国家互联网应急中心

2015 年第 34 期

8 月 17 日-8 月 23 日

网络安全信息与动态周报

本周网络安全基本态势

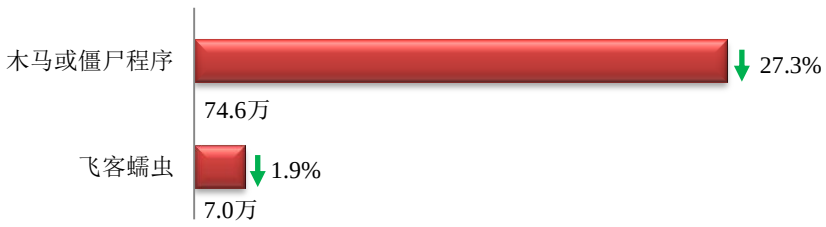
优 | 良 | 中 | 差 | 危

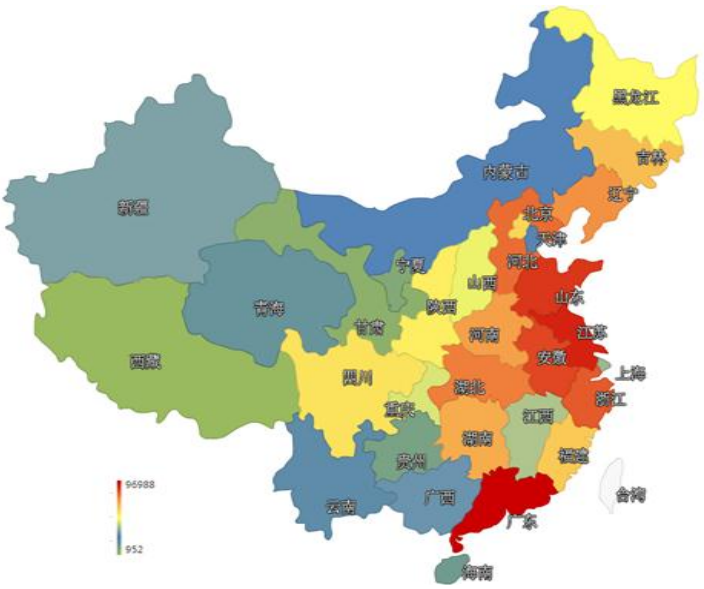
境内感染网络病毒的主机数量	•81.6万	↓ 25.6%
境内被篡改网站总数 其中政府网站数量	•2062 •43	↓ 62.0% ↓ 62.6%
境内被植入后门网站总数 其中政府网站数量	•3197 •169	↑ 18.3% ↑ 26.1%
针对境内网站的仿冒页面数量	•5877	↓ 7.6%
新增信息安全漏洞数量 其中高危漏洞数量	•183 •85	↑ 40.8% ↑ 41.7%

═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 81.6 万个，其中包括境内被木马或被僵尸程序控制的主机约 74.6 万以及境内感染飞客（conficker）蠕虫的主机约 7.0 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、江苏省和山东省。

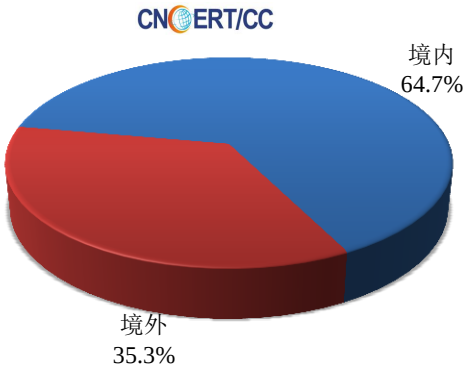
TOP3

广东省	•约9.7万个（约占中国大陆总感染量的13.0%）
江苏省	•约8.2万个（约占中国大陆总感染量的10.9%）
山东省	•约5.9万个（约占中国大陆总感染量的7.9%）

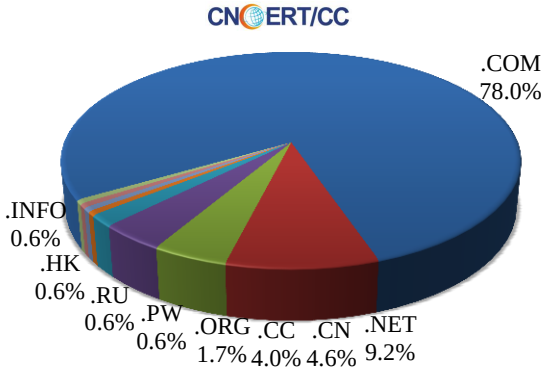
本周 CNCERT 捕获了大量新增网络病毒文件，按网络病毒名称统计新增 23 个，按网络病毒家族统计无新增。

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 173 个，涉及 IP 地址 269 个。在 173 个域名中，有约 35.3%为境外注册，且顶级域为.com 的约占 78.0%；在 269 个 IP 中，有约 23.0%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 48 个 IP。

本周放马站点域名注册所属境内外分布
(8/17-8/23)



本周放马站点域名所属顶级域的分布
(8/17-8/23)



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。

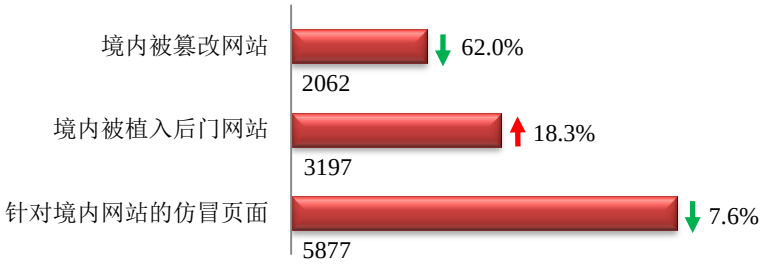
ANVA恶意地址黑名单发布地址

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。

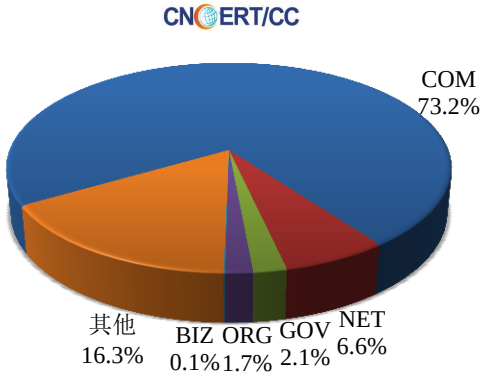
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 2062 个；境内被植入后门的网站数量为 3197 个；针对境内网站的仿冒页面数量为 5877。

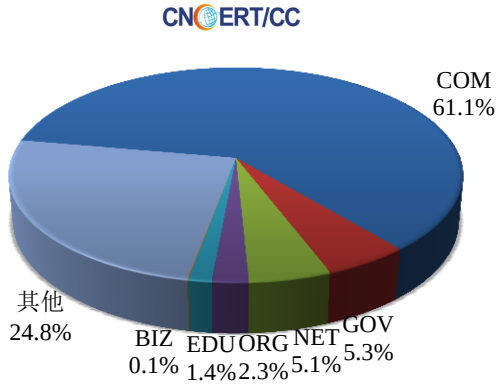


本周境内被篡改政府网站(GOV 类)数量为 43 个（约占境内 2.1%），较上周环比下降了 62.6%；境内被植入后门的政府网站(GOV 类)数量为 169 个（约占境内 5.3%），较上周环比上升了 26.1%；针对境内网站的仿冒页面涉及域名 5124 个，IP 地址 864 个，平均每个 IP 地址承载了约 7 个仿冒页面。

本周我国境内被篡改网站按类型分布
(8/17-8/23)



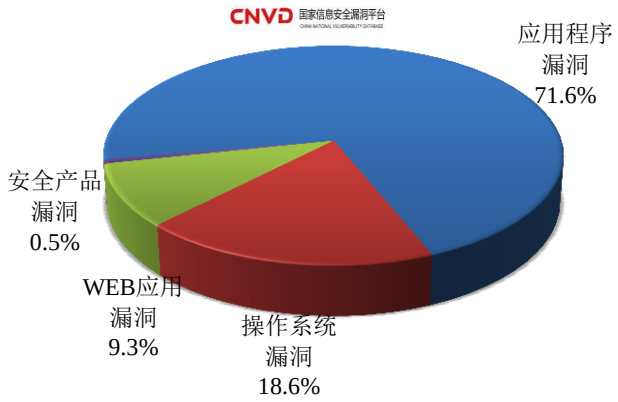
本周我国境内被植入后门网站按类型分布
(8/17-8/23)



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 183 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
(8/17-8/23)



本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是操作系统漏洞和 WEB 应用漏洞。

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

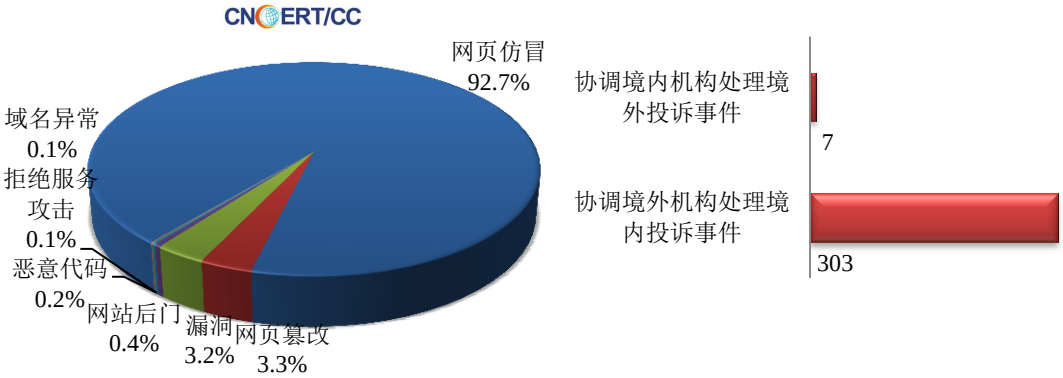
http://www.cnvd.org.cn/webinfo/list?type=4

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

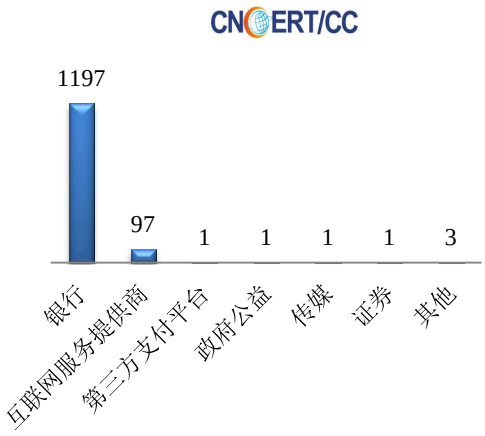
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 1403 起，其中跨境网络安全事件 310 起。

本周CNCERT处理的事件数量按类型分布
(8/17-8/23)

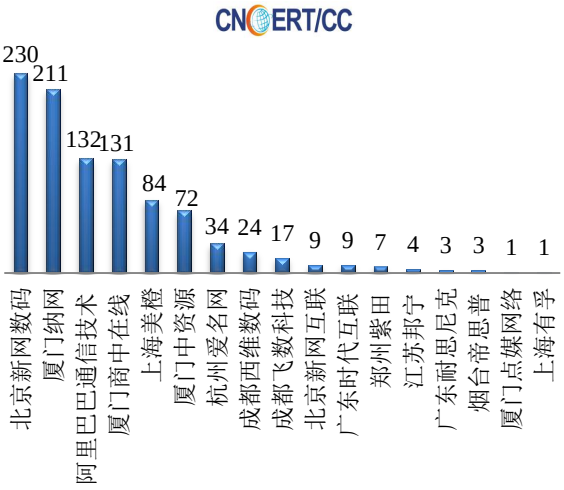


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 1301 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 1197 起和互联网服务提供商仿冒事件 97 起。

本周CNCERT处理网页仿冒事件数量
按仿冒对象涉及行业统计(8/17-8/23)

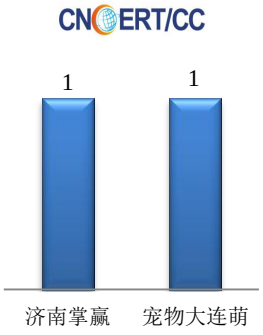


本周CNCERT协调境内域名注册机构处理
网页仿冒事件数量排名 (8/17-8/23)



本周，CNCERT 协调 2 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 2 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 (8/17-8/23)



业界新闻速递

1、斯诺登再爆料：包括监听联合国总部 AT&T 助美国安局监控国内外网络

新华网 8 月 17 日消息 新加坡联合早报网 17 日报道称，新近披露的文件显示，美国历史最悠久和最大电信公司之一的美国电话电报公司长期与美国国家安全局合作，监控大批经过美国国内网络的通信数据，包括为国安局提供技术支援，暗中执行一项庭令，窃听进出联合国总部的所有互联网通信。《纽约时报》和纽约非营利组织 ProPublica 联合检视了美国中央情报局前雇员斯诺登披露的最新文件后，星期天封面报道了美国电话电报公司与国安局之间这项长达几十年的合作。该报也在网站公开总共 74 页、志日从 2003 年至 2013 年的文件。目前不清楚美国电话电报公司与国安局之间是否还存在这样的合作。报道说，尽管美国电信公司与国安局合作监控通信人尽皆知，但新披露的文件首次揭露了美国电话电报公司与国安局非常密切、独特及高生产力的合作关系。

文件揭露，美国电话电报公司给予国安局技术援助，执行一项允许监控联合国总部所有互联网通信的秘密庭令。美国电话电报公司是联合国总部的电信服务供应商。国安局监控联合国总部通信此前已经公诸于世，但美国法庭曾发出秘密庭令及美国电话电报公司的参与，则是首次曝光。美国电话电报公司在全国至少 17 个互联网枢纽安装了监控设备，数量远多于其竞争对手、也与国安局合作的电信公司威瑞森通信。此外，美国电话电报公司是第一家采用国安局研发的新监控技术的电信公司。

2、外媒称英国斥巨资提升网战能力：研更多恶意软件

参考消息网 8 月 17 日消息 英国《星期日泰晤士报》网站 8 月 16 日发表题为《英国将启动耗资 20 亿英镑的网络空间攻势》的报道称，今后 5 年，将有 20 亿英镑投入英国的攻击性网络项目中，以抵制来自外国的黑客威胁。联合部队司令部（JFC）一直呼吁招募大约 300 名网络专家，并研发更多恶意软件。英军方消息人士说，JFC 为英国这一高度机密项目建议的预算为每年 4 亿英镑，这是目前水平的 10 倍。虽然政府的审议结果要到今年晚些时候才会公布，国防部一名消息人士说，文职官员和军方领导人都渴望扩大英国的网络战能力，并对在这个领域加大投入抱支持态度。加大投入资金能帮助军方研发一些网络攻击系统，来破坏敌人的通信，或闯入对手警察、政府部门或银行等机构的网络。英国军方将会有能力监控电子邮件、窃听电话和拦截其他通信。网络战专家、JFC 前成员彼得 罗伯茨说，向相关领域大幅增加投入的种种迹象显示，英国“希望在攻击性网络空间中成为头号角色”。

3、日本制定新网络安全战略 政府系统将脱离互联网

中新网 8 月 20 日消息 据日媒报道，本月 20 日，日本政府在首相官邸召开了由阁僚和专家组成的“网络安全战略总部”(部长为该国内阁官房长官菅义伟)会议。据悉，与会者就日本年金机构信息泄露的原因及防止再次发生的措施进行商讨，并敲定今后网络攻击对策指针“网络安全战略”修改方案。菅义伟在会上强调：“要吸取泄露事件的教训，为 2020 年东京奥运会和残奥会的举办汇总应对战略”。日媒称，为减少黑客入侵的途径，修改方案中提出将日本政府机关处理重要信息的信息系统与网络分离开来。据了解，日本政府原定于 6 月的内阁会议通过新战略，考虑到日本年金机构信息泄露事件，对内容进行了重新探讨。新战略还写明将积极参与制定自由安全网络空间所需的国际准则。

4、儿童智能手表曝高危漏洞 可被黑客监控

环球网 8 月 19 日消息 近日，有白帽黑客在国内安全平台乌云上曝光了儿童安全手表的相关漏洞。攻击者可利用漏洞查询智能手表连接的服务器，查看客户信息，并根据相应 ID 直接查看孩子的地理位置、实时监控孩子的地理坐标、日常活动轨迹及环境录音等隐私内容。另据报道，漏洞源自一个儿童智能手表的设计方案。目前在淘宝销售前 32 位的儿童智能手表产品中有 13 款均存在该漏洞，品牌涉及久方、普耐尔、智多星、安得乐、Wonsee、锋立、亦青藤等。根据这些品牌的儿童智能手表出货量估算，影响儿童或在百万左右。目前类似小米手环、360 儿童卫士智能手表、AppleWatch 等厂商出品的智能穿戴设备，并都不存在问题。

5、Web.com 被黑致 93000 信用卡信息被盗

360 安全播报 8 月 20 日消息 Web.com 是美国的一个著名互联网服务提供商，日前，有一名身份未知的黑客入侵了这家公司的网站，网站入侵导致该公司的一个计算机系统发生了数据泄漏。泄漏的数据中包括大约

93000 名 Web.com 用户的信用卡数据，这些数据有用户姓名，地址，以及其他个人数据。但泄漏的数据并不包括社保号以及信用卡验证码，此次泄漏出来的数据只有在 Web.com 支付服务中使用到的那些信用卡信息。根据公司在周二所发布的 FAQ 文件，研究人员在 2015 年 8 月 13 日检测到了此次攻击。但是，公司并没有透露这名未知身份的攻击者入侵系统的时间长短。但是公司表示，安全人员快速地检测到了此次未经授权的入侵行为。公司的发言人表示：“公司在对其系统进行安全检测的过程中发现了这个未经授权的行为，并迅速地切断了这个访问进程，而且立即与一家国际著名的 IT 安全公司一同合作，共同对此事件进行深入的调查。我们已经将此次攻击事件的具体信息报告给了信用卡服务商，相关的联邦政府，以及有关当局。”除此之外，公司还表示：“公司已经采取了非常复杂且功能完善的安全措施了，目的就是为了保护公司的计算机系统。而且公司还会定期对计算机系统的安全协议进行检查和更新。”

6、Gozi 木马不断拓展攻击范围 东欧国家拉响警报

FreeBuf8 月 19 日消息 本月早些时候，IBM 安全研究员发现并分析了一个新的 Gozi 木马配置文件，发现该木马专门针对的是保加利亚的银行。之前版本的 Gozi 木马针对的主要是美国、英国、澳大利亚、沙特阿拉伯、波斯湾等地的银行，这是第一次出现在保加利亚地区。保加利亚的银行存在的一个最普遍的问题是可被用于跨国取钱或者洗黑钱。当 Carbanak heist 问题覆盖全球时，保加利亚的银行也遭遇了网络攻击，并损失惨重。保加利亚打击网络犯罪组织的首席理事 VasilPetkov 指出：Gozi 木马，也被称为 ISFB 或者 Ursnif，是目前发现的时间最为长久的银行木马。首次发现于 2007 年，由一个已经解散的恶意程序组织运营，主要对说英语的国家发动网上银行欺诈。2010 年 9 月，Gozi 团队在进行版本更新时（也就是 Gozi v2），其中一位开发者不小心将源码（ISFB）泄露了出去。2010 年底 Gozi v2 变种开始出现，它使用了新的 web 注入机制，主要针对的是欧洲和美国的银行。在过去的 5 年内，Gozi v2 的开发者不断的提升其技术和方法，扩大其攻击范围。有证据表明 Gozi 一直活跃至今，并且还在不停更新技术和方法，以绕过在线服务的安全防护。IBM 通过对 Gozi 的分析发现，2015 年初的时候，它的攻击目标依然集中在美国和英国，而在 3 月到 5 月间扩展到了一些其他的领域。Gozi 的攻击习惯是，先在一个地区找出一个攻击目标，持续数月，然后再在该区域扩展攻击目标。

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 2014 年，CNCERT 与 63 个国家和地区的 144 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：温森浩

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82991373