国家互联网应急中心

2019 年第 27 期

7 月 1 日-7 月 7 日

网络安全信息与动态周报

本周网络安全基本态势

境内感染网络病毒的主机数量	•19.5万	↑1.9%
境内被植入后门网站总数 其中政府网站数量	•3211 •32	↓7.0% ↓48.4%
针对境内网站的仿冒页面数量	•775	↓59.0%
新增信息安全漏洞数量 其中高危漏洞数量	•207 •74	↓3.0% ↑2.8%

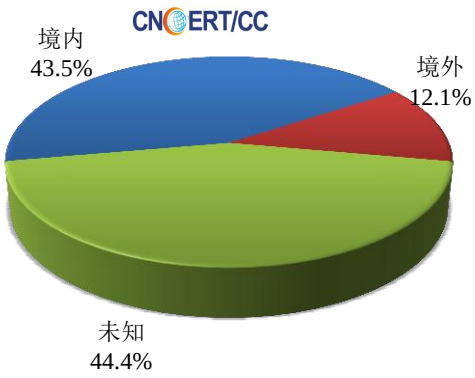
=表示数量与上周相同　↑表示数量较上周环比增加　↓表示数量较上周环比减少

本周网络病毒活动情况

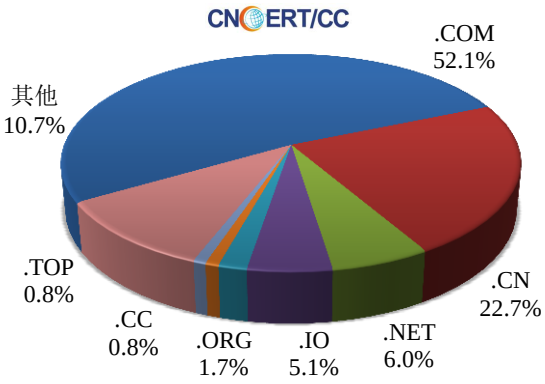
本周境内感染网络病毒的主机数量约为 19.5 万个，其中包括境内被木马或被僵尸程序控制的主机约 11.5 万以及境内感染飞客（conficker）蠕虫的主机约 8.0 万。

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 3329 个，涉及 IP 地址 5802 个。在 3329 个域名中，有 12.1%为境外注册，且顶级域为.com 的约占 52.1%；在 5802 个 IP 中，有约 41.6%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 671 个 IP。

本周放马站点域名注册所属境内外分布
(7/1-7/7)



本周放马站点域名所属顶级域的分布
(7/1-7/7)



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。

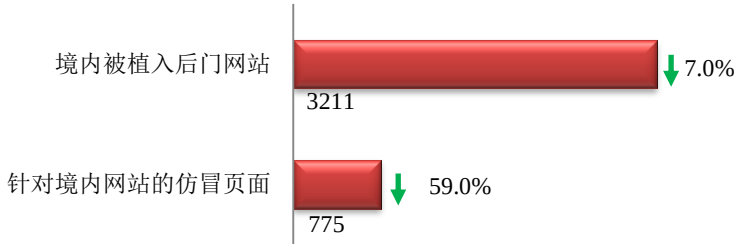
ANVA恶意地址黑名单发布地址

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。

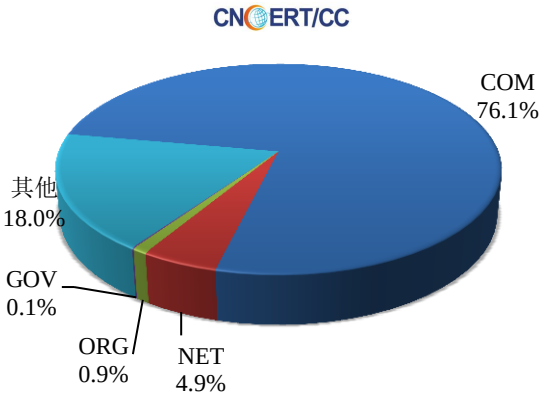
本周网站安全情况

本周 CNCERT 监测发现境内被植入后门的网站数量为 3211 个；针对境内网站的仿冒页面数量 775 个。

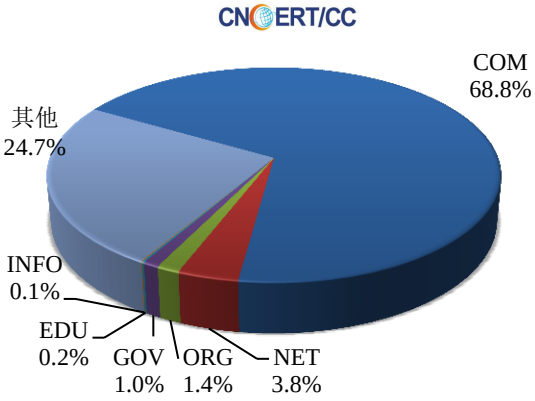


本周境内被篡改政府网站（GOV 类）数量为 1 个（约占境内 0.1%），较上周环比下降 92.3%；境内被植入后门的政府网站（GOV 类）数量为 32 个（约占境内 1.4%），较上周环比下降 48.4%；针对境内网站的仿冒页面涉及域名 428 个，IP 地址 216 个，平均每个 IP 地址承载了约 4 个仿冒页面。

本周我国境内被篡改网站按类型分布
(7/1-7/7)

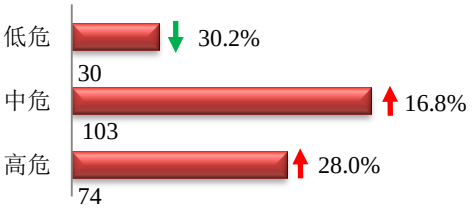


本周我国境内被植入后门网站按类型分布
(7/1-7/7)

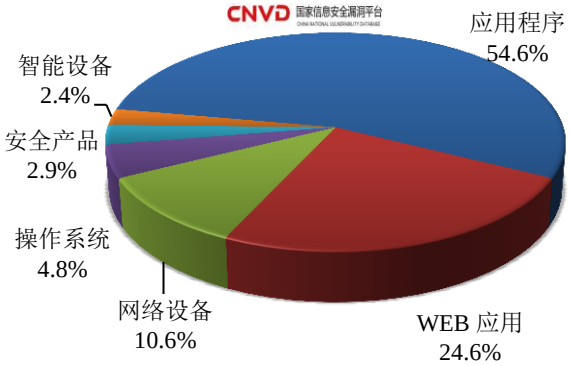


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 207 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
(7/1-7/7)



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

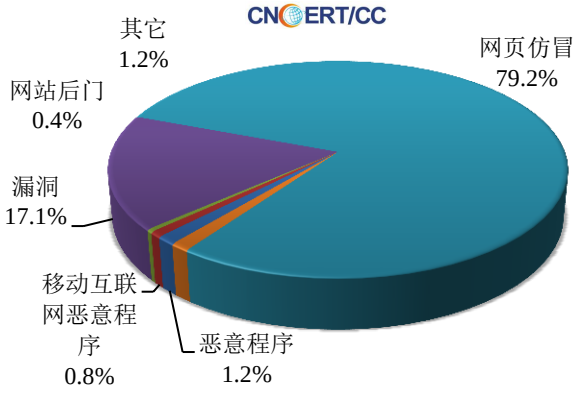
http://www.cnvd.org.cn/webinfo/list?type=4

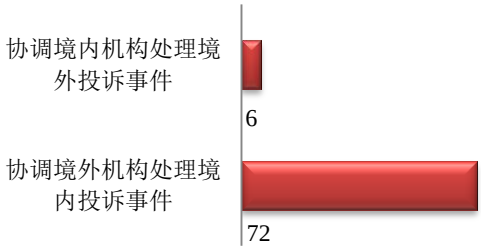
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 245 起，其中跨境网络安全事件 78 起。

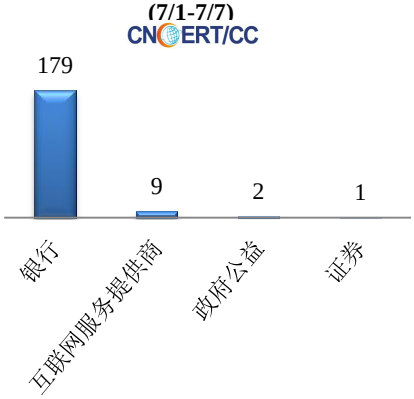
本周CNCERT处理的事件数量按类型分布 (7/1-7/7)



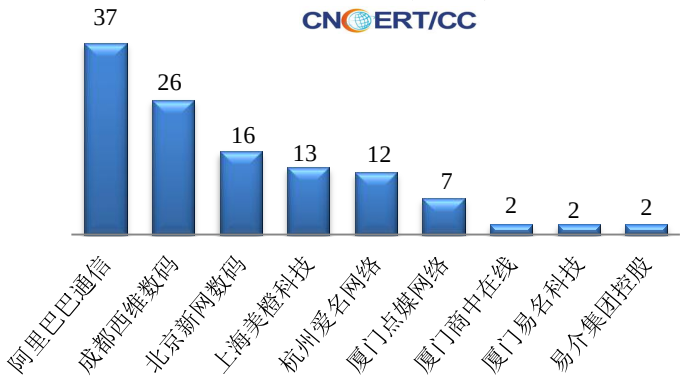


s

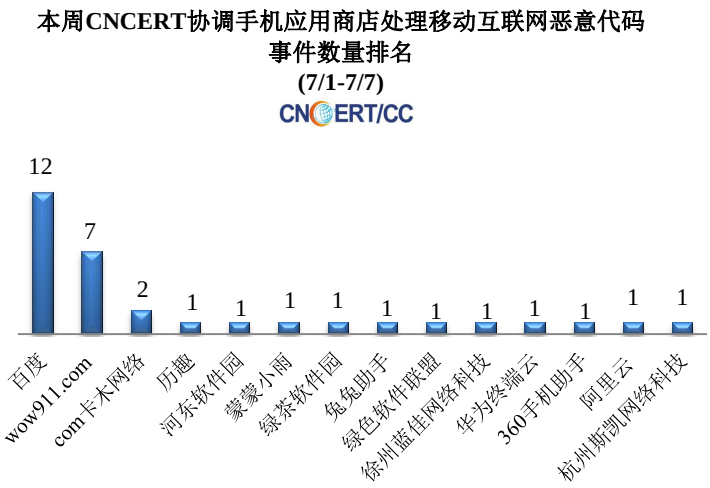
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (7/1-7/7)



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 (7/1-7/7)



本周，CNCERT 协调 28 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 32 个。



业界新闻速递

1、 工信部印发《电信和互联网行业提升网络数据安全保护能力专项行动方案》

工信部官网 7 月 1 日消息 为贯彻落实党中央、国务院决策部署要求，积极应对新形势新情况新问题，切实做好新中国成立 70 周年网络数据安全保障工作，全面提升电信和互联网行业网络数据安全保护能力，工业和信息化部近日印发《电信和互联网行业提升网络数据安全保护能力专项行动方案》，在行业内部署开展为期一年的提升网络数据安全保护能力专项行动。

2、 法国计划对互联网巨头征收“数字税”

人民网 7 月 3 日消息 法国参议院日前投票通过向大型互联网企业征收数字税的法律草案。根据该草案，自 2019 年 1 月 1 日起，谷歌、亚马逊、脸书等 30 余家全球数字业务营业收入不低于 7.5 亿欧元，同时在法国营业收入超过 2500 万欧元的互联网企业将被征收相当于其在法国营业额 3%的数字税。

3、 迈阿密 1TB 警用数据被公开

Cnbeta.COM6 月 27 日消息 infosec 的一份商业报告显示，大量的闲置警用摄像头视频内容被公开，任何人都可以观看。目前已经确认泄露了 1TB 的视频内容，这些视频原本存储在迈阿密警察局(Miami Police Department)、美国其他城市以及其他地方警察局未受保护的互联网的数据库中。据悉，这些文件名和附带的目录(大约有 65000 个)符合监视技术行业的需求重点。文件包括.xlsx 文件(以位置和邮政编码命名)、.jpg 文件(以“driver”和“scene”命名)、.docx 文件(与 ICE 等假定的政府客户端关联)、日期和时间戳为.jpg 和.mp4 的文件。

有许多其他类型的文件:.htm、.html、.txt、.doc、.asp、.tdb、.mdb、.json、.rtf、.xls 和.tif 等等，而许多图像文件都与违规车牌相关。

4、 日本 7-11 电子支付应用上线现漏洞，损失共计 350 万

澎湃新闻 7 月 5 日消息 日本柒和伊控股公司 4 日发布消息称，可在 7-Eleven 便利店使用的手机支付 APP“7pay”因遭遇第三方非法入侵，可能已造成约 900 名用户合计损失约 5500 万日元（约合人民币 350 万元）。该公司将予以全额补偿。由于 APP 注册量达到 150 万，损失可能进一步扩大，目前已暂停所有充值和新用户注册。7 月 1 日，7-11 便利店推出了一款名为 “7pay” 的无现金智能手机支付应用程序。据美国科技网站 ZDNet 报道 ，7pay 的密码重置功能存在严重的安全漏洞：密码重置链接可以被发到任意第三方电子邮箱，而不是原账户持有者的注册邮箱。由于没有二次验证，黑客只需要在网络上找到原账户持有人的电子邮件地址、出生日期和电话号码，并填写自己控制的邮箱地址，就可以重置任意用户的密码并盗用账户。

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：010-82990315