国家互联网应急中心

网络安全信息与动态周报

2017 年第 34 期

8 月 14 日-8 月 20 日

CNCERT/CC

本周网络安全基本态势

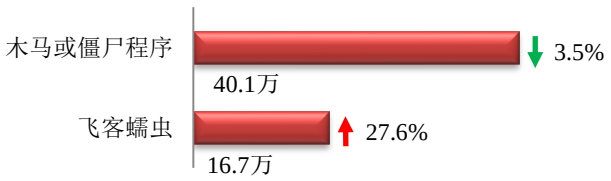
境内感染网络病毒的主机数量	•56.8万	4.0%
境内被篡改网站总数 其中政府网站数量	•2338 •55	13.2% 14.1%
境内被植入后门网站总数 其中政府网站数量	•1032 •72	11.3% 16.1%
针对境内网站的仿冒页面数量	•440	276.1%
新增信息安全漏洞数量 其中高危漏洞数量	•397 •160	31.5% 49.5%

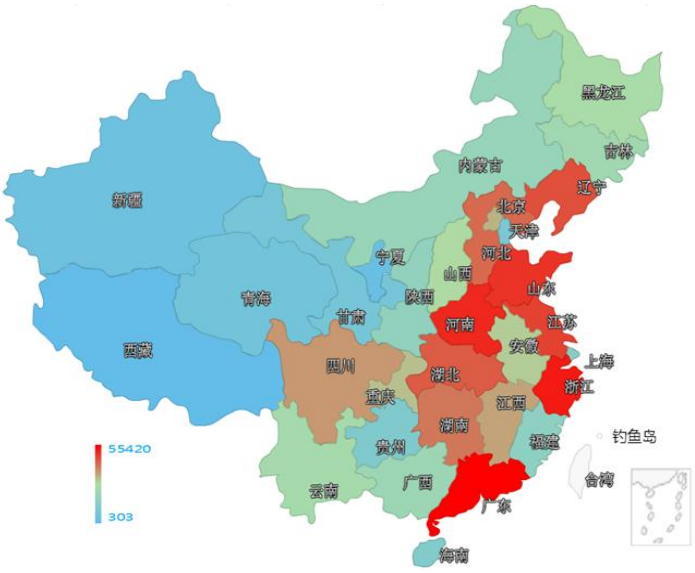
v

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 56.8 万个，其中包括境内被木马或被僵尸程序控制的主机约 40.1 万以及境内感染飞客（conficker）蠕虫的主机约 16.7 万。





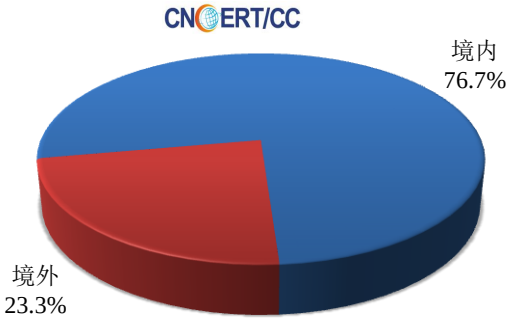
木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、浙江省和河南省。

TOP3

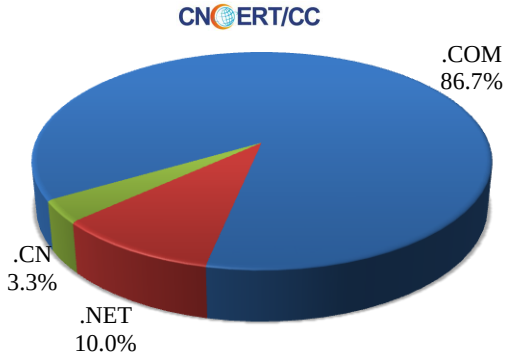
广东省	•约5.5万个（约占中国大陆总感染量的13.8%）
浙江省	•约3.6万个（约占中国大陆总感染量的8.9%）
河南省	•约3.5万个（约占中国大陆总感染量的8.8%）

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 30 个，涉及 IP 地址 45 个。在 30 个域名中，有 23.3%为境外注册，且顶级域为.com 的约占 86.7%；在 45 个 IP 中，有约 6.7%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 1 个 IP。

本周放马站点域名注册所属境内外分布
(8/14-8/20)



本周放马站点域名所属顶级域的分布
(8/14-8/20)



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。

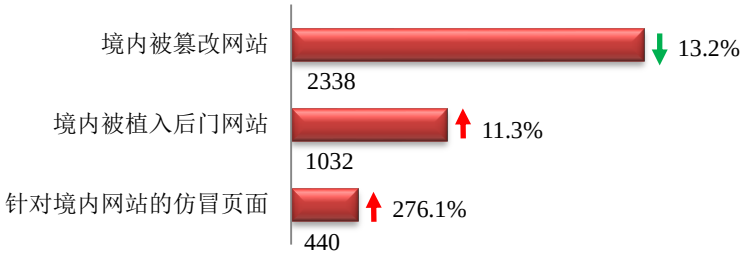
ANVA恶意地址黑名单发布地址

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。

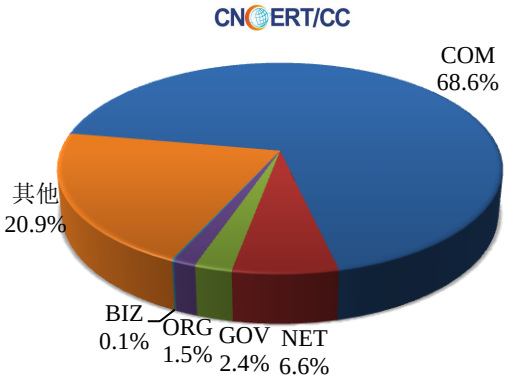
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 2338 个；境内被植入后门的网站数量为 1032 个；针对境内网站的仿冒页面数量为 440。

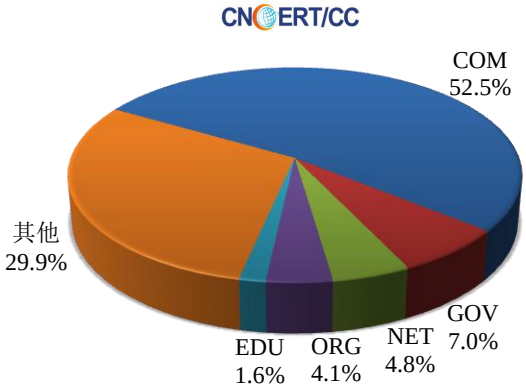


本周境内被篡改政府网站（GOV 类）数量为 55 个（约占境内 2.4%），较上周环比下降了 14.1%；境内被植入后门的政府网站（GOV 类）数量为 72 个（约占境内 7.0%），较上周环比上升了 16.1%；针对境内网站的仿冒页面涉及域名 338 个，IP 地址 134 个，平均每个 IP 地址承载了约 3 个仿冒页面。

本周我国境内被篡改网站按类型分布
(8/14-8/20)

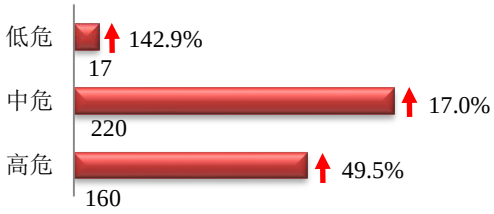


本周我国境内被植入后门网站按类型分布
(8/14-8/20)

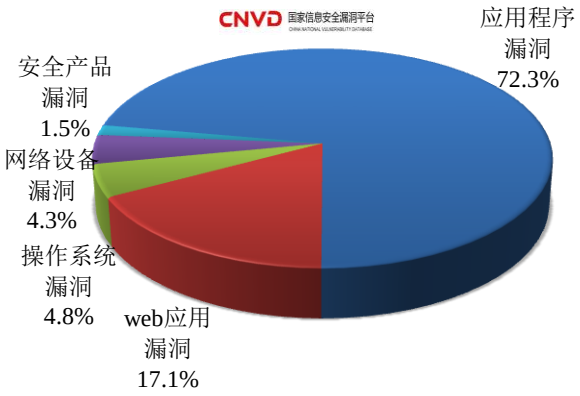


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 397 个，信息安全漏洞威胁整体评价级别为高。



本周CNVD收录漏洞按影响对象类型分布
(8/14-8/20)



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

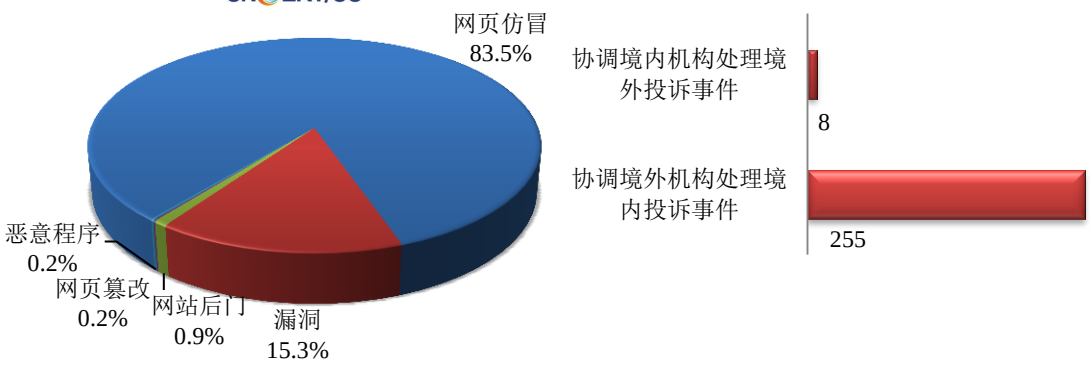
http://www.cnvd.org.cn/webinfo/list?type=4

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

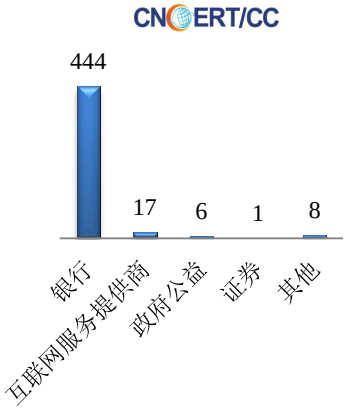
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 570 起，其中跨境网络安全事件 263 起。

本周CNCERT处理的事件数量按类型分布
(8/14-8/20)

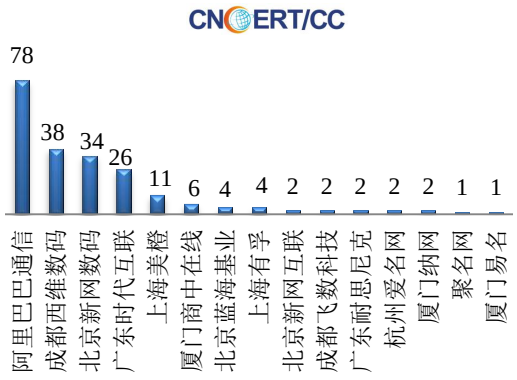


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 476 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 444 起和互联网服务提供商仿冒事件 17 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(8/14-8/20)

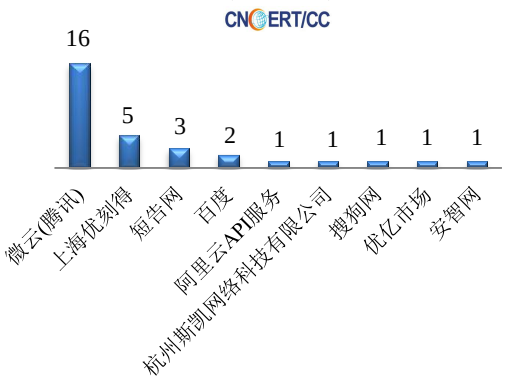


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (8/14-8/20)



本周，CNCERT 协调 9 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 31 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
(8/14-8/20)



业界新闻速递

1、美国提升网络部队级别 加强应对网络攻击

新浪网 8 月 19 日消息 美国总统特朗普 8 月 18 日宣布，把战略司令部旗下的“网络司令部”升级为与战略司令部同级的联合作战司令部。鉴于来自俄罗斯、中国、朝鲜等的网络攻击威胁不断增加，此举旨在强化应对能力。2016 年美国总统大选中，俄罗斯被指涉嫌发起网络攻击干涉选举，引起争议，美国议会中要求提升网络防御能力的呼声高涨。国防部高官 18 日在记者会上表示:“这是我们决心在所有战斗场合保持美军优势的体现。”特朗普 18 日下达指示，要求国防部长马蒂斯推荐担任新网络司令部司令的人选。参议院批准总统提名后，该部队将正式升级。目前则仍由国家安全局（NSA）局长罗杰斯兼任网络司令部司令。共和党的参议院军事委员会主席麦凯恩在声明中强调，“必须制定旨在对抗网络攻击威胁的明确的政策及战略”。

2、美国国务院建立网络技术安全处

E 安全 8 月 17 日消息 美国国务院于今年早些时候悄然在其外交安全处内建立起新的办公室，专门负责防范及应对各类网络安全威胁。美国国务院此次启动的新办公室被定名为网络技术安全处（简称 CTS），且已经于 5 月 28 日得到相关官员证实。联邦新闻广播公司于上周首度以媒体方式报道了该部门的成立。这位官员在采访当中解释称，他们通过先进的创新型网络安全规划与风险管理技术方案以保护生命、财产及信息资产，从而支持美国全球外交活动的实施。该官员同时指出，“CTS 提供先进的网络威胁分析、事件检测与响应、网络调查支持以及其它新兴技术解决方案。”一位政府官在接受联邦新闻广播采访时表示，这一新晋主管部门将为国务院首席信息官提供联络点，旨在确保各大使馆、领事馆以及外事官员免受网络威胁的侵扰。该新晋部门还将负责应对美国国务院所面临的各类潜在网络安全问题。

3、乌克兰央行发布警告：国有与私人银行再度遭受新型勒索软件钓鱼攻击

HackerNews.cc8 月 20 日消息 据外媒报道，乌克兰中央银行于 8 月 18 日发表声明，警示乌克兰国有与私人银行再度遭受新勒索软件攻击，其类型与 6 月袭击全球各企业网络系统的勒索软件 NotPetya 相似。6 月下旬，NotPetya 勒索软件网络攻击首次袭击乌克兰与俄罗斯公司，旨在加密电脑私人数据并要求受害用户缴纳 300 美元赎金。调查显示，此次攻击活动通过一款广泛使用的会计软件 MeDoc 感染恶意代码并于全球范围内肆意传播，而 TNT 快递、美国默克等知名企业在网络系统运营中普遍使用该款软件。据悉，安全专家于 8 月 11 日发现新型勒索软件攻击后当即通过邮件迅速向各银行机构通报其恶意代码、特性指标，以及预防措施。经安全专家深入调查后发现，新型勒索软件通过网络钓鱼邮件附带的恶意办公文档进行肆意传播。目前，乌克兰央行正与国家 CERT 及地方当局密切合作，旨在提高其关键基础设施的网络系统防御能力（特别是乌克兰各大银行）。

4、因选票公司错误设置 180 万芝加哥选民信息泄露

中新网 8 月 18 日消息 据美国侨报网报道，美国一家选票计算机公司在服务器上进行了错误的安全设置后，将 180 万芝加哥选民的记录泄露到了网络上。据美国有线电视新闻网（CNN）消息，内布拉斯加州的投票软件及选举管理公司 Election Systems & Software（ES&S）17 日确认了这次泄露事件。该公司在一篇博客文章中说，

泄露的选民数据包括名字、地址、出生日期、一部分社会安全号码、驾照和州身份证号码。这些信息原本储存在服务器的备份文件中。警方在8月12日就泄露事件通知ES&S，目前数据已得到保护。计算机安全公司UpGuard一名安全研究员发现了这个漏洞。数据不包括投票信息，比如选民的投票结果。芝加哥选举委员会发言人艾伦（Jim Allen)说，泄露不包含也不影响任何人的投票结果。这些信息由另一家公司负责。

5、Check Point 安全报告：尼日利亚黑客掀起能源、矿产与基础设施行业的攻击浪潮

HackerNews.cc8 月 17 日消息 据外媒 8 月 15 日报道，Check Point 研究人员近期发布安全报告，指出一名尼日利亚黑客利用网络钓鱼邮件在过去 4 个月内针对全球超过 4000 家组织展开网络攻击活动，旨在感染企业网络系统、窃取银行数据并进行诱导欺诈，其中涉及多家关于石油、天然气、银行与建筑等行业的国际知名公司。研究人员经调查后发现，黑客伪造来自世界第二大石油生产厂商沙特阿拉伯国有石油公司（Saudi Aramco）的银行密件抄送给众多目标企业的内部财务人员邮箱，以诱导他们披露更多公司财务信息，或点击下载感染恶意软件 NetWire 及 Hawkeye 附件。其中，受影响公司主要包括克罗地亚海洋能源解决方案公司、阿布扎比运输公司、埃及矿业公司、迪拜建筑公司、科威特石油与天然气公司与德国建筑机构。恶意软件 NetWire 是一种远程访问木马程序，可以完全控制受感染机器，而 Hawkeye 是一种键盘记录程序，允许黑客获取敏感信息。

6、新型“脉冲波”DDoS 攻击来袭：锁定多目标+大流量攻击

E 安全 8 月 20 日消息 据 Imperva Incapsula8 月 16 日报告指出，新型“脉冲波”DDoS 攻击同时锁定多个目标发起猛攻。黑客利用传统 DDoS 缓解措施中的弱点发起新型 DDoS 攻击，旨在增强攻击强度。攻击者利用此类攻击可让目标网络长时间瘫痪，与此同时还能攻击多个目标。专家指出，这类攻击可能会使传统 DDoS 缓解措施毫无用武之地。Imperva 安全研究人员表示，极端“脉冲波”DDoS 攻击持续数天，峰值高达 350 Gbps。Imperva 在分析报告中指出，脉冲波攻击包含一系列短脉冲，如发条般的接连发生。研究人员认为，脉冲波攻击出自高级黑客之手，利用“设备优先，云其次”混合缓解方案中的弱点提升攻击强度，并拓宽范围。传统的 DDoS 攻击的流量通常会逐步攀升，然而“脉冲波”攻击则包含“高度重复”的短脉冲攻击（由每十分钟一次或多次脉冲构成）。这类新型攻击持续时间超过一小时，乃至数天。单脉冲的规模及强度足以致网络堵塞。研究人员还指出，“脉冲波”攻击最大的特点是不存在流量逐渐攀升一说，而是将所有攻击资源一次性汇入，仅需数秒就能达到峰值，并在持续过程中保持峰值居高不下。

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：贾子骁

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158