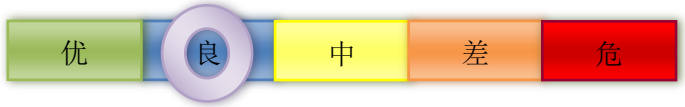
国家互联网应急中心

2017 年第 37 期

9 月 4 日-9 月 10 日

网络安全信息与动态周报

本周网络安全基本态势

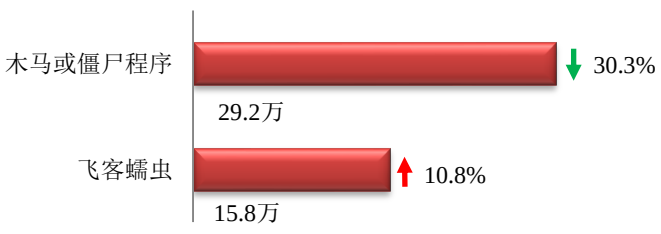


境内感染网络病毒的主机数量	•45.0万	↓ 19.8%
境内被篡改网站总数 其中政府网站数量	•2,514 •55	↑ 2.9% ↑ 41.0%
境内被植入后门网站总数 其中政府网站数量	•763 •33	↓ 20.6% ↓ 37.7%
针对境内网站的仿冒页面数量	•378	↑ 23.5%
新增信息安全漏洞数量 其中高危漏洞数量	•335 •94	↓ 3.7% ↓ 13.0%

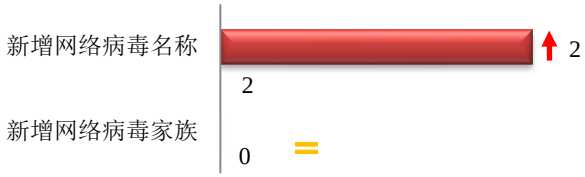
═表示数量与上周相同　↑表示数量较上周环比增加　↓表示数量较上周环比减少

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 45.0 万个，其中包括境内被木马或被僵尸程序控制的主机约 29.2 万以及境内感染飞客（conficker）蠕虫的主机约 15.8 万。

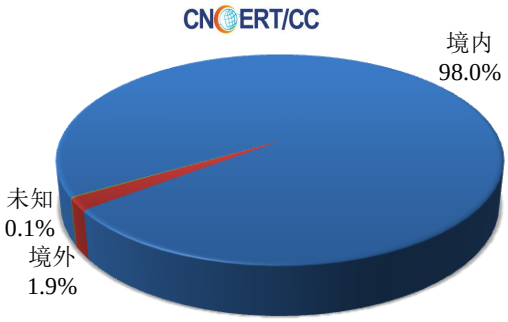


本周 CNCERT 捕获的新增网络病毒文件，按网络病毒名称统计新增 2 个，按网络病毒家族统计无新增。

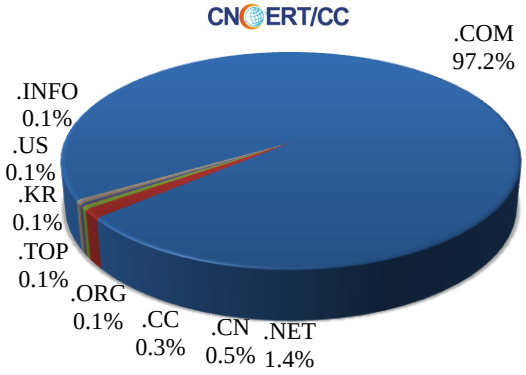


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 798 个，涉及 IP 地址 370 个。在 798 个域名中，有 1.9%为境外注册，且顶级域为.com 的约占 97.2%；在 370 个 IP 中，有约 6.8%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 5 个 IP。

本周放马站点域名注册所属境内外分布
(9/4-9/10)



本周放马站点域名所属顶级域的分布
(9/4-9/10)



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。

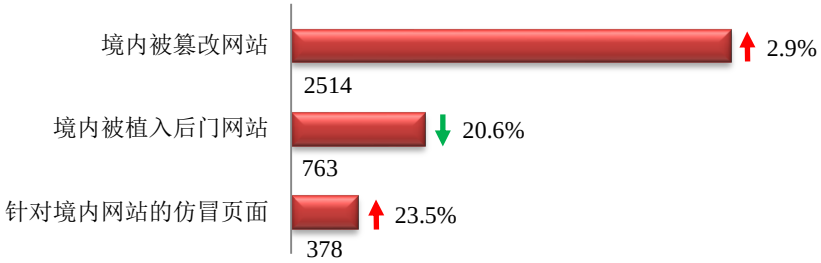
ANVA恶意地址黑名单发布地址

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。

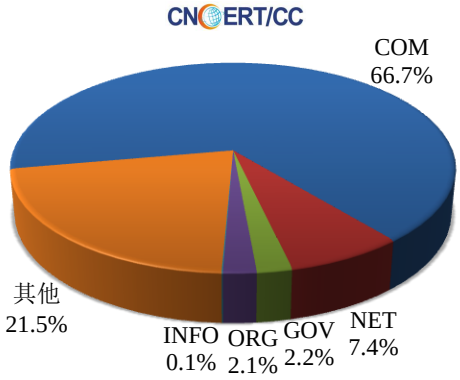
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 2514 个；境内被植入后门的网站数量为 763 个；针对境内网站的仿冒页面数量为 378。

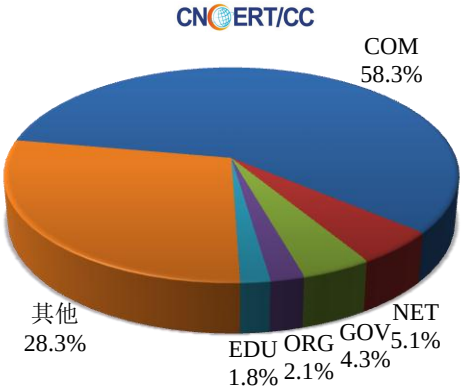


本周境内被篡改政府网站（GOV 类）数量为 55 个（约占境内 2.2%），较上周环比上升了 41.0%；境内被植入后门的政府网站（GOV 类）数量为 33 个（约占境内 4.3%），较上周环比下降了 37.7%；针对境内网站的仿冒页面涉及域名 81 个，IP 地址 157 个，平均每个 IP 地址承载了约 2 个仿冒页面。

本周我国境内被篡改网站按类型分布
(9/4-9/10)

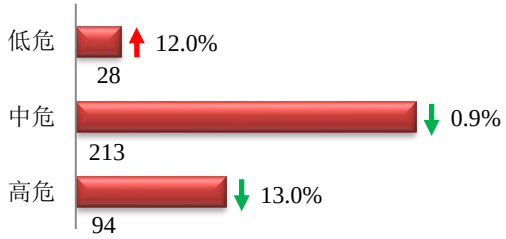


本周我国境内被植入后门网站按类型分布
(9/4-9/10)

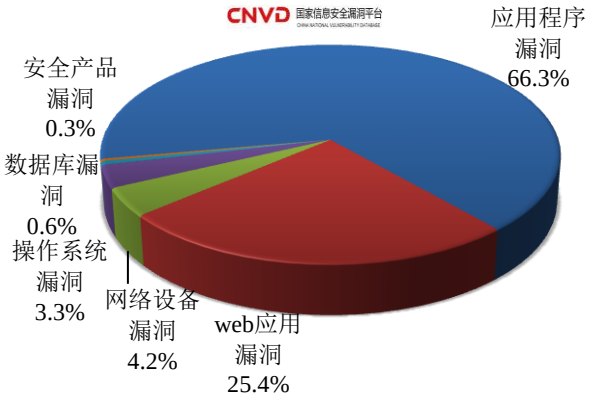


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 335 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
(9/4-9/10)



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

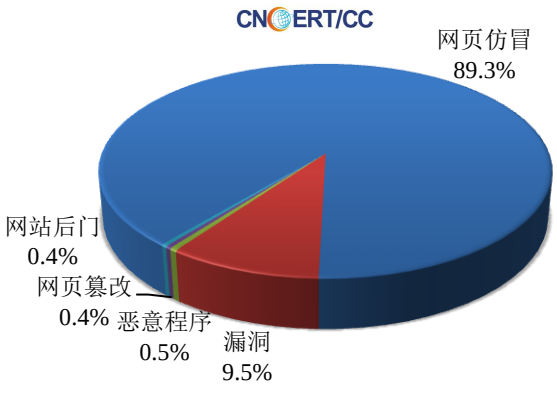
http://www.cnvd.org.cn/webinfo/list?type=4

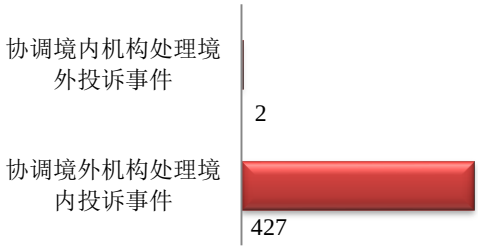
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 851 起，其中跨境网络安全事件 429 起。

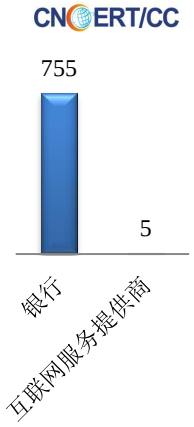
本周CNCERT处理的事件数量按类型分布
(9/4-9/10)



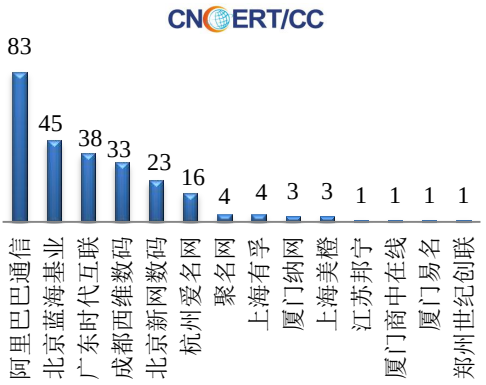


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 760 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 755 起和互联网服务提供商仿冒事件 5 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(9/4-9/10)

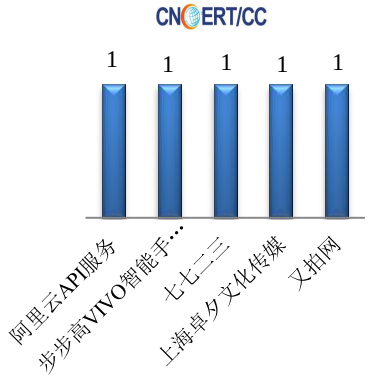


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (9/4-9/10)



本周，CNCERT 协调 5 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 5 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 (9/4-9/10)



业界新闻速递

1、国家网络安全宣传周 9 月 16 日起举行

新华网 9 月 9 日消息 记者 9 月 8 日从中央网信办、上海市委网信办在京举办的新闻发布会上获悉：2017 年国家网络安全宣传周将于 9 月 16 日至 24 日在全国范围内统一举行。今年网络安全宣传周的主题是“网络安全为人民，网络安全靠人民”，由中央宣传部、中央网信办、教育部、工业和信息化部、公安部、中国人民银行、新闻出版广电总局、中华全国总工会、共青团中央等九部门共同举办，宣传周的开幕式、网络安全博览会暨网络安全成就展等重要活动将在上海市举办。据介绍，今年宣传周将举办网络安全博览会暨网络安全成就展、网

络安全技术高峰论坛、主题日活动、一流网络安全学院示范高校评选活动等，此外还将表彰网络安全先进典型。据悉，各省区市都将结合实际，在本地区同步举办网络安全宣传周活动。

2、针对北约网站攻击猛增 60% 欧盟非正式防长会聚焦网络安全

新浪网 9 月 8 日消息 9 月 7 日，欧盟非正式防长会在爱沙尼亚首都塔林召开，会议主要议题集中在“如何应对日益增长的网络攻击”。当天的会议上，欧盟各国防长参加了一场战略级的“桌面网络防御演习”，以测试在面对网络攻击时，各国防长的管理战略和综合能力，同时推动欧盟与北约在网络空间的防务合作。有统计数据显示，2016 年，针对欧盟服务器的网络攻击达到 110 次，比上一年增加了 20%，而针对北约网站的攻击更是猛增了 60%。面对挑战，欧盟已升级安全措施——高级公务员被告知利用电邮加密技术；同时，欧盟委员会也正与北约扩大网络安全合作。

3、2017 年欧美百座电站遭到“蜻蜓”等黑客攻击

电缆网 9 月 9 日消息 根据计算机安全公司 Symantec 日前发布的一份报告中，2017 年，欧洲和北美电力公司和核电站运营商已经遭遇被称为“蜻蜓”（Dragonfly）和“能量熊”（Energetic Bear）等与俄罗斯有关的黑客群体一系列网络攻击。根据初步统计，今年以来，全球电力公司和核电站运营商已经遭到约 100 次黑客网络袭击，其中一半在美国。这个发现是令人担忧的，因为“蜻蜓”是少数具备攻击电网控制网络的黑客团体之一。另外一个与俄罗斯有关的黑客组织曾经用行动证明克里姆林宫的能力和使用这种专门知识导致电力停电的意愿，两次都发生在乌克兰，一次是在 2015 年 12 月，另一次是在 2016 年。Symantec 认为，美国的电站遭袭行为可能会进入相似的情形。Symantec 在报告中总结说：“原来的‘蜻蜓’运动似乎更像是一个探索性的阶段，攻击者只是想要访问目标组织的网络。但是现在，攻击者可能正在进入一个新的阶段，最近的行动可能会进入运营系统，达到破坏性的目的。”

4、美征信巨头信息泄露或影响上亿消费者

新华网 9 月 8 日消息 美国征信公司伊奎法克斯 9 月 7 日发布声明说，由于此前公司文件遭遇非授权访问，约有 1.43 亿美国消费者信息或已泄露。声明说，遭到非授权访问的个人信息包括客户姓名、生日、地址、社会安全号、驾驶证号等。此外，约 20.9 万美国消费者的信用卡号以及一些英国和加拿大居民的个人信息也遭遇未授权访问。声明还说，公司 7 月 29 日发现非授权访问行为后堵住漏洞。此后的调查显示，非授权访问行为早在今年 5 月中旬就已开始。不过，没有证据显示公司核心消费者及商业信用报告数据库遭到非授权访问。该公司首席执行官理查德·史密斯在声明中就信息泄露向消费者和客户致歉。公司正就这起网络安全事件联系美国相关监管机构，并已书面通报美国各州总检察长。伊奎法克斯是美国三家主要个人征信公司之一。这些征信公司有偿向银行、保险公司和房地产商等提供个人信用报告。

5、时代华纳逾 400 万客户信息在线泄露

HackerNews.cc9 月 8 日消息 据外媒 9 月 6 日报道，继美国私人安全公司 TigerSwan 9,400 份雇佣简历在未受保护的 AWS 数据库上泄露后，安全公司研究人员 Kromtech 再次曝光另一起 AWS 存储数据泄露事件——知名云服务供应商 BroadSoft 未妥善保护时代华纳托管在亚马逊存储服务器的数据，导致逾 400 万客户信息在线

泄露，其中包括客户地址、账户设置、电话号码、用户名、MAC 地址、调制解调器硬件序列号等敏感信息。调查显示，研究人员 Kromtech 于 8 月底针对该公司基于云服务存储数据库进行安全检查时发现，管理人员因配置错误未关闭服务器公共访问权限，导致任意用户均可匿名访问。因此，攻击者只需使用匿名登录就可从该数据库中窃取想要信息。目前，BroadSoft 并未作出任何置评，而时代华纳在事件发生后当即通知受害用户并告知供应商删除所有数据记录。

6、MoneyBack 数据泄漏：400GB 墨西哥游客个人资料暴露于不安全数据库中

HackerNews.cc9 月 10 日消息 据外媒 9 月 8 日报道，网络安全公司 Kromtech 研究人员 Bob Diachenko 近期发现国际知名退税公司 MoneyBack 运行了一台不安全数据库，导致逾 400GB 墨西哥游客敏感信息在线泄露，其中包括用户姓名、地址、电话号码、信用卡数据等。Bob Diachenko 近期在一篇博客中表示：“我们于今年 8 月首次发现该数据库因无密码保护，允许任意黑客轻易访问并通过 MoneyBack.mx 告知用户虚假增值税率以骗取钱财。随后，我们于 9 月 4 日对其进行审查与分析，以便确定影响范围”。研究人员通过扫描 455038 份文件发现，该数据库还包含来自美国、加拿大、阿根廷、哥伦比亚、意大利等多国公民护照信息。此外，他们检测到上传该数据库的第一份文件可追溯至 2015 年，而最近的上传日期为 2017 年 5 月。据悉，MoneyBack 在该事件曝光后立即修改访问权限以确保用户数据安全。不过，研究人员尚不清楚数据信息是否已被黑客利用。目前，MoneyBack 并未作出任何置评。

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。截止 2016 年，CNCERT 与 69 个国家和地区的 185 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：韩志辉

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158