国家互联网应急中心

2015 年第 37 期

9 月 7 日-9 月 13 日

网络安全信息与动态周报

本周网络安全基本态势

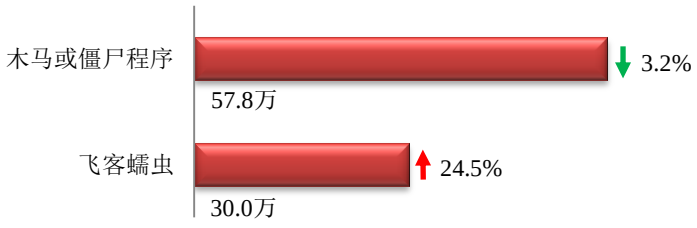
优 良 中 差 危

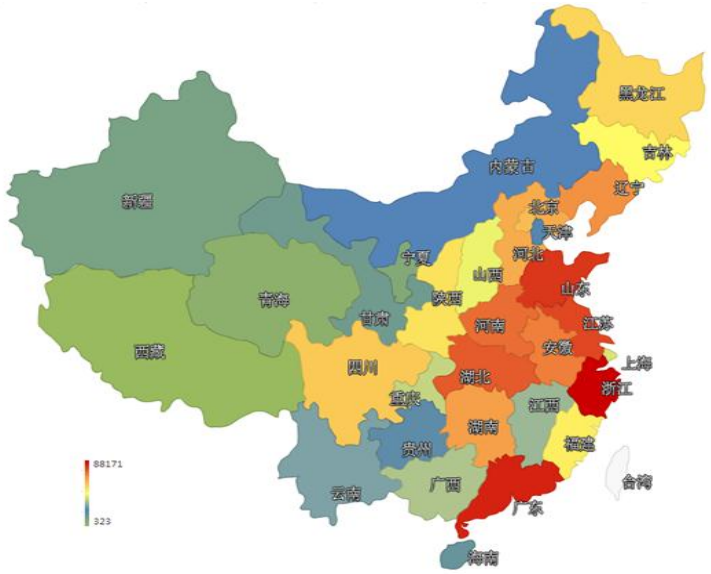
境内感染网络病毒的主机数量	•87.8万	↑ 4.8%
境内被篡改网站总数 其中政府网站数量	•3133 •52	↓ 41.5% ↓ 39.5%
境内被植入后门网站总数 其中政府网站数量	•3140 •129	↓ 21.8% ↓ 5.1%
针对境内网站的仿冒页面数量	•3451	↑ 3.9%
新增信息安全漏洞数量 其中高危漏洞数量	•144 •65	↑ 56.5% ↑ 62.5%

═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 87.8 万个，其中包括境内被木马或被僵尸程序控制的主机约 57.8 万以及境内感染飞客（conficker）蠕虫的主机约 30.0 万。



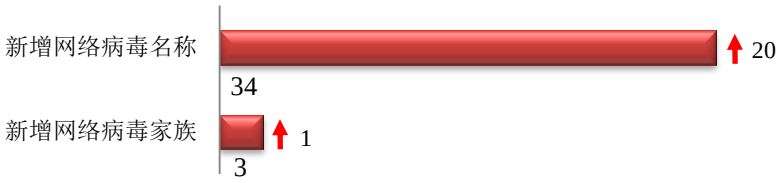


木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是浙江省、广东省和山东省。

TOP3

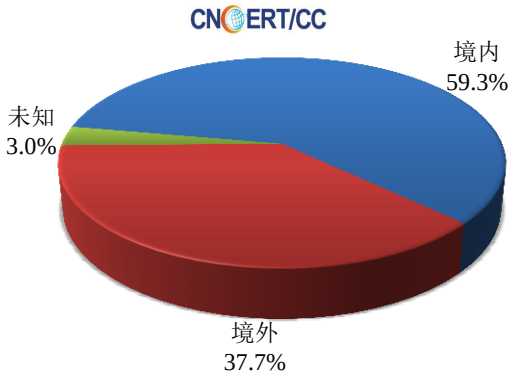
浙江省	•约8.8万个（约占中国大陆总感染量的15.3%）
广东省	•约6.9万个（约占中国大陆总感染量的12.0%）
山东省	•约5.0万个（约占中国大陆总感染量的8.7%）

本周 CNCERT 捕获了大量新增网络病毒文件，按网络病毒名称统计新增 34 个，按网络病毒家族统计新增 3 个。

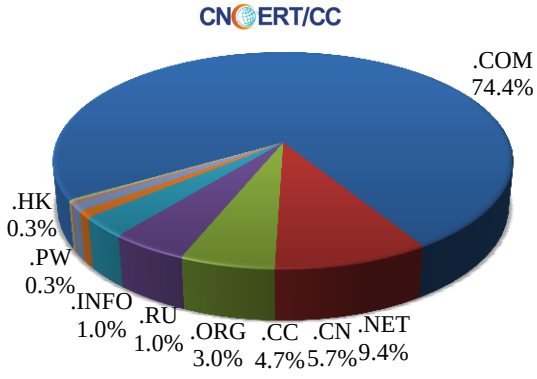


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 297 个，涉及 IP 地址 477 个。在 297 个域名中，有约 37.7%为境外注册，且顶级域为.com 的约占 74.4%；在 477 个 IP 中，有约 24.7%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 102 个 IP。

本周放马站点域名注册所属境内外分布
(9/7-9/13)



本周放马站点域名所属顶级域的分布
(9/7-9/13)



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。

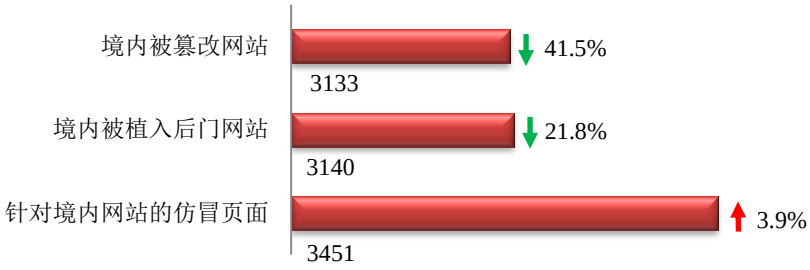
ANVA恶意地址黑名单发布地址

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。

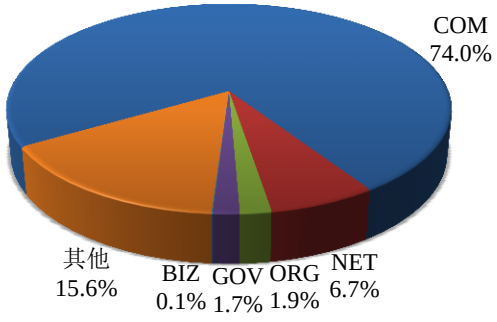
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 3133 个；境内被植入后门的网站数量为 3140 个；针对境内网站的仿冒页面数量为 3451。

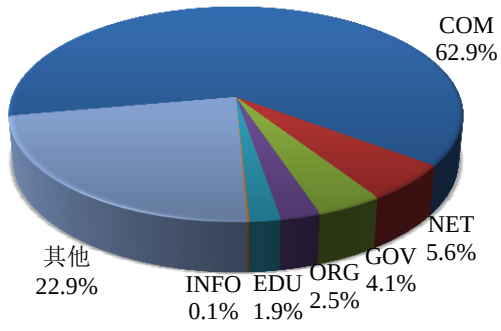


本周境内被篡改政府网站(GOV 类)数量为 52 个（约占境内 1.7%），较上周环比下降了 39.5%；境内被植入后门的政府网站(GOV 类)数量为 129 个（约占境内 4.1%），较上周环比下降了 5.1%；针对境内网站的仿冒页面涉及域名 2758 个，IP 地址 880 个，平均每个 IP 地址承载了约 4 个仿冒页面。

本周我国境内被篡改网站按类型分布
(9/7-9/13)

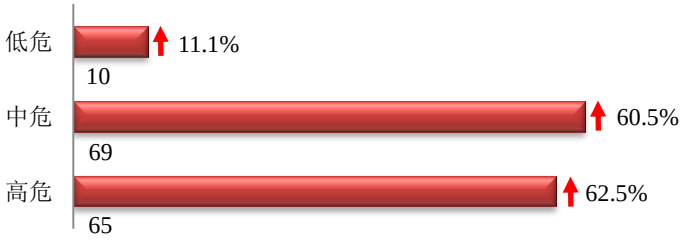


本周我国境内被植入后门网站按类型分布
(9/7-9/13)

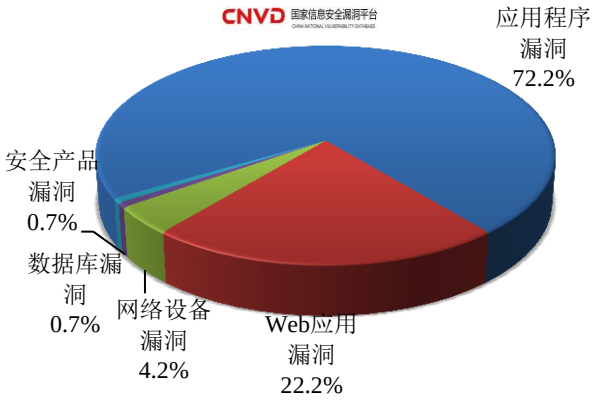


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 144 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
(9/7-9/13)



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

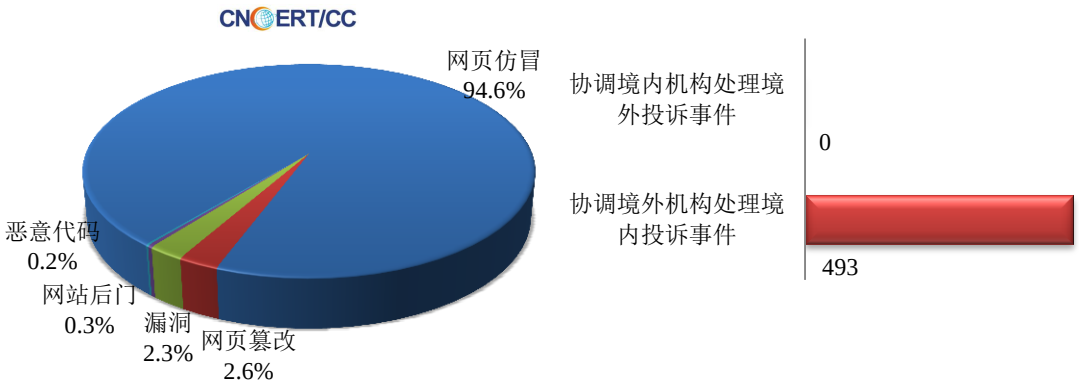
http://www.cnvd.org.cn/webinfo/list?type=4

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

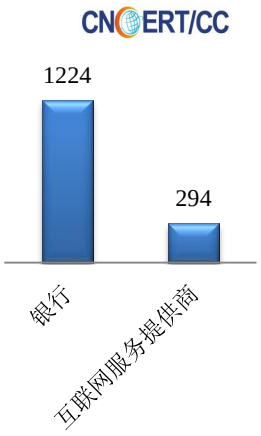
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 1604 起，其中跨境网络安全事件 493 起。

本周CNCERT处理的事件数量按类型分布
(9/7-9/13)

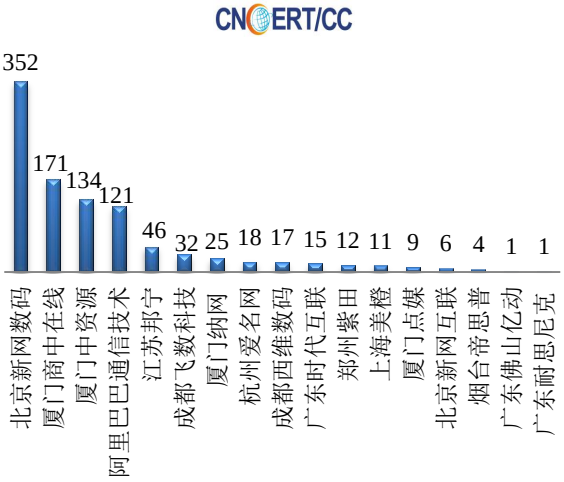


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 1518 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 1224 起和互联网服务提供商仿冒事件 294 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(9/7-9/13)



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 (9/7-9/13)



业界新闻速递

1、孟建柱访美就共同打击网络犯罪开展执法合作

人民网 9 月 13 日消息 9 月 9 日至 12 日，习近平主席特使、中共中央政治局委员、中央政法委书记孟建柱，率公安、安全、司法、网信等部门有关负责人访问美国，同美国国务卿克里、国土安全部部长约翰逊、总统国家安全事务助理赖斯等举行会谈，就共同打击网络犯罪等执法安全领域的突出问题深入交换意见，达成重要共识。孟建柱指出，中美两国都是互联网大国，在当前网络空间事端频发、网络安全威胁不断上升的大背景下，双方加强网络安全领域互信与合作尤为重要。孟建柱强调，中方反对网络攻击和网络商业窃密的立场是坚定的，不管什么人，在我境内实施网络攻击和网络商业窃密都是违反国家法律的，都应受到法律的追究。中美两国开展对话合作、共同打击网络犯罪，符合双方和国际社会的共同利益。

2、美国国防部发布云安全指南

中国信息产业网 9 月 9 日消息 美国国防信息系统局（DISA）日前发布了新版云安全指南，旨在辅助国防部（DoD）保护本国网络免遭黑客攻击。新指南由三部分构成，包括两份新版需求文件和一份新版作战概念手册。同以往相比，该指南对云安全的概念、实现云安全的步骤均做了更加全面的诠释。此外，新指南还规定组织机构及管理者在利用商业云产品时应承担的责任。该指南的发布印证了国防部增加采用商业云产品的事实。其中一份名为《无线云接入点功能需求文件》（CAPFRD）规定，在国防部信息网络（DoDIN）与互联网公共云服务产品间设立保护防线，引导防务部门保障其连接点的安全。DISA 所建立的 CAP 是对本国无保密互联网协议路由器网络（NIPRNet）网关的修正。新版云安全指南还指出：“由于 DoD 力求达到部门负责人最大利用云计算的目标，因而必须一直保护 DoDIN 边界不受外部连接网络的威胁。CAP 能积极主动地阻断黑客攻击 DoDIN 基础设施，尤其能提高云服务环境中任务应用的通畅度，因而植入多重信息保障功能以检测和防范不同类型的外部攻击。”

3、加拿大防御网络犯罪追加千万加元

中国信息产业网 9 月 9 日消息 加拿大近日宣布将投入 1420 万加元（约 6800 万元人民币）用于加强网络安全措施，并帮助私营企业防御网络攻击。新一轮的资金，使得在过去 5 年内加拿大政府的“网络安全战略”获得的投入资金总额达到了 2.37 亿加元。加拿大联邦政府各主要部门的网站 6 月 17 日下午遭到黑客攻击，加外交部、交通部、司法部和移民局等部门的网站出现短暂混乱。一个匿名黑客组织宣称实施了针对加拿大参议院和联邦政府网站的攻击，而两周后的 6 月 30 日，黑客封锁了加拿大情报局网站。加拿大公共安全部长史蒂文 •布莱尼表示，“只要我们的数字基础设施不断发展，就总会有人试图利用漏洞来破坏加拿大的国家安全、公共安全和经济繁荣。与关键基础设施部门和私营部门伙伴的合作与信息共享是我们最好的防御手段，以保护我们的关键网络系统。”加拿大公共安全部表示将与私营企业合作，改进网络安全，而最新投入的资金将帮助加拿大网络事故响应中心应对和减轻发生在私营企业的网络入侵事件。这项计划还将通过“专门的资源和培训，提升可以检测和破坏网络犯罪活动”的专业技术水平。公共安全部强调，“网络犯罪给加拿大的国家安全和经济发展带来巨大威胁。”

4、互联网网络安全威胁治理行动单月处理投诉超万件

新华网 9 月 11 日消息 记者 11 日从国家互联网应急中心获悉，于 7 月底开展的互联网网络安全威胁治理行动至今，已协调行动参与单位处置投诉网络安全事件 11277 起。据互联网应急中心相关负责人介绍，近期互联网应急中心联合中国互联网协会网络与信息安全工作委员会共同开展的互联网网络安全威胁治理行动，行动时间为 8 月至 10 月，主要以加强行业自律为目的，动员行业内相关企业、单位加强监测，通过密切配合、积极处置、曝光黑名单等措施，有效提升我国行业内防范和治理互 联网网络安全能力。该负责人表示，行动开展一个多月以来，共通过公开平台网民举报事件 22548 起。经验证分析后，重点针对互联网上最难防御的网络安全威胁 DDoS 攻击、网页暗链篡改等与互联网黑色地下产业密切相关的事件进行重点处置。目前，已协调处置事件 11277 起，其中处置 DDoS 攻击服务售卖平台 14 个，DDoS 攻击控制服务器 32 个，参与网络攻击的博彩、私服等网站链接 3257 个；正在做关停处理的未备案网站 37 个；通 知 1085 个被篡改和 521 个被植入后门的网站用户单位对网站进行修复。此外，为提高网民规避网络诈骗、计算机中毒的风险，行动还组织开展了恶意网址黑名单访问提示拦截工作。互联网应急中心组织 QQ、360、搜狗和百度 4 款浏览器对列入“黑名单”的恶意地址进行拦截并提出警告。截至 9 月 6 日，互联网应急中心已公布“黑名单”恶意网址 16040 条。

5、多家金融机构被曝存在漏洞黑客：价钱合适数据都能买到

央广网 9 月 8 日消息 据中国之声《新闻晚高峰》报道，近日，包括乌云、补天等漏洞响应平台曝光了多家银行、券商、保险、基金公司网站存在漏洞。这些漏洞主要集中在跨站脚本攻击、金融 APP 安全问题等，如果不及时处理，包括银行的转账信息、投资者的个人信息、账号密码、交易记录都存在着被泄露的风险。名字、手机、证件号码等信息，在普通人看来，都是极隐私的内容。但是在一些黑客眼中，却成了牟利的工具，一条个人金融信息，从几十块钱到几毛钱不等，一位卖家甚至表示，只要买方的需求不是特别过分，基本都可以满足。乌云网运营人员孟卓说，如果目标网站存在相关的漏洞，这位卖家说的情况，是完全有可能出现的，尽管各家金融机构漏洞的表现不完全一致，但其中有不少共性问题。更具体来说，在银行方面，面临的风险是转账记录有可能泄露，比如包商银行网站的一个系统漏洞此前可被利用查看部分银行转账记录，包括转账的金额、

时间以及持卡人户名、账号、电话号码等信息，目前大多数银行系统漏洞已经被金融机构确认并修复。证券公司方面，投资者开户信息遭遇泄露风险。专家都表示，目前，网络安全信息的泄露是比较严重的，想要确保金融系统的安全，一方面需要预警平台及时的发现问题，另一方面相关的金融网站需要重视漏洞风险，及时修复。

6、日媒：联网汽车存巨大安全隐患或遭黑客攻击

环球网 9 月 9 日消息 2015 年 7 月，美国两名计算机安全研究人员实施了一项利用笔记本电脑入侵并远程控制联网汽车的实验，并取得了成功，该视频被上传至网络后立即引发了轰动反响，美国某知名汽车公司也因此采取了大规模的汽车召回，而联网汽车的安全性则再次遭受质疑。据 Record Japan 网站 9 月 9 日报道，在该实验中，两名研究人员利用笔记本电脑入侵了一辆在高速道路上行驶的汽车的软件系统，并对汽车的各项功能进行了控制，比如调节音量、关闭雨刮器、控制车速等等，尽管驾驶员事先知道这是一项实验，但是在整个实验过程中依然陷入了恐慌。该实验视频被上传至网络后，立即引起了热议，而参与实验的研究人员则表示，该实验的主要目的是为了证明目前联网汽车所存在的一个重要安全隐患，很可能遭遇黑客的攻击与控制，甚至窃取车主信息，同时呼吁汽车制造商能够更加重视这一问题。

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 2014 年，CNCERT 与 63 个国家和地区的 144 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：姚力

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82991373