国家互联网应急中心

网络安全信息与动态周报

2019 年第 28 期

7 月 8 日-7 月 14 日

CNCERT/CC

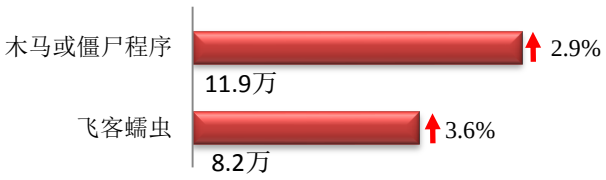
本周网络安全基本态势

境内感染网络病毒的主机数量	•20.1万	↑ 3.2%
境内被植入后门网站总数 其中政府网站数量	•3571 •28	↑ 11.2% ↓ 12.5%
针对境内网站的仿冒页面数量	•571	↓ 26.3%
新增信息安全漏洞数量 其中高危漏洞数量	•316 •123	↑ 52.7% ↑ 66.2%

═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

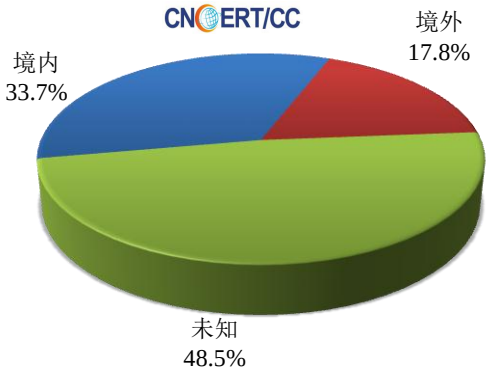
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 20.1 万个，其中包括境内被木马或被僵尸程序控制的主机约 11.9 万以及境内感染飞客（conficker）蠕虫的主机约 8.2 万。

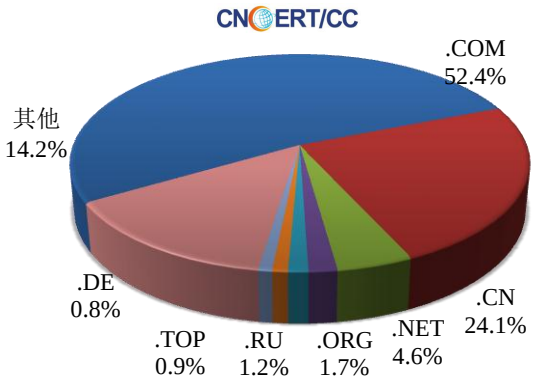


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 2141 个，涉及 IP 地址 3070 个。在 2141 个域名中，有 17.8%为境外注册，且顶级域为.com 的约占 52.4%；在 3070 个 IP 中，有约 55.3%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 517 个 IP。

本周放马站点域名注册所属境内外分布
(7/8-7/14)



本周放马站点域名所属顶级域的分布
(7/8-7/14)



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。

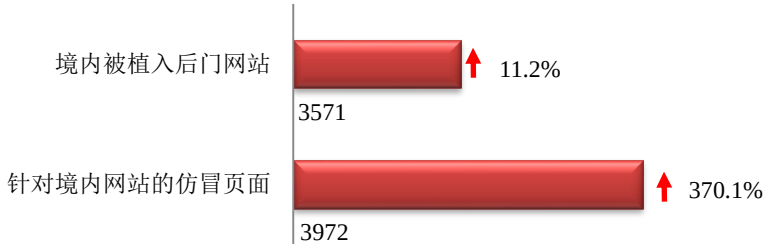
ANVA恶意地址黑名单发布地址

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。

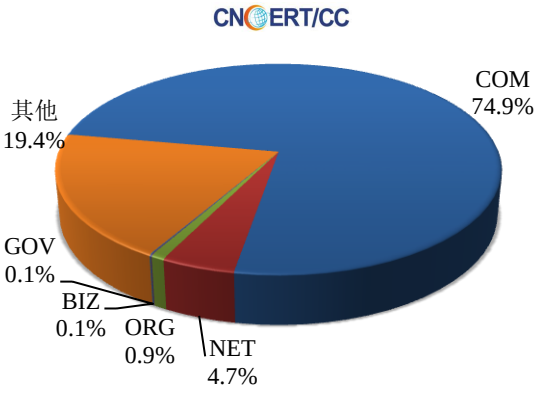
本周网站安全情况

本周 CNCERT 监测发现境内植入后门的网站数量为 3571 个；针对境内网站的仿冒页面数量 571 个。

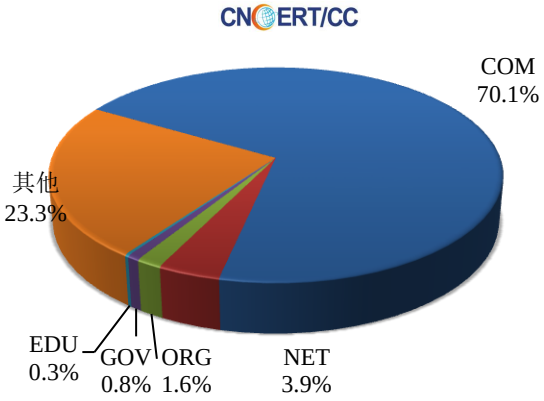


本周境内被篡改政府网站（GOV 类）数量为 4 个（约占境内 0.1%），较上周环比上涨 300.0%；境内被植入后门的政府网站（GOV 类）数量为 28 个（约占境内 0.8%），较上周环比下降 12.5%；针对境内网站的仿冒页面涉及域名 433 个，IP 地址 214 个，平均每个 IP 地址承载了约 3 个仿冒页面。

本周我国境内被篡改网站按类型分布
(7/8-7/14)

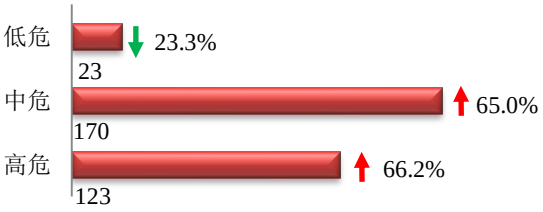


本周我国境内被植入后门网站按类型分布
(7/8-7/14)

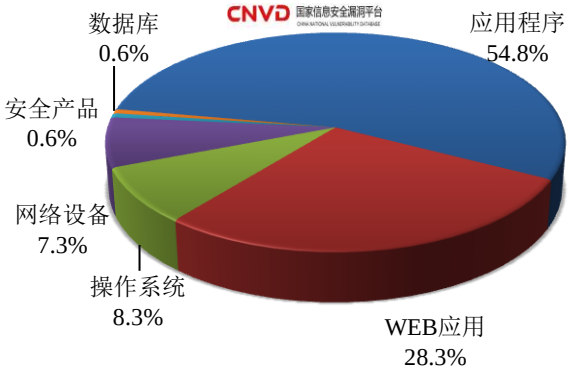


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 316 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
(7/8-7/14)



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

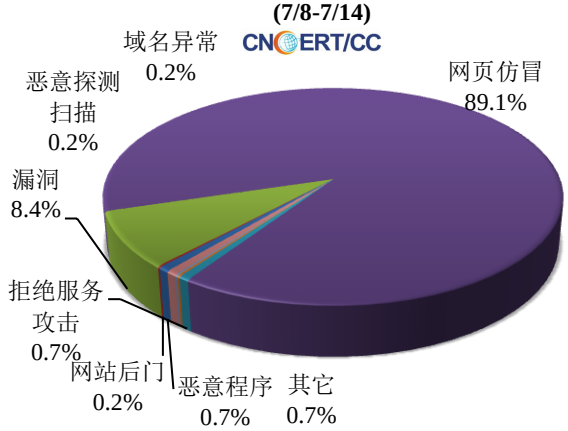
http://www.cnvd.org.cn/webinfo/list?type=4

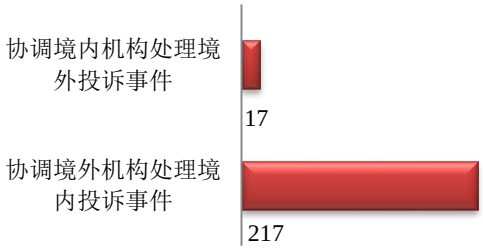
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 588 起，其中跨境网络安全事件 234 起。

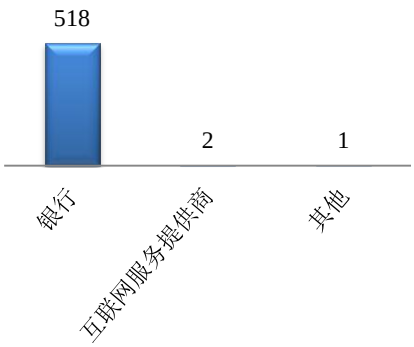
本周CNCERT处理的事件数量按类型分布 (7/8-7/14)



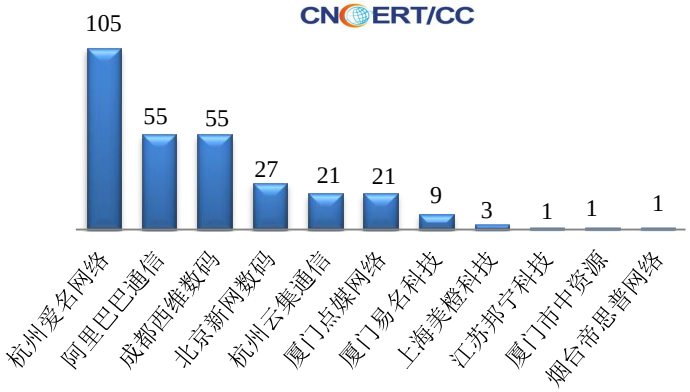


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 521 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 518 起和互联网服务提供商仿冒事件 2 起。

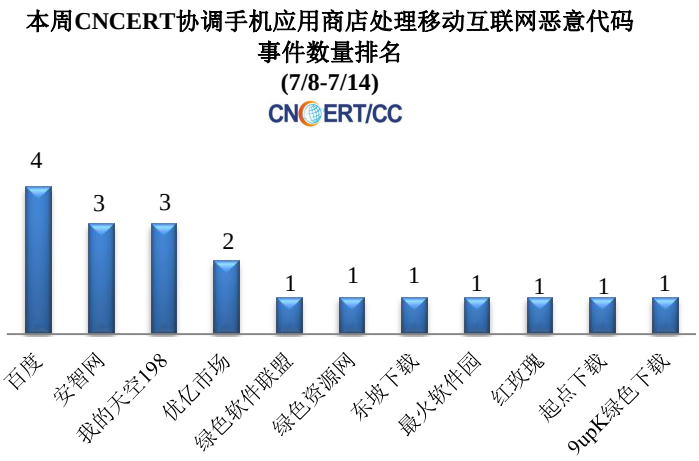
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (7/8-7/14)



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 (7/8-7/14)



本周，CNCERT 协调 11 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 19 个。



业界新闻速递

1、 《卫星网络国际申报简易程序规定（试行）》印发

工信部官网 7 月 10 日消息 为加快卫星网络国际申报，简化申报程序，提升申报效率，根据《中华人民共和国无线电管理条例》，工业和信息化部近日印发了《卫星网络国际申报简易程序规定（试行）》。

2、 工业和信息化部会同相关部门组织重点互联网企业签订防范治理电信网络诈骗责任书

工信部官网 7 月 10 日消息 工业和信息化部网络安全管理局会同公安部刑事侦查局、中央网信办网络综合协调管理和执法督查局，在中国互联网大会“2019 防范治理电信网络诈骗论坛”上，组织阿里巴巴、腾讯、百度、京东、字节跳动、拼多多、新浪微博、58 同城、美团、世纪佳缘、网宿科技 11 家单位，签订“重点互联网企业防范治理电信网络诈骗责任书”。

3、 英国航空公司因数据泄露面临 1.83 亿英镑巨额罚款

央视网 7 月 9 日消息 英国数据安全监管部门——信息专员办公室宣布，将对英国航空公司 2018 年客户数据遭泄露事件开出 1.83 亿英镑（≈2.3 亿美元≈15.8 亿人民币）的巨额罚单。黑客在其网站上进行了“恶意的犯罪攻击”，约有 380,000 笔交易受到影响，但被盗数据不包括旅行或护照详情。

4、 K12.com 暴露了多达 700 万条涉及学生个人信息的数据库记录

cnBeta.COM7 月 14 日消息 在线教育平台 K12.com 本周无意中暴露了近 700 万学生的个人信息。暴露的数据库包含全名，电子邮件地址，出生日期和性别身份，以及学生就读的学校，同时还可访问其帐户的身份验证密钥和其他内部数据。这些信息在线提供了一个多星期，目前还不清楚数据库是否被恶意行为者访问或者获取。据发现数据暴露的研究人员称，该问题影响了 K12.com 的 A+nyWhere 学习系统（A + LS），该系统被美国 1100 多个学区使用。数据库配置错误可能是导致它可以在 BinaryEdge 和 Shodan 上公开访问和发现的原因，这两个搜索引擎专门为面向公众的数据库编制索引。 6 月 25 日发现的曝光首次发生在 6 月 23 日，直到 7 月 1 日才得以修复。

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：周昊

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315