网络信息安全周报

【2017】第 6 期

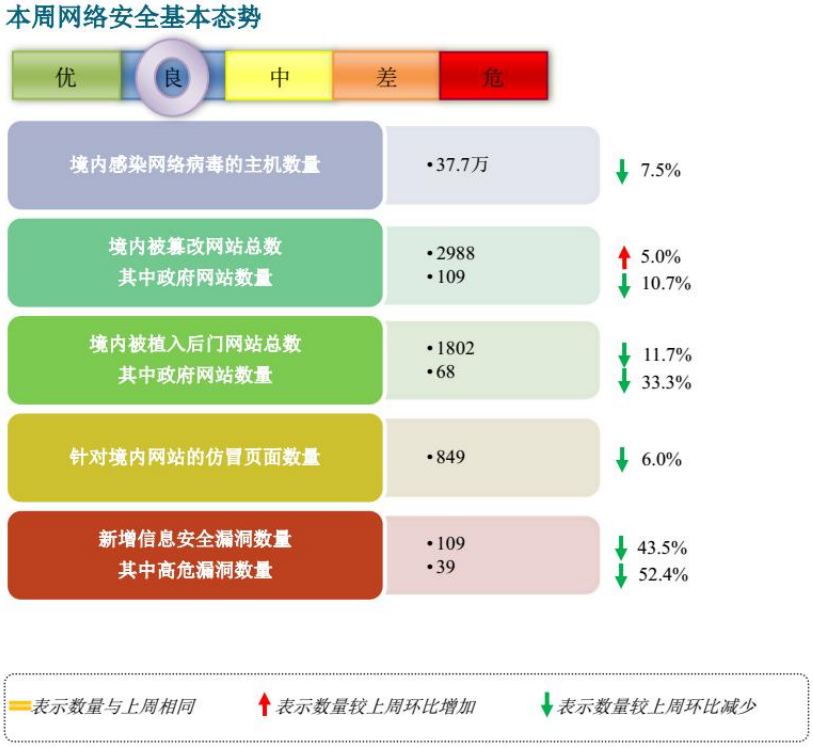
党委宣传部
信息网络中心　编　　2017 年 4 月 6 日

本期要目

- 网络安全信息与动态（2017 年 3 月 20 日—3 月 26 日）
- 为什么修改 DNS 就能提高网速解决卡顿,告诉你真正的原因!
- 小知识：中国互联网举报中心 www.12377.cn
- 安全警示：电脑出现来历不明的广告？小心木马病毒“幽浮”

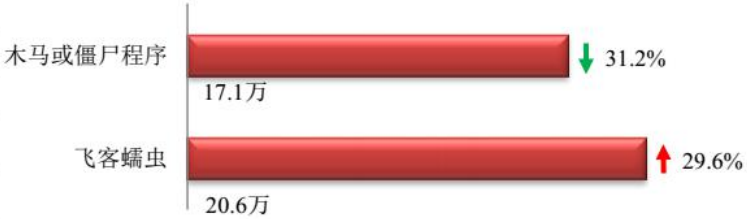
网络安全信息与动态（2017 年 3 月 20 日—3 月 26 日）

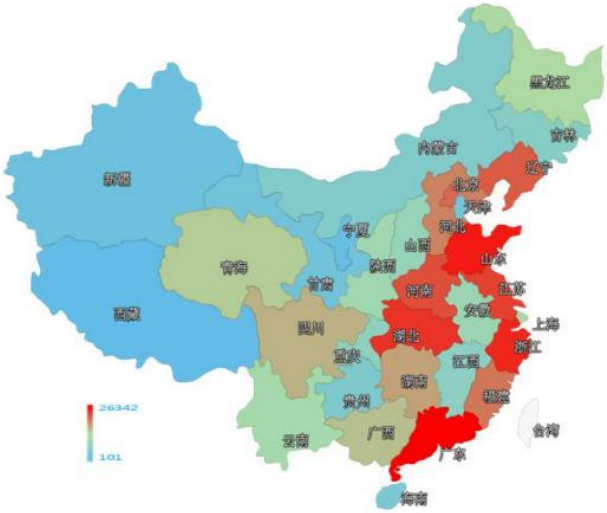
根据国家互联网应急中心最新公告数据：



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 37.7 万个，其中包括境内被木马或被僵尸程序控制的主机约 17.1 万以及境内感染飞客（conficker）蠕虫的主机约 20.6 万。





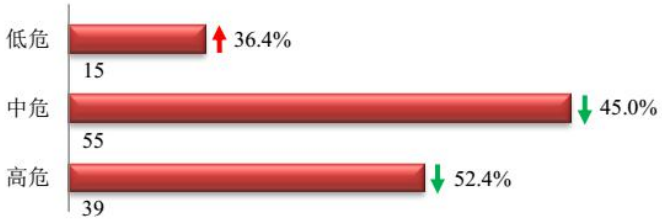
木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、山东省和浙江省。

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 2988 个；境内被植入后门的网站数量为 1802 个；针对境内网站的仿冒页面数量为 849。

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 109 个，信息安全漏洞威胁整体评价级别为高。



为什么修改 DNS 就能提高网速解决卡顿，告诉你真正的原因!

来源：智能电视网（www.znds.com） 时间：2016-3-8

经常听到说修改一下 DNS 就可以让网速飞起来，看视频卡顿也能解决，那么 DNS 到底是什么呢？那么神奇是什么原理呢？下面小编就告诉大家为什么.....

一、何为 DNS

DNS 是域名系统(Domain Name System)的缩写，它是由解析器和域名服务器组成的，即域名解析服务器，靠它把你要访问的网址找到然后把信息送到你电脑上。

光看名字就有点莫名其妙是吧？其实，DNS 的作用和我们电话的 114 查号台一样，它的作用就是把域名和 IP 地址联系在一起。事实上，每一个网站在网络上的识别标志是我们平常听到的 IP 地址，而不是什么之类的域名，但因为 IP 地址为纯数字的，很难记，所以就有专业的服务器将一个个域名和特定的服务器的 IP 地址联起来，这样，在我们上网查找网页的时候，就可以输入容易记忆的域名了。

各地运营商均有自己的 DNS 服务器，小运营商会为了利益，劫持用户 DNS，以达到域名劫持，修改注册信息，劫持解析结果来获利。最简单的例子，你输错网址的时候会弹出一堆小广告。

使用第三方公认的纯净 DNS 的好处：高速、稳定、可靠、纯净无劫持。

二、DNS 的由来

你可能会很奇怪，为什么需要 DNS 这样一种东西？为什么不一开始就使用文字形式的网络地址。其实这里有个“历史遗留问题”。在早起的网络世界里，每台电脑都只用 IP 地址来表示，那时的电脑主机很少，所以记忆起来也不难。不久，仅仅用脑子和纸笔记忆这些 IP 地址就太麻烦了，于是一些 UNIX（一种操作系统，主要用于服务器)的使用者就建立一个 hosts 对应表(这个我后面再解释)，将 IP 地址和主机名称对应起来。这样，用户只需输入电脑名字就可以代替 IP 来进行沟通了。

三、修改 DNS 能够提升网速的原因

大中型网站目前都使用 CDN 做内容分发，确保用户就近接入而提高访问速度。CDN 是怎么做到就近接入的呢？关键就在于你用的 DNS，你用哪个地方的 DNS 互联网公司基本认为你就是那个地方的宽带用户。如果你将 DNS 写错了，比如深

圳宽带用户将 DNS 填写成北京的 DNS，那么无论你访问 taobao、sina 你都被引导到北京去，网速自然慢了许多。所以说，DNS 是流量牵引器，必须选合适的。

以阿里公共 DNS 为例，它的特点就是快速、稳定和智能。

快速：阿里公共 DNS 通过 BGP anycast 技术，让用户访问到离自己较近的 DNS 集群。主动同步 com/net 域名、万网注册域名的变更，减小 ttl 时间的影响，快速访问到正确的记录。主动缓存热点域名的，提高查询 CACHE 命中率，减少递归过程，快速应答。

稳定：异地多机房高可用架构；基于 DPDK 自主研发的高性能 DNS 系统；Aliguard 多种攻击防御策略；持久化保存热点记录，当“根”或域名的权威 DNS 出现异常后，阿里公共 DNS 具备快速恢复正常访问的能力。

智能：结合阿里优质 CDN 资源和精准的 IP 地址库，让用户访问到较近的网站。

四、论坛上的教程中所提到的 DNS 地址真的是危险的吗？

以当贝市场中 DNS 优选软件中 114DNS 和阿里云 DNS 为例。

权威的 DNS 服务

抗攻击 DNS ：抵御针对 DNS 的各种攻击，采用与 DNS 根节点一样的 BGP AnyCast 架构

超高可靠：为您自有域名作权威解析，金融级安全，可提供 99.999% 超高可靠服务

智能解析：分省、分运营商解析解决南北互通问题，灵活方便的自定义分区设置

透明保护 ：充当您自有 NS 服务的挡箭牌，但将 ISP 递归 DNS 的 IP 透传给您的 NS

五、DNS 的弊端

国内有很多使用 8.8.8.8 谷歌 DNS 的用户，在这里小编谈谈谷歌 DNS 的缺点。如果你将 DNS 填 8.8.8.8，互联网公司都以为你是国外的用户，无法给你选出就近的服务器，随便给你个能用的就行了，你的网速自然慢了许多。如果你无法忍受 ISP 的 DNS 劫持，又想访问一些用 ISP 的 DNS 无法访问的网页，那可以使用

114.114.114.114，它在国内有几十个点，能引导你到最近的网站，没有 8.8.8.8 的弊端。

六、如何设置家庭网络内的 DNS

进入路由器后台，启动路由的 DHCP 设置。可以修改为 114.114.114.114 或者如图所示的阿里官方提供的云 DNS：223.5.5.5 、223.6.6.6（小编一直在用）不同路由器的方法可能有所区别，有些是叫“手动设置 DNS”。

建议大家使用 http://ip.dnspod.cn/的 DNS 本地优化，检查并设置你的计算机的 DNS 设置的优化程度；或者使用 360 安全卫士的 DNS 优选工具优化并设置本地 DNS。设置路由器 DNS，一劳永逸，整个家庭网络都可纯净上网！

小知识：中国互联网举报中心 www.12377.cn

12377 是互联网违法和不良信息举报中心设立的免费举报电话、举报网站、举报邮箱。

举报中心的工作目标是维护互联网信息传播秩序，维护网民权益，搭建公众参与网络治理的平台，建设文明健康有序的网络空间。

12377 对打击网络谣言、保护公民个人隐私、净化网络环境等工作取得了重大作用。

主要职责

接受和处置社会公众对互联网违法和不良信息的举报；指导全国各地各网站开展举报工作；指导全国具有新闻登载业务资质的网站开展行业自律；开展国际交流，向境外网站举报违反中国法律法规的有害信息。

号码作用

个人隐私维护

中国互联网络信息中心（CNNIC）发布的第 35 次《中国互联网络发展状况统计报告》显示，2014 年总体网民中有 46.3%遭遇过网络安全问题，而在安全事件中，账号或密码被盗情况最为严重，达到 25.9%。而据媒体披露，通过 QQ 群、微信等网络工具，仅花费 5 毛钱，就能买到包括姓名、电话、地址、工作单位、开户行等完整个人信息的一条信用卡开户数据。有了“12377”，可以更方便直接地向举报中心提供线索，打击侵犯公民个人隐私的非法行为。

举报违法信息

登录举报中心官网发现，除了可以通过“12377”进行个人隐私维护外，还可以对“网络敲诈和有偿删帖”、“暴恐音视频有害信息”、违反法律法规底线等“七条底线有害信息”、淫秽色情等“违法和不良信息”进行举报。

据举报中心官网数据显示，2014 年网民举报 1091762 件，其中淫秽色情有害信息 820620 件，诈骗有害信息 116716 件，暴恐音视频有害信息 23191 件，网络侵权有害信息 21277 件，其他侵害网民权益的有害信息 109958 件。

此外，举报中心还负责督促各网站快速处置违法和不良信息。据了解，2014 年百家网站共有效处置公众举报近 2.5 亿件次，其中腾讯有效处置举报信息近 2 亿件次。据了解，对于网民的举报，举报中心均及时核查并转交相关部门依法处置，有效遏制了违法有害信息的网上传播。

其他方法

根据四部委公布，举报中心另有“12321”、“12390“两个免费举报电话，另外还有传统的固定电话，除了电话举报，还有邮件方式，可以发邮件，发短信，也可以从网站上直接举报，可能部分的举报中心还提供 web 方式举报，比如从手机上网举报，有五种可行的办法。

安全警示：电脑出现来历不明的广告？小心木马病毒“幽浮”

2017-03-27　来源：　新华社

360 安全卫士发布安全播报称，近日有不少网友反映，浏览网页时屡屡被强制“插播”各种浮动广告，不胜其扰。在试图安装具有广告过滤功能的浏览器时，又被恶意软件强制关闭安装程序。经分析，这是名为“幽浮”的木马在作祟。

安全播报指出，“幽浮”木马主要靠一些盗版系统预装传播。它会霸占主页，并阻止一些安全软件和浏览器的安装，具有较强的破坏性。

“幽浮”木马的作案过程如拦路抢劫：当浏览器向服务器发送请求并接收响应，这个过程会传输数据包。“幽浮”木马则是埋藏在数据传输必经之路上的山贼，它劫持并篡改数据响应包，插入用于执行恶意推广的攻击代码。

为了不让中招者起疑心，“幽浮”会一边执行正常的网页响应，一边悄悄做着坏事。恶意代码会直接写入开机启动项以常驻系统，也就是说，“幽浮”就如它的名字一样，你的电脑一旦中招，它就像幽灵一般始终盘旋在电脑中阴魂不散。

安全专家表示，如果电脑发现经常出现来历不明的广告，浏览器主页无法正常设置，甚至无法安装新的浏览器等情况时，系统很可能已经被“幽浮”木马感染。建议中招网友尽快下载有效的安全软件进行全盘扫描杀毒。

（原标题：360 预警：“幽浮”木马强行插播广告具有较强的破坏性需警惕）

抄送：校领导