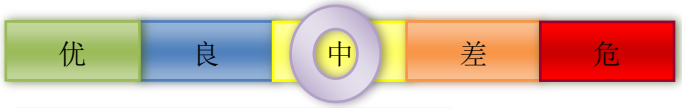
国家互联网应急中心

2019 年第 29 期
7 月 15 日-7 月 21 日

网络安全信息与动态周报

本周网络安全基本态势

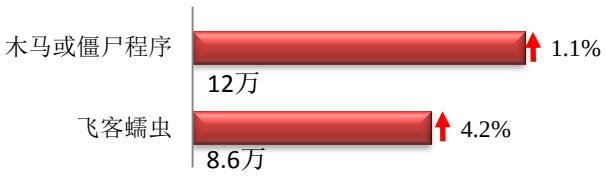


境内感染网络病毒的主机数量	•20.6万	2.4%
境内被篡改网站总数[1] 其中政府网站数量	•5135 •5	29.3% 25.0%
境内被植入后门网站总数 其中政府网站数量	•3462 •46	3.1% 64.3%
针对境内网站的仿冒页面数量	•542	5.1%
新增信息安全漏洞数量 其中高危漏洞数量	•417 •138	32.0% 12.2%

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

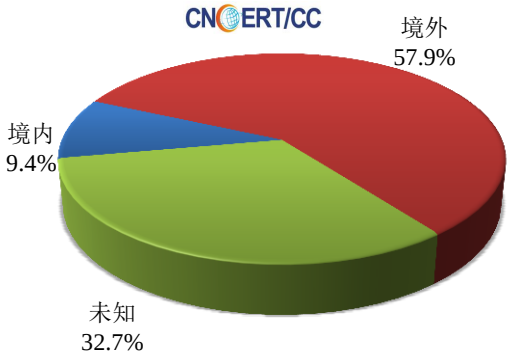
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 20.6 万个，其中包括境内被木马或被僵尸程序控制的主机约 12.0 万以及境内感染飞客（conficker）蠕虫的主机约 8.6 万。

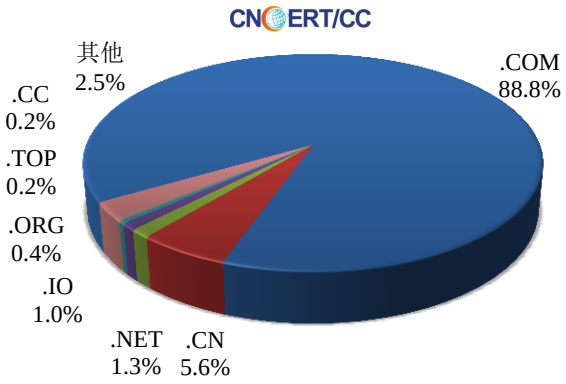


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 12360 个，涉及 IP 地址 4789 个。在 12360 个域名中，有 57.9 为境外注册，且顶级域为.com 的约占 88.8%；在 4789 个 IP 中，有约 45.3%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 756 个 IP。

本周放马站点域名注册所属境内外分布
(7/15-7/21)



本周放马站点域名所属顶级域的分布
(7/15-7/21)



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。

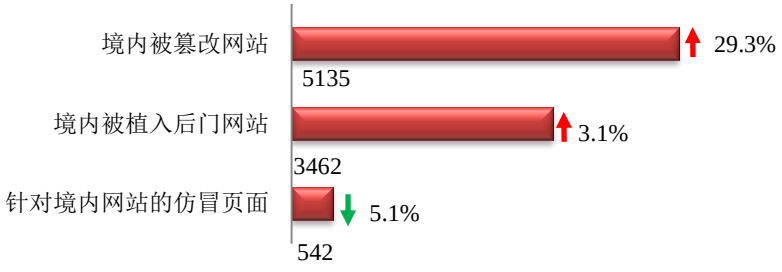
ANVA恶意地址黑名单发布地址

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。

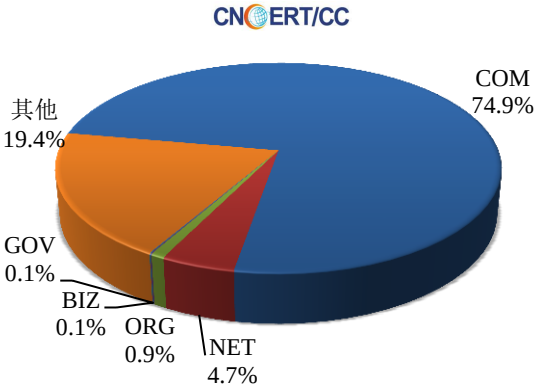
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 5135 个；境内被植入后门的网站数量为 3462 个；针对境内网站的仿冒页面数量 542 个。

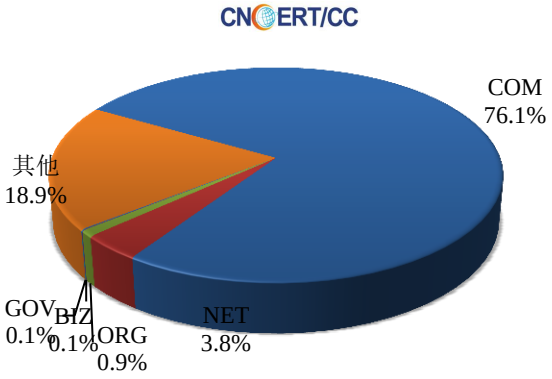


本周境内被篡改政府网站（GOV 类）数量为 5 个（约占境内 0.1%），较上周环比上涨 25.0%；境内被植入后门的政府网站（GOV 类）数量为 46 个（约占境内 1.3%），较上周环比上涨 64.3%；针对境内网站的仿冒页面涉及域名 385 个，IP 地址 180 个，平均每个 IP 地址承载了约 3 个仿冒页面。

本周我国境内被篡改网站按类型分布
(7/15-7/21)

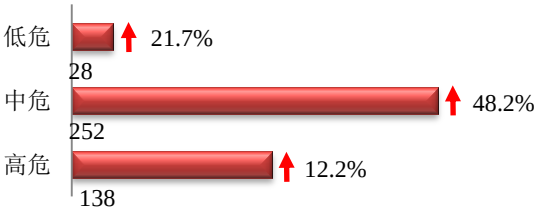


本周我国境内被植入后门网站按类型分布
(7/15-7/21)

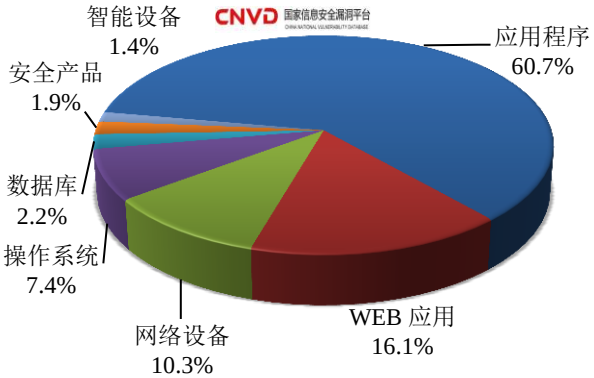


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 417 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
(7/15-7/21)



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

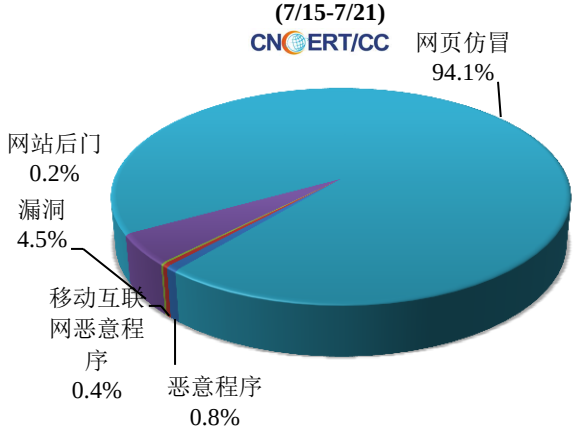
http://www.cnvd.org.cn/webinfo/list?type=4

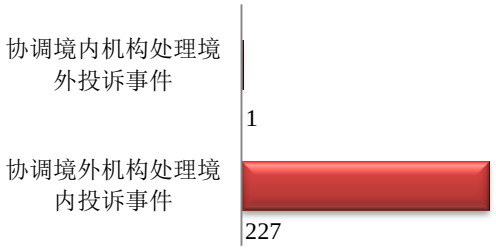
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 529 起，其中跨境网络安全事件 228 起。

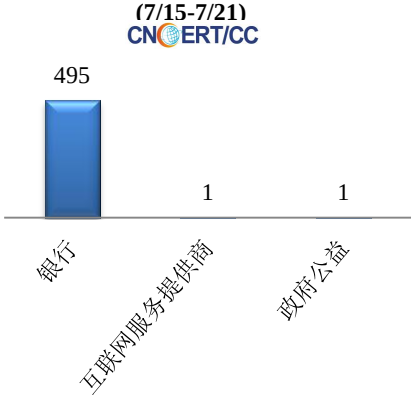
本周CNCERT处理的事件数量按类型分布 (7/15-7/21)



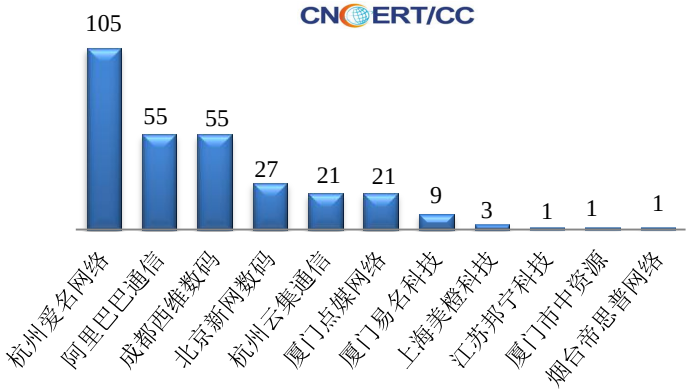


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 497 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 495 起和互联网服务提供商仿冒事件 1 起。

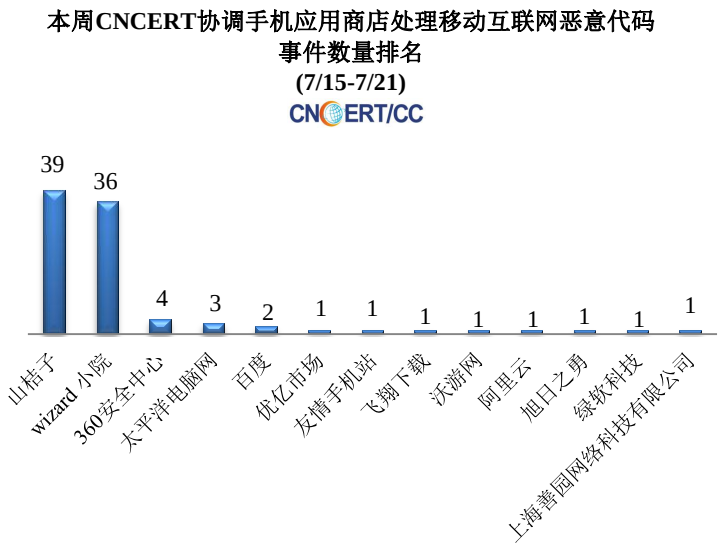
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (7/15-7/21)



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 (7/15-7/21)



本周，CNCERT 协调 13 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 92 个。



业界新闻速递

1、 工业和信息化部部署电信和互联网行业提升网络数据安全保护能力专项行动工作

工信部官网 7 月 17 日消息 工业和信息化部网络安全管理局召开全国视频会议，深入部署推进电信和互联网行业提升网络数据安全保护能力专项行动。部网络安全管理局对《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》进行了解读。中国移动、腾讯、网易、中国信息通信研究院相关负责人分别代表有关企业和单位作了交流发言，介绍了各自数据安全工作开展情况和后续贯彻落实专项行动的有关考虑。

2、 哈萨克斯坦周三开始实施互联网加密流量过滤政策

Hacker.News7 月 17 日报道 哈萨克斯坦政府开始拦截境内的一切 HTTPS 互联网通讯。当地政府已经指示当地互联网服务供应商们（ISP）强制各自用户在所有设备上及每个浏览器中安装政府发布的证书,允许当地政府机构解密用户的 HTTPS 通讯，查看其内容，然后再用他们的证书加密后发送至接收方。

3、 黑客攻入俄罗斯联邦安全局承包商服务器 窃取 7.5TB 的数据

cnBeta.COM7 月 21 日消息 黑客入侵了俄罗斯国家情报部门 FSBRussia’s Federal Security Service 的承包商 SyTech，并从那里窃取了该公司为 FSB 工作的内部项目的信息，包括用于对 Tor 流量进行去匿名化的信息。英国航空公司因数据泄露面临 1.83 亿英镑巨额罚款。

4、 保加利亚遭黑客入侵 500 万民众信息外泄

澎湃新闻 7 月 18 日消息 在一家新闻机构收到一封宣布对信息失窃一事负责的邮件之后，保加利亚当局才公开承认了国家收入署的数据库遭到黑客攻击的事实。在这个只有 700 万人口的国家，500 万保加利亚人和外国人的姓名、地址、收入和社会保障信息都受到了波及。保加利亚国家收入署在 6 月遭到黑客攻击，攻击可能持续了较长时间。

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：高川

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315