国家互联网应急中心

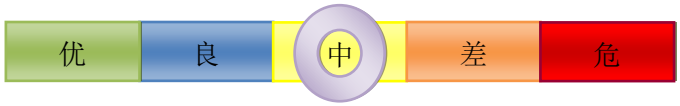
网络安全信息与动态周报

2016 年第 17 期

4 月 18 日-4 月 24 日

CNCERT/CC

本周网络安全基本态势

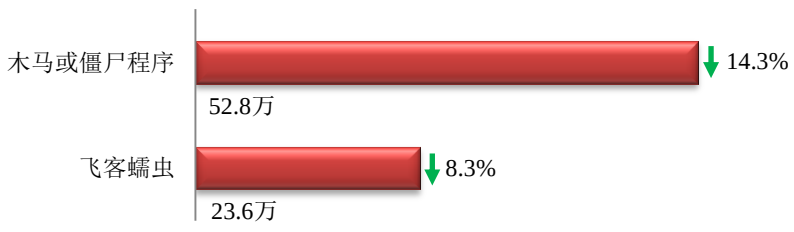


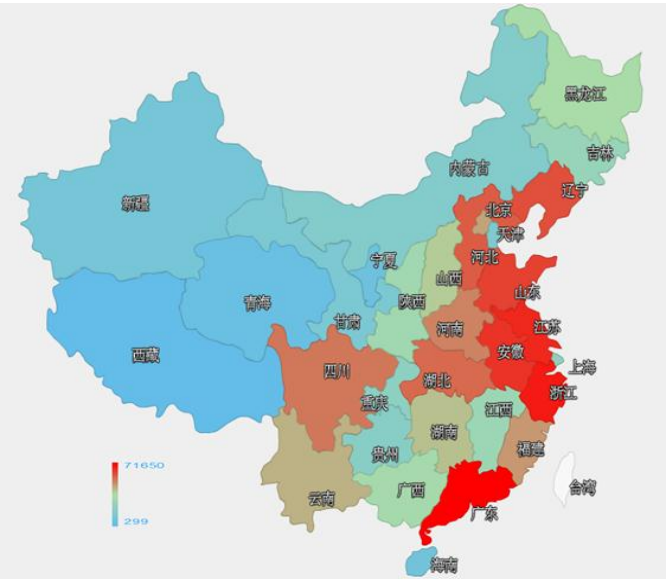
境内感染网络病毒的主机数量	• 76.4万	↓ 12.5%
境内被篡改网站总数 其中政府网站数量	• 4059 • 97	↓ 7.7% ↓ 16.4%
境内被植入后门网站总数 其中政府网站数量	• 2462 • 101	↓ 54.2% ↓ 58.1%
针对境内网站的仿冒页面数量	• 2892	↓ 23.2%
新增信息安全漏洞数量 其中高危漏洞数量	• 193 • 61	↑ 27.8% ↓ 7.6%

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 76.4 万个，其中包括境内被木马或被僵尸程序控制的主机约 52.8 万以及境内感染飞客（conficker）蠕虫的主机约 23.6 万。



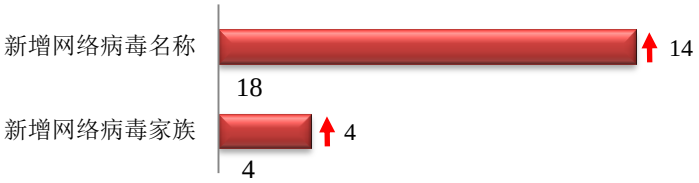


木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、浙江省和江苏省。

TOP3

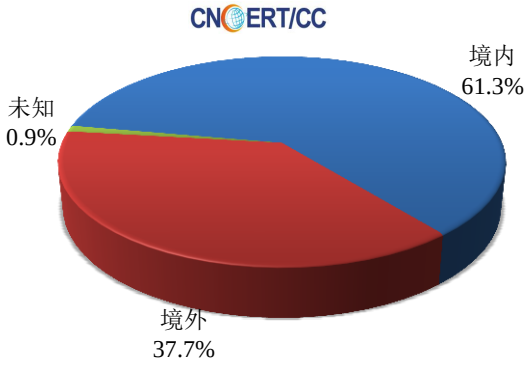
广东省	•约7.2万个（约占中国大陆总感染量的13.6%）
浙江省	•约5.8万个（约占中国大陆总感染量的11.0%）
江苏省	•约4.4万个（约占中国大陆总感染量的8.3%）

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 18 个，按网络病毒家族统计新增 4 个。

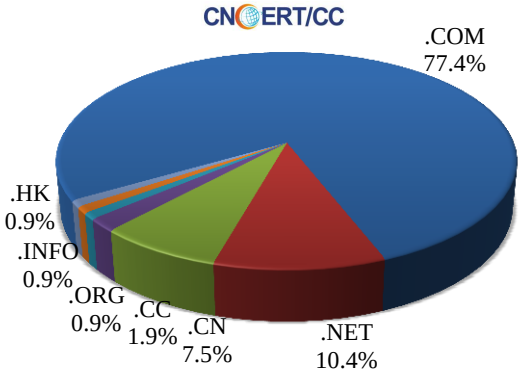


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 106 个，涉及 IP 地址 325 个。在 106 个域名中，有 37.7%为境外注册，且顶级域为.com 的约占 77.4%；在 325 个 IP 中，有约 5.5%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 25 个 IP。

本周放马站点域名注册所属境内外分布
(4/18-4/24)



本周放马站点域名所属顶级域的分布
(4/18-4/24)



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。

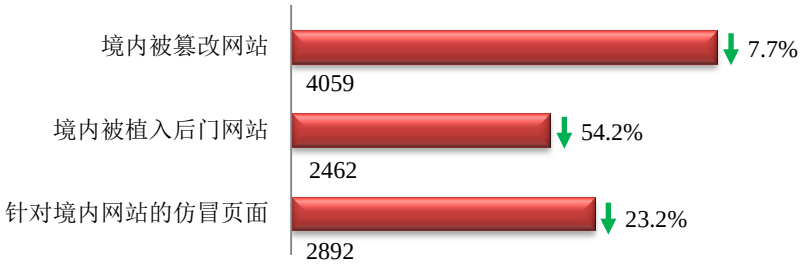
ANVA恶意地址黑名单发布地址

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。

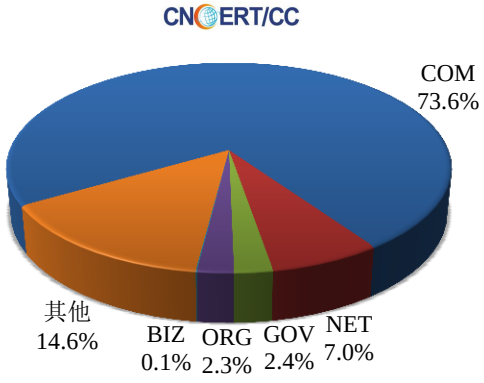
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 4059 个；境内被植入后门的网站数量为 2462 个；针对境内网站的仿冒页面数量为 2892。

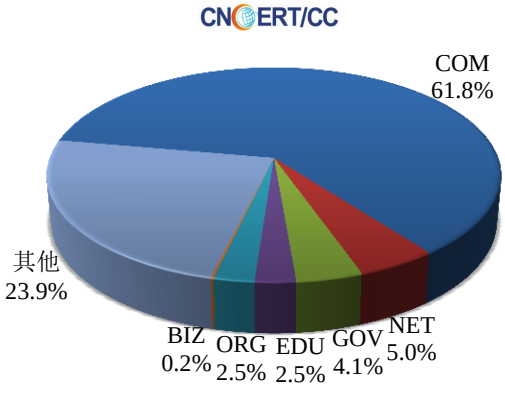


本周境内被篡改政府网站（GOV 类）数量为 97 个（约占境内 2.4%），较上周环比下降了 16.4%；境内被植入后门的政府网站（GOV 类）数量为 101 个（约占境内 4.1%），较上周环比下降了 58.1%；针对境内网站的仿冒页面涉及域名 2504 个，IP 地址 790 个，平均每个 IP 地址承载了约 4 个仿冒页面。

本周我国境内被篡改网站按类型分布
(4/18-4/24)

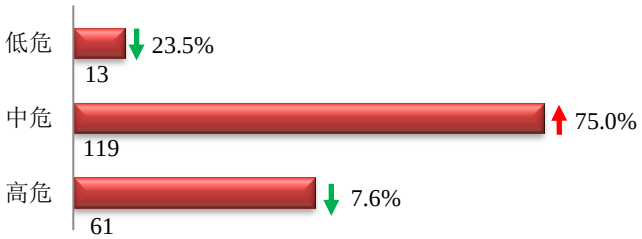


本周我国境内被植入后门网站按类型分布
(4/18-4/24)

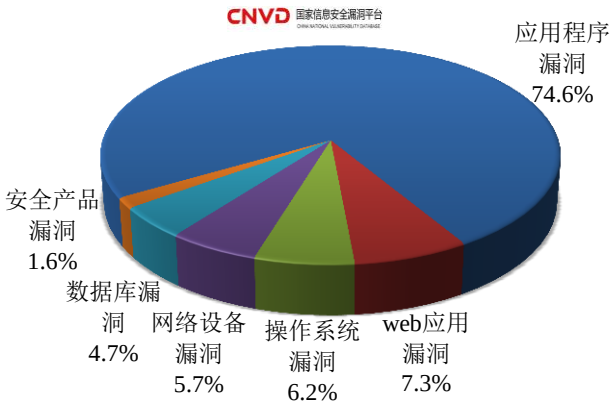


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 193 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
(4/18-4/24)



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

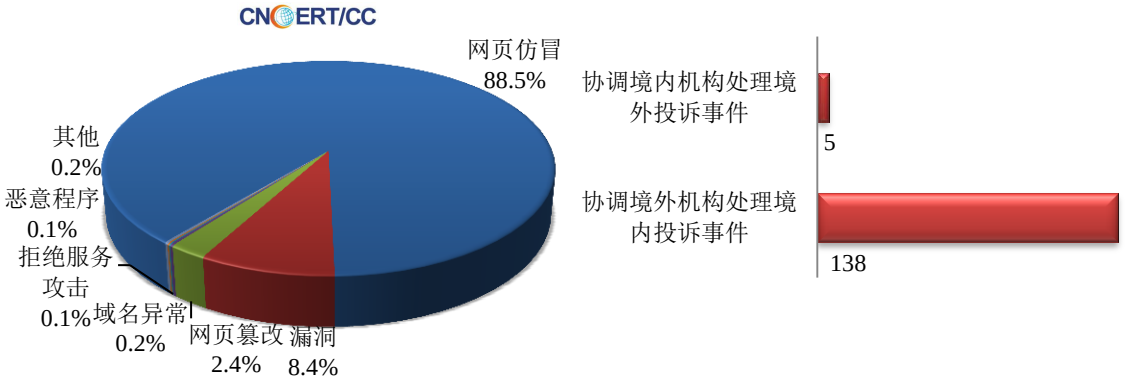
http://www.cnvd.org.cn/webinfo/list?type=4

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 914 起，其中跨境网络安全事件 143 起。

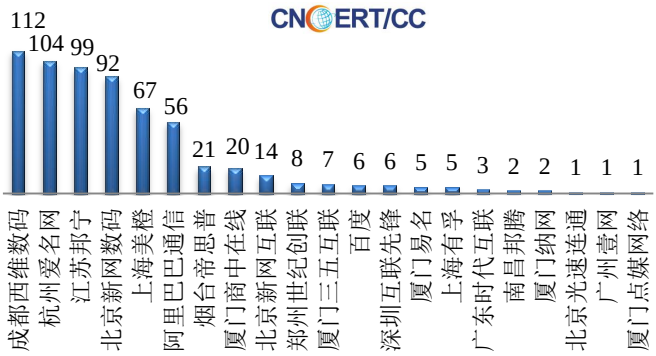
本周CNCERT处理的事件数量按类型分布
(4/18-4/24)



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 809 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 678 起和互联网服务提供商仿冒事件 106 起。

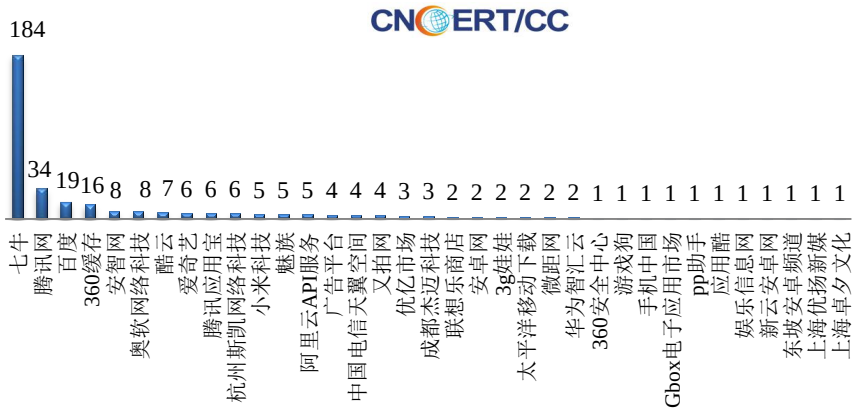
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(4/18-4/24)

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 (4/18-4/24)



本周，CNCERT 协调 35 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 350 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 (4/18-4/24)



业界新闻速递

1、习近平主持召开网络安全和信息化工作座谈会

新华网 4 月 19 日消息 中共中央总书记、国家主席、中央军委主席、中央网络安全和信息化领导小组组长习近平 4 月 19 日上午在京主持召开网络安全和信息化工作座谈会并发表重要讲话，强调按照创新、协调、绿色、开放、共享的发展理念推动我国经济社会发展，是当前和今后一个时期我国发展的总要求和大趋势，我国网信事业发展要适应这个大趋势，在践行新发展理念上先行一步，推进网络强国建设，推动我国网信事业发展，让互联网更好造福国家和人民。中共中央政治局常委、中央网络安全和信息化领导小组副组长李克强、刘云山出席座谈会。

2、美俄举行网络安全会晤 避免误会引发网络战

环球网 4 月 18 日消息 美国 CNN 当地时间 4 月 17 日消息称，美俄网络安全高官本周在日内瓦举行网络安全会议。这是双方为避免因误会引发的网络战的新一轮努力。报道称，赴日内瓦参会的美方官员来自白宫、国务院、联邦调查局等部门。会上双方将重审 2013 年签订的网络安全协议。去年 12 月乌克兰部分电网因网络攻击遭破坏后，美俄双方决定进行会晤。美调查机构称，此类针对民用基础设施的网络攻击模式前所未见。虽然奥巴马政府并未公开指责俄方，但一些美方高级官员认为该攻击由俄方幕后主使。此类网络攻击因为难以确定攻击源，所以很难对攻击方下结论。而自乌克兰危机中，俄方掌握克里米亚以来，美俄关系已跌至冰点。报道还称，虽然俄方官员建议双方再次会晤代表着恢复正常，但是美方官员却尽力淡化本次日内瓦会议的作用。“本次会晤并非恢复双边总统委员会工作组（2014 年乌克兰危机后停止），但是代表了我们有兴趣同俄方讨论网络安全问题，包括重审 2013 年签订的美俄双边网络安全协议”，美方高级官员说。该协议的条款包括网络安全危机期间在美俄官员间建立应急热线。目前的担忧是，如果一方受到的网络攻击如果被查到攻击源在对方境内，则或将导致双方展开网络战。一名高级官员称，目前双方的热线仍然有效。

3、澳公布网络国防计划 首次承认有能力策动网络攻击

环球网 4 月 21 日消息 据新加坡《联合早报》4 月 21 日报道，澳大利亚总理特恩布尔 21 日公布总值 2.4 亿澳元的网络安全策略，以加强其抵抗网络攻击的能力。据报道，特恩布尔公布的这份政策纲领指出，堪培拉政府将加强与商界在网络安全方面的合作，并将专门任命一位网络安全大使。特恩布尔还在这份文件中首次承认其具备策动网络攻击的能力，并称这是应对外来威胁的手段。但特恩布尔强调，有关行动受到法律严格监管。曾经从事互联网行业的特恩布尔也首次证实，澳洲气象局曾遭受黑客攻击。当时的报道称，此次攻击规模庞大，由于气象局的系统与国防部系统有连线，攻击对整个联邦电脑系统造成破坏。澳洲网络安全中心（ACSC）去年发表报告说，澳洲企业日益成为网络间谍活动的目标，黑客活动对其盈利能力与生存空间造成威胁。据报道，21 日发表的文件指出，全球黑客攻击所造成的经济损失占澳洲国内生产总值（GDP）的 1%，澳洲媒体以此推算，黑客攻击每年为澳洲造成 170 亿澳元的损失。报告也提到，根据 2013 年的一份商界报告，网络攻击对澳洲造成的直接经济损失为 10 亿澳元。

4、乌克兰发布新版《网络安全战略》

网易4月18日消息 乌克兰总统波罗申科日前批准通过乌克兰新版《网络安全战略》。总统办公室发言人称，鉴于最近几个月针对乌克兰关键IT设施和社会基础设施的网络攻击数量显著上升，发布新的《网络安全战略》十分必要。新战略在符合欧盟和北约标准的前提下，为乌克兰网络安全设计新的标准，同时加速网络安全研发活动。战略还扩大了乌克兰参与的国际网络安全合作，由乌克兰国家安全和国防委员会负责。新战略旨在减少针对乌克兰能源设备的黑客攻击。2015年年末，乌克兰电力公司电网遭受攻击，造成22万用户断电。调查报告认为，此次攻击有来自俄罗斯的黑客参与，攻击通过使电网公司的电脑感染恶意软件 BlackEnergy 实现，该恶意软件由俄罗斯黑客组织开发并广泛使用在僵尸网络。2014年，F-Secure 团队发现 Blackenergy 恶意软件的特定样本开始以乌克兰政府作为目标来收集情报。乌克兰国家安全部一位发言人称，乌克兰的核电站、机场、铁路系统和其他关键基础设施都面临严峻的网络威胁，因此将专门成立由权威IT安全专家组成的网络安全团队对关键基础设施网络的战略性入口进行管理以防止网络攻击。乌克兰军队也会成立专门的网络防御部门。乌克兰政府宣布将不再从俄罗斯公司购买软件和IT技术，尤其是卡巴斯基的产品。在乌克兰总统大选期间，卡巴斯基的反病毒系统多次未能测出对国家核心网络资源的攻击，给选举造成威胁。新战略同时包含乌克兰国家银行为国家金融体系起草的网络安全标准。

5、印度借助企业力量应对网络攻击

中国信息产业网4月18日消息 据印度内务部数据显示，近年来，印度的网络攻击案件迅速增加，与2012年相比，2013年印度的网络攻击案件数增加了64%，2014年则增加了近70%。对此，印度政府决定招募私营部门的网络安全专家，通过主动监控和使用前瞻性战略打击网络犯罪。在此次招募的第一阶段，印度内务部要求有意愿从事打击网络犯罪、维护网络安全工作的企业或组织参与4月12日、19日举行的特别发布会。内政部官员表示，希望参会企业能充分展示其在打击网络犯罪、维护网络安全领域的专业性，主要涉及但不限于妇女和儿童保护领域。同时，有兴趣的企业也可针对网络威胁处理和网络空间监控能力提出前瞻性思维方式，防止针对妇女和儿童的网络犯罪发生。此外，在打击网络犯罪工具的研发以及防范管理上有建树的企业也可参与会议的演示与讨论。每个企业或组织将有45分钟的时间作相关的专题介绍。印度政府近日发布消息称，将出资40亿卢比（约合3.9亿元人民币）成立“印度国家网络犯罪处理协调中心”，旨在审查网络犯罪，打击儿童色情和滥用网络等行为。据悉，该中心的首要职责之一就是核查企图渗透到印度政府官方网络实施黑客攻击的国际犯罪组织。只要是与网络犯罪相关的案件，该中心都将为印度中央调查局和国家警察署提供一切必要的技术支持。

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：严寒冰

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话： 010-82990158