国家互联网应急中心

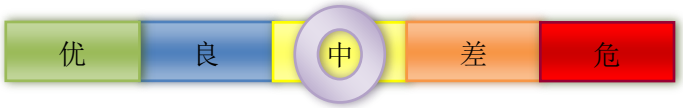
网络安全信息与动态周报

2016 年第 30 期

7 月 18 日-7 月 24 日

CNCERT/CC

本周网络安全基本态势

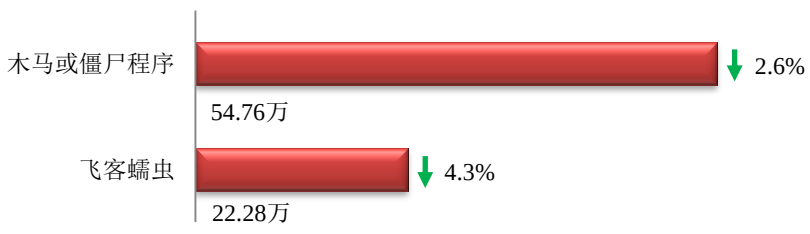


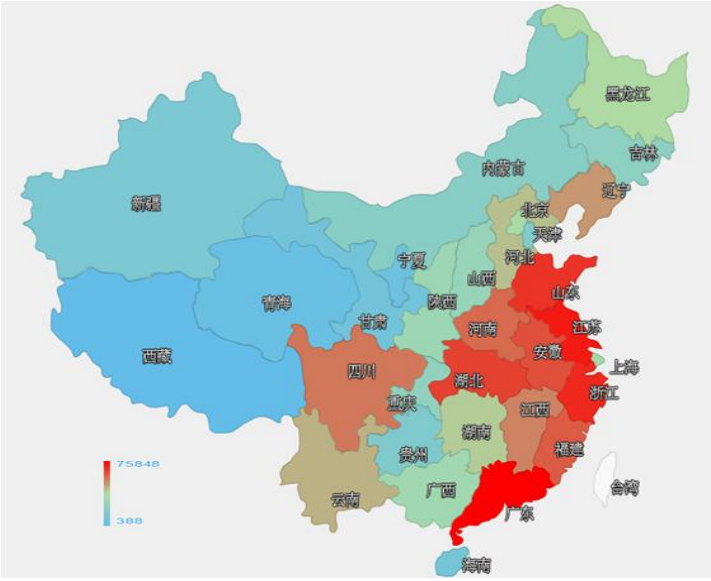
境内感染网络病毒的主机数量	• 77.04万	↓ 3.1%
境内被篡改网站总数 其中政府网站数量	• 3118 • 73	↑ 21.4% ↑ 15.9%
境内被植入后门网站总数 其中政府网站数量	• 2334 • 80	↓ 1.6% ↓ 10.1%
针对境内网站的仿冒页面数量	• 7410	↓ 11.6%
新增信息安全漏洞数量 其中高危漏洞数量	• 370 • 159	↑ 84.1% ↑ 54.4%

═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 77.04 万个，其中包括境内被木马或被僵尸程序控制的主机约 54.76 万以及境内感染飞客（conficker）蠕虫的主机约 22.28 万。





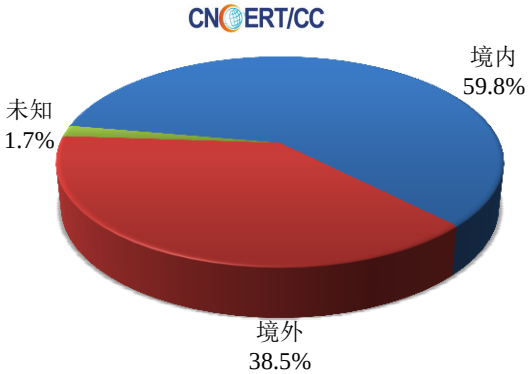
木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、江苏省和浙江省。

TOP3

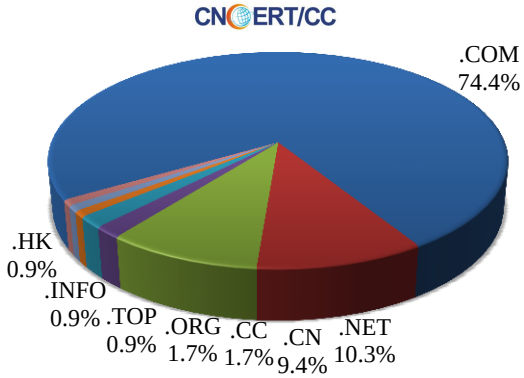
广东省	•约7.6万个（约占中国大陆总感染量的13.9%）
江苏省	•约5.5万个（约占中国大陆总感染量的10.0%）
浙江省	•约4.0万个（约占中国大陆总感染量的7.3%）

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 117 个，涉及 IP 地址 290 个。在 117 个域名中，有 38.5%为境外注册，且顶级域为.com 的约占 74.4%；在 290 个 IP 中，有约 5.9%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 15 个 IP。

本周放马站点域名注册所属境内外分布
(7/18-7/24)



本周放马站点域名所属顶级域的分布
(7/18-7/24)



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。

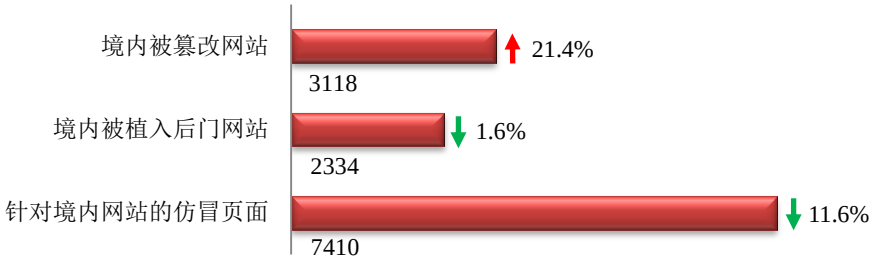
ANVA恶意地址黑名单发布地址

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。

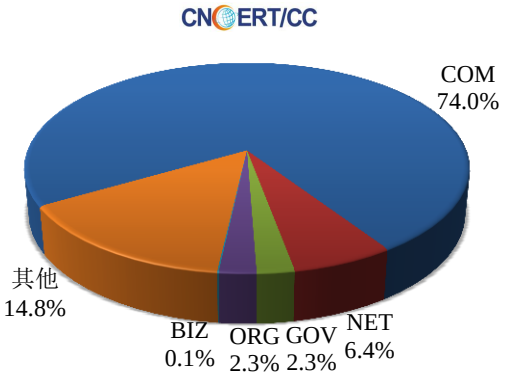
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 3118 个；境内被植入后门的网站数量为 2334 个；针对境内网站的仿冒页面数量为 7410。

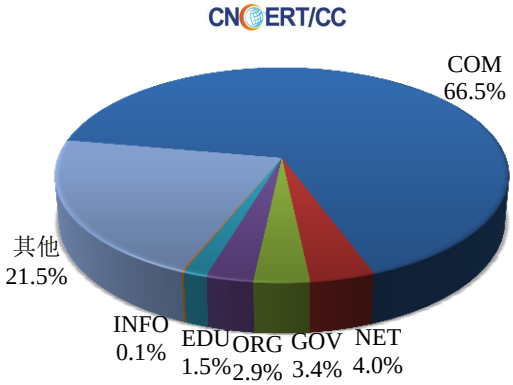


本周境内被篡改政府网站（GOV 类）数量为 73 个（约占境内 2.3%），较上周环比上升了 15.9%；境内被植入后门的政府网站（GOV 类）数量为 80 个（约占境内 3.4%），较上周环比下降了 10.1%；针对境内网站的仿冒页面涉及域名 1458 个，IP 地址 514 个，平均每个 IP 地址承载了约 14 个仿冒页面。

本周我国境内被篡改网站按类型分布
(7/18-7/24)

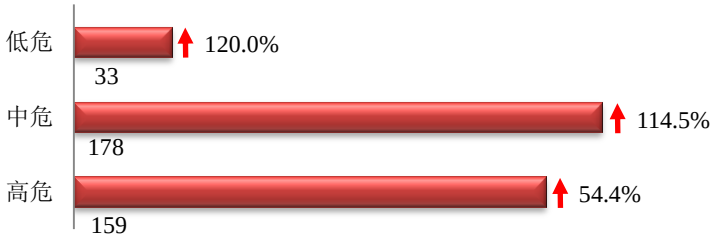


本周我国境内被植入后门网站按类型分布
(7/18-7/24)

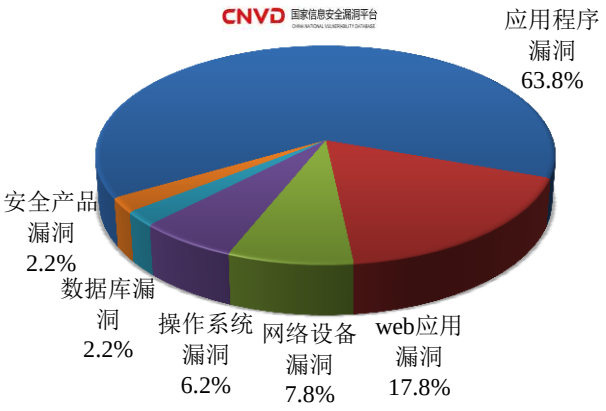


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 370 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
(7/18-7/24)



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

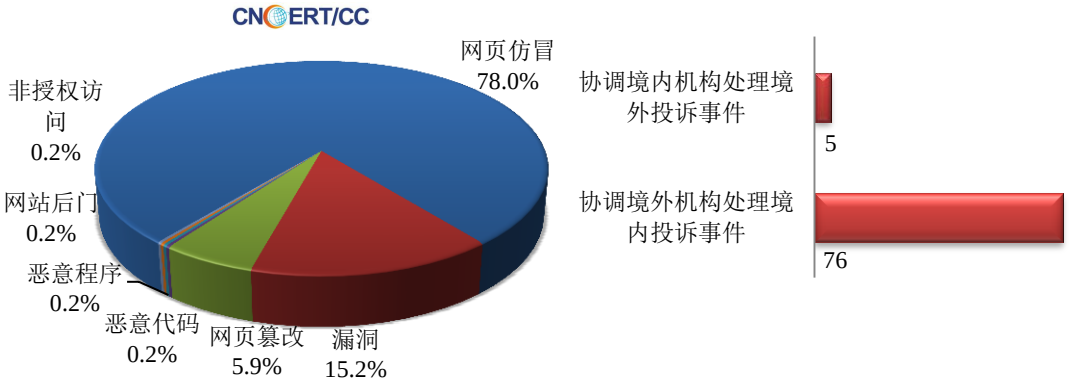
http://www.cnvd.org.cn/webinfo/list?type=4

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

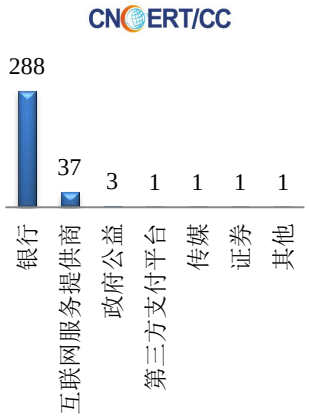
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 427 起，其中跨境网络安全事件 81 起。

本周CNCERT处理的事件数量按类型分布
(7/18-7/24)

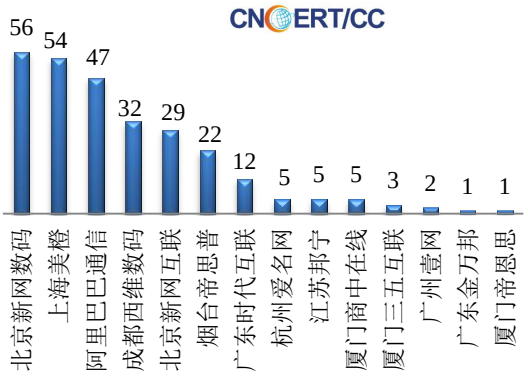


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 332 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事 288 起和互联网服务提供商仿冒事件 37 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(7/18-7/24)

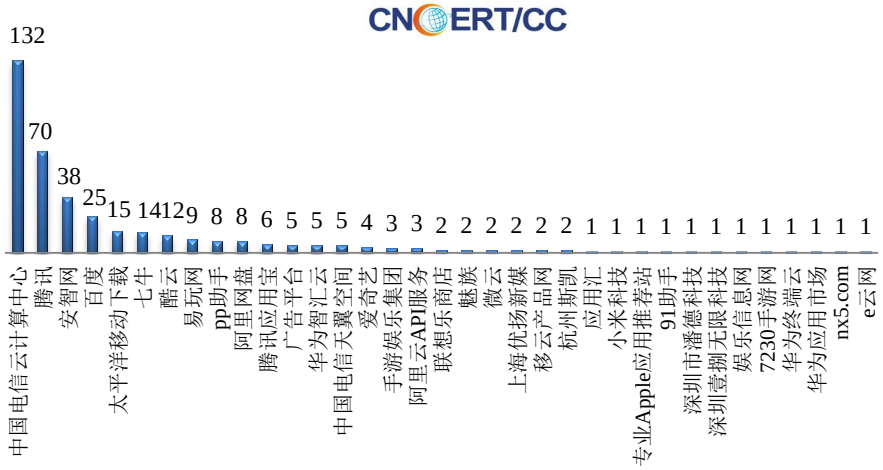


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (7/18-7/24)



本周，CNCERT 协调 35 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 386 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 (7/18-7/24)



业界新闻速递

1、国际清算银行发布安全指南 保护金融市场基础设施网络安全

中国信息产业网 7 月 18 日消息 在针对金融领域的网络攻击日益增多的背景下，国际清算银行近日发布《金融市场基础设施网络安全指南》。该指南在经过三个月的公开征求意见后，由国际支付和市场基础设施委员会和国际证监会组织合发布，旨在提高金融市场基础设施在遭受持续攻击时快速恢复和继续运行的能力。这份长达 32 页的指南关注的重点领域包括：如何通过特定的程序和方法辨别金融市场基础设施潜在网络威胁，如何处理网络威胁情报，如何确定搜集威胁情报的范围。其他内容还包括：如何提高预测和防范风险的能力，如何实现信息共享。指南还为企业应对网络安全威胁提供一系列指导和行为准则。在该指南出台前，金融领域接连出现几起重大网络安全事件，包括黑客通过恶意软件入侵环球银行间金融通信协会的转账支付系统，网络犯罪分子从孟加拉中央银行盗窃 8100 万美元，以及比特币平台 Gatecoin 被窃取总值 200 万美元的比特币和以太币等。

2、美国组建了一支网络部队 专门开发恶意软件

腾讯网 7 月 18 日消息 美国网络司令部上将 Michael S. Rogers 组建了一支网络部队，这支部队专门开发恶意软件组件以及数字化武器，用来开展与 ISIS 的数字化战争。五角大楼在今年年初就要求网络司令部对伊斯兰国发动网络攻击，不幸的是，据美国华盛顿邮报报道，网络司令部尚未做好充分的准备，用于发动攻击的网络工具非常缺乏，并且从事此项任务的人员也并不合适此项工作。华盛顿邮报还指出，新的团队名为“战神联合特遣队（Joint Task Force Ares）”，他们执行的任务可能包括：破坏恐怖组织的支付系统、破坏恐怖组织聊天联络工具等等。五角大楼通过使用这一特遣队还可减少平民伤亡的风险，比如可以通过网络攻击切断恐怖分子藏身处的通讯系统，而无需使用炸弹等武器进行打击。然而，即使战神联合特遣队负责进攻行动的时候，他们的任务也不是为军队寻找空袭目标，而是在伊拉克和叙利亚境内的 ISIS 组织发动网络攻击。五角大楼官方发言人向华盛顿邮报透露，该特遣队未来将可以在全球执行任务。

3、美国海军向罗柯公司订购网络电台用于网络中心战

搜狐网 7 月 20 日消息 据军事与航空电子网站 2016 年 7 月 19 日报道，美国海军与罗克韦尔·柯林斯公司签署价值 2490 万美元的合同，旨在为美国海军提供先进的网络电台，用于网络中心战。根据美国海军航空作战中心武器分部要求，罗克韦尔·柯林斯公司将提供 194 个 Quint 网络技术（QNT）电台、379 套相关硬件，并为 AN/ALQ-231(V)“猛虎”电子攻击系统提供 36482 小时附带设备修正服务，以支持联合电子攻击兼容性办公室。QNT 项目由美国国防先期研究计划局（DARPA）监管，旨在开发模块化网络数据链，在有人机、无人战斗机（UCAV）、武器系统、战术无人机、地面步兵部队之间建立多频带通信。QNT 技术将利用数据链把战术无人机、步兵、武器系统集成到未来数字战场，以用于网络中心作战，在作战中将采用分布式传感器平台来实时发现、锁定、追踪、攻击重要的静止或运动目标。该合同按计划将于 2021 年 5 月完成。

4、韩政府鼓励民众设防毒软件 应对网络攻击

环球网 7 月 22 日消息 据韩国纽西斯通讯社 7 月 22 日报道，韩国未来创造科学部 21 日表示，根据今年上半年（1-6 月）韩国网络攻击结果分析，与 2015 年相比，2016 年韩国电脑网络的被攻击次数增长了 200%以上。据未来创造科学部表示，网络攻击的主要形式有入侵智能手机，给政府官员持续发送病毒邮件，入侵 IT 信息保护企业等多种形式。除了网络攻击，还包括试图入侵 13 万台韩国企业电脑和服务器，窃取国防工业的相关文件。韩国政府提高警惕，检查国内主要基础设施，倾注全力强化政府应对姿态，推动对曾经受到黑客入侵的机关和网页的集中检查。韩国政府正在讨论如何应对与暴力恐怖结合的网络恐怖行为。未来创造科学部有关人士表示，为了应对网络攻击，韩国民众对个人电脑或智能手机应该设置最新的防毒软件，不要浏览可疑邮件。

5、美国国会网站遭受 DDoS 攻击长达三天

E 安全 7 月 20 日消息 美国国会遭受长达三天的 DDoS 攻击，三大政府网站：congress.gov、美国国会图书馆网站（loc.gov）以及美国版权局（coypright.gov）不幸躺枪。7 月 17 日，美国国会图书馆网站遭受攻击，同一服务器基础设备上托管的另外两大网站也未能幸免于难。尽管最初采取了防御措施，但攻击在接下来的两天逐渐升级，继续给政府官员和网站访客制造麻烦，直到当地时间 7 月 19 日晚才恢复。目前，这三大网站已正常运营。其它美国政府门户网站未受影响。美国国会图书馆发言人表示，DDoS 洪水攻击涉及某种“DNS 攻击。”虽然未经官方证实，通过技术专业知识可以推断，这是一次 DNS 反射 DDoS 攻击，这是目前最最常见的 DDoS 攻击类型。此次攻击中，黑客创建畸形 UDP 数据包发送至 DNS 服务器。DNS 服务器设置包含漏洞，可以繁殖并反射数据包至目标。DDoS 攻击通常用来掩盖更声势浩大的入侵，外媒表示希望这些机构的网站管理员也调查网络的其它部分。

6、维基解密遭持续网络攻击：疑为土耳其政府所为

比特网 7 月 19 日消息 当地时间周一，维基解密遭到了持续的网络攻击，而就在攻击发生之前，该机构宣布将公布一批土耳其政治权力结构的详细说明文档。维基解密在 Twitter 上写道：“我们的基础设施正在遭受持续的攻击。”据了解，维基解密计划公布 30 万封邮件和 50 万份文档，它们都与上周爆发的土耳其政变相关。维基解密暗示，他们现遭遇的网络攻击很有可能就是土耳其政府发起的。“我们不确定这次攻击真正的源头。但这个时间点表明是土耳其国家权力机构或其盟友。我们终将胜利并发布文档。”维基解密随后写道。据称，在土耳其发生政变的那天，该国的人民都无法访问 Facebook、Twitter、YouTube，但还是有许多用户借助 VPN 分享了与该政变相关的推特、视频等内容。

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：朱天

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话： 010-82990158