国家互联网应急中心

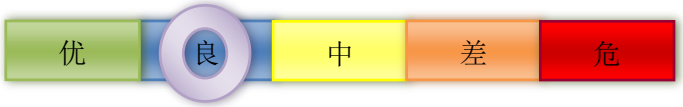
网络安全信息与动态周报

2017 年第 26 期

6 月 19 日-6 月 25 日

CNCERT/CC

本周网络安全基本态势

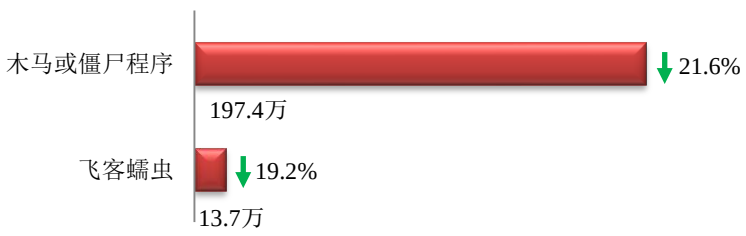


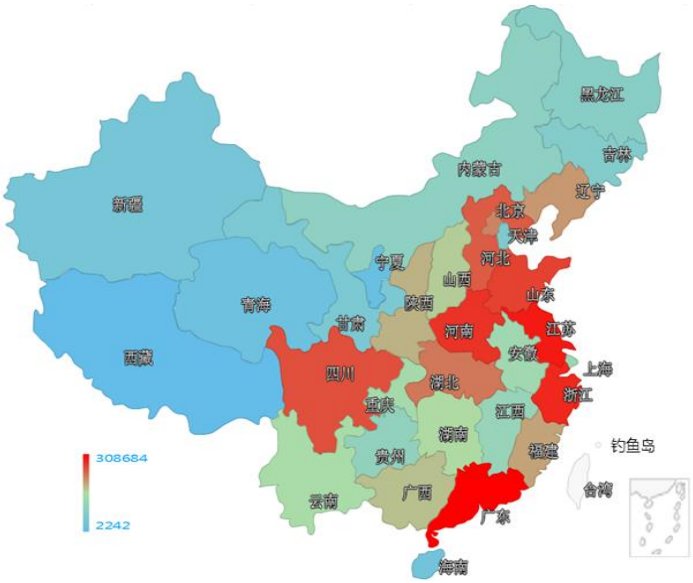
境内感染网络病毒的主机数量	•211.1万	21.4%
境内被篡改网站总数 其中政府网站数量	•1475 •32	27.6% 50.8%
境内被植入后门网站总数 其中政府网站数量	•1364 •47	1.3% 32.9%
针对境内网站的仿冒页面数量	•441	8.3%
新增信息安全漏洞数量 其中高危漏洞数量	•326 •128	10.1% 23.1%

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 211.1 万个，其中包括境内被木马或被僵尸程序控制的主机约 197.4 万以及境内感染飞客（conficker）蠕虫的主机约 13.7 万。





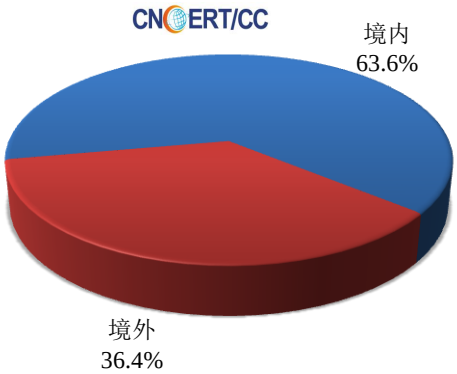
木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、江苏省和浙江省。

TOP3

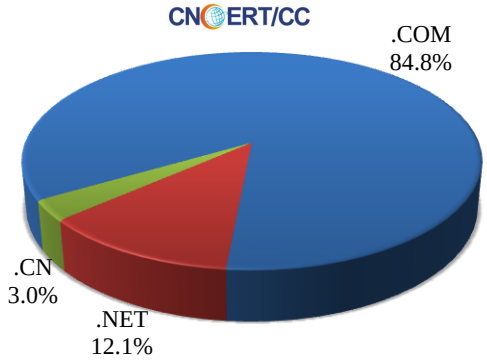
广东省	•约30.9万个（约占中国大陆总感染量的15.5%）
江苏省	•约13.8万个（约占中国大陆总感染量的6.9%）
浙江省	•约13.2万个（约占中国大陆总感染量的6.6%）

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 33 个，涉及 IP 地址 72 个。在 33 个域名中，有 36.4%为境外注册，且顶级域为.com 的约占 84.8%；在 72 个 IP 中，有约 4.2%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
(6/19-6/25)



本周放马站点域名所属顶级域的分布
(6/19-6/25)



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。

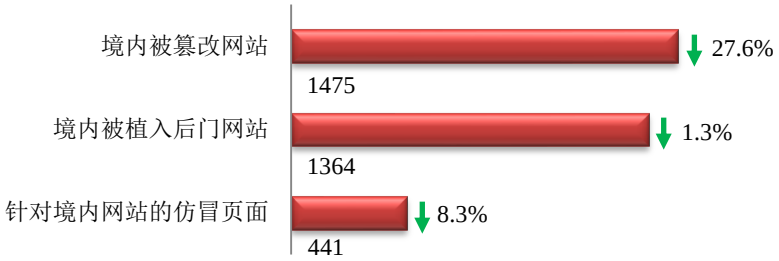
ANVA恶意地址黑名单发布地址

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。

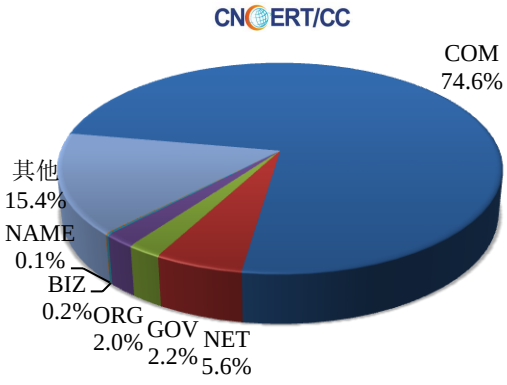
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1475 个；境内被植入后门的网站数量为 1364 个；针对境内网站的仿冒页面数量为 441。

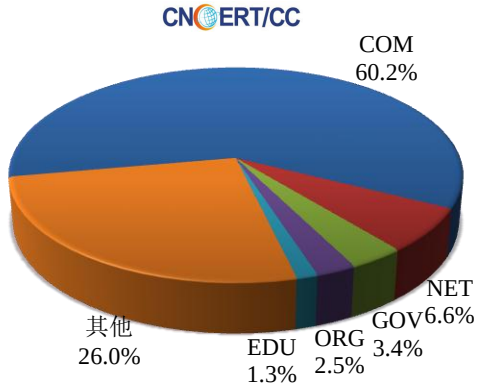


本周境内被篡改政府网站（GOV 类）数量为 32 个（约占境内 2.2%），较上周环比下降了 50.8%；境内被植入后门的政府网站（GOV 类）数量为 47 个（约占境内 3.4%），较上周环比下降了 32.9%；针对境内网站的仿冒页面涉及域名 380 个，IP 地址 182 个，平均每个 IP 地址承载了约 2 个仿冒页面。

本周我国境内被篡改网站按类型分布
(6/19-6/25)

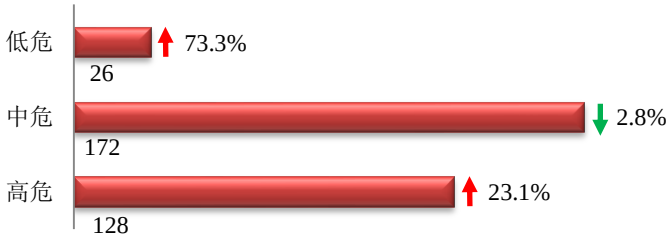


本周我国境内被植入后门网站按类型分布
(6/19-6/25)

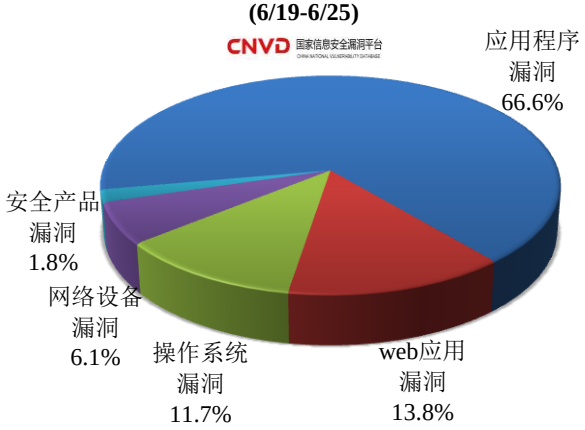


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 326 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
(6/19-6/25)



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

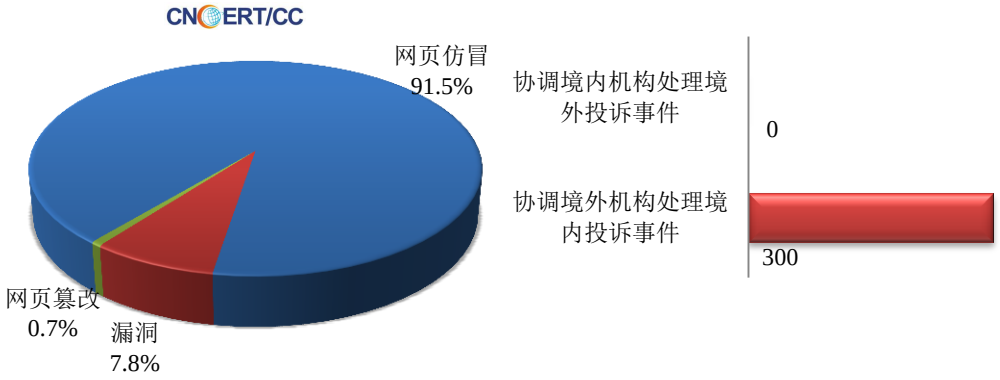
http://www.cnvd.org.cn/webinfo/list?type=4

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

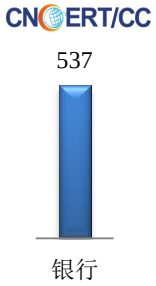
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 587 起，其中跨境网络安全事件 300 起。

本周CNCERT处理的事件数量按类型分布
(6/19-6/25)

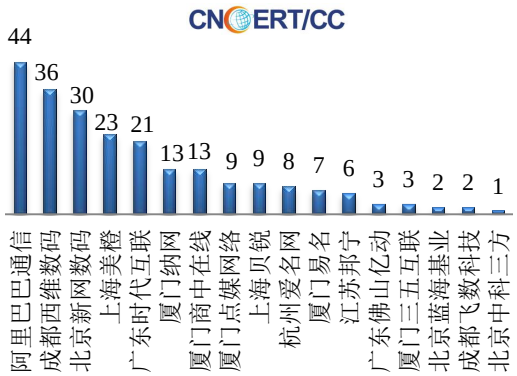


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 537 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 537 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(6/19-6/25)

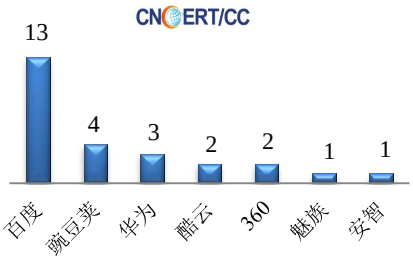


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (6/19-6/25)



本周，CNCERT 协调 7 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 26 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
(6/19-6/25)



业界新闻速递

1、欧盟 28 国联合对抗国家支持型黑客行动

E 安全 6 月 22 日消息 据报道，欧盟 28 国集团就如何惩治黑客达成协议，今后将共同惩治黑客。周一，欧盟理事会宣布推出“网络外交工具箱”（Cyber Diplomacy Toolbox）联合框架，以指导盟国统一应对恶意网络活动，该框架还包括采取措施联合实施经济制裁、禁止入境旅游、冻结资产，并对责任方发出全面禁令。欧盟官员表示，欧盟成员国将根据具体情形决定应采取的应对措施，以此推进态势感知共享、信息共享和高效的决策制定。欧盟成员国应根据“网络外交工具箱”，制定追踪网络攻击归因的程序。欧盟成员国本着自愿原则使用该框架，任何集体响应将需要欧盟成员国支持。简言之，该框架表明，欧盟伙伴国同心协力将未来响应网络攻击的计划程序标准化，今后还可用来孤立某组织、国家或犯罪分子。

2、欧洲议会提出修正案草案 建议禁止使用加密后门

cnBeta.COM6 月 20 日消息 据外媒报道，在发生一系列恐怖袭击之后，来自世界各国的政府都已经开始呼吁寻找一种能让调查人员访问民众通信数据的途径。这已经成为了热议话题，尽管有一些人热衷于通过在软件和设备上使用后门来减弱加密在调查过程带来的麻烦，但欧洲议会的公民自由、司法与家庭事务委员会却认为应当禁止这种行为。该委员会提出的修正案方案跟保护欧盟国家每位民众的基本权利、使其享有对其私人与家庭生活、家庭以及通信获得尊重的《欧盟基本权利宪章》第 7 条内容相关。委员会认为，这种保密原则应当适用于当下以及未来所有的通讯方式。修正案提案指出，加密、逆向工程或监控通讯的这些行为都应当禁止，通信服务运营商不应被要求提供后门。另外，提案还称，政府不仅要保护现使用的通讯内容而且还要保护诸如拨通的电话号码、访问的网站地址、地址位置、时间、日前、通话时间等元数据，因为它们也会揭露跟用户私人生活相关的信息。目前，这项修正案需要先在议会获得批准才能进入欧盟理事会进行下一步的动作。

3、日本自民党促政府拥有网络攻击能力 增加防卫费

中新网 6 月 21 日消息 据日媒报道，日本自民党安全保障调查会本月 20 日在党总部召开与国防小组的联席会议，汇总了就防卫力建设向日本政府提出建议的中期报告。调查会要求让自卫队拥有独立的网络攻击能力，还要求导入探知弹道导弹发射的预警卫星（SEW）。据报道，日本政府计划在 2018 年制定继现行《中期防卫力整备计划》（中期防）之后的下一期“中期防”，调查会将在明年春天前汇总最后建议。此次中期报告指出，对于日本政府在网络空间对来自他国的网络攻击实施反击的情况，应该从法律的角度加以梳理，确认这是否相当于行使自卫权。报告还敦促日本政府为强化在太空的信息收集能力，推进费用方面和技术上的探讨。有关防卫费，报告参考北大西洋公约组织（NATO）成员国提出了国防费在国内生产总值（GDP）中占比超过 2%的目标，指出“需要确保足够规模”，强调了增加金额的必要性。

4、共和党合作数据公司意外泄漏近 2 亿美国选民的个人资料

cnBeta.COM6 月 20 日消息 在共和党国家委员会签约的一家营销公司本月泄漏了超过 1.98 亿美国公民的政治数据。数据泄露包含大约 61%的美国人大量个人信息。除了家庭地址，出生日期和电话号码之外，这些记

录还包括政治团体采用的先进情绪分析来预测个人选民如何处理热门问题，如枪支所有权，干细胞研究和堕胎权，以及宗教信仰和种族。Deep Root Analytics 是一个共和党的数据公司供应商，用于确定政治广告的受众群体。UpGuard 网络风险分析师 Chris Vickery 上周在线发现了这些数据。超过 1TB 的存储在云服务器上，无需保护密码，任何人可以访问，这引起了重大的隐私问题，这对有恶意目的的人来说是有价值的。

5、英国会网络系统遭攻击 暂停电子邮件登录及联络

中新网 6 月 25 日消息 据外媒报道，英国国会发生网络系统遭攻击事件，英国当局已经展开调查。英国国会 24 日以书面声明的方式证实，当地时间 24 日发现有“未获授权的意图要进入国会议员的使用者帐户”，国会除了持续在调查事件，也会进一步采取措施来确保电脑系统的安全。事发后英国国会全面暂停所有议员和职员登入国会的网络以及电子邮件系统，以保护整个系统的安全。自由民主党议员克里斯•瑞纳德在推特上表示，如果有重要联络事项，应透过手机简讯联系，因为国会议员的电子邮件无法远端操作。英国国会成为网络攻击的目标，引发各界高度瞩目。目前尚不清楚这起网络攻击事件有多少人受到影响以及损害程度如何，包括英国国家网络安全中心以及国家犯罪机构已就事件展开调查。英国国家网络安全中心表示，在获知有关情况后，将重新制定政府部门针对网络安全的指引。

6、韩多家银行遭黑客组织勒索 金融监督院进入紧急状态

中新网 6 月 23 日消息 据英国《金融时报》报道，韩国有关部门已进入“紧急状态”，忙于防范黑客组织威胁要对该国最大几家银行发起的网络攻击。被称为“无敌舰队组织”（Armada Collective）的黑客组织 21 日表示，韩国 7 家主要银行如果未能用虚拟货币比特币（Bitcoin）支付赎金，将对其发起分布式拒绝服务（DDoS）攻击。“在 7 家银行收到无敌舰队组织发出的威胁电子邮件后，金融监督院进入了紧急状态，”韩国金融监督院 IT 团队负责人 22 日表示。“我们正在准备各种方法来防止 DDoS 攻击，包括屏蔽不必要的 IP 地址、分散流量以及设置一个清洁区。”黑客通过电子邮件向 7 家银行发出威胁，包括韩国的五大银行：韩国国民银行、新韩银行、友利银行、KEB 韩亚银行以及韩国农协银行，要求它们最迟在周一支付约 30 万美元。“由于我们不知道他们何时会发起 DDoS 攻击，我们将会保持紧急状态一段时间，”金融监督院负责人表示。

7、黑客组织“匿名者”再次发起针对金融机构的攻击

HackerNews6 月 21 日消息 近日，黑客组织“匿名者（Anonymous）”向全球超过 140 个金融机构发起了新一轮的攻击行动，代号为#Opicarus2017。“匿名者”曾于 2015、2016 年发起过持续 4 波针对银行的大规模 DDoS 攻击，在其攻击下汇丰银行、土耳其银行、希腊央行、塞浦路斯央行、墨西哥银行 、墨西哥北方银行、孟加拉国银行等多家银行纷纷中招，就连美国联邦储备银行、世界银行、国际货币基金组织、纽约证券交易所以及英格兰银行等大牌金融机构也受到严重影响。此次“匿名者”发起代号为#Opicarus2017 的攻击行动，包括中国人民银行（pbc.gov.cn）、香港金融管理局（hkma.gov.hk）在内的全球近 140 家金融机构均在其公布的攻击列表中。此次攻击，在保持了 DDoS 让金融机构服务不可用的同时，攻击者还将针对性的寻找金融机构的数据库注入攻击点，以达到窃取敏感数据的目的。目前全球超过 9 家金融机构已经被黑客进行数据库注入攻击，印度卡纳塔克邦格莱明银行和亚洲开发银行的数据敏感信息被黑客窃取，此外部分金融机构受到 DDoS 攻击而导致网站服务不可用。本轮攻击还在持续进行中。

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：李挺

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话： 010-82990158