国家互联网应急中心

2016 年第 35 期

8 月 22 日-8 月 28 日

网络安全信息与动态周报

本周网络安全基本态势

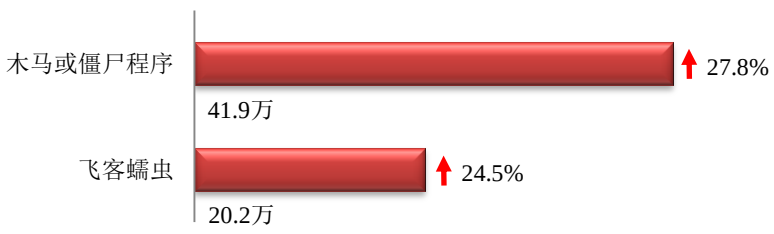
优 | 良 | 中 | 差 | 危

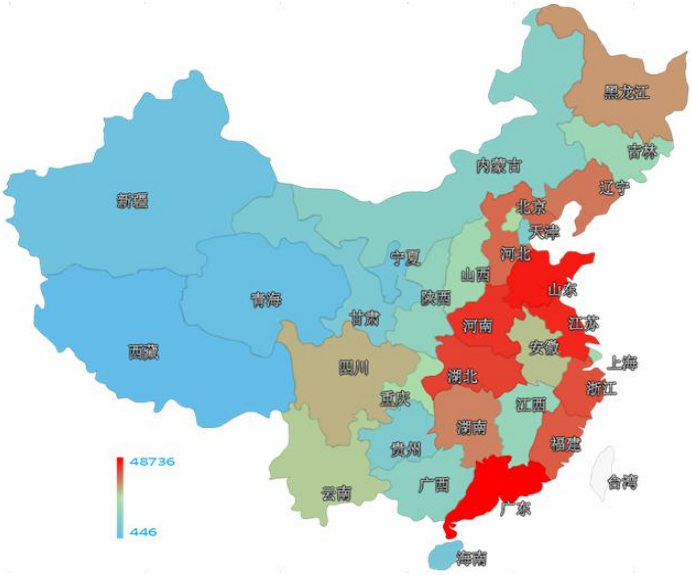
境内感染网络病毒的主机数量	•62.1万	26.7%
境内被篡改网站总数 其中政府网站数量	•3217 •68	21.0% 24.4%
境内被植入后门网站总数 其中政府网站数量	•2596 •112	11.4% 24.4%
针对境内网站的仿冒页面数量	•5082	45.8%
新增信息安全漏洞数量 其中高危漏洞数量	•343 •203	81.5% 150.6%

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 62.1 万个，其中包括境内被木马或被僵尸程序控制的主机约 41.9 万以及境内感染飞客（conficker）蠕虫的主机约 20.2 万。





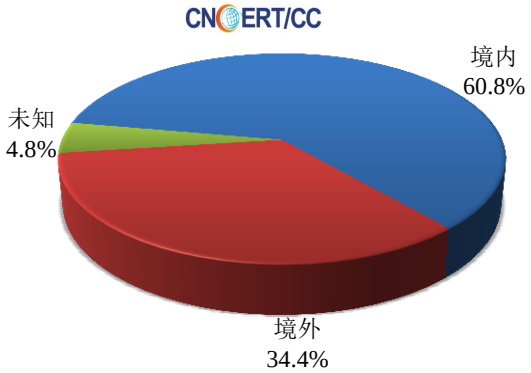
木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、山东省和江苏省。

TOP3

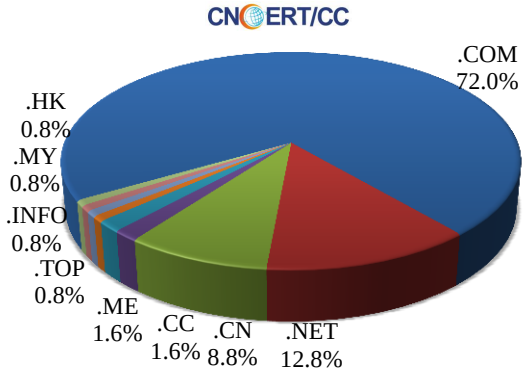
广东省	•约4.9万个（约占中国大陆总感染量的11.6%）
山东省	•约4.7万个（约占中国大陆总感染量的11.3%）
江苏省	•约4.4万个（约占中国大陆总感染量的10.5%）

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 125 个，涉及 IP 地址 312 个。在 125 个域名中，有 34.4%为境外注册，且顶级域为.com 的约占 72.0%；在 312 个 IP 中，有约 6.1%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
(8/22-8/28)



本周放马站点域名所属顶级域的分布
(8/22-8/28)



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。

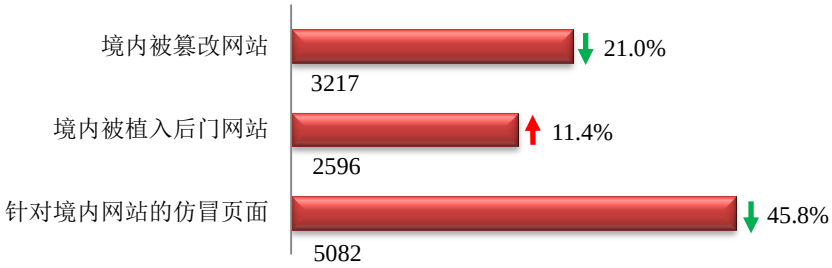
ANVA恶意地址黑名单发布地址

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。

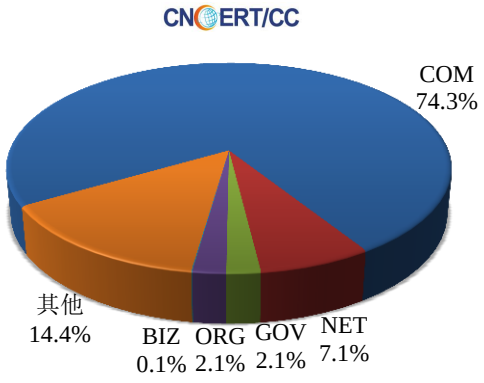
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 3217 个；境内被植入后门的网站数量为 2596 个；针对境内网站的仿冒页面数量为 5082。

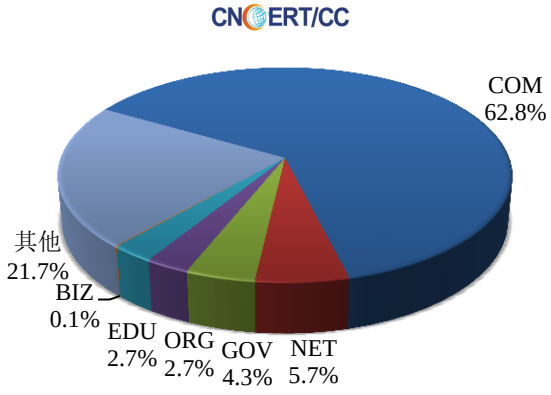


本周境内被篡改政府网站（GOV 类）数量为 68 个（约占境内 2.1%），较上周环比下降了 24.4%；境内被植入后门的政府网站（GOV 类）数量为 112 个（约占境内 4.3%），较上周环比上升了 24.4%；针对境内网站的仿冒页面涉及域名 1419 个，IP 地址 519 个，平均每个 IP 地址承载了约 10 个仿冒页面。

本周我国境内被篡改网站按类型分布
(8/22-8/28)

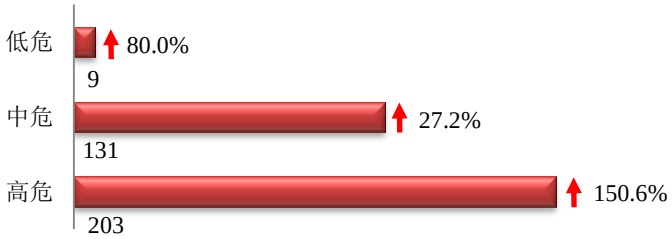


本周我国境内被植入后门网站按类型分布
(8/22-8/28)

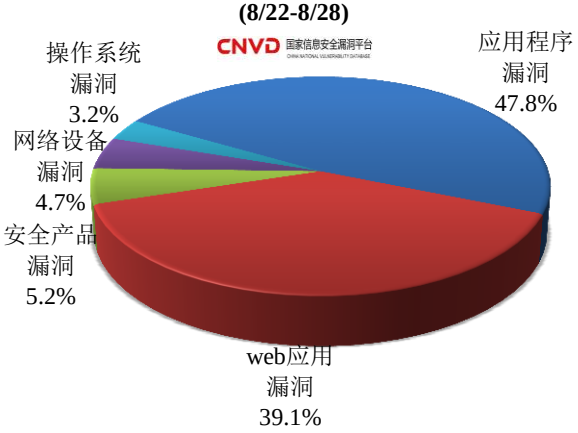


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 343 个，信息安全漏洞威胁整体评价级别为高。



本周CNVD收录漏洞按影响对象类型分布
(8/22-8/28)



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 应用漏洞和安全产品漏洞。

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

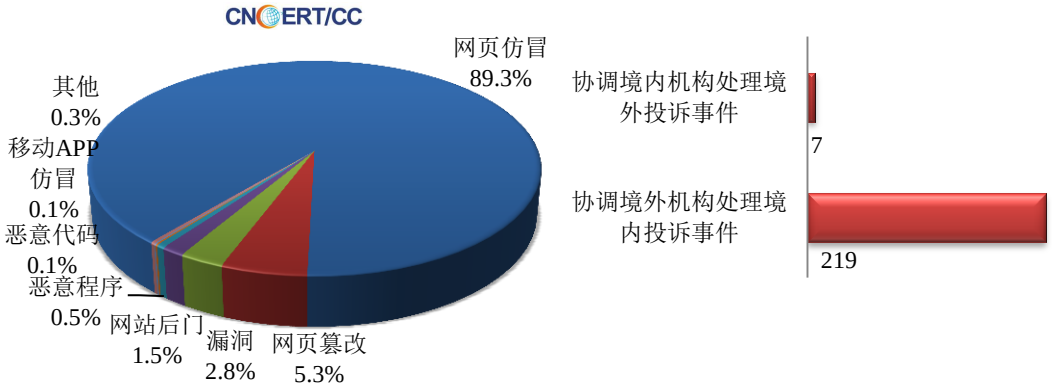
http://www.cnvd.org.cn/webinfo/list?type=4

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 749 起，其中跨境网络安全事件 226 起。

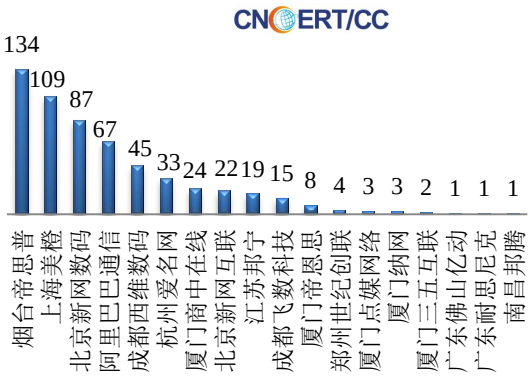
本周CNCERT处理的事件数量按类型分布
(8/22-8/28)



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 669 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 637 起和互联网服务提供商仿冒事件 22 起。

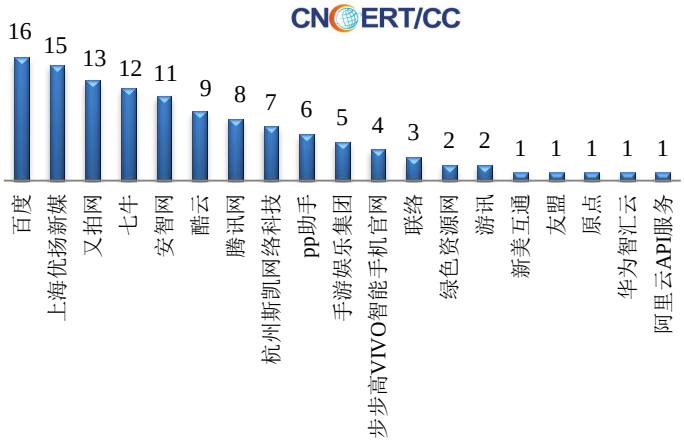
本周CNCERT处理网页仿冒事件数量
按仿冒对象涉及行业统计(8/22-8/28)

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 (8/22-8/28)



本周，CNCERT 协调 19 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 118 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 (8/22-8/28)



业界新闻速递

1、中央网信办等三部门联合发文 加强国家网络安全标准化工作

新华网 8 月 24 日消息 经中央网络安全和信息化领导小组同意，中央网信办、国家质检总局、国家标准委近日联合印发《关于加强国家网络安全标准化工作的若干意见》，要建立统筹协调、分工协作的工作机制，加强标准体系建设，提升标准质量和基础能力，强化标准宣传实施，加强国际标准化工作，抓好标准化人才队伍建设，做好资金保障。《意见》明确，全国信息安全标准化技术委员会在国家标准委的领导下，在中央网信办的统筹协调和有关网络安全主管部门的支持下，对网络安全国家标准进行统一技术归口，统一组织申报、送审和报批；探索建立网络安全行业标准联络员机制和会商机制；建立重大工程、重大科技项目标准信息共享机制；建立军民网络安全标准协调机制和联络员机制。《意见》要求，推动网络安全标准与国家相关法律法规的配套衔接，促进网络安全标准与信息化应用标准同步规划、同步制定；整合精简强制性标准，在国家关键信息基础设施保护、涉密网络等领域制定强制性国家标准，优化完善推荐性标准，视情在行业特殊需求的领域制定推荐性行业标准，原则上不制定网络安全地方标准。

2、联合国将制定自动驾驶车辆安全标准防其遭网络攻击

环球网 8 月 24 日消息 据台湾“中广网”8 月 23 日报道，随着发展自动驾驶车成为全球趋势，联合国相关人士表示，为防止汽车自动驾驶系统所使用的通信网路受黑客攻击，负责制定汽车国际法规的联合国机构将在今年 11 月通过汽车自动驾驶安全标准。报道称，此标准由在自动驾驶技术研发中处于领先地位的日本和德国主导，主要包括阻止黑客攻击及探测到攻击时警告司机并防止失控等措施。未来将会要求各汽车厂商依新标准采取具体措施。在日内瓦的联合国世界车辆法规协调论坛正在就汽车自动驾驶安全标准展开讨论。他们先前已着手起草高速公路安全行车技术标准，今后也将展开涉及网络安全的标准制定。据悉，自动驾驶系统借助的是人工智能（AI），使得在无需人类控制方向盘和煞车的情况下车辆就能自动行驶。如果汽车遭到网络攻击，就可能使汽车面临被劫持甚至失控的危险。

3、日本拟新设培训机构 强化基础设施防御黑客攻击

中新网 8 月 22 日消息 据日媒报道，为迎接 2020 年东京奥运会和残奥会，日本政府将于 2017 年度新设培养专家的训练机构，以加强发电站等重要基础设施防御黑客攻击的能力。日媒指出，日本政府此举旨在防范以奥运会为目标的大规模停电，以及有关发电站设计的高度机密情报外泄。日本政府计划在 2016 年度第二次补充预算案中写入确保讲师和制订教学计划的经费。据悉，该训练机构暂定名为“产业系网络安全推进中心”。该机构将设在东京，预计每年将有 100 名左右来自电力公司等的员工参加训练。除了招募原黑客等担任讲师外，还将建造发电站和煤气厂的模拟系统，分为攻击方和防守方实施为期最长 1 年的实战训练以提高应对能力。日本政府还计划日后与美国等“网络先进国家”的技术人士实施联合演习。计划由专门研究网络对策的日本独立行政法人“情报处理推进机构”（IPA）负责该中心的运营。电力公司系统中有一套以管理发电站等各种设备为目的的部门“监控管理系统”，独立于与外部网络相连接的总部办公室。日本政府计划新设立的训练机构是为了应

对针对监控管理系统的黑客攻击。据政府介绍称，这是日本首次正式设立人才培养机构以防护监控管理系统免受黑客攻击。

4、泰国 ATM 机被入侵导致 1200 万泰铢被盗

FreeBuf 8 月 26 日消息 在本周三，泰国警方表示他们发现泰国大约一千台 ATM 机被入侵，并且 1200 万泰铢已经被盗。经过调查发现，这个黑客组织属于东欧的一个黑手党组织。目前该组织已经成功入侵了泰国 ATM 机的骨干网络，在曼谷有大约 21 台 ATM 机收到影响。目前，泰国中央银行已经向各个支行发出警告。泰国政府储蓄银行（GSB）目前已经关闭了大约 3000 台 ATM 机，并且积极配合警方的调查。据说，政府已经锁定了一部分黑客，正在确定他们是否有这个能力入侵 ATM 骨干网络，以便进一步调查。于此同时，泰国警方表示，参与犯罪的人员最少有 25 名东欧人。这个案件和前不久台湾 ATM 机被黑事件很相似。犯罪人员都是欧洲面孔，同时也是通过恶意软件感染 ATM 机器。所以不可否认，这些犯罪人员或许来源于同一个组织。泰国警方目前已经逮捕了三名犯罪嫌疑人，据他们所交代，他们组织大约有三十名东欧人，其中大部分都从事于 ATM 工作领域很多年，同时表示组织内部还有三名俄罗斯人。他们感染 ATM 机主要是通过一个被编码的芯片插入到 ATM 上，随后在 ATM 内部写入恶意程序，从而达到吐钞的效果。

5、iOS 曝严重安全漏洞：iPhone 用户或已被监听数年

比特网 8 月 26 日消息 iOS 9.3.5 今天紧急上线，苹果更新日志中提到修复了“重要安全问题”，建议用户尽快更新，因为这次涉及的 iOS 安全问题可能是“前所未有”的。苹果所指的重要安全问题乃是说 3 个 0-day 漏洞，这 3 个漏洞足以让攻击者对全球范围内的 iPhone 进行监听。Lookout 在报告中说，利用这些漏洞，攻击者可对设备进行全面控制，还能获取设备中的数据，通过麦克风监听对话，检测 GPS 信号位置，跟踪即时通讯应用的对话内容等等。这“是我们在终端设备上见过最复杂精致的攻击”。这 3 个漏洞分别是：Webkit 的 Memory Corruption：Safari Webkit 引擎漏洞，用户点击恶意链接后，就能对设备产生危害；内核信息泄露：kernel base mapping 漏洞，泄露的信息可致攻击者算出内存中的内核位置；Kernel Memory corruption 导致越狱：32 位/64 为 iOS 内核级别漏洞，可致攻击者悄悄对设备进行越狱，并安装窃听软件。利用这 3 个漏洞的是款软件套装，名为 Pegasus（希腊神话中带翅膀的飞马）。据说这款软件是由以色列的 NSO Group 集团开发的，而且卖给全球范围内的政府客户——政府用来做什么，自然就很清楚了。

6、攻击者利用虚拟机“掩盖”恶意行为

FreeBuf 8 月 25 日消息 最近有黑客盯上了虚拟机。最近 SecureWorks 接收到一个紧急通知，他们的一个客户公司称 7 月 28 日在其安全平台上检测到一些异常的情况。从该公司的系统管理员那里请求到了更多的日志后，SecureWorks 的研究人员发现了使他们的产品触发警报的日志报告。SecureWorks 公司反威胁团队（CTU）研究人员指出：“对方得到了访问权限，使他能够通过终端服务客户端的 Windows 资源管理器外壳进行交互。”攻击试图在感染的主机上启动虚拟机。所幸，他们获得访问权限的机器是单独的一台虚拟机本身而它无法跟其他虚拟机相互嵌套。虽然攻击者在他的尝试中失败了，但是这说明一个新的威胁出现了，攻击者能够利用虚拟机来掩盖他们的恶意操作。攻击者在建立和启动虚拟机之后，他们就已经能够连接到虚拟机，并执行恶意操作，如穿插敏感数据，这些都是安全产品无法触及的地方。

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：吕利锋

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话： 010-82990158