国家互联网应急中心

2019 年第 25 期
6 月 17 日-6 月 23 日

网络安全信息与动态周报

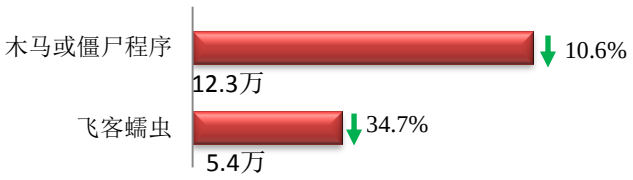
本周网络安全基本态势

境内感染网络病毒的主机数量	•17.7万	↓19.7%
境内被篡改网站总数 其中政府网站数量	•390 •0	↓94.2% ↓100.0%
境内被植入后门网站总数 其中政府网站数量	•3259 •48	↓1.1% ↑6.7%
针对境内网站的仿冒页面数量	•8206	↓21.9%
新增信息安全漏洞数量 其中高危漏洞数量	•200 •50	↓31.7% ↓54.5%

═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

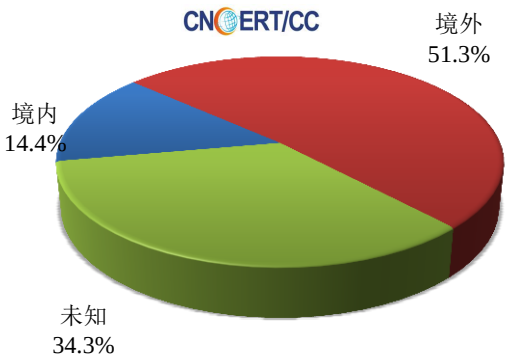
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 17.7 万个，其中包括境内被木马或被僵尸程序控制的主机约 12.3 万以及境内感染飞客（conficker）蠕虫的主机约 5.4 万。

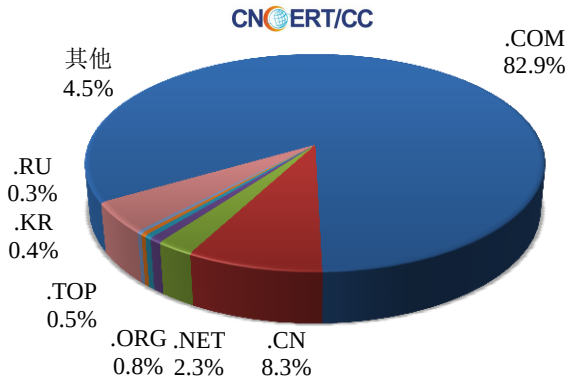


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 4601 个，涉及 IP 地址 3242 个。在 4601 个域名中，有 51.3%为境外注册，且顶级域为.com 的约占 82.9%；在 3242 个 IP 中，有约 53.7%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 504 个 IP。

本周放马站点域名注册所属境内外分布
(6/17-6/23)



本周放马站点域名所属顶级域的分布
(6/17-6/23)



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。

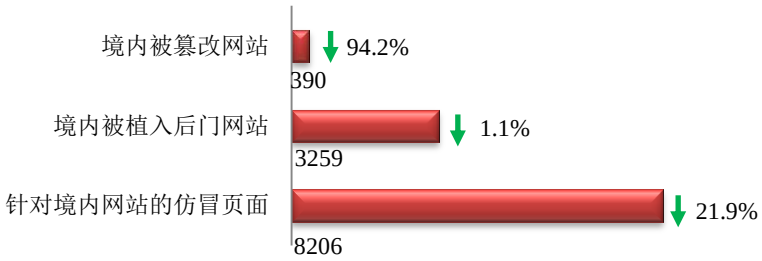
ANVA恶意地址黑名单发布地址

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。

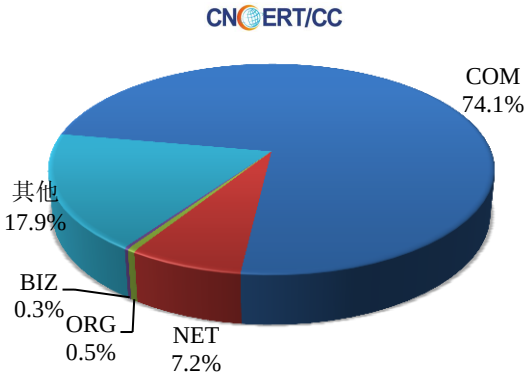
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 390 个；境内被植入后门的网站数量为 3259 个；针对境内网站的仿冒页面数量 8206 个。

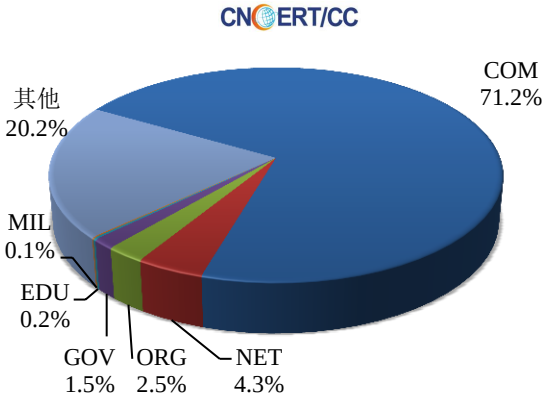


本周境内被篡改政府网站（GOV 类）数量为 0 个，较上周环比下降 100.0%；境内被植入后门的政府网站（GOV 类）数量为 48 个（约占境内 1.5%），较上周环比下降上升 6.7%；针对境内网站的仿冒页面涉及域名 712 个，IP 地址 405 个，平均每个 IP 地址承载了约 20 个仿冒页面。

本周我国境内被篡改网站按类型分布
(6/17-6/23)

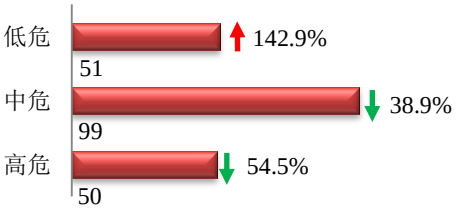


本周我国境内被植入后门网站按类型分布
(6/17-6/23)

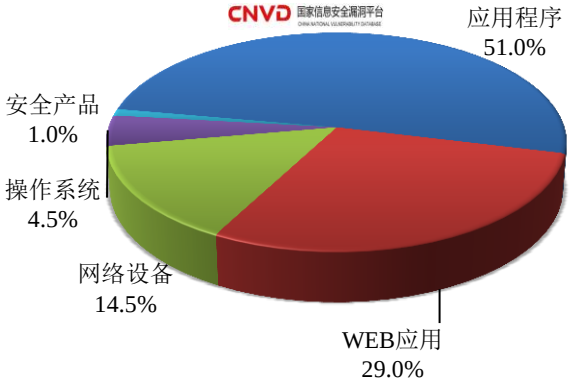


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 200 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
(6/17-6/23)



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

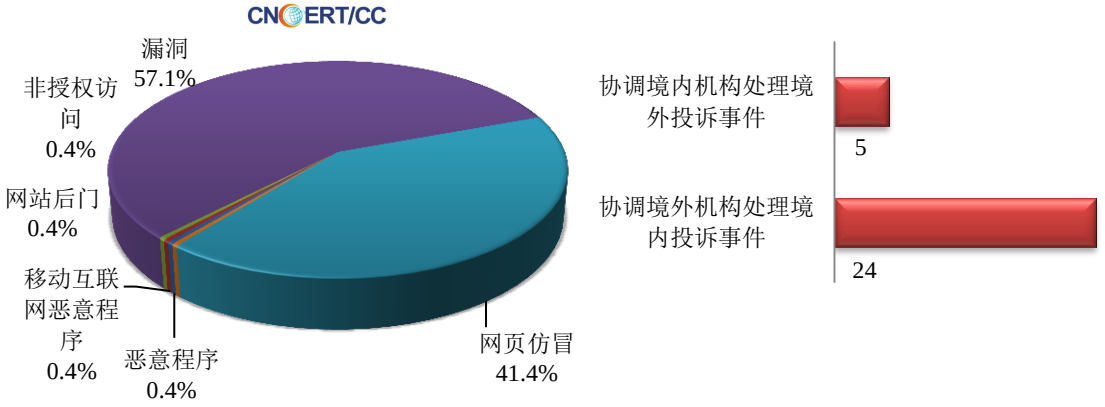
http://www.cnvd.org.cn/webinfo/list?type=4

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

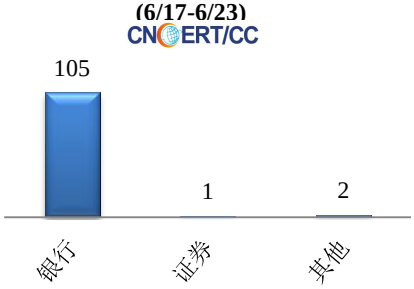
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 261 起，其中跨境网络安全事件 29 起。

本周CNCERT处理的事件数量按类型分布 (6/17-6/23)

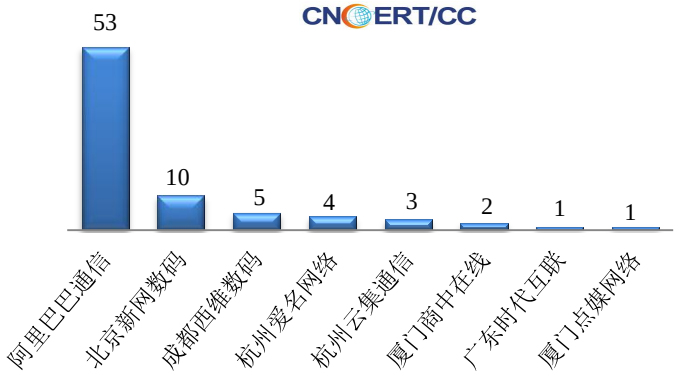


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 108 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 105 起和证券仿冒事件 1 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (6/17-6/23)

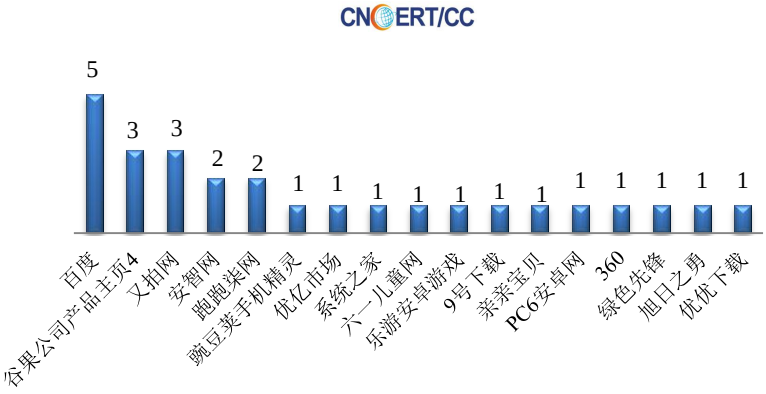


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (6/17-6/23)



本周，CNCERT 协调 17 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 27 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
(6/17-6/23)



业界新闻速递

1、 CBP 分包商出现重大数据泄露事件 至少 5 万名美国车牌信息在暗网出售

Cnbeta.COM6 月 18 日消息 援引美国有线电视新闻网（CNN）报道，美国海关和边境保护局（CBP）所雇佣的分包商 Perceptics 出现重大数据泄露事件，在对已经泄露的数据分析后发现至少有 5 万名美国车牌号码数据在暗网上被销售。更为重要的是，CBP 向 CNN 透露从未向该公司授权保留这些车主信息。CNN 对分包商 Perceptics 泄露的数据进行了分析，这些数据目前已经在暗网上进行出售。它显示了至少 5 万个独特的美国车牌号码记录。

2、 美媒曝美国已在俄电网植入病毒 可随时发动攻击

环球时报 6 月 16 日消息 美国政府官员承认，早在 2012 年就已在俄罗斯电网中植入病毒程序，可随时发起网络攻击。这一惊人爆料立即引发世界关注。《纽约时报》称，不太为人关注的是，去年夏天美国已经开始放宽了相关的法律授权限制，允许在发生冲突时对对方国家的网络进行瘫痪性攻击。多名中国学者 16 日接受《环球时报》采访时表示，显然，无论在技术上、法律上，还是战略上，美国的网络战略已经变成攻击性的网络战略，美国已经成为全球网络安全的最大威胁。

3、 美国三所大学发生数据泄露事件

E 安全 6 月 20 日消息 美国格雷斯兰大学、俄勒冈州立大学和密苏里南方州立大学披露了数据泄露事件，黑客未经授权访问了员工的电子邮件账户，影响了学生或员工的个人身份信息。在调查涉及三所大学的公开资

料私隐事件时，并没有发现受影响的个人资料被窃取或恶意使用的证据。格雷斯兰大学在 6 月 14 日发布的一份数据泄露通知中称，未经授权的用户分别于 2019 年 3 月 29 日、2019 年 4 月 1 日至 30 日和 4 月 12 日至 5 月 1 日访问了员工的电子邮件账户。泄露的资料包括、姓名、社保号、出生日期、地址、电话号码、电子邮件地址、父母/孩子、工资信息、格雷斯兰招生的财务信息。

4、 佛罗里达州一家广告公司泄露了美国退伍军人战争伤害的数据

Cnbeta.COM6 月 20 日消息 一家总部位于佛罗里达州的广告代理商的一个数据库在网上被泄露。该数据库包括了过去广告活动的详细信息，包括有关医疗事故案件的信息，以及美国退伍军人战争伤害的敏感细节。该数据库由 vpnMentor 的安全研究人员发现，属于 X Social Media，这是一家为法律行业开展 Facebook 和 Instagram 广告活动的广告公司。该公司的主要兴趣和重点之一是针对医疗事故诉讼和与伤害相关的集体诉讼进行广告宣传。这些广告活动的目的是收集可能的各方兴趣，用户被重定向到专门的网站，在那里他们填写表格，看看他们是否有资格获得特定案件和可能的法律援助。该数据库包含了填写表格的用户的 150,000 多条回复。这些表格中包含的数据通常包括全名、电子邮件地址、家庭住址、电话号码以及与其案件相关的详细信息 - 主要针对医疗损伤。

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：张宇鹏

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315