国家互联网应急中心

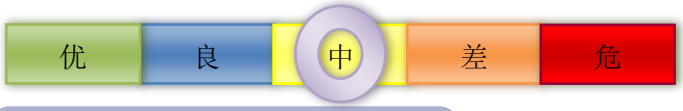
网络安全信息与动态周报

2019 年第 39 期

9 月 23 日-9 月 29 日

CNCERT/CC

本周网络安全基本态势

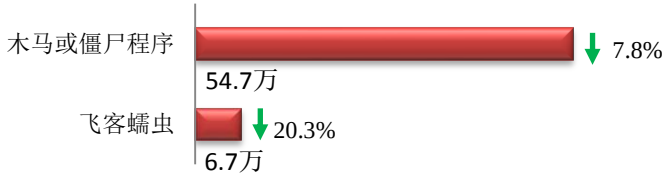


境内感染网络病毒的主机数量	•61.4 万	↓9.4%
境内被植入后门网站总数 其中政府网站数量	•3419 •33	↑5.7% ↓19.5%
针对境内网站的仿冒页面数量	•54	↑0.0%
新增信息安全漏洞数量 其中高危漏洞数量	•505 •126	↑24.7% ↑43.2%

=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

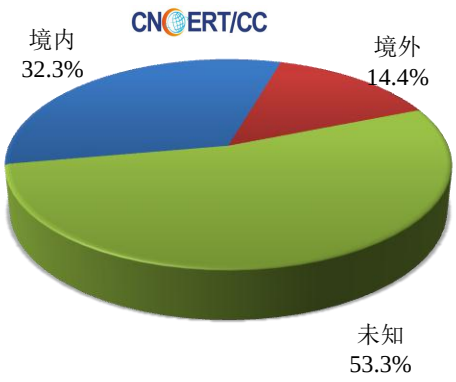
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 61.4 万个，其中包括境内被木马或被僵尸程序控制的主机约 54.7 万以及境内感染飞客（conficker）蠕虫的主机约 6.7 万。

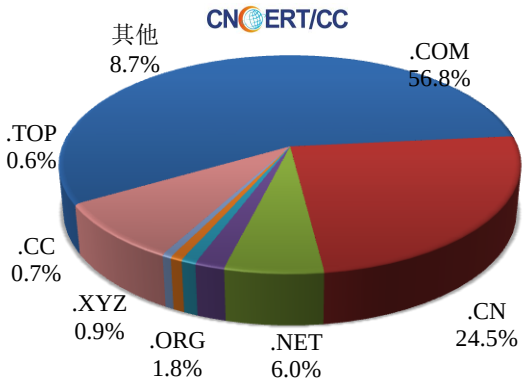


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域 1210 个，涉及 IP 地 2881 个。在 1210 个域名中，有 14.4%为境外注册，且顶级域为.com 的约占 56.8%；在 2881 个 IP 中，有约 24.7%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 350 个 IP。

本周放马站点域名注册所属境内外分布
(9/23-9/29)



本周放马站点域名所属顶级域的分布
(9/23-9/29)



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。

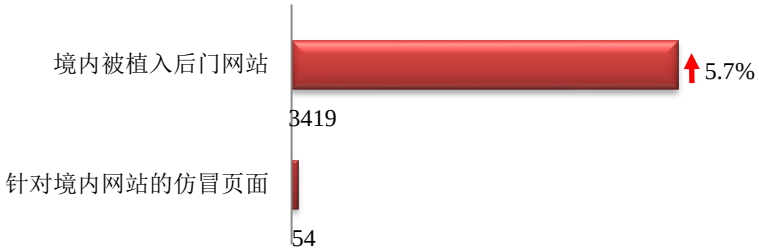
ANVA恶意地址黑名单发布地址

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。

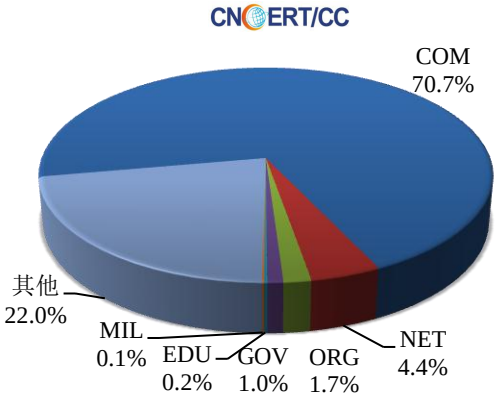
本周网站安全情况

本周 CNCERT 监测发现境内被植入后门的网站数量为 3419 个；针对境内网站的仿冒页面数量 54 个。



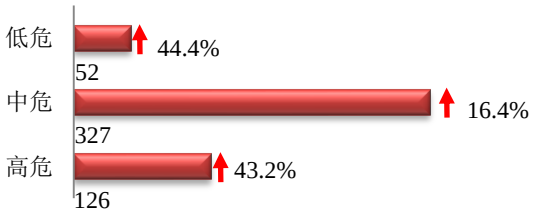
本周境内境内被植入后门的政府网站（GOV 类）数量为 33 个（约占境内 1.0%），较上周环比下降 19.5%；针对境内网站的仿冒页面涉及域名 30 个，IP 地址 27 个，平均每个 IP 地址承载了约 2 个仿冒页面。

本周我国境内被植入后门网站按类型分布
(9/23-9/29)

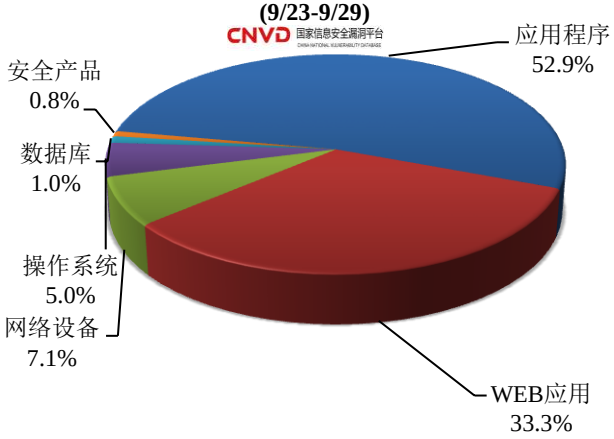


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 505 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
(9/23-9/29)



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

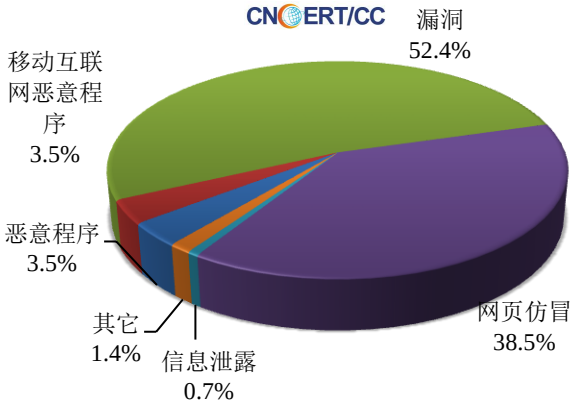
http://www.cnvd.org.cn/webinfo/list?type=4

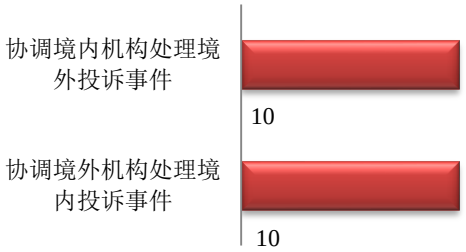
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 143 起，其中跨境网络安全事件 20 起。

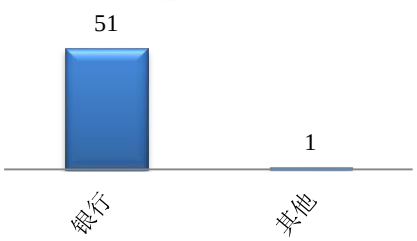
本周CNCERT处理的事件数量按类型分布 (9/23-9/29)



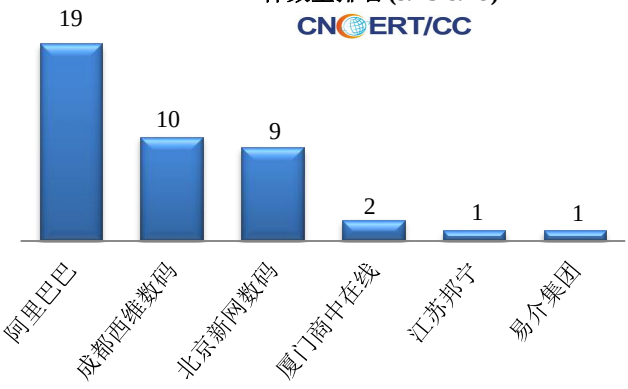


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 52 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 51 起和其他事件 1 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (9/23-9/29)

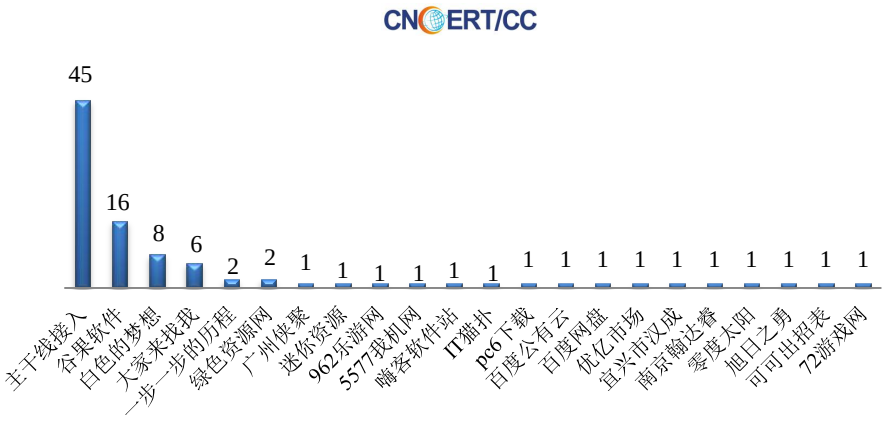


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (9/23-9/29)



本周，CNCERT 协调 22 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 95 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
(9/23-9/29)



业界新闻速递

1、工信部：《关于促进网络安全产业发展的指导意见》公开征求意见

9 月 27 日,中华人民共和国工业与信息部官网消息，为了进一步贯彻落实《中华人民共和国网络安全法》，积极发展网络安全产业，工业和信息化部会同有关部门起草了《关于促进网络安全产业发展的指导意见（征求意见稿）》（见附件），现面向社会公开征求意见。如有意见或建议，限于 2019 年 10 月 11 日前反馈。

2、航旅纵横新功能泄露用户隐私 回应：完全不符合事实

9 月 24 日新浪科技消息，针对航旅纵横 App 的社交新功能泄露用户隐私的新闻报道，航旅纵横在微博发布声明称近期个别媒体针对航旅纵横发表了泄露用户隐私等完全不符合事实的报道，对其产生了严重的负面影响，对不实报道将保留法律追诉权。

据报道，有网友反映，在航旅纵横上选座之后，陌生人可以看到自己的名字和头像（并且已经受到骚扰），自己也可以查询到陌生人的名字和头像，以此质疑航旅纵横泄露客户的隐私。对于质疑，航旅纵横回应称出行互动功能是航旅纵横在 2018 年 6 月上线的一个探索性功能，至今未做更新迭代。该功能默认关闭，虚拟身份与真实身份也是完全隔离的。

在此次的微博声明中，航旅纵横表示一直高度重视信息安全工作，通过多种技术手段以严格保护用户信息安全，并通过了相关主管部门的审核认定。

3、谷歌发布全新数据库 以帮助检测深度假冒视频音频

9 月 26 日 ZDNet 消息,谷歌与 Jigsaw 近日合作推出了一个全新可视化深度虚假数据集。新的数据集已被集成到相关基准测试软件当中，这将将有助于识别伪造的视频。现在用户可以在 FaceForensics Github 页面上下载这个数据集。

谷歌表示，该领域进展迅速，随着 DeepFake 技术发展，它将被添加到数据集中。谷歌还承诺将继续与该领域的合作伙伴合作。谷歌坚信支持一个蓬勃发展的研究社区，将减轻滥用合成媒体造成的潜在危害。

4、美国外卖服务 DoorDash 数据泄露：影响 490 万人

9 月 27 日 CNN 消息，美国外卖服务 DoorDash 周四宣布，一项安全漏洞暴露了该公司大约 490 万客户、商家和送货员的个人数据。这家总部位于旧金山的公司在一份声明中说，此次泄露的信息可能包括大约 10 万名送货工人的驾驶执照号码，其他数据可能包括“姓名、电子邮件地址、交货地址、订单历史记录、电话号码”等。

该公司还在声明说，一些消费者支付卡的最后四位数字也可能被暴露出来，但其中没有包含足够的数据来进行欺诈性收费。送货员和商家的银行帐号最后四位数可能已被他人访问。另外,DoorDash 的一位发言人表示，该数据泄露行为涉及第三方服务提供商，目前正在进行调查。

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：李明

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315