国家互联网应急中心

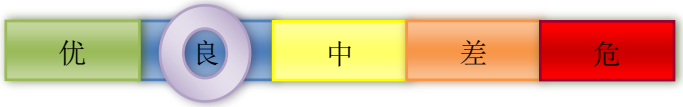
2018 年第 25 期

6 月 18 日-6 月 24 日

网络安全信息与动态周报

CNCERT/CC

本周网络安全基本态势

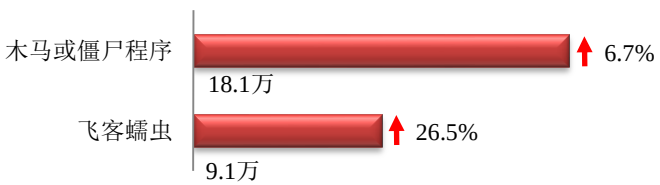


境内感染网络病毒的主机数量	•27.2万	↑ 12.6%
境内被篡改网站总数 其中政府网站数量	•1033 •32	↓ 8.7% ↑ 6.7%
境内被植入后门网站总数 其中政府网站数量	•660 •21	↓ 9.8% ↑ 31.3%
针对境内网站的仿冒页面数量	•959	↑ 2.3%
新增信息安全漏洞数量 其中高危漏洞数量	•217 •69	↓ 28.1% ↓ 36.7%

═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

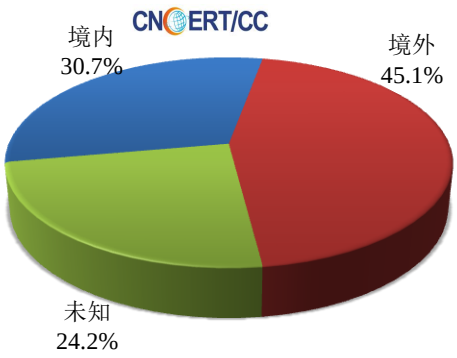
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 27.2 万个，其中包括境内被木马或被僵尸程序控制的主机约 18.1 万以及境内感染飞客（conficker）蠕虫的主机约 9.1 万。

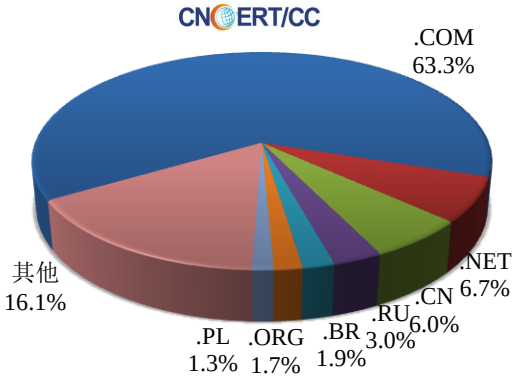


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 466 个，涉及 IP 地址 23861 个。在 466 个域名中，有 45.1%为境外注册，且顶级域为.com 的约占 63.3%；在 23861 个 IP 中，有约 33.2%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 57 个 IP。

本周放马站点域名注册所属境内外分布
(6/18-6/24)



本周放马站点域名所属顶级域的分布
(6/18-6/24)



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。

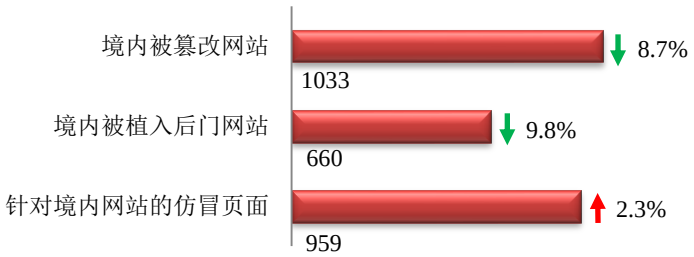
ANVA恶意地址黑名单发布地址

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。

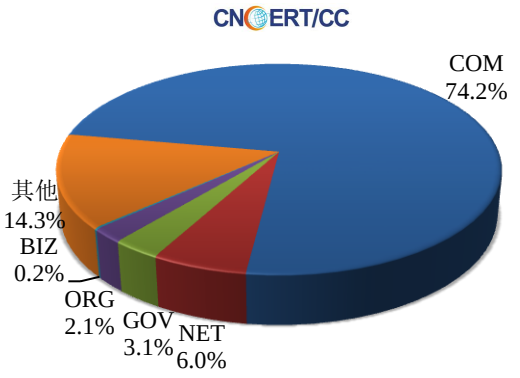
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1033 个；境内被植入后门的网站数量为 660 个；针对境内网站的仿冒页面数量为 959。

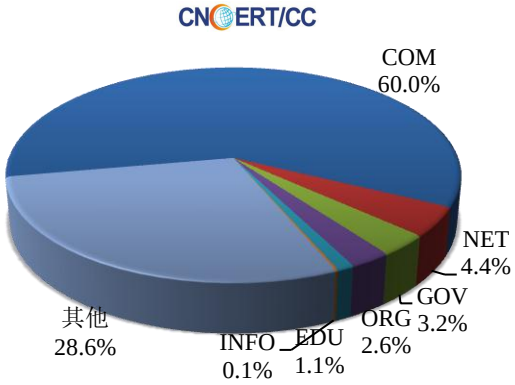


本周境内被篡改政府网站（GOV 类）数量为 32 个（约占境内 3.1%），较上周环比上升了 6.7%；境内被植入后门的政府网站（GOV 类）数量为 21 个（约占境内 3.2%），较上周环比上升了 31.3%；针对境内网站的仿冒页面涉及域名 375 个，IP 地址 187 个，平均每个 IP 地址承载了约 5 个仿冒页面。

本周我国境内被篡改网站按类型分布
(6/18-6/24)

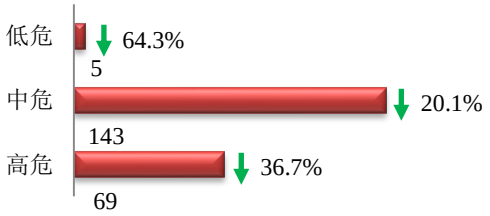


本周我国境内被植入后门网站按类型分布
(6/18-6/24)

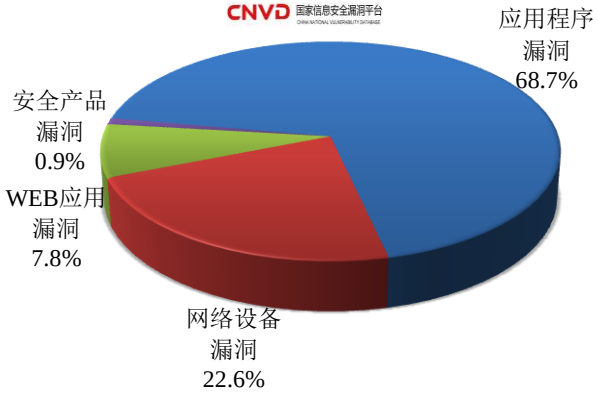


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 217 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
(6/18-6/24)



本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是网络设备漏洞和 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

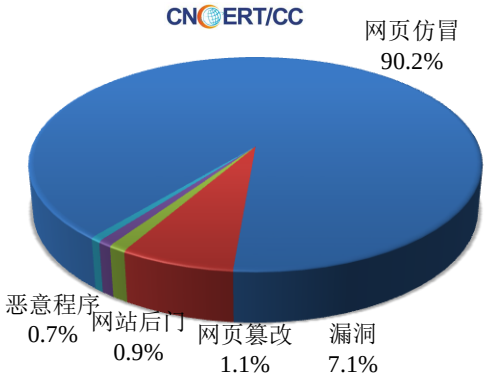
http://www.cnvd.org.cn/webinfo/list?type=4

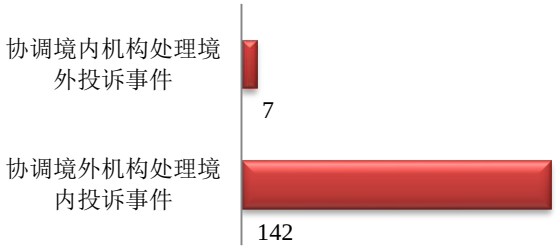
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 451 起，其中跨境网络安全事件 149 起。

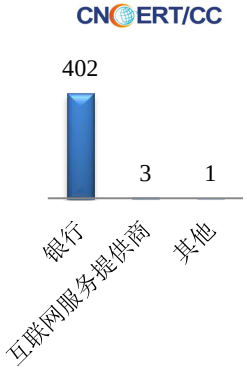
本周CNCERT处理的事件数量按类型分布 (6/18-6/24)



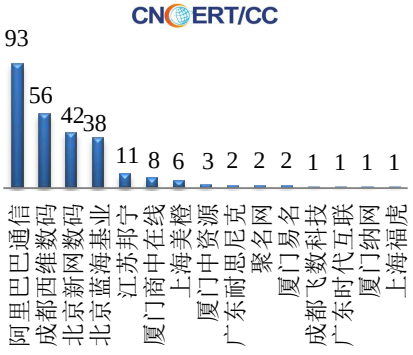


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 406 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 402 起和互联网服务提供商仿冒事件 3 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(6/18-6/24)

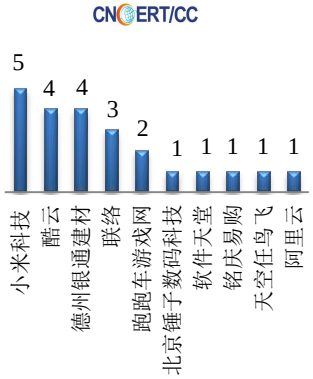


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (6/18-6/24)



本周，CNCERT 协调 10 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 23 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
(6/18-6/24)



业界新闻速递

1、美国网络司令部获权先发制人防止黑客攻击

环球网 美媒 6 月 17 日报道称，美国五角大楼已悄悄授权美国网络司令部采取“更为激进的方式”保护美国免受网络攻击。这个转变代表这支部队将有权对外国网络进行日常黑客突击检查。报道称，此前，网络司令部只是防御黑客网络攻击，很少进行报复性进攻。但据战略文件以及军事和情报官员透露，今年春天，五角大楼提升网络司令部的地位后，司令部几乎每天都会打击外国网络，试图在对方网络武器释放之前使其丧失能力。美媒表示，目前尚不清楚在进行机密操作时，政府如何权衡这项计划所涉及的各种风险。但美国的军事黑客现在必须"在敌人的危险行动可能带来损失之前对予以反击"。美国将中国、朝鲜、伊朗和俄罗斯视作网络空间的敌人。

2、欧盟 9 国将组建快速回应小组 应对网络攻击

环球网 6 月 22 日消息 瑞士资讯 6 月 21 日援引法新社报道称，领导部分欧洲国家成立网络快速回应小组的立陶宛于当地时间 6 月 21 日宣布，欧盟 9 个成员国将在欧盟新制订的防卫协定架构下成立快速回应小组，以对抗网络攻击。立陶宛国防部长雷蒙达斯•卡罗布利斯告诉法新社，9 国已同意加入，目标是要成立各国轮值的欧盟网络快速回应小组。他解释说，克罗地亚、爱沙尼亚、荷兰和罗马尼亚的国防部长 25 日将和他一起在卢森堡签署协议;另外，芬兰、法国、波兰和西班牙会在下半年加入。卡罗布利斯表示，由各国轮流召集专家组成的回应小组，将准备协助各国政府应对网络攻击，轮值日程表预定会在 2019 年通过。他期望欧盟会拨出资金购买软件和其他设备，并指出会继续和欧盟各机构讨论法律和技术性方面问题。

3、前 CIA 雇员被指控向维基解密泄露黑客攻击工具

cnBeta.COM6 月 19 日消息 周一的时候，一名前中央情报局雇员被指控向维基解密泄露了黑客工具。美国

司法部周一表示，在一个大陪审团做出的 13 项指控中，29 岁的 Joshua Adam Schulte 被指窃取了机密的国防信息。由起诉书可知，2016 年的时候，Schulte 从一个 CIA 网络中窃取了机密信息，然后将之传输给了起诉书中未被确认的某个组织。维基解密将这批泄露信息称作“七号金库”（Vault 7），披露美国中央情报局借助这些工具来入侵手机、计算机和电视。

4、韩国最大虚拟币交易平台被黑 约 2 亿元资产被盗

中新网 6 月 20 日消息 据韩联社报道，韩国最大虚拟货币交易平台 Bithumb 遭黑客入侵，约 350 亿韩元（约合人民币 2.04 亿元）资产被盗。据 Bithumb 介绍，公司于当地时间 19 日下午 11 时发现异常情况，于 20 日凌晨 1 时 30 分许采取限制存储措施后清点资产发现了平台被黑情况，随后于当天上午 9 时 40 分许向韩国网络振兴院（KISA）举报。Bithumb 通知，损失的部分将由公司赔偿，客户资产已转移到未接入互联网的外部存储设备。

5、航班追踪服务 Flightradar24 遭遇数据泄露 称超过 23 万用户受影响

黑客视界 6 月 22 日消息 从本周早些时候开始，一些 Flightradar24 用户开始都收到电子邮件，并附有密码重置链接，强制要求他们更改密码。电子邮件提醒用户，由于安全漏洞，在 2016 年 3 月 16 日之前注册的用户（超过 23 万人）可能遭遇个人信息泄露，这包括与注册账户相关的电子邮箱地址以及哈希密码。Flightradar24 公司之后在其官方论坛以及 Twitter 上对此进行了回应，称数据泄露事件的确真实存在。该公司同时也强调，遭泄露的数据仅限于电子邮件中提到的，付款信息或者其他个人信息均未受到损害。该公司的一位发言人证实，安全漏洞仅限于其中一台服务器，而付款信息并不存储在其中。在上周晚些时候发现该服务器早入侵后，他们就立即进行了关机处理。

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：饶毓

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158