国家互联网应急中心

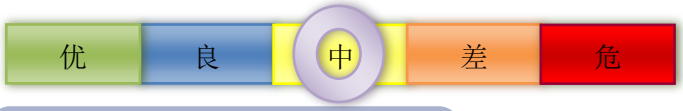
2019 年第 35 期

8 月 26 日-9 月 1 日

网络安全信息与动态周报

CNCERT/CC

本周网络安全基本态势

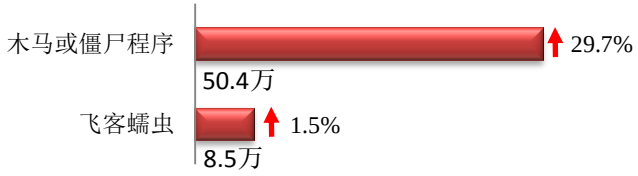


境内感染网络病毒的主机数量	•58.9 万	↑ 24.7%
境内被植入后门网站总数 其中政府网站数量	•2447 •22	↓ 22.9% ↓ 24.1%
针对境内网站的仿冒页面数量	•82	↓ 80.5%
新增信息安全漏洞数量 其中高危漏洞数量	•401 •79	↑ 4.7% ↓ 24.0%

═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

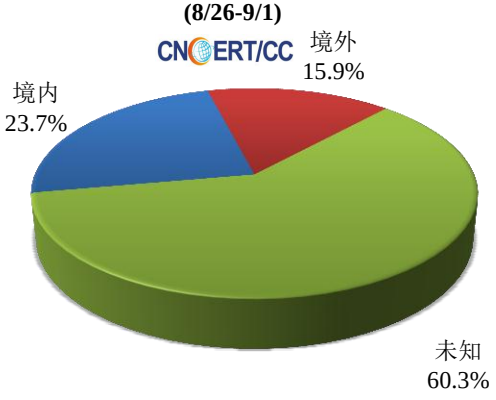
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 58.9 万个，其中包括境内被木马或被僵尸程序控制的主机约 50.4 万以及境内感染飞客（conficker）蠕虫的主机约 8.5 万。

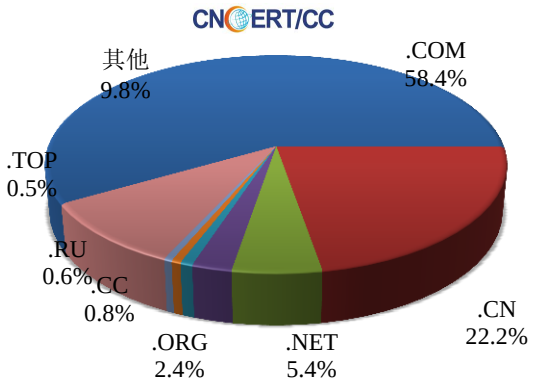


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域 2232 个，涉及 IP 地 3780 个。在 2232 个域名中，有 15.9%为境外注册，且顶级域为.com 的约占 58.4%；在 3780 个 IP 中，有约 46.2%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 689 个 IP。

本周放马站点域名注册所属境内外分布
(8/26-9/1)



本周放马站点域名所属顶级域的分布
(8/26-9/1)



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。

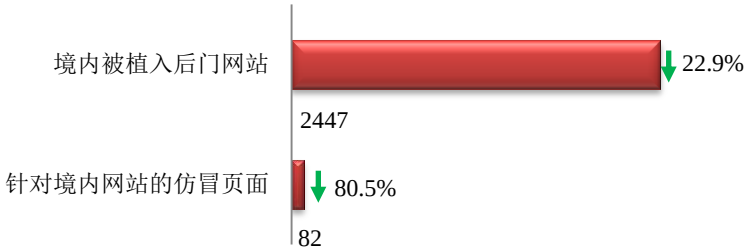
ANVA恶意地址黑名单发布地址

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。

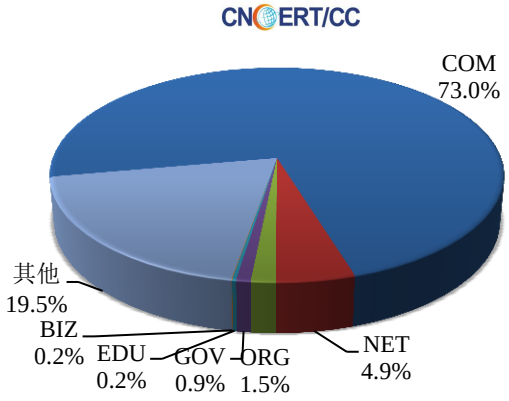
本周网站安全情况

本周 CNCERT 监测发现境内被植入后门的网站数量为 2447 个；针对境内网站的仿冒页面数量 82 个。



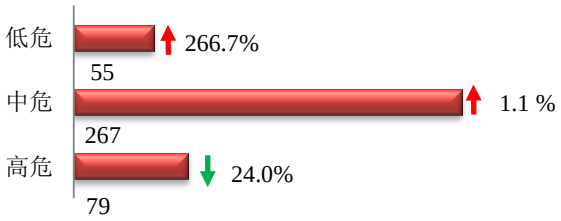
本周境内境内被植入后门的政府网站（GOV 类）数量为 22 个（约占境内 0.9%），较上周环比下降 24.1%；针对境内网站的仿冒页面涉及域名 61 个，IP 地址 57 个，平均每个 IP 地址承载了约 1 个仿冒页面。

本周我国境内被植入后门网站按类型分布
(8/26-9/1)

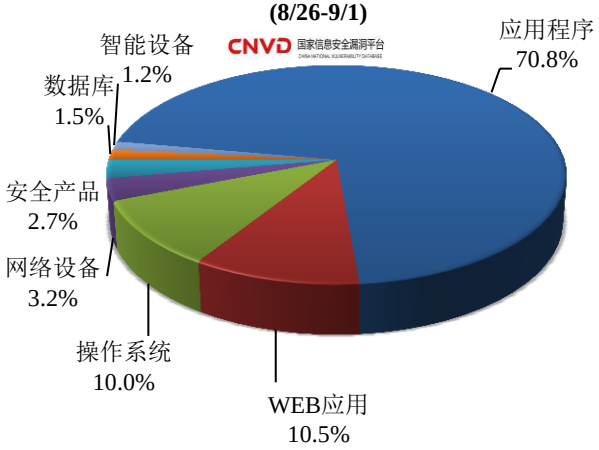


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 401 个，信息安全漏洞威胁整体评价级别为良。



本周CNVD收录漏洞按影响对象类型分布
(8/26-9/1)



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 应用漏洞和操作系统。

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

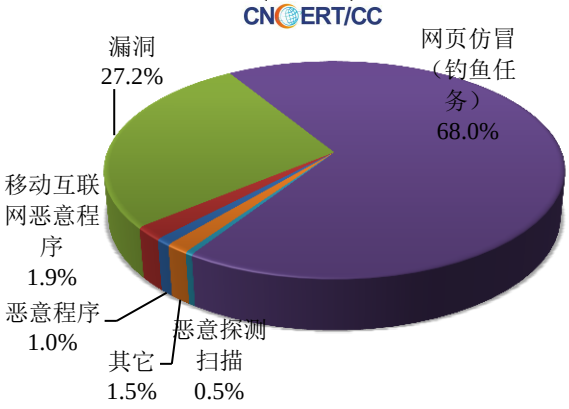
http://www.cnvd.org.cn/webinfo/list?type=4

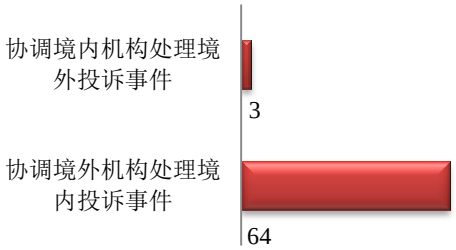
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 206 起，其中跨境网络安全事件 67 起。

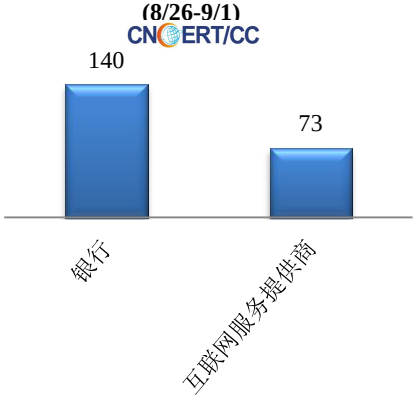
本周CNCERT处理的事件数量按类型分布 (8/26-9/1)



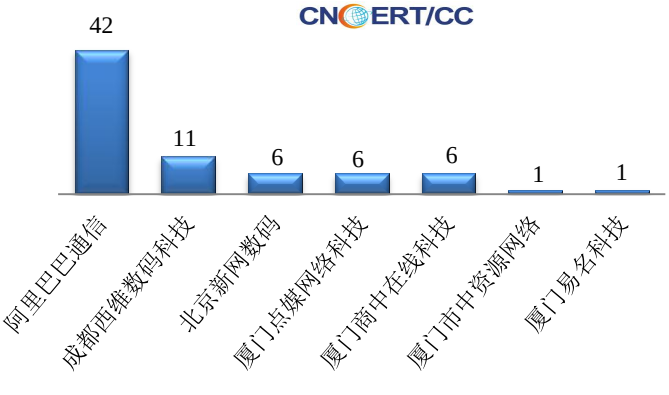


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 213 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 140 起和互联网服务提供商 73 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (8/26-9/1)

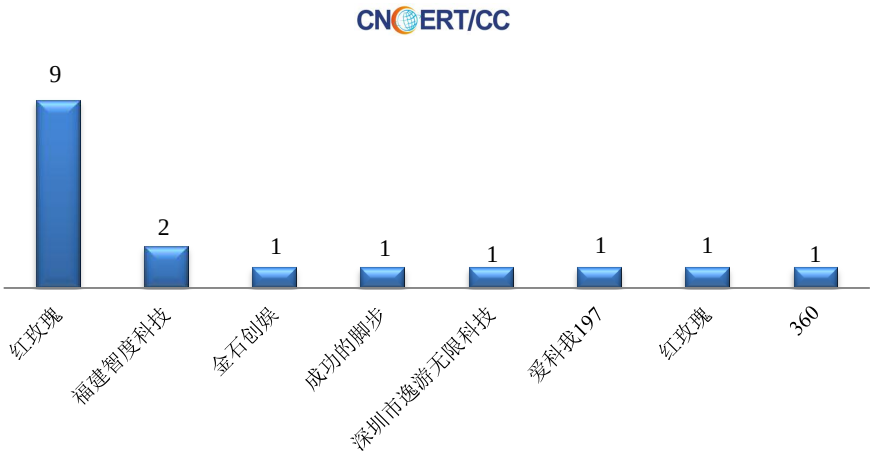


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (8/26-9/1)



本周，CNCERT 协调 8 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 17 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
(8/26-9/1)



业界新闻速递

1、工信部等十部门发文 支持工业互联网安全产业发展

8 月 29 日人民网消息，28 日中华人民共和国工业和信息化部网站正式发布由工业和信息化部、教育部、人力资源和社会保障部、生态环境部、卫生健康委、应急管理部、国务院国资委、国家市场监管总局、国家能源局、国防科工局十部门联合出台实施的《加强工业互联网安全工作的指导意见》，这不仅是工业互联安全工作的专门指引和纲领性文件，更是强化安全体系化建设、协同发力的重要举措，事关当前形势和长远发展，对推进国家网络安全全局工作具有重要意义。

2、刘鹤：尊重和保护个人隐私，规范大规模数据采集活动

8 月 26 日第一财经消息，中共中央政治局委员、国务院副总理刘鹤在第二届中国国际智能产业博览会上表示， 智能产业发展迎来重大机遇，同时也带来一些挑战，我们要从促进人类发展和维护世界和平的高度，坚持好四个原则，即坚持增进人类福祉导向、坚持提高效率与创造就业等方面的平衡、尊重和保护个人隐私以及坚持维护伦理道德底线，从而把握好智能化的发展方向。

3、美司法部阻止一中美公司海底电缆合作项目

8 月 28 日,据《华尔街日报》报道，消息人士称，美国司法部的官员正试图阻止一个由谷歌、Facebook 和

一家中国合作伙伴共同建设的海底光缆项目。该项目名为 PLCN（Pacific LightCableNetwork），是一条穿过太平洋连接中国和美国的海底光缆，全长 8,000 英里（13,000 公里），可以为太平洋两岸的用户提供更快的连接速度。目前为止，该项目的临时许可证 9 月份将会到期，但依然在进行。但知情人士表示，该项目有可能无法获得开展业务所需的执照。同时知情人士说，美国司法部已发出坚决反对该项目的信号。

4、世界最大加密货币交易所发生数据泄露事故

8 月 26 日 TheHackerNews 消息，世界最大加密货币交易所 Binance 确认黑客已从第三方获取了被称为“客户了解”的用户身份证明图像。消息人士称，黑客在窃取信息后，曾威胁该交易所支付 300 比特币，否则将公开其窃取的所有 KYC 图像。为此，Binance 表示，它将为所有受到影响的用户提供终身 VIP 会员资格。

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：刘立伟

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315