国家互联网应急中心

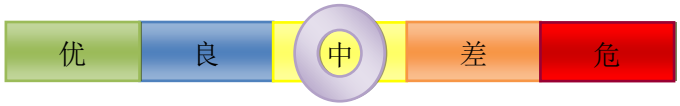
网络安全信息与动态周报

2016 年第 16 期

4 月 11 日-4 月 17 日

CNCERT/CC

本周网络安全基本态势

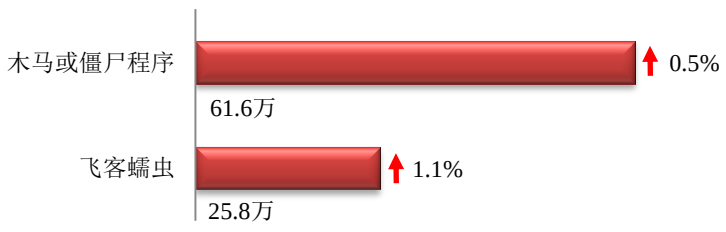


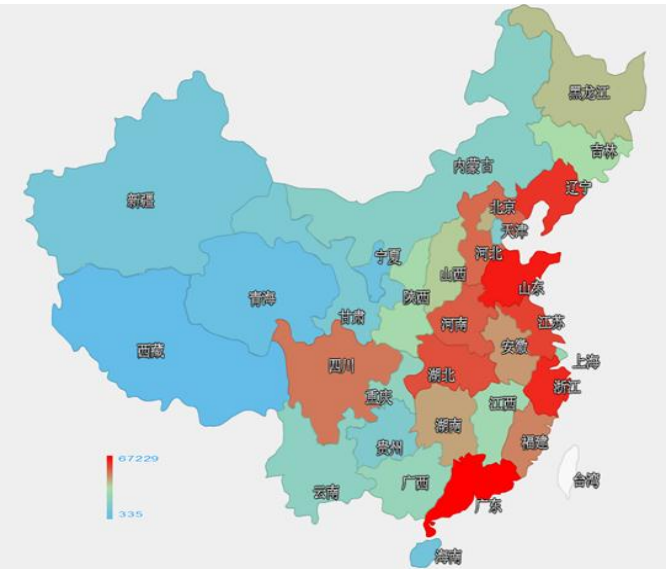
境内感染网络病毒的主机数量	•87.4万	↑ 0.7%
境内被篡改网站总数 其中政府网站数量	•4396 •116	↑ 65.1% ↑ 141.7%
境内被植入后门网站总数 其中政府网站数量	•5372 •241	↑ 21.0% ↓ 13.6%
针对境内网站的仿冒页面数量	•3768	↑ 1.2%
新增信息安全漏洞数量 其中高危漏洞数量	•151 •66	↑ 42.5% ↑ 94.1%

═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 87.4 万个，其中包括境内被木马或被僵尸程序控制的主机约 61.6 万以及境内感染飞客（conficker）蠕虫的主机约 25.8 万。



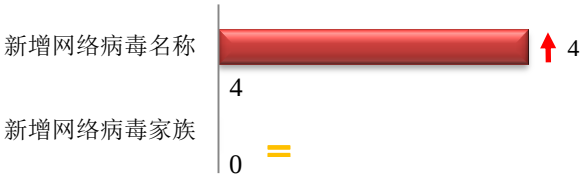


木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、山东省和浙江省。

TOP3

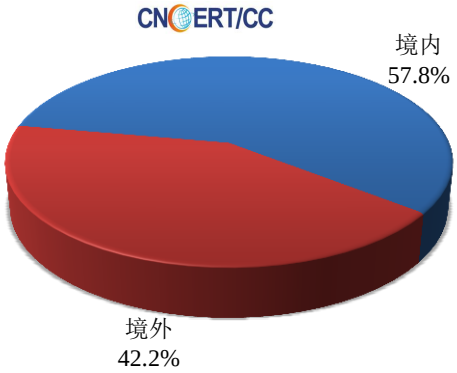
广东省	•约6.7万个（约占中国大陆总感染量的10.9%）
山东省	•约5.21万个（约占中国大陆总感染量的8.5%）
浙江省	•约5.19万个（约占中国大陆总感染量的8.4%）

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 4 个，按网络病毒家族统计无新增。

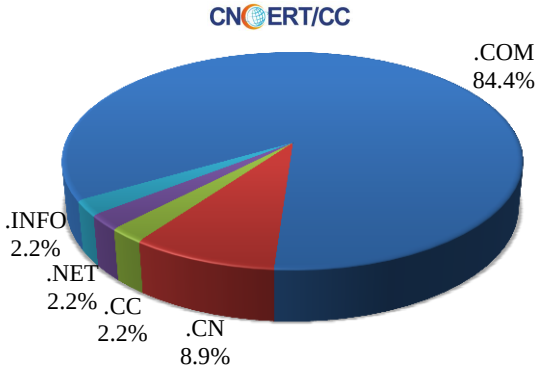


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 45 个，涉及 IP 地址 94 个。在 45 个域名中，有 42.2%为境外注册，且顶级域为.com 的约占 84.4%；在 94 个 IP 中，有约 4.3%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 6 个 IP。

本周放马站点域名注册所属境内外分布
(4/11-4/17)



本周放马站点域名所属顶级域的分布
(4/11-4/17)



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。

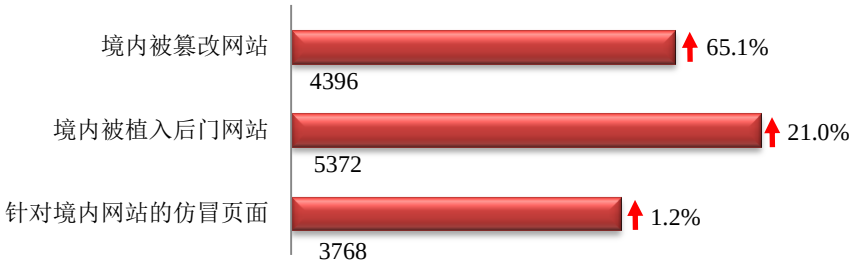
ANVA恶意地址黑名单发布地址

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。

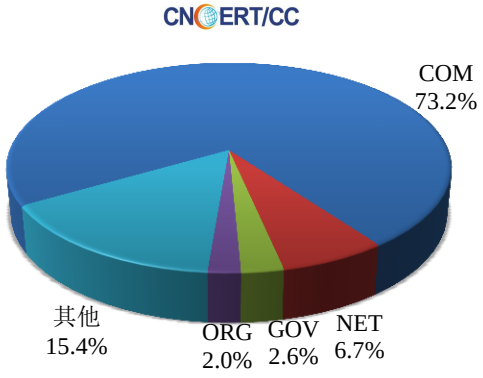
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 4396 个；境内被植入后门的网站数量为 5372 个；针对境内网站的仿冒页面数量为 3768。

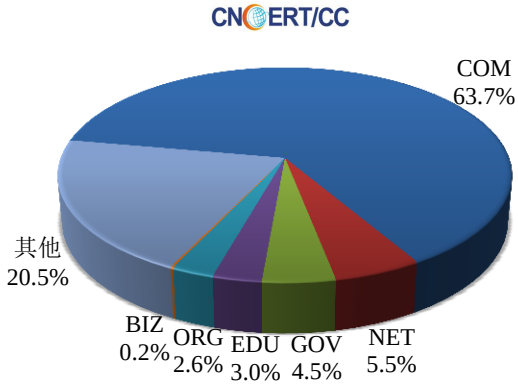


本周境内被篡改政府网站(GOV 类)数量为 116 个（约占境内 2.6%），较上周环比上升了 141.7%；境内被植入后门的政府网站(GOV 类)数量为 241 个（约占境内 4.5%），较上周环比下降了 13.6%；针对境内网站的仿冒页面涉及域名 3210 个，IP 地址 940 个，平均每个 IP 地址承载了约 4 个仿冒页面。

本周我国境内被篡改网站按类型分布
(4/11-4/17)

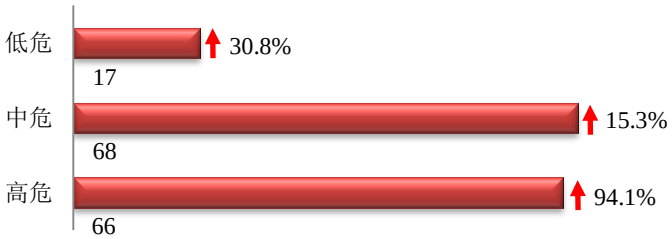


本周我国境内被植入后门网站按类型分布
(4/11-4/17)

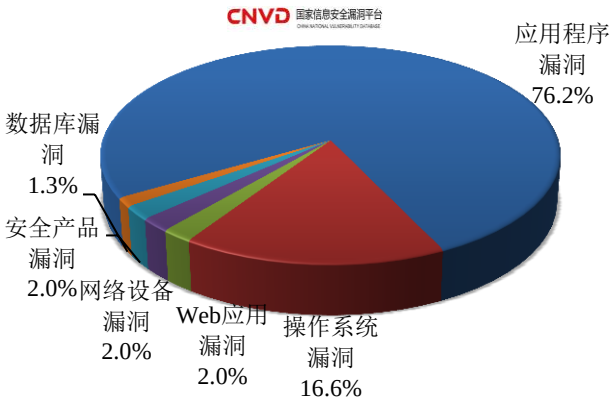


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 151 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
(4/11-4/17)



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

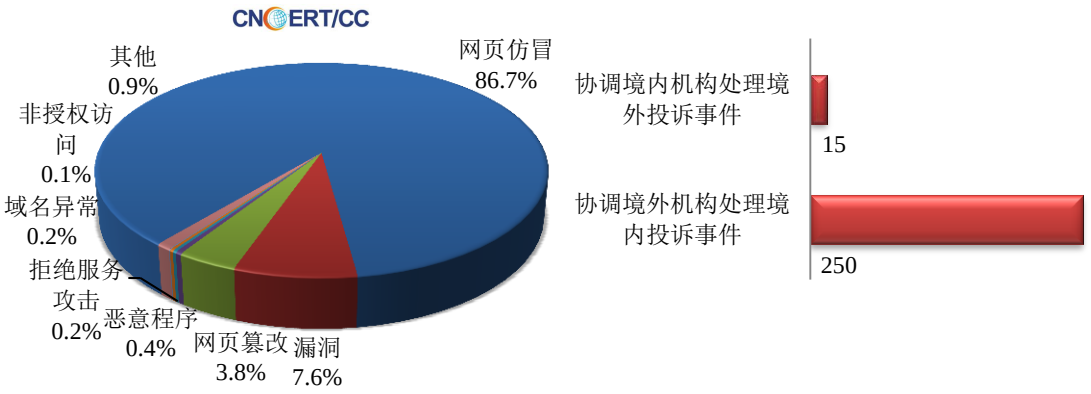
http://www.cnvd.org.cn/webinfo/list?type=4

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

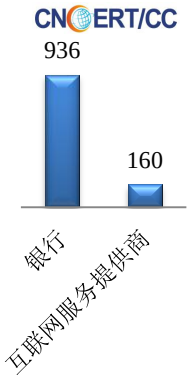
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 1264 起，其中跨境网络安全事件 265 起。

本周CNCERT处理的事件数量按类型分布
(4/11-4/17)

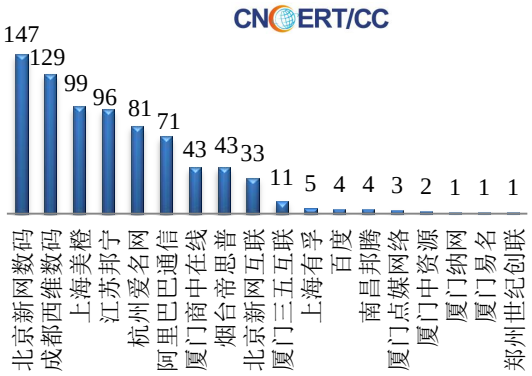


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 1096 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事 936 起和互联网服务提供商仿冒事件 160 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(4/11-4/17)

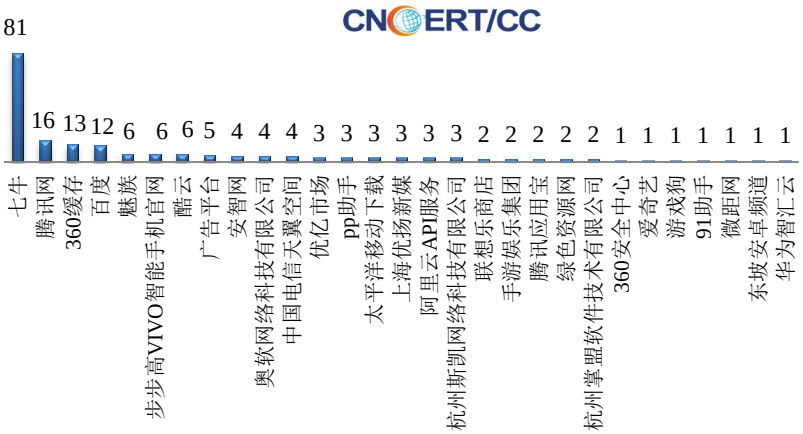


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (4/11-4/17)



本周，CNCERT 协调 29 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 192 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 (4/11-4/17)



业界新闻速递

1、首届内地-香港网络安全论坛在港召开

中国网信网 4 月 12 日消息 4 月 12 日，首届内地-香港网络安全论坛在香港举办。本届论坛由国家互联网信息办公室网络安全协调局和香港特别行政区政府资讯科技总监办公室联合举办，旨在加强两地网络安全合作交流，探讨产业经验，促进人才培养，提高民众安全意识。来自内地和香港的政府、企业和学术界近 200 人参加了论坛，阿里巴巴、安恒信息、IBM 以及香港应用科技研究院等企业专家代表在论坛期间就网络安全的发展与挑战与各界人士进行交流，分享经验。论坛期间，国家互联网信息办公室网络安全协调局与香港特别行政区政府资讯科技总监办公室签署了合作共识。双方同意在网络安全技术与产业、网络安全人才培养、网络安全宣传周活动等方面加强合作。据了解，内地-香港网络安全论坛今后将每年轮流在内地和香港举办。

2、奥巴马宣布成立国家网络安全强化委员会

搜狐网 4 月 14 日消息 今年 2 月，美国总统奥巴马公布了一网络安全国家行动计划（简称 CNAP），旨在通过一系列长期与短期举措改善美国的网络安全态势。此项计划的一大主要特点在于无党派国家网络安全强化委员会的成立，其将由来自企业、技术及学术界的重要思想领袖组成，并负责提出建议以帮助国家在未来十年内强化公共与私营部门层面的网络安全水平。奥巴马与国会两党各领导人在美国华盛顿时间 4 月 13 日已经选定了委员会的 12 位初始成员。这 12 位成员将负责向美国联邦政府、私营部门以及国家整体提供建议与可行性举措，从而进一步提升当今数字化时代之下的网络安全水平，且自去年 12 月开始生 效。他们将于明天在美国商务部召开首次公开会议，并与商务部部长 Penny Pritzker、总统国土安全与反恐事务助理 Lisa Monaco 及其他高层人士共同探讨该委员会面临的核心工作。该委员会的职责是制定详细的建议，从而在未来十年内强化各私营部门的网络安全意识与保护举措，最终实现隐私保护、公众安全保障、经济与国家安全防御以及引导美国民众更好地控制自有数字化资产的目标。为了确定承担这项任务的具体人选，奥巴马和他的执政团队咨询了来自国家安全、网络安全、企业、技术、学术界以及其它多个领域的领导者们的意见。另外，美国国 会两党各从领导层成员中选出一位参与此委员会，以确保建议能够最终被交付至国家层面并受到广泛支持。

3、美国国会公布加密法案征求意见稿 引发强烈反对

网易 4 月 14 日消息 据路透社报道，两名美国参议员周三公布了加密法案草案的正式内容。这项颇具争议的法案将赋予法院权力，使其能强制要求苹果这样的科技公司协助政府破解加密设备或通信，以满足情报或执法需要。一份版本较早的草案数日前曾在网上泄露，并引发了安全研究人员和民权人士的抨击。这类人士称，该法案将威胁到互联网的安全，并将个人数据暴露给黑客。同样的人士在周三表示，新草案与此前泄露的版本没有什么区别。该法案的出炉适逢美国司法部努力通过法院强制苹果解锁加密 iPhone 手机之际。美国参议院情报委员会主席理查德·伯尔（Richard Burr），以及副主席黛安·范斯坦（Dianne Feinstein）在声明中表示，他们现在希望“在法案正式推出前，先征求公众与核心利益相关者的意见”。这份新草案并不要求制造商或通信公司以特定格式处理、传输或存储数据。但它要求公司在接到法院强制令后，用“可识读的格式”将数据提交给政

府。即使这些数据加密，只能由所有者查看也不例外。该法案指出，公司必须确保它们的产品“能够满足（法案要求）”。批评人士称，这等于是在禁止强加密。新版法案收窄了强制令的使用范围。法案内容指出，除海外情报需要外，法院可以针对导致或可能导致死亡、严重伤害、贩卖毒品或儿童犯罪的刑事案发布强制令。电子前沿基金会（EFF）的法务专员表示，虽然征求意见稿改动很小，但该法案仍然会威胁到互联网安全，因为如果要想满足法案要求，公司就只能在所有产品上弱化加密。该法案料将引发科技行业与隐私权利人士的强烈反对。整个立法过程在国会也将面临重重阻碍。

4、欧盟批准更加严格数据保护规则保护个人隐私

C114 中国通信网 4 月 15 日消息 据 Engadget UK 网站报道，欧洲议会今天宣布投票支持新的数据保护法，后者将适用于位于欧盟的所有公司，无论他们的总部位于哪里。这一法律早在四年前提出，它代表了对 1995 年起草的规则的意义重大现代化更新，当时网络和数字服务远没有现在这么成熟。去年底在各个欧盟有关当局同意这些规则后，现在这些规则正式上线，这使得公司必须负责数据保护，也让公民对与他们有关的信息拥有更大的控制权。根据通用数据保护规则（GDPR）,公司必须确保在默认状态下自己的产品和服务尽可能少的获取和处理个人信息。这迫使例如社交网络这样的服务必须确保用户拥有最严格的隐私设定，而不是必须从菜单里寻找如何退出他们在注册时就自动包含的项目或者特征。这与公司负有保证数据收集更加透明化的责任相一致。公司必须获得用户“清晰明确的”同意才能处理他们的个人数据，并提供撤回同意权的简单方式，此外，数据将用于什么用途必须以“清晰直白的语言”陈述清楚。在新的数据保护规则下，任何处理大量个人数据的业务必须雇佣一名数据保护官员，违反这些规则必须在 72 小时内公开揭露。欧洲议会表示最新的规则将让公司受益，因为它引入了单一一套必须遵守的法律（而不是 28 个成员国各自的规则）以及单一的监管机构。切不可对 GDPR 掉以轻心，如果任何公司或者组织违反或者不遵守这一规则将处于高达 4%全球营业额的罚款。现在既然这些规则已经被批准，GDPR 和数据保护指令将很快变成欧盟法律的一部分，但这些规则要等到 2018 年 4 月才真正生效。这给成员国提供了两年时间将这些规则复制粘贴到自己本国的法律和流程中。当然这些规则可能在此之前就会产生影响。

5、“匿名者”及 LulzSec 对意大利招聘网站发起网络攻击

网易 4 月 11 日消息 据外媒报道，两大国际黑客组织“匿名者(Anonymous)”和“LulzSec”在当地时间 4 月 9 日宣布向意大利众多招聘网站发起名为#NessunDorma 的行动，并在网上公布了近 180 万用户的真实信息，数据的总量达到了 1.5GB。这两个组织声称希望借此提高意大利企业对改善本地及外国工人工作环境的意识。黑客表现了对意大利劳动与社会政策部部长 Giuliano Poletti 及意大利总理 Matteo Renzi 的强烈不满，两名官员近日准备颁布有利于一项意大利企业的新法律。 黑客希望意大利政府能将最低工资标准提高到每小时 8 欧元，并希望意大利企业为临时工的医疗保险负责。此外，这些黑客还声称拥有近五十万求职者的评估信息，及意大利近 7000 个主要企业的联系方式。黑客目前已经将部分数据分成六个不同的文档，并上传至 MEGA 网络硬盘。

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：周敏智

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话： 010-82990158