国家互联网应急中心

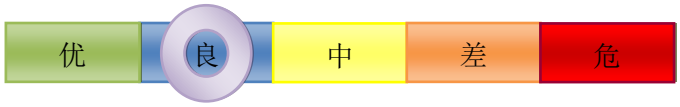
2016 年第 6 期

2 月 1 日-2 月 7 日

网络安全信息与动态周报

CNCERT/CC

本周网络安全基本态势

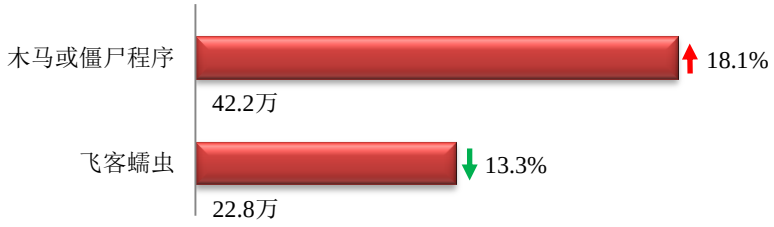


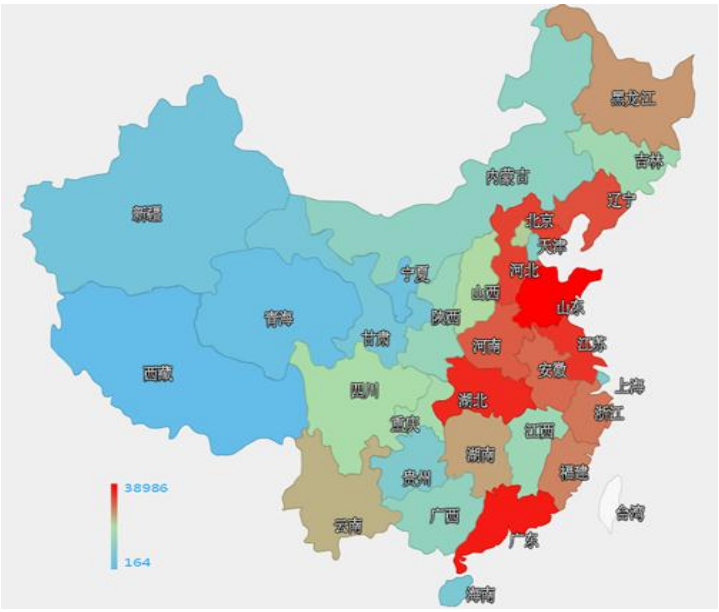
境内感染网络病毒的主机数量	•65.0万	↑4.8%
境内被篡改网站总数 其中政府网站数量	•4208 •54	↑1.8% ↓6.9%
境内被植入后门网站总数 其中政府网站数量	•947 •28	↓8.5% ↓22.2%
针对境内网站的仿冒页面数量	•1769	↓3.1%

=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 65.0 万个，其中包括境内被木马或被僵尸程序控制的主机约 42.2 万以及境内感染飞客（conficker）蠕虫的主机约 22.8 万。



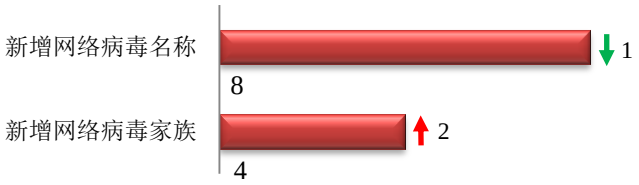


木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是山东省、广东省和湖北省。

TOP3

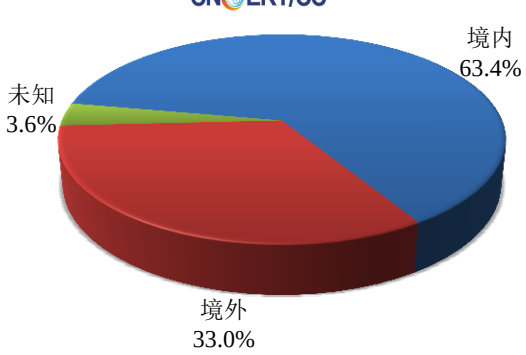
山东省	•约3.9万个（约占中国大陆总感染量的9.2%）
广东省	•约3.6万个（约占中国大陆总感染量的8.6%）
湖北省	•约3.3万个（约占中国大陆总感染量的7.8%）

本周 CNCERT 捕获的新增网络病毒文件，按网络病毒名称统计新增 8 个，按网络病毒家族统计新增 4 个。

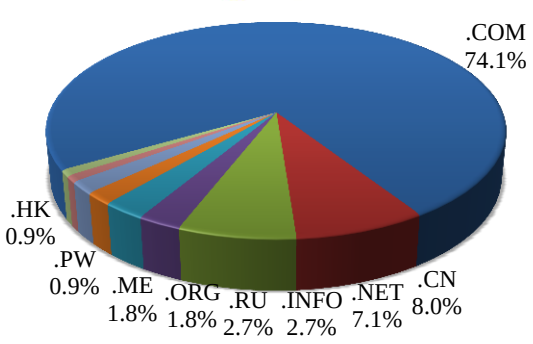


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 112 个，涉及 IP 地址 267 个。在 112 个域名中，有约 33.0%为境外注册，且顶级域为.com 的约占 74.1%；在 267 个 IP 中，有约 11.6%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 28 个 IP。

本周放马站点域名注册所属境内外分布
(2/1-2/7)



本周放马站点域名所属顶级域的分布
(2/1-2/7)



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。

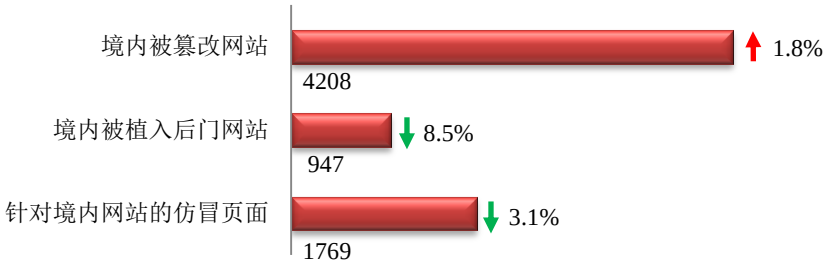
ANVA恶意地址黑名单发布地址

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。

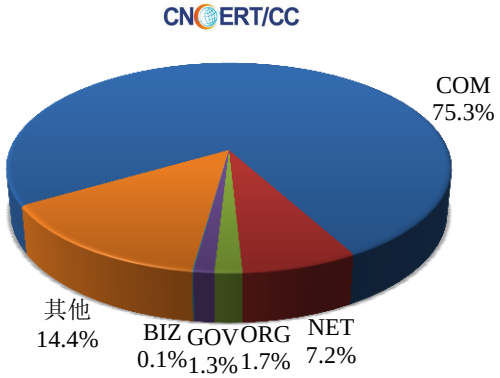
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 4208 个；境内被植入后门的网站数量为 947 个；针对境内网站的仿冒页面数量为 1769。

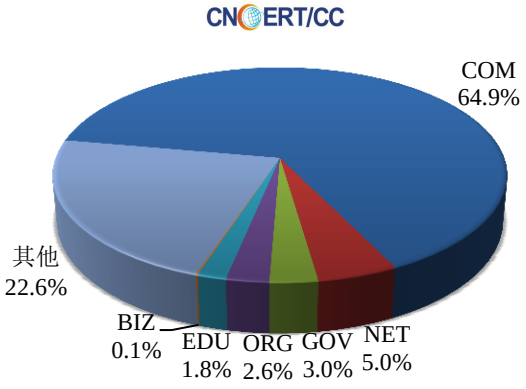


本周境内被篡改政府网站(GOV 类)数量为 54 个（约占境内 1.3%），较上周环比下降了 6.9%；境内被植入后门的政府网站(GOV 类)数量为 28 个（约占境内 3.0%），较上周环比下降了 22.2%；针对境内网站的仿冒页面涉及域名 1673 个，IP 地址 272 个，平均每个 IP 地址承载了约 7 个仿冒页面。

本周我国境内被篡改网站按类型分布
(2/1-2/7)



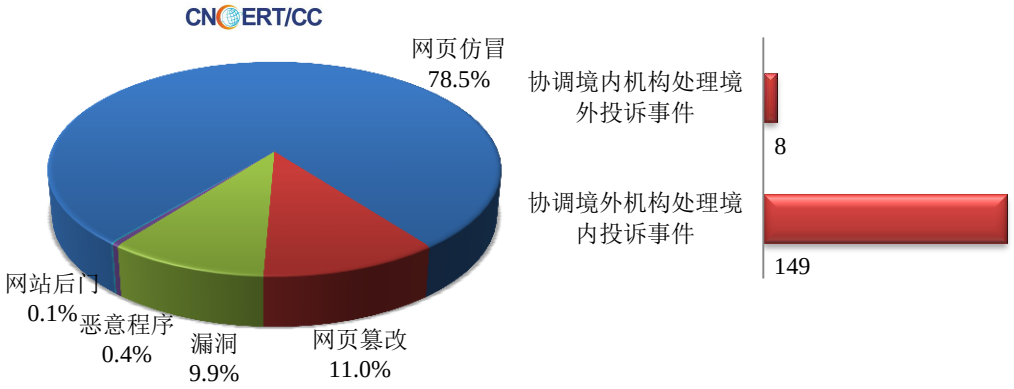
本周我国境内被植入后门网站按类型分布
(2/1-2/7)



本周事件处理情况

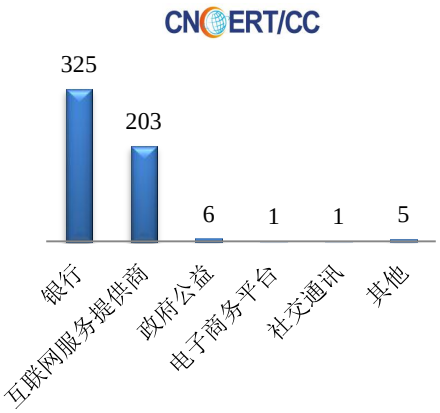
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 689 起，其中跨境网络安全事件 157 起。

本周CNCERT处理的事件数量按类型分布 (2/1-2/7)

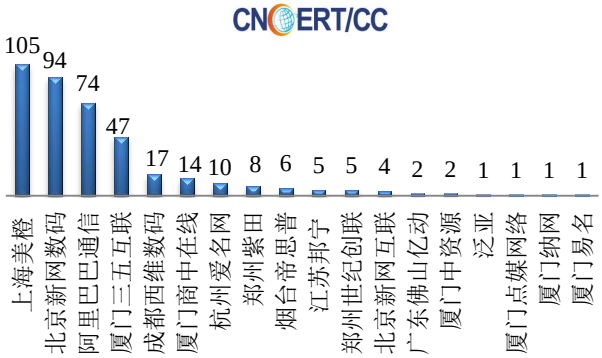


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 541 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事 325 起和互联网服务提供商仿冒事件 203 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(2/1-2/7)

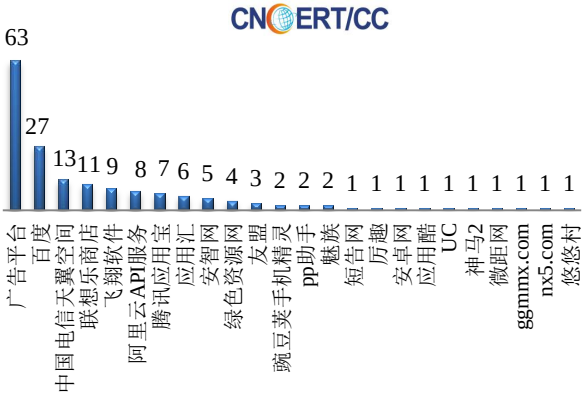


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (2/1-2/7)



本周，CNCERT 协调 24 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 172 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 (2/1-2/7)



业界新闻速递

1、欧盟美国就个人数据跨境交换达成共识

网易 2 月 3 日消息 据路透社报道，欧盟和美国谈判代表周二就欧洲用户的数据跨境交换问题达成一致意见。根据新协议，类似谷歌和亚马逊等公司将不再受到欧盟个人数据保护条例的限制，可跨越太平洋将用户信息传回至美国。不过新协议目前仍然需要获得政治上的批准。欧洲数据保护部门当前正在布鲁塞尔进行为期两天的会议，该机构曾一度表示会限制数据传输，除非有好的交易达成。欧盟委员会表示，新的隐私保护条例将会让美国企业在保护欧洲公民个人数据上承担更多的责任，并也会要求美国相关部门提供更严格的监视和执行。“我们第一次收到了来自美国的书面保证，其中详细说明了美方将如何保护和限制他们的监视项目。”欧盟委员会副主席安德鲁斯·安西普（Andrus Ansip）表示，“在商业领域，我们将会获得美国商务部和联邦贸易委员会的支持，他们将负责保证美国的公司遵守保护欧盟用户个人数据的义务。”

2、美英两国拟达成电邮、聊天记录互查协议

凤凰网 2 月 6 日消息 据路透社报道，多名美英官员周五表示，根据达成的一项初步双边协议，美英两国的警方及情报机构，很快将被允许到对方国家的媒体公司，直接查询本国被调查人的电邮、聊天记录。英国公民，当然也包括罪犯在内，他们大都使用了美国公司谷歌、Facebook 以及微软提供的数据服务，这使得英国当局在刑事或反恐调查过程中，很难访问到被调查人的聊天记录或者电子邮件等在线数据。《华盛顿邮报》的报道称，此次两国会谈所关注的焦点，是让英国“军情五处”（MI5）以及类似情报部门能够向美国公司开出数据“查询通知单”，令后者对涉及英国公民的聊天记录进行“实时拦截”，此外，这些英国机构还可以向美国公司提出电子邮件等存储数据的查询。当前，全球各国政府和在线媒体公司都在努力寻找隐私保护和法律询查之间的平衡点。三名美国官员证实美英两国正在围绕协议展开讨论，但表示这一协议仍需得到国会批准。美国司法部一名

官员表示：“尚在讨论中的这一协议，将使双方受益，而且要求立法生效。”援引一位要求匿名的美国政府消息人士称，尽管犯罪调查常常依靠跨国通信展开，但通常情况下，美国法律禁止本国公司向境外机构提供数据请求。因此，美国公司可能面临一个艰难选择：要么违反法律、选择合作，要么遵守法律、驳回数据请求。

3、美国或同意出口部分黑客工具 称用于保护网络安全

新浪网 2 月 5 日消息 美联社 2 月 2 日发表题为《美国将修改有关黑客工具出口的军控规则》的报道称，美国政府正在修改根据 20 年前制定的军控规则的一项提案，以简化与黑客和监视软件有关工具的出口，因为这些工具也用于保护计算机网络的安全。根据 2 日公开的一封信，白宫称，它支持向海外提供用于合法网络安全活动的网络入侵工具。行业组织和议员们此前已经提出担忧，称旨在限制此类黑客工具传播的规定会对国家网络安全和研究造成意外的负面影响。作为 1996 年《瓦瑟纳尔协定》的 41 个成员国之一，美国 2013 年同意限制可能落入压迫性政权之手的与网络“入侵软件”有关的工具。该协定是有关对武器和某些技术的出口控制。根据来自国家安全委员会立法事务高级主管卡罗琳·特丝的一封信，奥巴马政府同意，“防止这些技术不落入非法行动者之手，不应以合法的网络安全活动为代价”。国会网络安全会议联合主席、民主党众议员吉姆·兰格文公开了这封信。特丝称，白宫加强了与美国官员和有关行业的讨论。2015 年 5 月，商务部工业和安全局提议禁止进攻性工具的转让，此类工具的定义是利用“零日”漏洞——即未加补丁的新漏洞的软件，以及利用“后门”能力——即令一个人能以管理员级别权限进入系统的软件。但制造渗透测试工具的快速 7 网络安全公司的发言人珍·埃利斯说，在网络中，“渗透是一种防御性行动，（可测试）防御手段的效果如何”。她说：“为了解这一点，你进行自我攻击，为防御目的而采取进攻性行动。这是证明我们无法划出一条清晰界限的一个典型例子。”

4、斯诺登最新泄露文件披露 GCHQ 数据挖掘技术

网易 2 月 7 日消息 日前，Boing Boing 在网上发布了一份长达 96 页关于英国情报机构 GCHQ 数据挖掘技术的电子书——《数据挖掘研究问题书(Data Mining Research Problem Book)》。据悉，这份文件最早由爱德华·斯诺登获得。Boing Boing 为这本电子书打上了一个“可能发生的最糟糕的情况是什么？”的副标题，并对其进行以下描述：一种为想要利用恶意软件寻找许可、感染敌人电脑或网络的间谍所使用的清单。从电子书中了解到，这份数据挖掘手册由来自海尔布隆数学研究所的研究人员和 GCHQ 和布里斯托尔大学的研究人员联合编写。据 Boing Boing 披露，相关人员一半的时间花在公共研究工作上，而另外一半时间则用在政府的秘密项目开发上。手册为 GCHQ 数据挖掘工作提供了非常具有价值的见解，至少在 2011 年 9 月编写完成的时候是非常有用的。那个时候，一些“传输者”—互联网连接—其速度为 10 gigabits/s。而手册中写道：“一个 10G 的传输者可以生产巨大的数据。为了让它们变得可管理，首先要做的就是丢掉大部分我们看得到的数据包。”然而重要的是，其实被丢掉的只是内容，而非源数据。这也就证实了 GCHQ 在对源数据监控中所扮演的中心角色，换句话说，这个机构甚至有可能在《监听者宪章（Snooper Charter）》到来之前就已经开始数据收集了。还有值得注意的部分则是隐写术—将信息隐藏在另外一个文件中，其中一个常用的办法就是通过对 JPEG 图像系数的修改将数据藏在里边，与此同时，对图片的改变则要尽量保持最小化。不过手册中大部分内容都集中在 GCHQ 大规模源数据储存的审查上。当有外媒就这一份文件真实性向 GCHQ 求证时，该机构发言人称：“我们不对此做评论，”仅简单地提供了一个非常官方的回应。

5、日本多个政府部门网站瘫痪 疑似遭到网络攻击

中新网 2 月 1 日消息 据日媒报道，日本厚生劳动省和财务省等部门的网站今年 1 月 31 日出现瘫痪，无法阅览。网站似乎受到了“DDoS 攻击”（短时间内收到大量外部访问请求）。这些部门已向东京警视厅求助。据日本厚劳省称，当地时间 1 月 31 日晚 10 点 40 分左右起网站陷入瘫痪，2 月 1 日 0 点 10 分左右起恢复。此外，日本厚劳省的网站在 1 月下旬曾两次在遭到同样的攻击后瘫痪，2015 年 11 月也一度无法阅览。有关其中的两次瘫痪，已确认曾有自称国际黑客组织“匿名者”的用户在推特上宣称将对厚劳省网站发起攻击。另一方面，日本财务省和众议院的网站也出现了瘫痪。日本金融厅网站主页（HP）1 月 31 日也深夜起陷入了难以浏览的状况。该厅发现自称是国际黑客组织“匿名者”的人物在网上发布了暗示网络攻击的声明，目前正在调查详细原因。据日本金融厅介绍，目前尚未发现网站被篡改和信息外泄。

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：马莉雅

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话： 010-82990158