年营收的 10%，公司的员工有可能面临最高 3 年的监禁。

3、Facebook 数百万用户数据被存储在 AWS 上

腾讯科技 4 月 4 日消息，网络安全公司 UpGuard 的研究人员发现，大量 Facebook 用户信息被公开发布在亚马逊公司的云计算服务器上。这一发现表明，在剑桥分析公司（Cambridge Analytica）的丑闻曝光一年之后，Facebook 在保护私人数据方面仍做得不够。多年来，Facebook 允许任何在其网站上开发应用程序的人获取使用该应用程序的用户及其朋友的信息。一旦数据脱离 Facebook 的掌控，开发者就可以对其为所欲为。

4、印度液化气公司 7 百万用户和分销商数据遭泄露

2019 年 4 月 6 日，印度液化石油气公司 Indane 近 700 万名用户和分销商的敏感数据遭到泄露。Indane 是世界第二大液化石油气营销商，拥有 9800 万客户群，9100 个分销商。这起事件的起因是其 IOS 应用程序提供的主要服务存在严重的访问控制漏洞，会导致未经授权的信息泄露。泄露的用户数据包括消费者姓名、地址、邮件、手机号码等；泄露的经销商信息包括银行账号、银行名称、绑定银行的收集号码等。此外，该漏洞还允许攻击者修改消费者的个人数据、关闭消费者的 Indane 账户等。

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：徐剑

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158