国家互联网应急中心

2015 年第 17 期

4 月 20 日-4 月 26 日

网络安全信息与动态周报

CNCERT/CC

本周网络安全基本态势

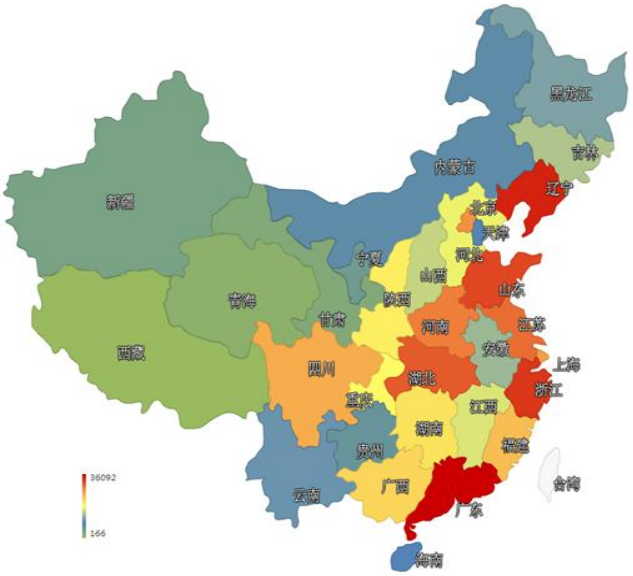
优 良 中 差 危

境内感染网络病毒的主机数量	• 39.8万	↓ 4.2%
境内被篡改网站总数 其中政府网站数量	• 2648 • 74	↑ 10.7% ↑ 13.8%
境内被植入后门网站总数 其中政府网站数量	• 2898 • 179	↑ 36.3% ↓ 8.7%
针对境内网站的仿冒页面数量	• 3948	↓ 22.6%
新增信息安全漏洞数量 其中高危漏洞数量	• 194 • 59	↓ 0.5% ↓ 23.4%

= 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 39.8 万个，其中包括境内被木马或被僵尸程序控制的主机约 23.3 万以及境内感染飞客（conficker）蠕虫的主机约 16.5 万。

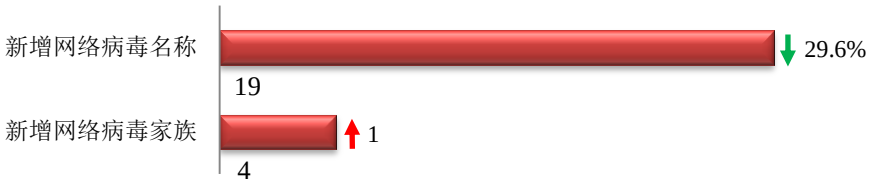


木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、辽宁省和浙江省。

TOP3

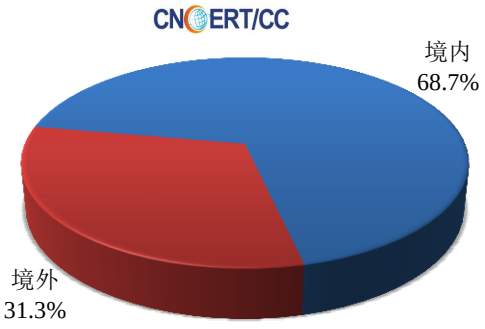
广东省	•约3.6万个（约占中国大陆总感染量的15.5%）
辽宁省	•约2.1万个（约占中国大陆总感染量的9.0%）
浙江省	•约1.6万个（约占中国大陆总感染量的6.9%）

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 19 个，按网络病毒家族统计新增 4 个。

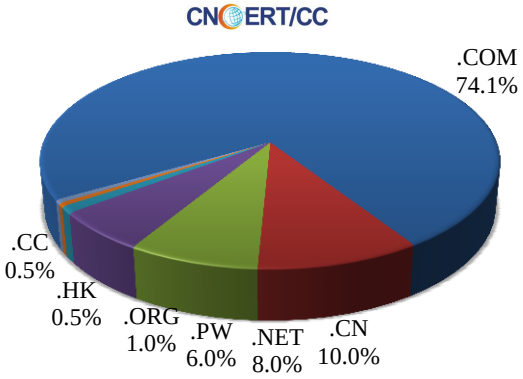


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 201 个，涉及 IP 地址 300 个。在 201 个域名中，有约 31.3%为境外注册，且顶级域为.com 的约 74.1%；在 300 个 IP 中，有约 8.3%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 31 个 IP。

本周放马站点域名注册所属境内外分布
(4/20-4/26)



本周放马站点域名所属顶级域的分布
(4/20-4/26)



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。

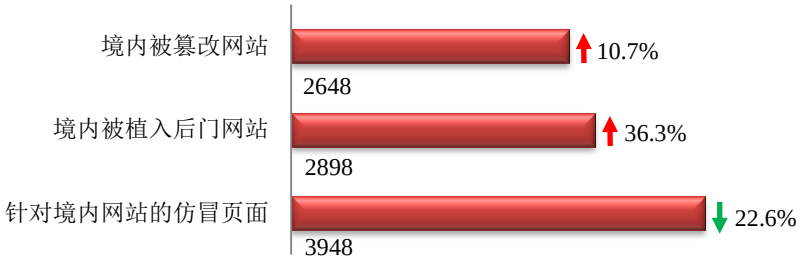
ANVA恶意地址黑名单发布地址

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。

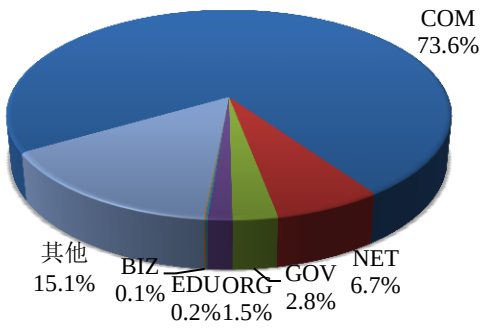
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 2648 个；境内被植入后门的网站数量为 2898 个；针对境内网站的仿冒页面数量为 3948。

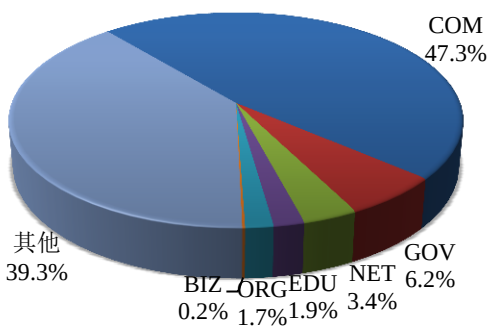


本周境内被篡改政府网站(GOV 类)数量为 74 个（约占境内 2.8%），较上周环比上升了 13.8%；境内被植入后门的政府网站(GOV 类)数量为 179 个（约占境内 6.2%），较上周环比下降了 8.7%；针对境内网站的仿冒页面涉及域名 3059 个，IP 地址 744 个，平均每个 IP 地址承载了约 5 个仿冒页面。

本周我国境内被篡改网站按类型分布
(4/20-4/26)

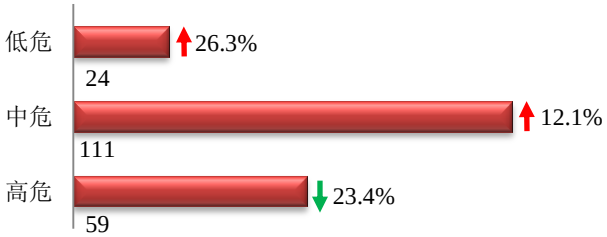


本周我国境内被植入后门网站按类型分布
(4/20-4/26)

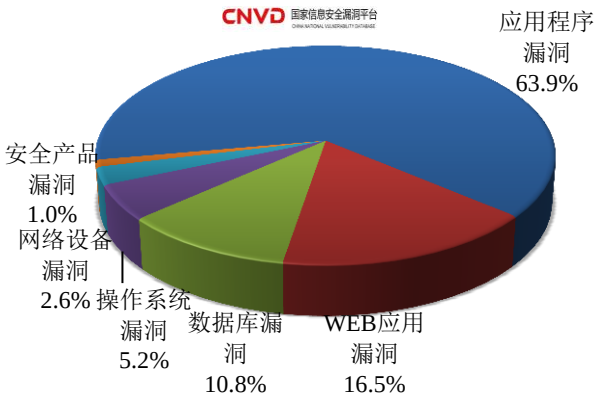


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 194 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
(4/20-4/26)



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 应用漏洞和数据库漏洞。

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

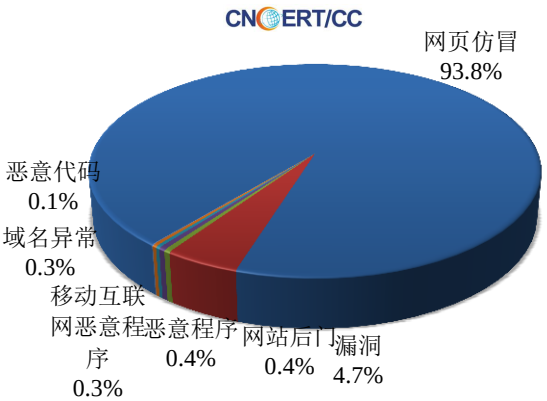
http://www.cnvd.org.cn/webinfo/list?type=4

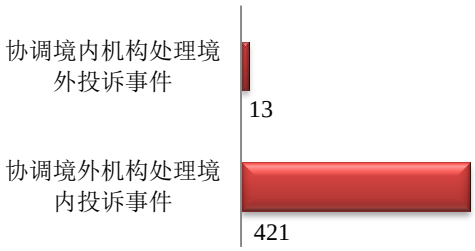
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 1412 起，其中跨境网络安全事件 434 起。

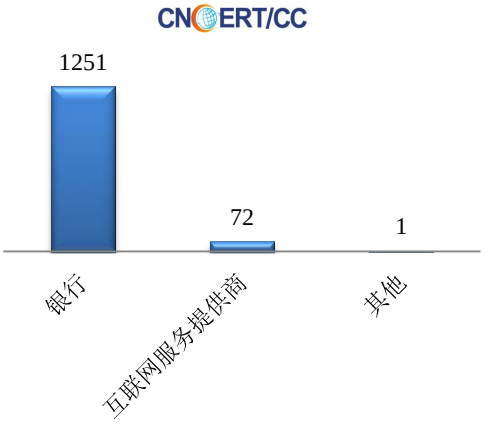
本周CNCERT处理的事件数量按类型分布
(4/20-4/26)



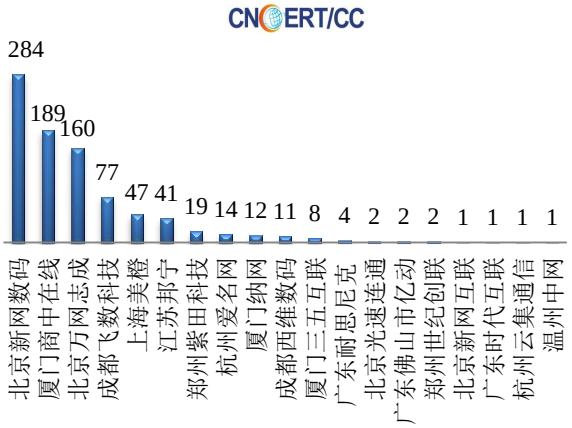


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 1324 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 1251 起和互联网服务提供商仿冒事件 72 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(4/20-4/26)

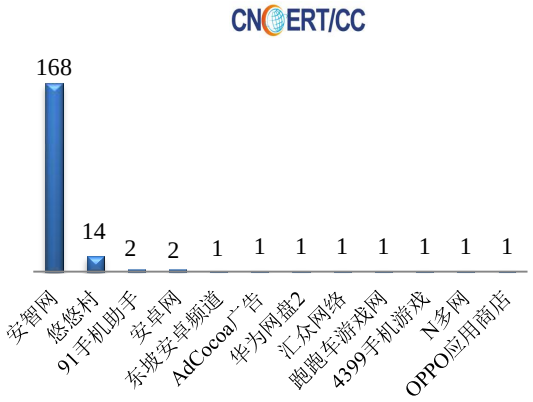


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (4/20-4/26)



本周，CNCERT 协调 12 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 194 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 (4/20-4/26)



业界新闻速递

1、美新网络安全战略攻击性升级 首将网络战作为选项

环球网 4 月 25 日消息 美国五角大楼 4 月 23 日发布新版网络安全战略，首次公开表示美军在与敌人发生冲突时，将把网络战作为选项之一。美联社称，这是五角大楼发布的第二份网络安全战略报告。美国防部 2011 年 7 月首次发布网络安全战略报告，很少提及五角大楼的网络攻击能力，美国官员对相关内容也很低调。中国复旦大学学者沈逸说，如果现在美国战略上仍是防御性的，那么它在战术上的攻击性已经明显提升，强调报复能力，让人隐约感到美国想要越过一些红线。“美国国防部的网络安全战略是一个整体行动指南。军队将据此制定网络行动指南，理解军队在国家网络安全中承担的使命和职责。”沈逸向《环球时报》记者介绍说。据美联社报道，这份长达 33 页的文件称，美国政府和企业受到的网络攻击比先前更严重和复杂，美国国防部“应当有能

力通过实施网络战，干扰敌人的指挥控制网络以及与军事有关的关键基础设施和武器设施”。对于新网络安全战略以更公开的方式提及网络战，美国官员的解释是，五角大楼希望网络任务更透明，同时给潜在对手以威慑。美联社称，美国防长卡特 24 日正走访硅谷，寻求高科技公司和专家帮助，以应对日益增长的网络安全威胁，确保美军拥有所需的最前沿技术。但他很可能将面对不容易取悦的听众，他们一直对美国的监听项目持怀疑态度。

2、美众院通过网络安全法案 企业将与政府分享信息

中新网 4 月 24 日消息 据美国媒体报道，在美国政府及私营部门发生一系列计算机安全事故之后，众议院做出了回应。当地时间周三（22 日），美国众议院通过了一项影响广泛的法案，该法案将迫使企业向联邦调查人员提供访问其计算机网络、查阅数据记录的权限。该法案过去数年中多次受挫，奥巴马政府也对该法案表达过失望，如今它终于有了进展。如果众议院和参议院携手推出最终法案，这将是美国联邦政府到目前为止针对一系列网络攻击事件做出的最为激进的反应。众议院通过的这项法案，将为那些在彼此之间或向政府部门共享网络威胁信息的公司提供保障，免除其法律责任。但参与了该法案磋商进程的人员，也在法案中添加了在他们看来十分关键的隐私保护条款。如果一家公司向美国政府分享信息，那么只有其数据经过了两轮清理，筛除其中的个人信息，才能受到法律保护，免于承担责任。第一轮筛选工作由该公司在将信息提交给政府之前完成，第二轮筛选工作由接收信息的政府机构负责——很多专家都认为，这是让企业遵守法律规定的关键。“要想让企业分享信息，就得为其提供保护，免除其责任，”信息技术产业协会（Information Technology Industry Council）的政府事务总监萨拉•贝丝•格罗沙尔特（Sarah Beth Groshart）说。“只有国会可以提供这种保护。”过去 10 年间，对美国的电脑网络进行执法的工作变得日益困难，部分原因在于共和党人担心这会增加私营部门的负担，而两党都有人主张采取更加严格的隐私保护举措。

3、欧洲委员会鼓励成员国议会对大规模监听监控展开调查

新华网 4 月 22 日消息 欧洲委员会议会大会 21 日通过决议，呼吁成员国对情报部门予以监督，停止非法大范围监听监控，并鼓励成员国议会对大规模监听监控活动展开调查。决议说，美国“棱镜”监听项目曝光者斯诺登揭秘的美国大规模监听监控不仅侵害人权，而且丝毫无助于反恐，因为它浪费了监控资源，分散了注意视线，从而给恐怖分子以可乘之机，这与情报部门给出的大规模监听监控的理由完全相反。决议说，德国联邦议院对美国国家安全局监听监控事件的调查是范例，其他国家议会可以借鉴德国的经验，对大规模监听监控活动展开调查。决议特别强调，应该对揭秘非法监听监控行为的人员给予保护，而目前对待斯诺登的过分做法不利于重建彼此间的信任和公众信任。去年 4 月，欧洲委员会在议会大会期间曾邀请斯诺登通过视频连线回答议会法律问题与人权委员会的提问。斯诺登肯定地说，大规模监听监控不仅不能有效防止恐怖行为，而且还会使社会更加缺乏宽容和安全。今年 3 月，欧洲委员会通过一项报告草案，呼吁美国政府允许斯诺登安全返回美国，并保证其免受刑事追究。

4、德国情报机构被指协助美国监听欧洲企业及政治家

中新网 4 月 24 日消息 据德国媒体 23 日报道，最新爆料显示，德国联邦情报局向美国国家安全局提供协助，刺探欧洲企业以及政治家。报道称，十多年来，德国联邦情报局在共同窃听的框架下，从美国国安局获取 IP 地址以及手机号码并将之植入自己的系统，便于情报局监督之用。以这种方式，国安局可以有针对性地拿到欧洲航空防务与航天公司（EADS）、空中客车直升机公司（Eurocopter）亦或法国政府的信息。该新闻一经传出，德国政界立刻哗然并对联邦情报局的做法进行了严词批评。按照德国法律，联邦情报局有着严格的约束规定，不

能任意对公民或企业进行监督。报道称，2008 年之后，联邦情报局的工作人员多次发现他们从美方得到的搜索任务与该情报局的性质不符。2002 年，德国同美国就全球共同反恐达成了协议，但美方的搜索目标无法得到以上文件的支持。报道说，德国联邦情报局在斯诺登事件发生后才开始仔细察看美国的搜索任务。在对 2000 个搜索目标调查后发现，该行动有悖于西欧国家以及德国的利益。但联邦情报局将这一信息扣下，没有向自己的上级即总理府汇报，而是委托一名处长级官员向美国国安局发出停止违法操作的请求。因联邦议会调查委员会的询问，后一轮调查发现了 4 万条可疑的搜索信息。媒体曝光该丑闻后，联邦议会调查委员会为询问政府代表而中断了会议。

5、美发现新浏览器攻击模式：可监控全球八成 PC

凤凰网 4 月 21 日消息 北京时间 4 月 21 日消息，据《福布斯》网站报道，美国哥伦比亚大学的一个安全小组最近发现了一种新型、隐蔽的电脑攻击模式，黑客利用这一攻击模式，可对全球八成 PC 实施监控。据悉，利用该漏洞，黑客可在不被检测到的情况下对 PC、网络应用或者云端虚拟机实施监控。任何使用英特尔最新处理器和 HTML5 网络浏览器的 PC 均为这一攻击的潜在对象，这意味着全球 80%的 PC 面临着这一攻击风险。该小组研究人员表示，黑客使用这一被称为“沙箱间谍”的安全漏洞对 PC 发动攻击，几乎不需要花费时间和金钱，不需要安装什么东西，而且勿需进入硬件系统。黑客所要做的，是将受害用户引诱到一个由攻击者控制的非授信内容页面上。黑客一旦得手，内置含有虚假内容的软件将启动一个程序，可以通过操纵受害人 PC 缓存数据的进出，从而对系统实施监控。

6、俄黑客组织或利用 Flash 和 Windows 漏洞窃取信息

新浪网 4 月 20 日消息 北京时间 4 月 20 日上午消息，美国网络安全公司 FireEye 发布的最新报告显示，一个俄罗斯黑客组织一直在利用 Flash 和 Windows 系统中的漏洞获取其他国家政府的信息。FireEye 去年 10 月还曾表示，这个名为 APT28 的俄罗斯黑客组织一直在搜集其他国家的政府、军方和安全组织的信息（其中也包括美国），并有可能“令俄罗斯政府受益”。FireEye 称，Adobe 已经发布了补丁，微软也在加紧开发补丁。路透社表示，微软漏洞的危险性可能较低，因为该漏洞与电脑上的“增强性能”有关，而普通用户通常不会接触这一领域。Adobe 和微软均未立刻对此置评。由于许多政府机构、新闻媒体和大型企业近期相继遭遇攻击，所以网络安全已经成为各个行业关注的焦点。去年 11 月的索尼被黑事件导致该公司损失惨重，大量敏感信息泄露。FireEye 表示，APT28 成立于 2007 年，有可能获得了俄罗斯政府的支持。其他安全公司还认为该组织与美国国务院的信息泄露事件有关，那起事件导致美国总统奥巴马的行程计划泄密。

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：张帅

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990170