国家互联网应急中心

2017 年第 28 期

7 月 3 日-7 月 9 日

网络安全信息与动态周报

CNCERT/CC

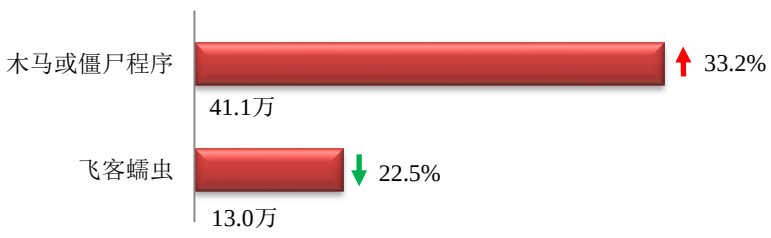
本周网络安全基本态势

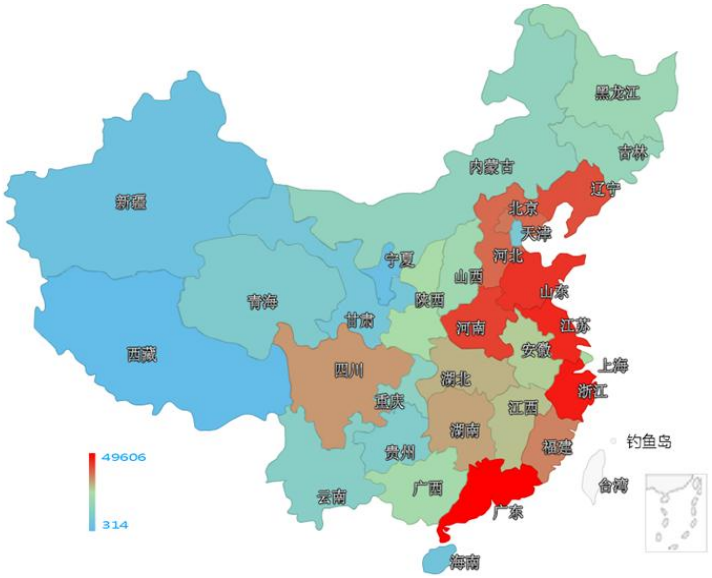
境内感染网络病毒的主机数量	•54.1万	↑ 13.6%
境内被篡改网站总数 其中政府网站数量	•1180 •48	↓ 28.7% ↑ 2.1%
境内被植入后门网站总数 其中政府网站数量	•1811 •105	↑ 20.0% ↑ 50.0%
针对境内网站的仿冒页面数量	•250	↓ 26.0%
新增信息安全漏洞数量 其中高危漏洞数量	•308 •112	↑ 0.3% ↑ 7.7%

═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 54.1 万个，其中包括境内被木马或被僵尸程序控制的主机约 41.1 万以及境内感染飞客（conficker）蠕虫的主机约 13.0 万。





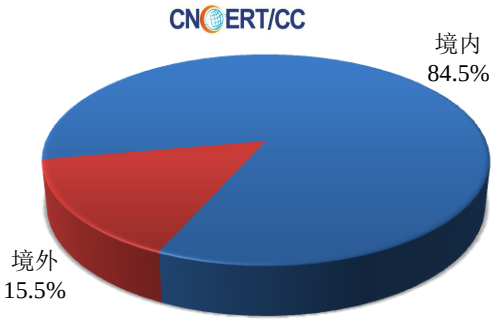
木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、浙江省和江苏省。

TOP3

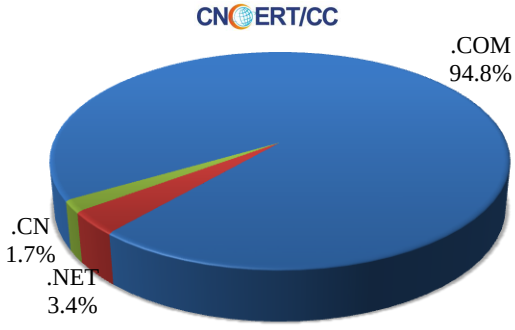
广东省	•约5.0万个（约占中国大陆总感染量的12.1%）
浙江省	•约4.5万个（约占中国大陆总感染量的11.0%）
江苏省	•约3.3万个（约占中国大陆总感染量的7.9%）

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 58 个，涉及 IP 地址 77 个。在 58 个域名中，有 15.5%为境外注册，且顶级域为.com 的约占 94.8%；在 77 个 IP 中，有约 3.9%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 2 个 IP。

本周放马站点域名注册所属境内外分布
(7/3-7/9)



本周放马站点域名所属顶级域的分布
(7/3-7/9)



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。

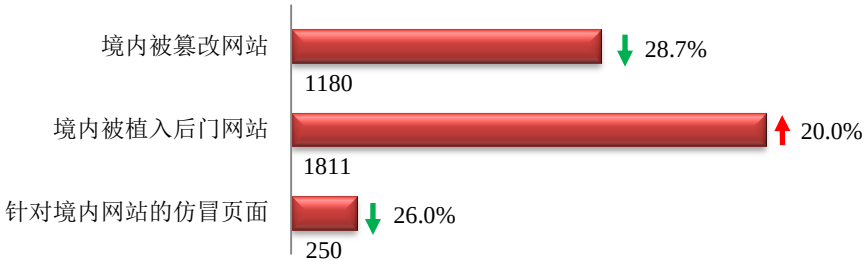
ANVA恶意地址黑名单发布地址

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。

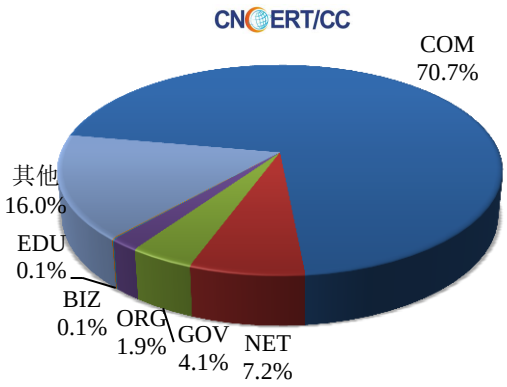
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1180 个；境内被植入后门的网站数量为 1811 个；针对境内网站的仿冒页面数量为 250。

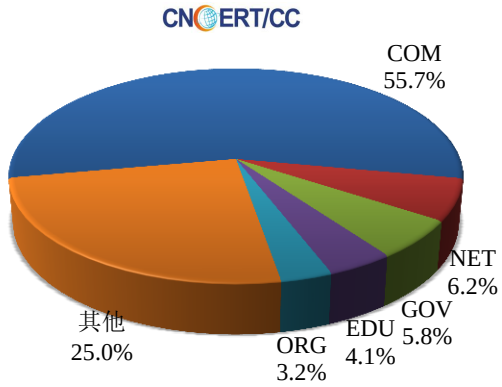


本周境内被篡改政府网站（GOV 类）数量为 48 个（约占境内 4.1%），较上周环比上升了 2.1%；境内被植入后门的政府网站（GOV 类）数量为 105 个（约占境内 5.8%），较上周环比上升了 50.0%；针对境内网站的仿冒页面涉及域名 191 个，IP 地址 99 个，平均每个 IP 地址承载了约 3 个仿冒页面。

本周我国境内被篡改网站按类型分布
(7/3-7/9)

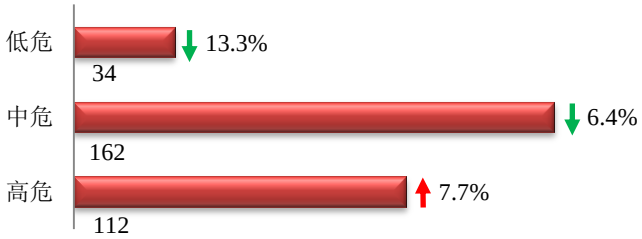


本周我国境内被植入后门网站按类型分布
(7/3-7/9)

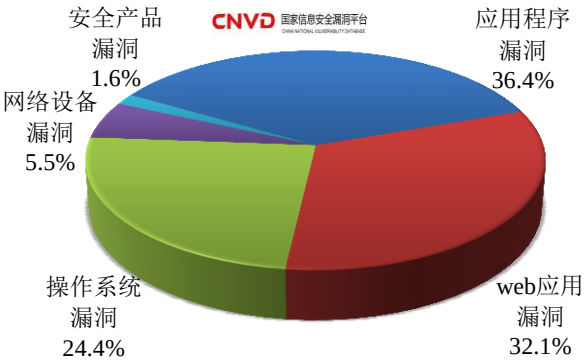


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 308 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
(7/3-7/9)



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

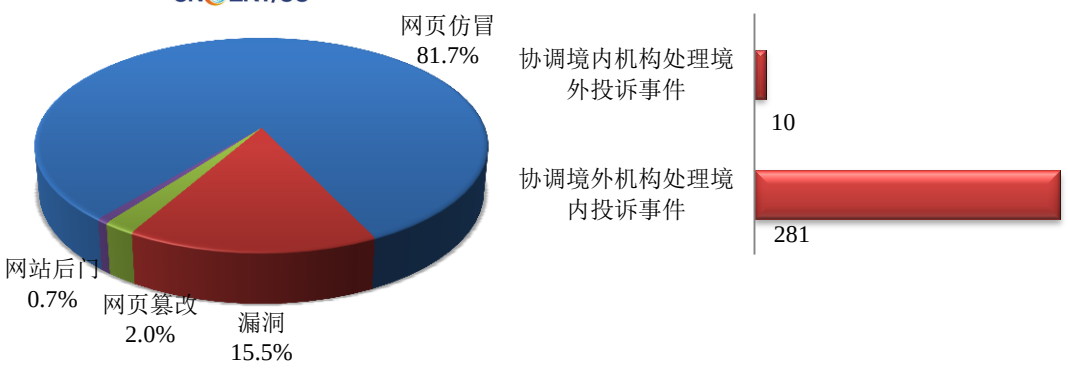
http://www.cnvd.org.cn/webinfo/list?type=4

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

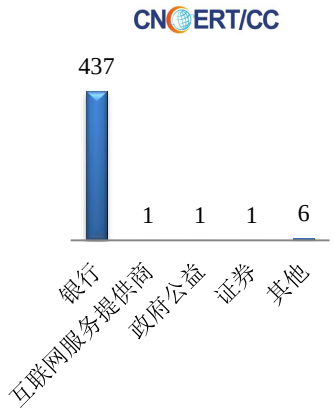
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 547 起，其中跨境网络安全事件 291 起。

本周CNCERT处理的事件数量按类型分布
(7/3-7/9)

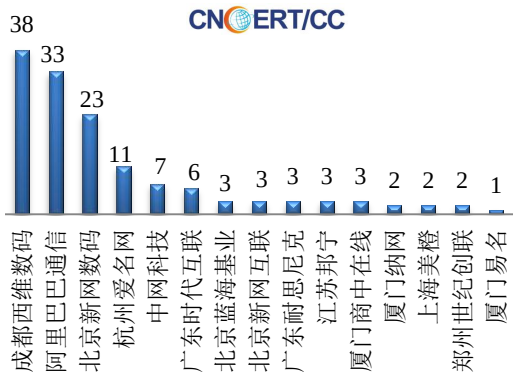


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 446 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 437 起和互联网服务提供商仿冒事件 1 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(7/3-7/9)

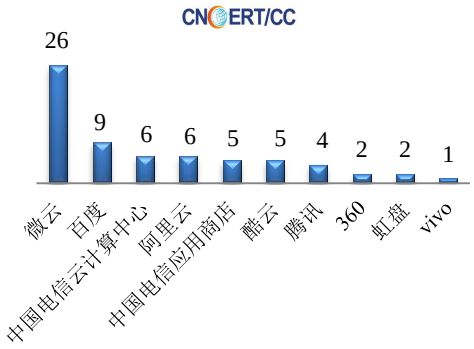


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (7/3-7/9)



本周，CNCERT 协调 10 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 66 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
(7/3-7/9)



业界新闻速递

1、国际电信联盟发布全球网络安全指数

新华网 7 月 6 日消息 国际电信联盟 7 月 5 日发布《2017 年全球网络安全指数》，以衡量各国在应对全球网络安全问题上的承诺和行动。新加坡在 193 个国际电信联盟成员国中排名第一。按这份报告所标注的位次，全球排名从第二到第十的国家依次是美国、马来西亚、阿曼、爱沙尼亚、毛里求斯、澳大利亚、格鲁吉亚、法国、加拿大、俄罗斯，其中格鲁吉亚和法国并列第八。此外，日本和韩国分别排在第 11 位和第 13 位，中国排在第 32 位。国际电信联盟发布这份全球网络安全指数，旨在推动各国政府改进应对网络安全威胁的措施，促进网络安全方面的双边和多边国际合作。为此，报告从法律框架、技术手段、组织架构、能力建设和相关合作五个方面，考察各国在加强网络安全方面所做出的努力和承诺。而报告的结论并不乐观。全球只有 38%的国家发布了网络安全战略，另有 12%的国家还在制定相关战略的过程中。这意味着全球大多数国家仍然没有清晰的网络威胁应对策略，不利于防范相关风险。报告认为，随着网络犯罪日趋频繁，各国政府应采取措施加强网络安全生态环境建设，以减少犯罪威胁，提高人们对使用网络服务的信心。

2、英国数字权利组织要求五眼情报联盟公布机密信息

HackerNews.cc7 月 8 日消息 据外媒 7 月 6 日报道，英国数字权利组织 Privacy International 已向美国提起联邦诉讼，要求发布五眼情报联盟披露相关信息。五眼情报联盟形成于二战期间，1946 年签署《英美通信情报协议》后正式成立。其联盟由美国、英国、澳大利亚、加拿大与新西兰五国情报机构组成，旨在实现各国政府企业间情报信息的互联互通，共享商业数据、窥探策略、技术手段与信息收集成果。调查显示，协议最新公开版本发布于 1955 年，揭示了情报数据传播途径。随着科技的迅猛发展，原有法律标准与限制已无法满足时代要求。在此情景下，Privacy International 要求公开五眼联盟情报收集的具体操作细节，因为现有方法极有可能将其他国家置于险地。前美国国家安全局（NSA）分析师爱德华•斯诺登（Edward Snowden）泄露的文件显示，包括英国政府通信总部（GCHQ）在内的情报机构均利用大型设备获取海量通信数据。据悉，Privacy International 在诉讼中要求五眼情报联盟发布当前最新版本的《英美协议》（UKUSA Agreement），内容包括政府如何实现协议条款、按协议要求交换情报标准与流程以及提供有关美国政府收购、储存、分析与传播美国通信的具体信息等。

3、美国核能公司遭遇黑客事件，多个核电站被入侵

E 安全 7 月 9 日消息 美国国土安全部（DHS）官员证实，美国官员上周警告工业公司，持续的黑客活动正在瞄准核能源行业的目标。在这波黑客事件中，操作系统未受到影响，只是行政和商业网络受到影响，公共安全并未受到威胁。DHS 和 FBI 发布报告指出，黑客向工程师发送鱼叉式网络钓鱼电子邮件，其中包含隐藏着恶意软件的虚假简历，企图访问目标设备和网络。据《纽约时报》报道，黑客还使用“水坑式攻击”感染目标（受害者）访问的合法网站。此外，黑客还实施了中间人攻击，其中目标（受害者）的互联网流量通过黑客的设备被重定向。上周，能源行业新闻网站 E&E News 报道称，多个核发电站遭遇网络入侵。

4、韩最大加密货币交易所被黑客攻击：3 万客户数据泄露

cnBeta.COM7 月 6 日消息 正当韩国正被对比特币和以太币等加密货币进行监管立法的时候，却有报道称该国最大的加密货币交易所 Bithumb 遭到了黑客入侵。据 BBC 报道，3 万名客户数据被泄露，黑客利用欺骗来的数据窃取用户账户里的资金。BraveNewCoin 则解释了 Bithumb 用户是“语音钓鱼”的受害者，因为有自称该交易所工作人员的骗子打电话来忽悠他们。据悉，本次泄露发生于 2 月份，原因是一名员工的家用 PC 涉入其中（而不是公司总部的计算机服务器出现了问题）。Bithumb 表示在 6 月 29 日发现了此事，并于次日向当局进行了汇报。作为全球五大比特币交易所之一，Bithumb 去年的比特币交易量达到了 2 万亿韩元左右（约合 118 亿 RMB），日交易量也超过了 1.3 万比特币（占全球交易量 10%）。Bithumb 已承诺初步向每位客户赔偿 10 万韩元（约 86 美元/590 元 RMB），剩余部分将在验证后补足。

5、勒索病毒源头乌克兰公司服务器被警察没收

腾讯网 7 月 5 日消息 据外媒报道，一名高级警官称，乌克兰警方周二没收了该国一家会计软件公司的服务器，因为该公司涉嫌传播导致全球很多大公司电脑系统瘫痪的勒索病毒。乌克兰网络警察局长沙希利-德梅德尤克（Serhiy Demedyuk）称，为了调查上周发生的肆虐全球的勒索病毒攻击案，警方没收了乌克兰最流行会计软件开发公司 M.E.Doc 的服务器。警方还在调查谁是真正的幕后黑手。乌克兰情报官员和安全公司声称，最初的一些勒索病毒是通过 M.E.Doc 公司发布的恶意升级程序传播的。对此，该公司予以了否认。在警方没收 M.E.Doc 公司的服务器前，网络安全调查员已在周二找出了新的证据，证明此次勒索病毒攻击活动是一些高级黑客提前好几个月策划的结果。这些黑客将病毒插入到了 M.E.Doc 公司的会计软件中。乌克兰在周二将其纳税日期推迟了一个月，以帮助被勒索病毒攻击的企业渡过难关。

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：李世淙

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话： 010-82990158