国家互联网应急中心

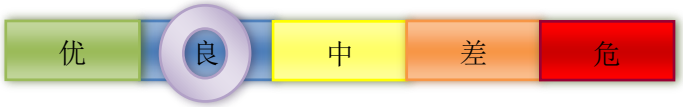
2016 年第 36 期

8 月 29 日-9 月 4 日

网络安全信息与动态周报

CNCERT/CC

本周网络安全基本态势

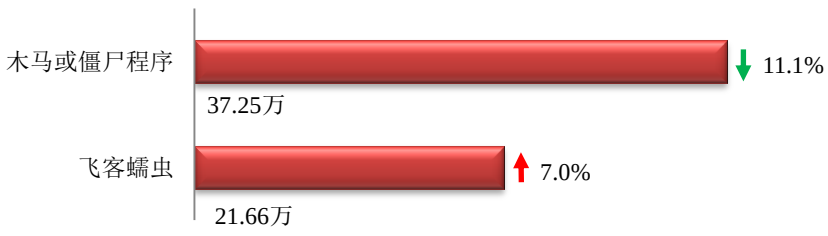


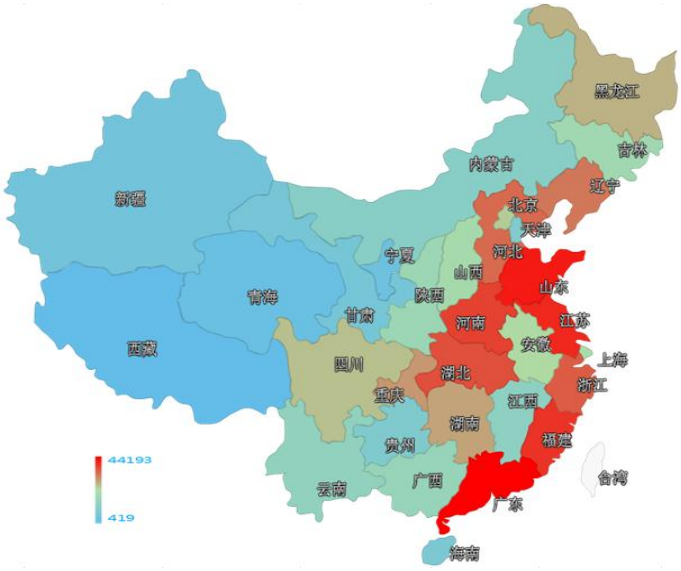
境内感染网络病毒的主机数量	• 58.91万	↓ 5.2%
境内被篡改网站总数 其中政府网站数量	• 3383 • 80	↑ 5.2% ↑ 17.6%
境内被植入后门网站总数 其中政府网站数量	• 6066 • 132	↑ 133.7% ↑ 17.9%
针对境内网站的仿冒页面数量	• 1091	↓ 78.5%
新增信息安全漏洞数量 其中高危漏洞数量	• 298 • 132	↓ 13.1% ↓ 35.0%

═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 58.91 万个，其中包括境内被木马或被僵尸程序控制的主机约 37.25 万以及境内感染飞客（conficker）蠕虫的主机约 21.66 万。





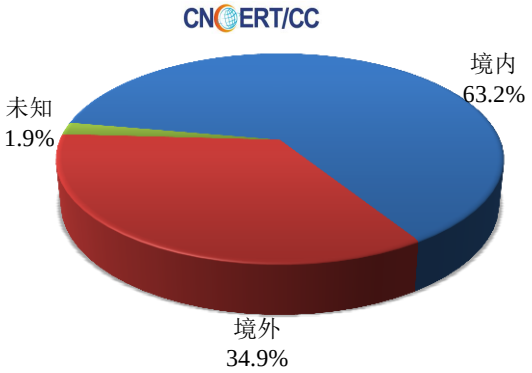
木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、山东省和江苏省。

TOP3

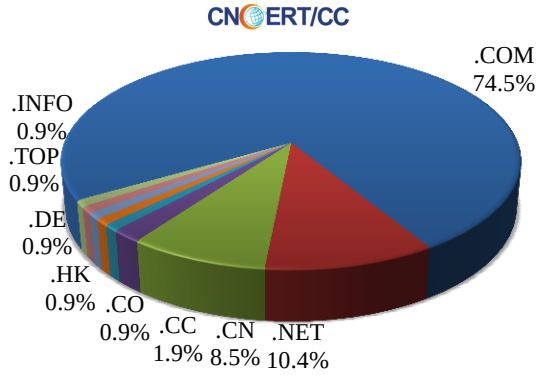
广东省	• 约4.4万个（约占中国大陆总感染量的11.9%）
山东省	• 约3.4万个（约占中国大陆总感染量的9.2%）
江苏省	• 约3.4万个（约占中国大陆总感染量的9.2%）

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 106 个，涉及 IP 地址 304 个。在 106 个域名中，有 34.9%为境外注册，且顶级域为.com 的约占 74.5%；在 304 个 IP 中，有约 4.9%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 14 个 IP。

本周放马站点域名注册所属境内外分布
(8/29-9/4)



本周放马站点域名所属顶级域的分布
(8/29-9/4)



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。

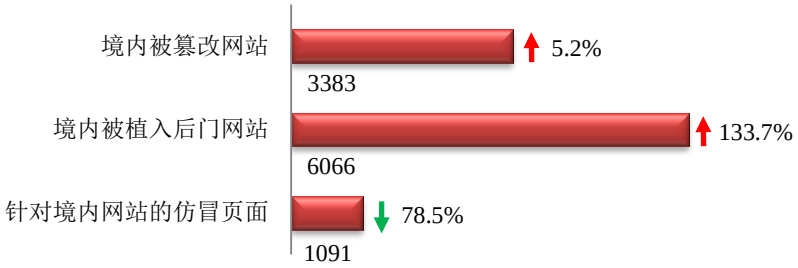
ANVA恶意地址黑名单发布地址

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。

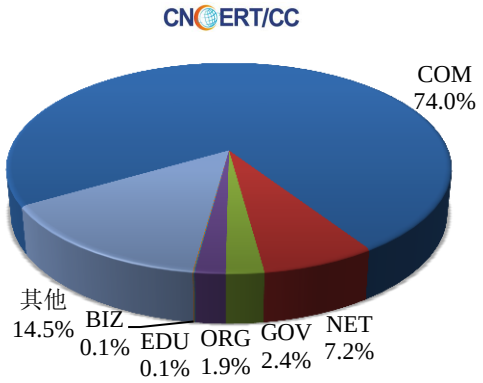
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 3383 个；境内被植入后门的网站数量为 6066 个；针对境内网站的仿冒页面数量为 1091。

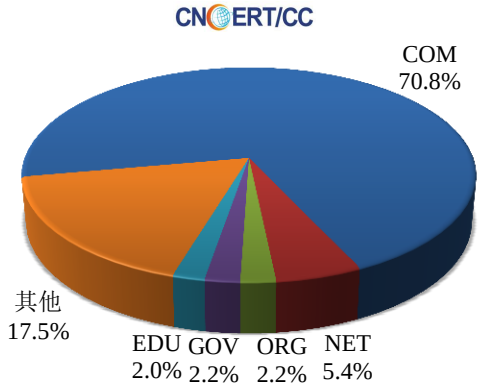


本周境内被篡改政府网站（GOV 类）数量为 80 个（约占境内 2.4%），较上周环比上升了 17.6%；境内被植入后门的政府网站（GOV 类）数量为 132 个（约占境内 2.2%），较上周环比上升了 17.9%；针对境内网站的仿冒页面涉及域名 1144 个，IP 地址 444 个，平均每个 IP 地址承载了约 2 个仿冒页面。

本周我国境内被篡改网站按类型分布
(8/29-9/4)

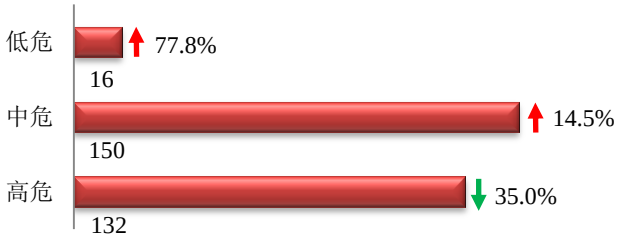


本周我国境内被植入后门网站按类型分布
(8/29-9/4)

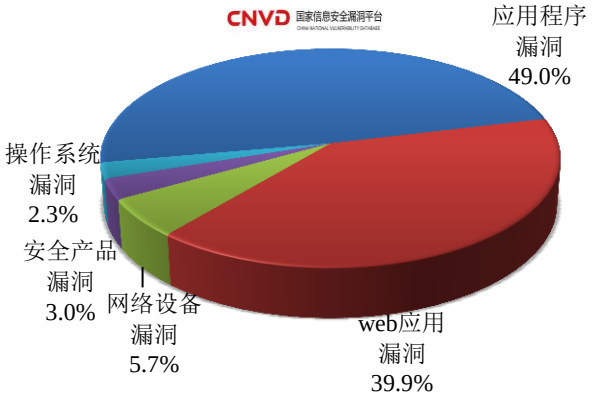


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 298 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
(8/29-9/4)



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

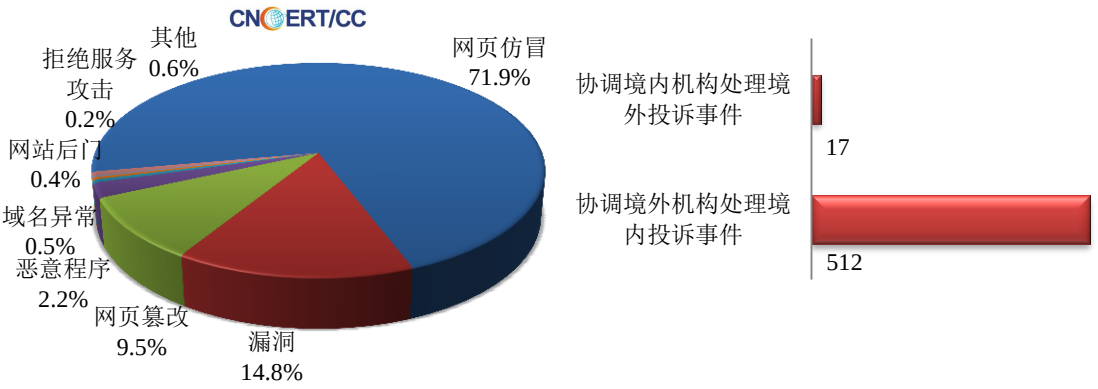
http://www.cnvd.org.cn/webinfo/list?type=4

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

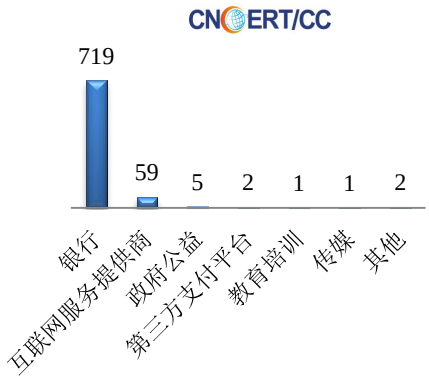
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 1098 起，其中跨境网络安全事件 529 起。

本周CNCERT处理的事件数量按类型分布
(8/29-9/4)

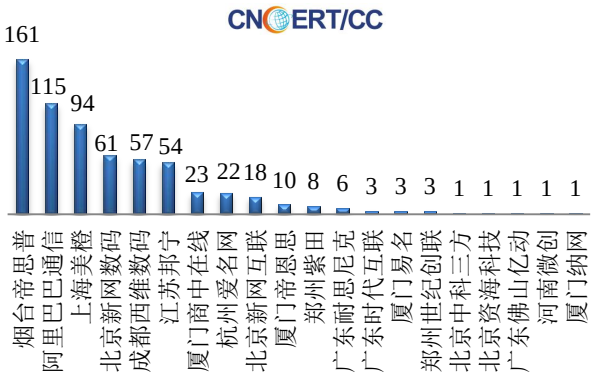


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 789 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事 719 起和互联网服务提供商仿冒事件 59 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(8/29-9/4)

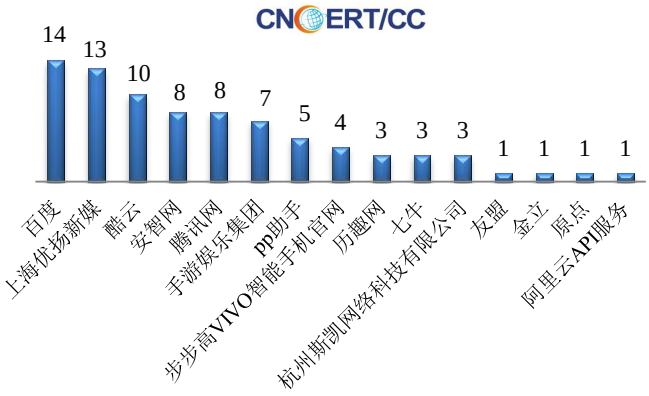


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (8/29-9/4)



本周，CNCERT 协调 15 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 82 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 (8/29-9/4)



业界新闻速递

1、中美打击网络犯罪及相关事项高级别联合对话联络热线开通

中国互联网协会 8 月 29 日消息 8 月 26 日，公安部副部长陈智敏通过热线电话，分别与美国国土安全部副部长斯波尔丁、美国司法部助理部长帮办斯沃茨和美国联邦调查局代表进行通话，宣布中美打击网络犯罪及相关事项高级别联合对话联络热线正式启用。为落实习近平主席与奥巴马总统在 2015 年 9 月就网络安全合作达成的重要共识，中美两国建立了打击网络犯罪及相关事项高级别联合对话机制。在此对话机制框架下，双方在打击网络犯罪和网络保护领域开展了一系列务实合作。根据两次中美打击网络犯罪及相关事项高级别联合对话成果安排，双方决定建立热线联络渠道，及时就重大网络案事件进行沟通交流。近日，双方有关部门交换了热线联络方式，并就热线工作程序达成一致。中美打击网络犯罪及相关事项联络热线的开通，将进一步加强双方在网络安全案事件上的沟通交流，有利于双方快速判明情况，采取有效措施，共同消除网络危害，打击网络犯罪，维护两国网络安全。

2、中国-东盟博览会网络信息安全研讨会将在邕举行

新华网 8 月 29 日消息 “中国-东盟博览会第三届网络信息安全研讨会”将于 2016 年 9 月 12 日在南宁国际会展中心举行。从“两会”指挥中心投资促进部了解到,由广西网络信息安全服务研究院和广西国际文化交流中心主办的“中国-东盟博览会第三届网络信息安全研讨会”将于 2016 年 9 月 12 日在南宁国际会展中心举行。本次研讨会以“打击网络犯罪，共治网络空间”为主题，将邀请全球及国内顶级信息安全专家,就互联网安全对社会的影响、互联网+金融信息安全技术应用、网络犯罪调查取证、网络空间开放治理框架、网络靶场与人才培养等前沿网络安全技术及热点问题展开讨论，全面展示业界顶级安全技术及产品，旨在打造面向东南亚的西部信息安全高端论坛。

3、英国多家企业向多个国家出售通讯间谍技术

E 安全 8 月 29 日消息 据外媒报道自 2015 年年初，已经有十余家英国企业获得相关牌照，有权将其强大的电信拦截技术出售至世界各国。其中一大主要出口产品门类为 IMSI 捕捉器，这些设备可对广泛区域内的大量移动手机加以监控。部分英国企业亦获准将产品出口至多个独裁国家，例如沙特阿拉伯、阿拉伯联合酋长国、土耳其以及埃及等等; 这些国家恶劣的人权记录已经充分证明，上述监控技术几乎必然遭到滥用。2015 年，英国商业、创新与技能（简称 BIS）部开始发布关于电信拦截类设备的基础出口数据。根据信息自由法案，我们了解到相关出口许可证以及更多相关细节，包括部分销售案例中的实际产品与厂商名称。其中包括国防巨头 BAE Systems 旗下一家子公司，外加 Pro-Solve International、ComsTrac、CellXion、Cobham 以及 Domo Tactical Communications（简称 DTC）等等。

4、微软计划在印度新德里设立新网络安全中心

cnBeta.COM9 月 1 日消息 据外媒最新报道，微软计划在印度新德里设立一个新的网络安全中心。该中心

将为当地政府和私营企业提供网络安全方面的协助。获悉，该中心将可能会选择设在康诺特广场。微软印度分部主席 Bhaskar Pramanik 表示，安全正在成为一个被热议的大型话题，特别当涉及到云服务时。另外，他为公司能跟当地政府部门之间持有这一相同观点而感到兴奋。今年 6 月，微软在印度 Gurugram 开设了一家网络安全合作中心。当时，Pramankik 也做出了表态——“网络安全对于数字印度来说非常重要。一个依靠数据驱动的经济体只有在政府、企业和个体都能访问超大规模、超级灵活以及非常安全的云端时才能茁壮成长。我们在 Gurgaon 设立的网络安全合作中心突显了我们在印度的数字转型道路上为其安全 而做出的不懈努力。”

5、惨遭黑客屡屡入侵 SWIFT 催促银行加强网络安全防护

E 安全 9 月 1 日消息 全球金融电讯协会 SWIFT 透露，黑客正利用 SWIFT 系统对全球银行发动新一轮网络攻击。出于隐私协议，SWIFT 公司未披露银行名称，但它表示，攻击属于新一轮攻击，自今年 6 月开始发起。路透社记者收到一封 SWIFT 发送给全球银行的信（副本），SWIFT 敦促全球银行增强安全防护措施。所有网络窃犯的盗窃方式如出一撤。黑客破坏银行的正常 IT 网络，搜索 SWIFT 系统，收集银行员工的 SWIFT 凭证，之后设法将银行账户的钱转入自己的账户。SWIFT 意识到问题的严重性，一直设法说服银行升级 IT 系统，并使用最新版的 SWIFT 软件。由于 SWIFT 仅仅是一个软件制造商，无权迫使任何金融机构部署更安全的网络环境。不过，路透社指出，SWIFT 在信中要求升级系统的最后期限为 11 月 9 日。SWIFT 表示，对于未保护自身及客户的银行，它将向监管机构汇报或告知同行的金融伙伴。

6、Opera 浏览器同步服务被黑，用户数据和存储密码泄露

FreeBuf8 月 30 日消息 8 月 26 日晚，知名浏览器厂商 Opera 发布公告，表示其云同步服务遭遇黑客攻击，开启了浏览器同步功能的用户将受影响。Opera 公司的一台用于存储用户同步数据的服务器被攻破，如果用户开启了跨平台数据同步功能，则存储在浏览器中的用户名密码以及其他敏感数据都可能已被黑客获取。目前 Opera 浏览器紧急重置了该服务器上所有用户的密码。据悉，Opera 公司拥有大约 3 亿 5000 万用户，其中上个月有 170 万用户开启了数据同步功能，此部分用户的存储在浏览器中的用户名密码已被泄露，其他未使用云同步的用户则不受影响。Opera 在发现黑客攻击后，第一时间重置了所有开启云同步的用户的密码并且邮件告知此次黑客攻击事件，将安全威胁尽可能降低。Opera 公司提醒所有开启同步的用户尽快修改掉他们的 Opera 账户密码，并且建议用户同时也将同步到云端的第三方网站的用户名密码也及时进行修改。

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 2015 年，CNCERT 与 66 个国家和地区的 165 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：何能强

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话： 010-82990158