国家互联网应急中心

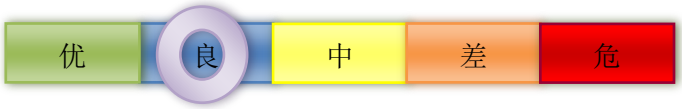
网络安全信息与动态周报

2019 年第 15 期

4 月 8 日-4 月 14 日

CNCERT/CC

本周网络安全基本态势

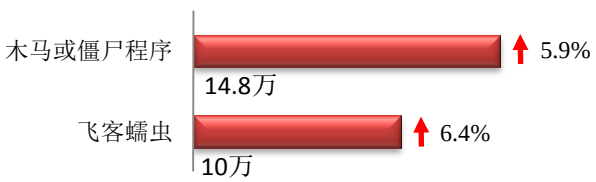


境内感染网络病毒的主机数量	•24.8万	↑6.2%
境内被篡改网站总数 其中政府网站数量	•512 •8	↑10.3% ↓76.5%
境内被植入后门网站总数 其中政府网站数量	•1057 •5	↑23.8% ↓28.6%
针对境内网站的仿冒页面数量	•2833	↑25.5%
新增信息安全漏洞数量 其中高危漏洞数量	•135 •47	↓25.0% ↓33.8%

=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

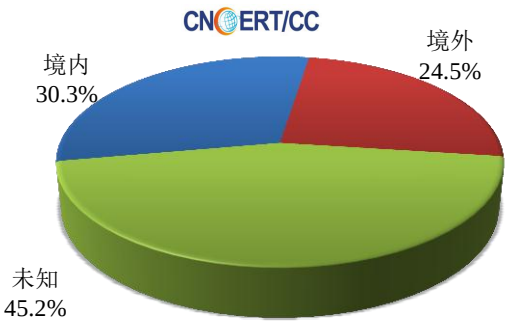
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 24.8 万个，其中包括境内被木马或被僵尸程序控制的主机约 14.8 万以及境内感染飞客（conficker）蠕虫的主机约 10.0 万。

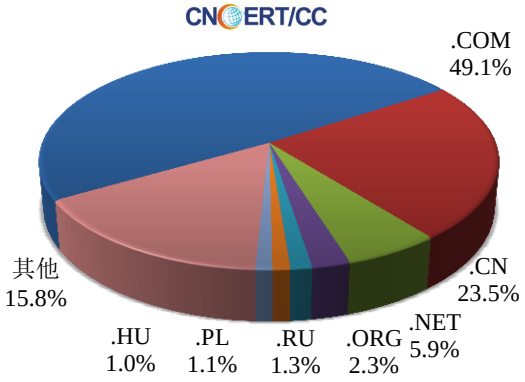


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 1691 个，涉及 IP 地址 2956 个。在 1691 个域名中，有 24.5%为境外注册，且顶级域为.com 的约占 49.1%；在 2956 个 IP 中，有约 43.0%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 341 个 IP。

本周放马站点域名注册所属境内外分布
(4/8-4/14)



本周放马站点域名所属顶级域的分布
(4/8-4/14)



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。

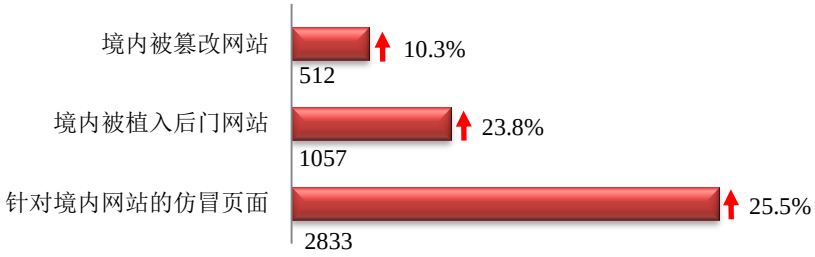
ANVA恶意地址黑名单发布地址

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。

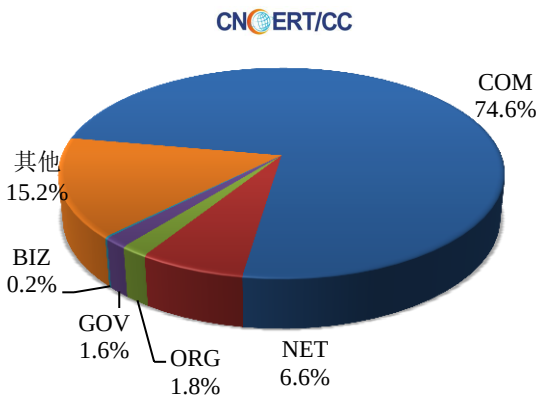
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 512 个；境内被植入后门的网站数量为 1057 个；针对境内网站的仿冒页面数量 2833 个。

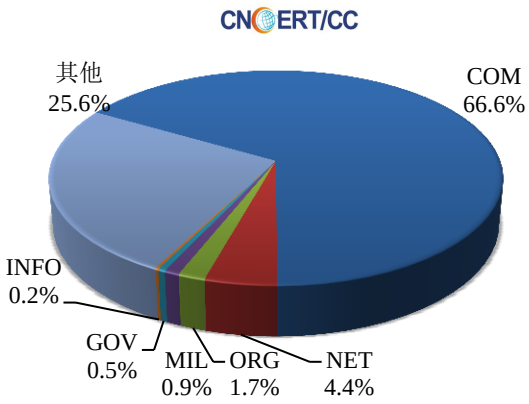


本周境内被篡改政府网站（GOV 类）数量为 8 个（约占境内 1.6%），较上周环比下降了 76.5%；境内被植入后门的政府网站（GOV 类）数量为 5 个（约占境内 0.5%），较上周环比下降了 28.6%；针对境内网站的仿冒页面涉及域名 852 个，IP 地址 439 个，平均每个 IP 地址承载了约 7 个仿冒页面。

本周我国境内被篡改网站按类型分布
(4/8-4/14)

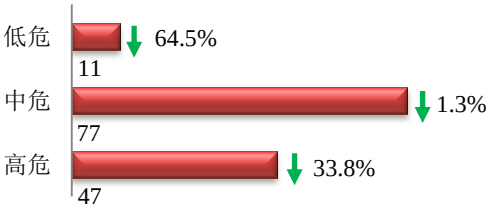


本周我国境内被植入后门网站按类型分布
(4/8-4/14)

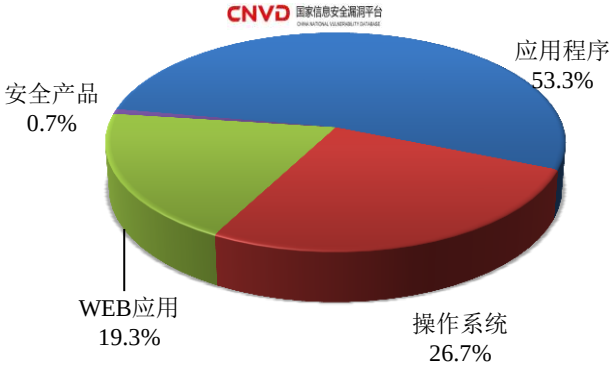


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 135 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
(4/8-4/14)



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

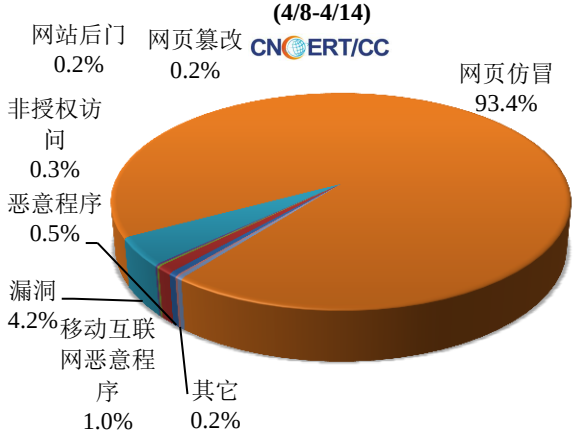
http://www.cnvd.org.cn/webinfo/list?type=4

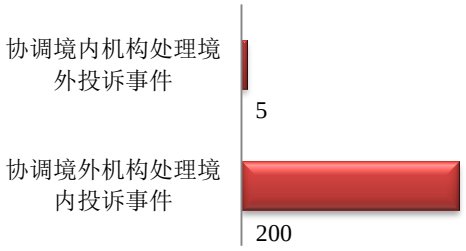
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 574 起，其中跨境网络安全事件 205 起。

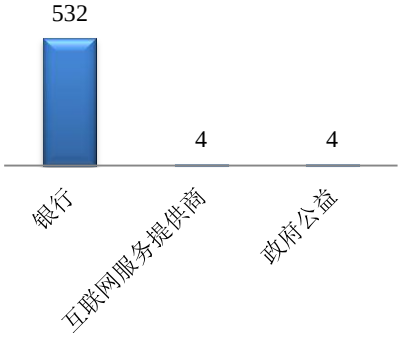
本周CNCERT处理的事件数量按类型分布 (4/8-4/14)



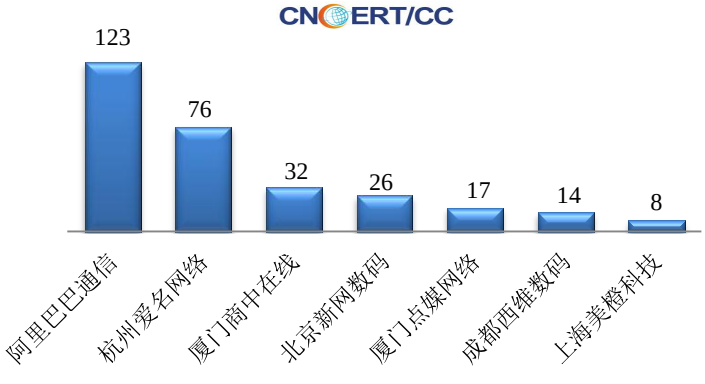


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 536 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 532 起和互联网服务提供商事件 4 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (4/8-4/14)

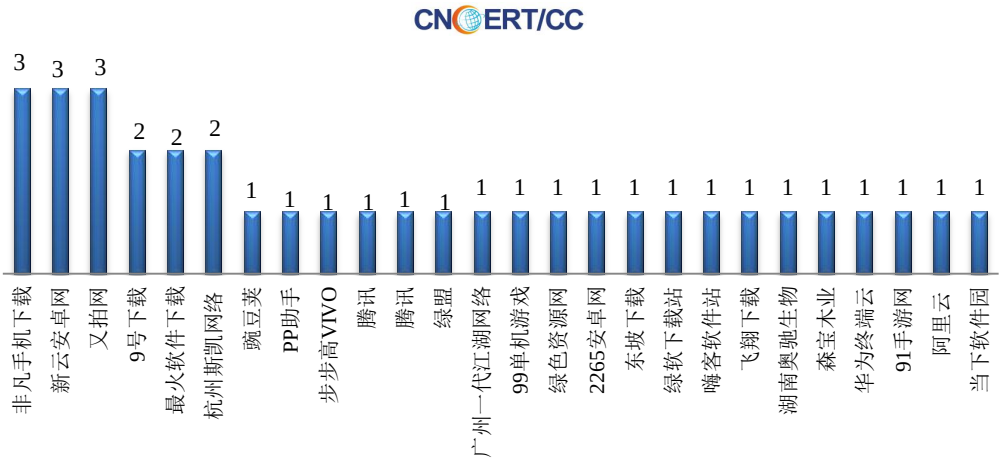


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (4/8-4/14)



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
(4/8-4/14)

本周，CNCERT 协调 26 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 35 个。



业界新闻速递

1、美司法部发布《CLOUD 法案白皮书》

安全内参 4 月 10 日消息 美国司法部（U.S.DepartmentofJustice）宣布公开发布一份关于《澄清合法海外使用数据法案》（DesignalOverseasUseofDataAct）即《云法案》（以下简称《云法案》）的白皮书。《云法案》于 2018 年 3 月颁布，更新了执法当局如何在尊重隐私利益和外国主权的情况下，要求提供保护公共安全所需的电子证据的法律框架。本次发布的白皮书《促进世界各地的公共安全、隐私和法治：云法的目的和影响》是在包括刑事司和国家安全司的律师在内的整个部门的投入下编写的。白皮书描述了促使颁布《云法案》的各种利益和关切，对该法的效果、范围和影响作了简要的逐点提炼，并回答了常见的问题。

2、美众议院民主党通过《拯救互联网法案》

cnBeta.COM4 月 11 日消息 美众议院民主党通过了一项法案，旨在恢复奥巴马时代的“网络中立规则”。但由于国会山的共和党人发誓要在参议院否决该法案，因此这场胜利很可能只是短暂的。民主党人周三以 232 票赞成、190 票反对通过了《拯救互联网法案》。《拯救互联网法案》（Save the Internet Act 或 HR 1644）将恢复 2015 年联邦通信委员会（FCC）通过的规则。这些规则禁止互联网服务提供商阻止或限制对互联网的访问，并且还阻止互联网服务提供商向公司收取额外费用以更快地为消费者提供其在线服务。此外，该法案还将恢复 FCC 管理和监督宽带网络的权力。

3、美参议员提出《隐私权法案》保护个人信息

安全内参 4 月 12 日消息 美参议员提出《隐私权法案》（Privacy Bill of Rights Act），目的是保护美国消费者的个人信息。该法案主要从三个层面切入，保护消费者的隐私：第一是公司层面：禁止公司在未经消费者同意的情况下分享消费者的个人数据；禁止公司将个人信息用于歧视性内容，如和性别有关的住房和就业广告等；加强公司的网络安全标准。第二是政府层面：赋予美国联邦贸易委员会制定规则的权力；允许州检察长对侵犯个人隐私权的公司提起诉讼。第三是个人层面：该法案规定，个人也有权采取行动，捍卫自己的隐私权。

4、FBI 网站被黑 黑客获取 100 万条联邦特工身份信息

Bianews 4 月 14 日消息 据外媒报道，一个黑客组织通过黑进数个联邦调查局（FBI）的附属网站，获取了成千上万条联邦特工和执法人员的个人信息，并计划出售。据悉，这些黑客通过攻击 FBI 国家学院协会（FBI National Academy Association）来获取这些个人信息，该协会是一个促进执法培训的非营利组织。黑客已经公布了部分个人信息到其网站上，外媒核对后发现了 4000 个包含姓名、职位、电子邮件、实际地址与电话号码的个人信息。黑客表示，他们手中有超过 100 万条联邦特工的个人信息，并计划在未来公布更多的政府数据，黑客还表示，这些信息很快就会被出售。

5、微软确认有黑客入侵了一些 Outlook.com 帐户 时间长达数月

cnBeta.COM4 月 13 日消息 微软已经开始通知一些 Outlook.com 用户，黑客能够在今年早些时候访问其帐户。公司发现支持代理的凭据因其网络邮件服务而受到损害，允许在 2019 年 1 月 1 日至 3 月 28 日期间未经授权访问某些帐户。微软称黑客可能已经查看了电子邮件账户，包括文件夹名称和主题行，但不包括电子邮件或附件的内容。目前尚不清楚有多少用户受到了黑客行为的影响，或者是谁参与了 Outlook.com 电子邮件帐户的访问。在此次入侵事件中，黑客无法窃取登录详细信息或其他个人信息，但出于谨慎，微软建议受影响的用户重置密码。

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