国家互联网应急中心

2019 年第 42 期
10 月 14 日-10 月 20 日

网络安全信息与动态周报

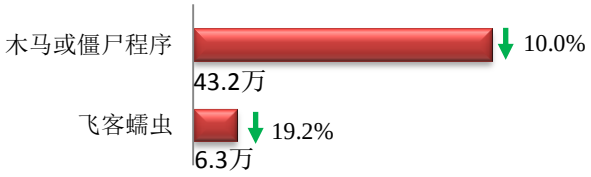
本周网络安全基本态势

境内感染网络病毒的主机数量	•49.6 万	11.3%
境内被植入后门网站总数 其中政府网站数量	•1959 •18	27.0% 63.6%
针对境内网站的仿冒页面数量	•574	63.5%
新增信息安全漏洞数量 其中高危漏洞数量	•406 •100	16.8% 13.8%

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

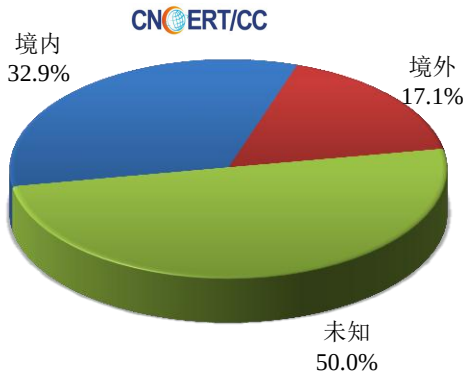
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 49.6 万个，其中包括境内被木马或被僵尸程序控制的主机约 43.2 万以及境内感染飞客（conficker）蠕虫的主机约 6.3 万。

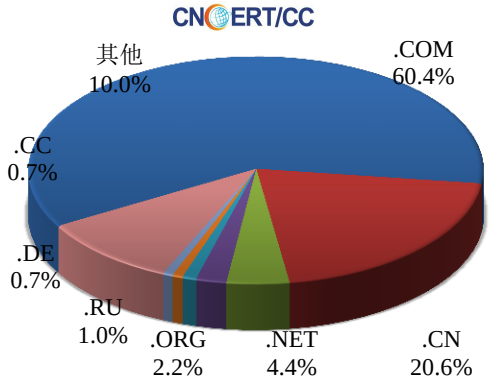


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域 1111 个，涉及 IP 地 1953 个。在 1111 个域名中，有 17.1%为境外注册，且顶级域为.com 的约占 60.4%；在 1953 个 IP 中，有约 43.6%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 307 个 IP。

本周放马站点域名注册所属境内外分布
(10/14-10/20)



本周放马站点域名所属顶级域的分布
(10/14-10/20)



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。

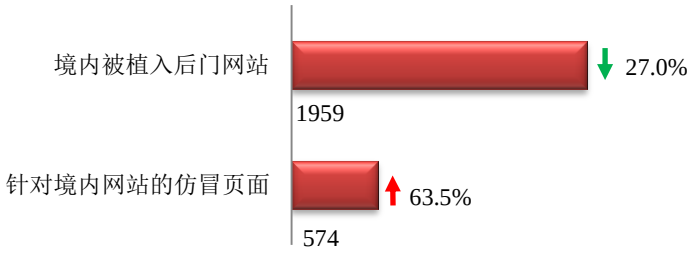
ANVA恶意地址黑名单发布地址

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。

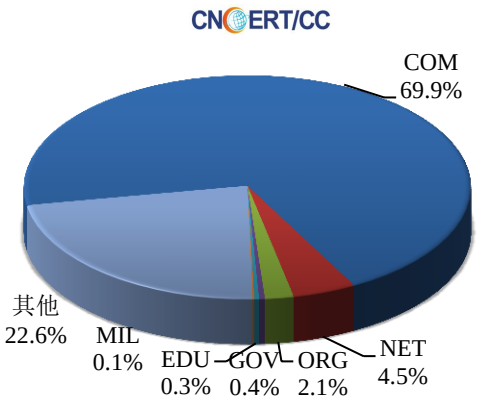
本周网站安全情况

本周 CNCERT 监测发现境内被植入后门的网站数量为 1959 个；针对境内网站的仿冒页面数量 574 个。



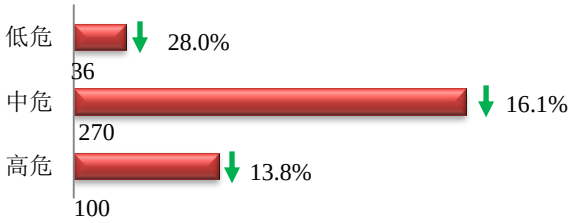
本周境内境内被植入后门的政府网站（GOV 类）数量为 18 个（约占境内 0.9%），较上周环比上涨 63.6%；针对境内网站的仿冒页面涉及域名 350 个，IP 地址 260 个，平均每个 IP 地址承载了约 3 个仿冒页面。

本周我国境内被植入后门网站按类型分布
(10/14-10/20)

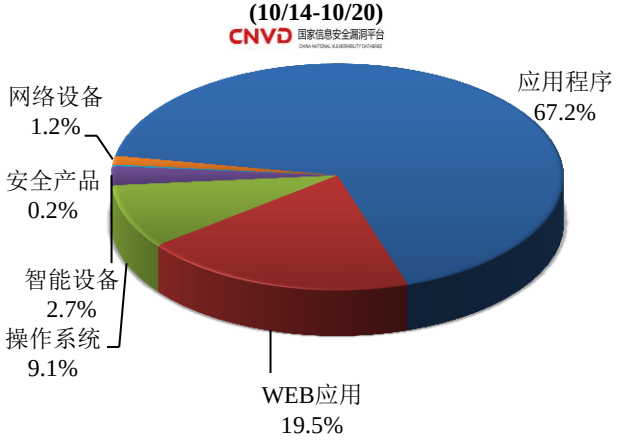


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 406 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
(10/14-10/20)



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

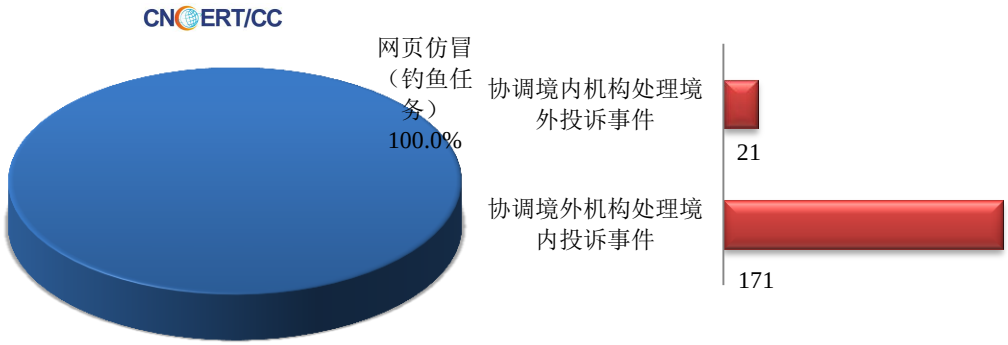
http://www.cnvd.org.cn/webinfo/list?type=4

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

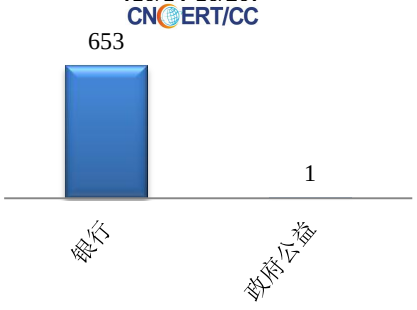
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 654 起，其中跨境网络安全事件 192 起。

本周CNCERT处理的事件数量按类型分布
(10/14-10/20)

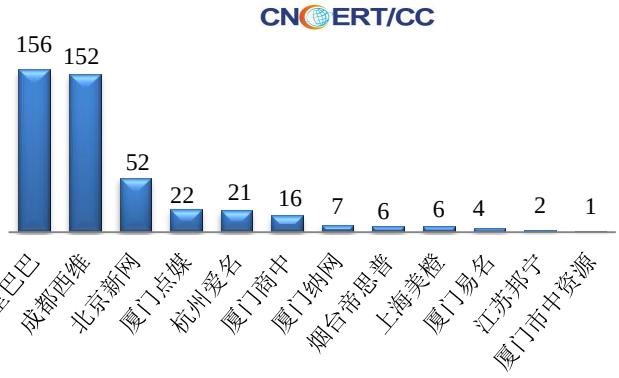


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 654 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 653 起和政府公益仿冒事件 1 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (10/14-10/20)

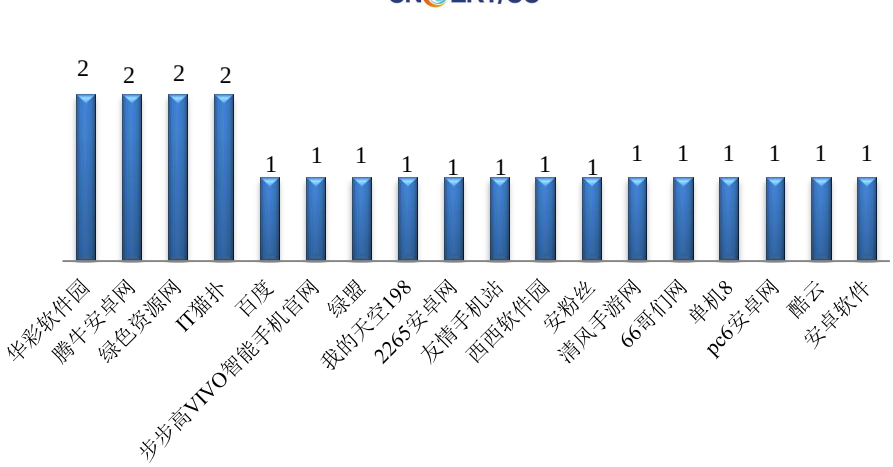


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (10/14-10/20)



本周，CNCERT 协调 18 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 22 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 (10/14-10/20)



业界新闻速递

1、 第六届世界互联网大会开幕 黄坤明宣读习近平主席贺信并发表主旨演讲

10 月 20 日新华社电，10 月 20 日，第六届世界互联网大会在浙江乌镇开幕。中共中央政治局委员、中宣部

部长黄坤明出席开幕式，宣读习近平主席贺信并发表主旨演讲。

黄坤明指出，习近平主席贺信提出的理念主张，充分体现了对互联网发展趋势的深刻洞察，对增进人类共同福祉的高度关切，展现了中国与世界各国携手构建网络空间命运共同体的真诚愿望。要坚持平等互利、包容互信、团结互助，大力发展数字经济、释放数字红利，让互联网成为促进变革创新、实现互利互惠的合作共赢之网。中国将一如既往发挥负责任大国作用，努力做网络空间发展的贡献者、网络空间开放的推动者、网络空间安全的捍卫者、国际网络空间治理的建设者，与国际社会共同推进全球互联网发展治理进程，更好造福世界、造福人类。

2、 工业和信息化部召开《加强工业互联网安全工作的指导意见》宣贯及工作部署全国电视电话会议

10 月 14 日工信部官网消息，当日，工业和信息化部组织召开电视电话会议，学习宣贯工业和信息化部等十部门联合印发的《加强工业互联网安全工作的指导意见》，扎实推进工业互联网安全工作。工业和信息化部网络安全管理局解读了《安全指导意见》的主要内容及下一步工作安排。应急管理部、国务院国资委、国家能源局、国家国防科技工业局相关部门负责人，各省、自治区、直辖市工业和信息化主管部门、通信管理局，部内相关司局，各基础电信企业、工业互联网企业等相关负责人分别在北京主会场和各地分会场参加会议。

3、美国对伊朗展开网络攻击

10 月 16 日路透社消息，美国两名官员表示，在 9 月 14 日沙特阿拉伯石油设施遭到袭击后，美国随后在月底对伊朗展开了一次秘密网络攻击行动，目标是德黑兰的宣传能力，袭击影响了实体硬件，但没有提供进一步的细节。

4、奔驰 App 在美爆安全漏洞可看其他车主信息

10 月 19 日科技媒体 Techcrunch 报道，10 月 18 日梅赛德斯 • 奔驰的应用程序（APP）出现明显漏洞，有用户反映 APP 错误地显示了其他车主的账户和车辆信息，包括姓名、最近的活动、电话号码等，随后该 APP 显示“网站维护”已下线。根据谷歌 Play 的排名，已经有超过 10 万客户安装了这款 APP。目前还不清楚这一安全漏洞是如何发生的，也不清楚这个安全问题出现的范围。

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：严寒冰

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315