国家互联网应急中心

2017 年第 27 期

6 月 26 日-7 月 2 日

网络安全信息与动态周报

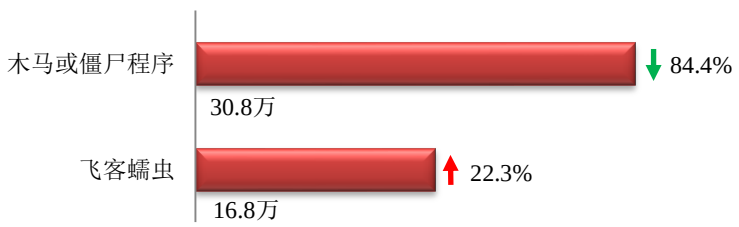
本周网络安全基本态势

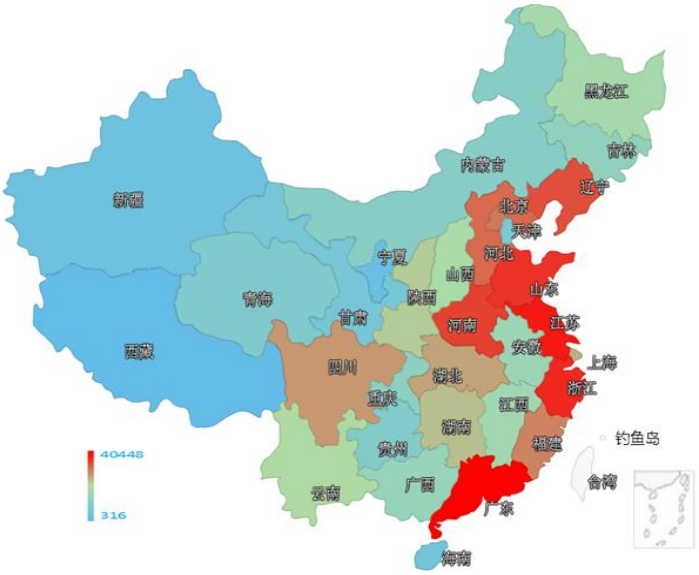
境内感染网络病毒的主机数量	• 47.6万	↓ 77.4%
境内被篡改网站总数 其中政府网站数量	• 1654 • 47	↑ 12.1% ↑ 46.9%
境内被植入后门网站总数 其中政府网站数量	• 1509 • 70	↑ 10.6% ↑ 48.9%
针对境内网站的仿冒页面数量	• 338	↓ 23.4%
新增信息安全漏洞数量 其中高危漏洞数量	• 307 • 104	↓ 5.8% ↓ 18.8%

= 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 47.6 万个，其中包括境内被木马或被僵尸程序控制的主机约 30.8 万以及境内感染飞客（conficker）蠕虫的主机约 16.8 万。





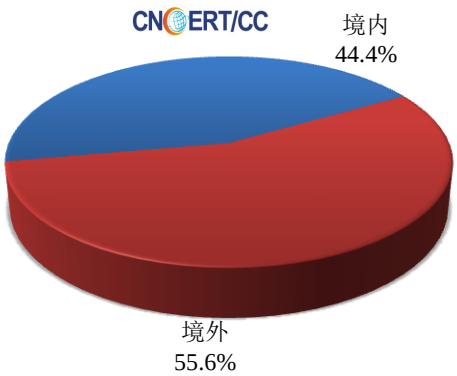
木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、江苏省和浙江省。

TOP3

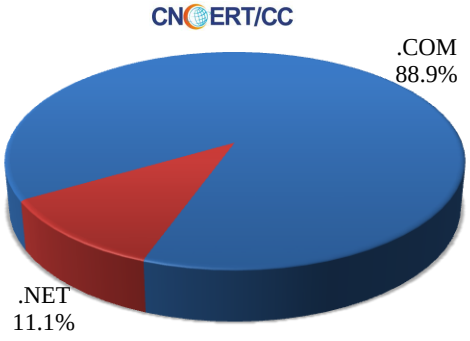
广东省	•约4.0万个（约占中国大陆总感染量的13.1%）
江苏省	•约2.5万个（约占中国大陆总感染量的8.1%）
浙江省	•约2.4万个（约占中国大陆总感染量的7.8%）

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 9 个，涉及 IP 地址 12 个。在 9 个域名中，有 55.6%为境外注册，且顶级域为.com 的约占 88.9%；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。

本周放马站点域名注册所属境内外分布
(6/26-7/2)



本周放马站点域名所属顶级域的分布
(6/26-7/2)



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。

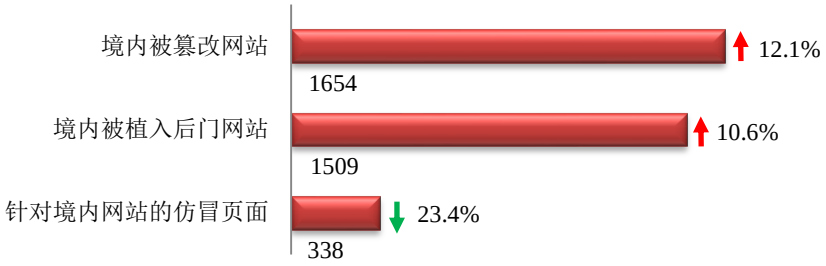
ANVA恶意地址黑名单发布地址

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。

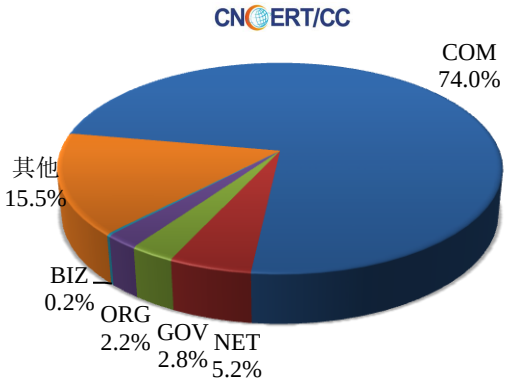
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1654 个；境内被植入后门的网站数量为 1509 个；针对境内网站的仿冒页面数量为 338。

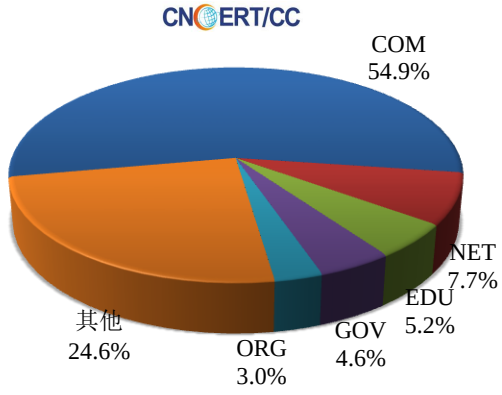


本周境内被篡改政府网站（GOV 类）数量为 47 个（约占境内 2.8%），较上周环比上升了 46.9%；境内被植入后门的政府网站（GOV 类）数量为 70 个（约占境内 4.6%），较上周环比上升了 48.9%；针对境内网站的仿冒页面涉及域名 280 个，IP 地址 138 个，平均每个 IP 地址承载了约 2 个仿冒页面。

本周我国境内被篡改网站按类型分布
(6/26-7/2)

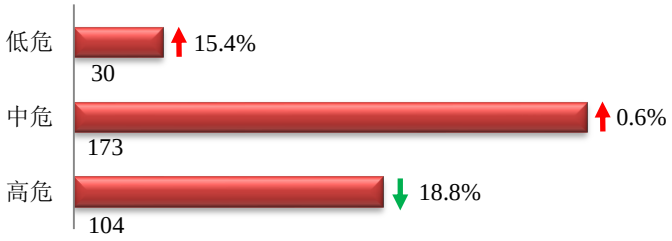


本周我国境内被植入后门网站按类型分布
(6/26-7/2)

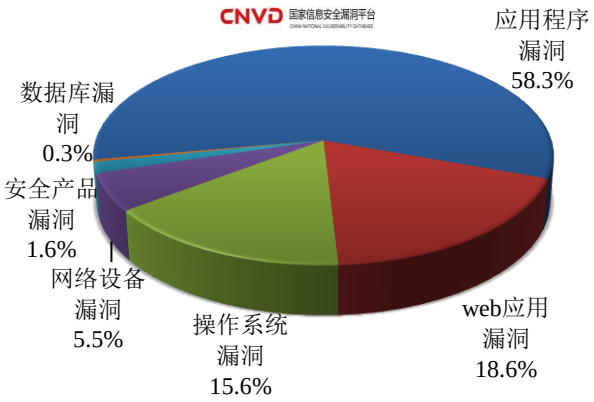


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 307 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
(6/26-7/2)



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

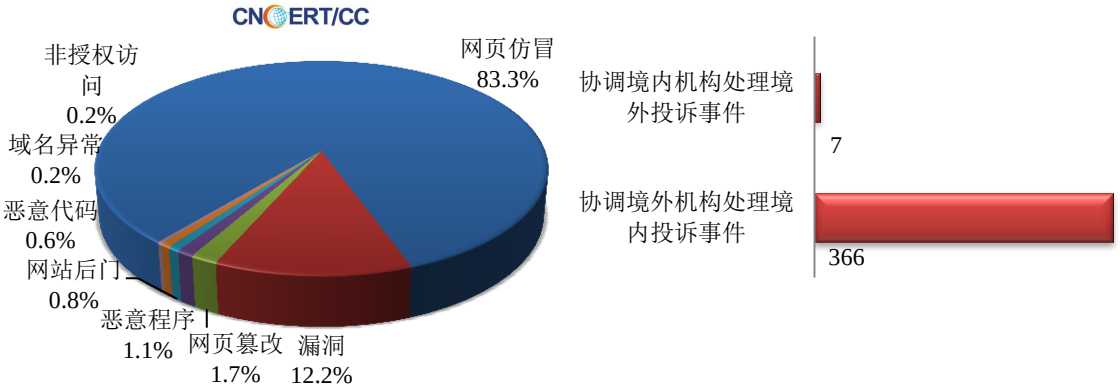
http://www.cnvd.org.cn/webinfo/list?type=4

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

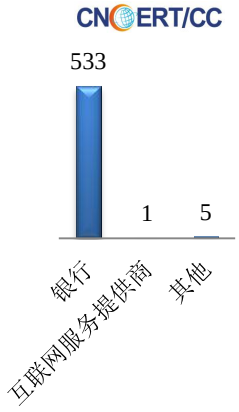
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 648 起，其中跨境网络安全事件 373 起。

本周CNCERT处理的事件数量按类型分布
(6/26-7/2)

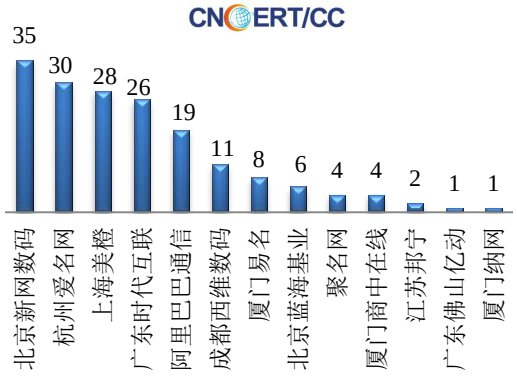


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 539 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 533 起和互联网服务提供商仿冒事件 1 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(6/26-7/2)

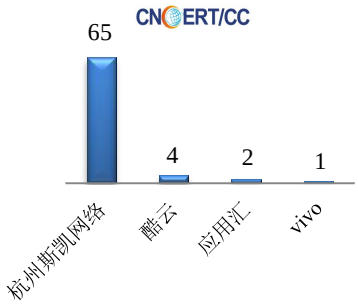


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (6/26-7/2)



本周，CNCERT 协调 4 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 72 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
(6/26-7/2)



业界新闻速递

1、国家网络安全应急办成立 负责跨部门跨地区协调

新京报网 6 月 28 日消息 近日，中央网络安全和信息化领导小组办公室印发《国家网络安全事件应急预案》（以下简称《预案》）。《预案》显示，我国成立国家网络安全应急办公室，具体工作由中央网信办网络安全协调局承担。《预案》表示，中央网络安全和信息化领导小组办公室（以下简称“中央网信办”）统筹协调组织国家网络安全事件应对工作，建立健全跨部门联动处置机制，工业和信息化部、公安部、国家保密局等相关部门按照职责分工负责相关网络安全事件应对工作。必要时成立国家网络安全事件应急指挥部（以下简称“指挥部”），负责特别重大网络安全事件处置的组织指挥和协调。《预案》透露，国家网络安全应急办公室（以下简称“应急办”）设在中央网信办，具体工作由中央网信办网络安全协调局承担。应急办负责网络安全应急跨部门、跨地区协调工作和指挥部的事务性工作，组织指导国家网络安全应急技术支撑队伍做好应急处置的技术支撑工作。此外，《预案》还提出，网络安全事件应急处置工作实行责任追究制。中央网信办及有关地区和部门对不按照规定制定预案和组织开展演练，迟报、谎报、瞒报和漏报网络安全事件重要情况或者应急管理工作中有其他失职、渎职行为的，依照相关规定对有关责任人给予处分；构成犯罪的，依法追究刑事责任。

2、中央网信办发布《国家网络安全事件应急预案》

通信世界网 6 月 28 日消息 中央网信办 6 月 27 日印发了《国家网络安全事件应急预案》，该预案自印发之日起实施。中央网信办将网络安全事件分为四级：特别重大网络安全事件、重大网络安全事件、较大网络安全事件、一般网络安全事件，并提出对应的预警和应急响应。根据预案规定，网络安全事件发生后，事发单位应立即启动应急预案，实施处置并及时报送信息。各有关地区、部门立即组织先期处置，控制事态，消除隐患，同时组织研判，注意保存证据，做好信息通报工作。对于初判为特别重大、重大网络安全事件的，立即报告应急办。除此之外，各地区、各部门网络安全事件应急指挥机构实行 24 小时值班，相关人员保持通信联络畅通。加强网络安全事件监测和事态发展信息搜集工作，组织指导应急支撑队伍、相关运行单位开展应急处置或准备、风险评估和控制工作，重要情况报应急办。

3、我国将加大工业互联网安全监测预警

新华网 6 月 30 日消息 工信部总工程师张峰在此间于北京举行的第二十一届中国国际软件博览会上表示，工信部将从加快平台建设和构建产业生态两方面推进工业互联网产业发展，加大力度提升工业互联网安全监测预警能力，应急处置能力，完善安全管理体系。随着信息技术与制造业的深度融合，个性化定制、柔性化生产、共享经济等新的生产、管理、营销模式加速铺开。工业互联网应用范围迅速扩展，其安全性也应得到足够重视和保障。与会专家建议成立包括政府部门、安全厂商、工业企业、工业控制器厂商等在内的工业互联网安全联盟，通过数据协同、智能协同和产业系统建立网络安全生态体系，提升安全防护能力。第二十一届中国国际软件博览会由工信部和北京市人民政府共同主办。

4、中国台湾地区正式成立网络部队

E 安全 6 月 30 日消息 中国台湾地区领导人蔡英文 6 月 29 日前往新北市新店营区出席参谋本部资通电军指挥部（资通电：信息、通讯、电子，以下简称网络部队）成立典礼。蔡英文致词时表示，就任以来，不断在强化网络空间防护的力量，目前也已经在行政院成立网络管理处，推动台湾地区第一部网络安全管理法。至于未来网络部队的角色，蔡英文表示，今天网络部队的成立典礼只是第一步，将会以网络攻防为核心，网络信息安全为基础，电磁发展为前瞻。蔡英文还当场下达三项任务：首先，要求积极整合，不仅整合军方信息、通讯和电子各个相关单位，必须与军方以外的其他部门密切配合，执行“机密”保护，以及关键基础设施防护等工作。第二，蔡英文要求，加强网络安全人才的培育。最后，蔡英文指示，要发挥领头的前导角色。网络部队的成立，是台湾地区政府整体网安政策的先锋，也要成为推动台湾地区产学发展的引擎。

5、美国以色列强强联手,达成新的网络安全合作协议

E 安全 6 月 29 日消息 美国白宫国土安全顾问汤姆·博塞特表示，美国和以色列周一宣布，两国将建立新的网络安全合作关系，以阻止网络对手，并确定让恶意攻击者承担责任的方法。汤姆·博塞特在特拉维夫市举办的 2017 年网络周开幕式上宣布，美国与以色列将成立双边网络工作组。该工作组由白宫网络安全协调员罗伯·乔伊斯和以色列国家网络局局长埃维塔·马塔尼亚负责。工作组将于本周展开会谈，其成员将包括美国和以色列军方、刑事司法和外交关系建立代表组成。博塞特表示，本周的会谈将专注一系列网络问题，例如关键基础设施、先进的研发、国际合作与人才。乔伊斯先前曾负责带领 NSA 特定入侵行动办公室（TAO）。马塔尼亚过去数年一直在帮助制定以色列网络安全政策。据以色列媒体报道，新的合作协议将使以色列网络公司更容易向美国政府出售产品。

6、澳大利亚国防部成立网络作战部门

新华网 7 月 1 日消息 澳大利亚政府 6 月 30 日宣布，从 7 月 1 日起，澳国防部内将成立一个具备攻击性能的网络作战部门，以确保国家网络安全。澳大利亚总理网络安全助理部长丹·特汉当天在宣布这一决定时说，新部门将负责澳军方信息作战行动、军方情报、电子战、情报行动，以及军方的太空行动，并有权开展自卫、被动防卫、主动防卫和主动进攻行动。特汉表示，新部门将与澳军方现有相关行动部门相融合。就新部门所具备的主动网络攻击职能，澳总理特恩布尔对当地媒体表示，澳大利亚对网络袭击的应对不应仅限于防卫领域，主动进攻是政府打击网络犯罪的武器，也是澳政府防范海外网络犯罪全面战略的一部分。2016 年，澳大利亚曾推出耗资 1.8 亿美元的网络安全战略，以应对和打击网络攻击与诈骗等网络犯罪活动。在当年国防白皮书中，澳政府还承诺，将斥资 3 亿美元提高国防部队的网络战能力。

7、多国遭大规模网络攻击 恐造成全球重大经济损失

环球网 6 月 28 日消息 6 月 27 日，黑客利用名为“Petya”的计算机病毒对欧洲多国突然发起网络攻击，乌克兰、英国、西班牙、荷兰、丹麦等国“中招”。英国《每日电讯报》称，乌克兰受伤严重，基辅的机场以及地铁、乌中央银行和部分企业遭黑客攻击导致瘫痪。乌克兰总统事务局新闻发言人表示，乌政府对这一事件“高度重视”。英国著名广告公司 WPP 表示，黑客使公司计算机系统崩溃。丹麦航运巨头马士基发表声明，称由于受到黑客攻击，全球多个站点和业务部门已经关闭。俄罗斯国家石油公司也表示，公司服务器遭受了“强大”攻击。《纽约时报》称，目前尚不清楚这一波网络攻击来自何方，背后由谁操控。网络专家称，“Petya”与之前

肆虐多国的“想哭”病毒一样，黑客通过控制电脑，勒索赎金。此轮网络攻击，恐造成全球重大经济损失。

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：陈阳

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话： 010-82990158