链滴

路由器弱口令引发的广告插入

作者：armstrong
原文链接：https://ld246.com/article/1377158675619
来源网站：链滴

     最近觉得家里的电脑太混乱了，装了几十个功能重叠而且各种广告弹窗的软件比如PPLive的PPAD进程，弹广告居然抢占了Play的端口。想着家里人都是直接下一步下一步的，各流氓软件捆绑软件满天飞，所以专门花了一个中午的时间重装系统，再打上个WIN7 64位的冰点还原装好了常用软件同时开启开机还原后，我以为这样就百毒不侵了。没想到才过两三天，新系统的Chroe里就广告满天飞，点都点不掉。
     在新系统上使用Chrome访问我的博客还有一些非著名网站都会被插入几层隐的全屏div，最可恶的是这些广告层不仅强迫点击弹窗，而且自身带有很淫荡的声音效果。第一次访别的网站被插入广告，我还以为是那个网站自身的广告。要知道现在的网站为了点点广告费不择手段放广告，诱导或强制点击。在别的网站出现这些广告还能理解，但当我访问自己的网站也被插播广告时候我就知道有人在坑爹了。到底谁那么没节操劫持会话，不顾网民感受，强制篡改计算机数据以盈。因为很久之前研究过电信网络插播广告的技术，而这种行为跟它非常像，所以第一时间怀疑是不是信某个旁路广告设备出现了故障。电信网络即使插播广告也没有现在这么频繁，基本达到每两次请求播一次；同时我也相信电信不会投放那么不正经的广告。要不是家里没有电信固话，我老早就想打电投诉了。
     今天实在受不了这些乱七八糟的广告，决定亲自动手定位故障点。暂且叫它故点吧，还不知道是故障还是人为原因。分析第一个现象，Chrome出现广告的概率很大，而IE和手机见过广告。可见这个广告推送是有针对性的。因此我怀疑Chrome是不是被感染了。Chrome是有腾软件管家安装的，所以为了保险起见，专门跑去Google官网下载离线版Chrome。正当准备重装Chrme，恍惚之间在网上搜到很多人也被插入了p1.0817tt.com打头的广告。网上骂声一片却没有所谓“相关机构”出来声明，也没有XX高手指出是某个地区的广告投放。网上骂战激烈，而这广告却不懂低调和收敛，所以可以断定一定不是官方行为。官方投放的广告只能默默承受，而其他行为造成的广插入完全可以追踪。
     百度百不出有效的解决方案，只有个域名屏蔽的方法。看到路由器界面，突然起前段时间网上流传的路由器弱口令导致DNS被恶意更改。我记得当时我还特意检查一遍家里路由器没被更改。而现在登入检查却发现默认DNS真的被更改成106.186.31.42和114.114.114.114。这下而易见了，电信DHCP不会分配像114.114.114.114这样的万金油DNS的，一般都会指派区域DNS以快解析速度。而106.186.31.42这是一个日本的DNS。看到被更改了默认DNS，我默默地捏了一把汗这个弱口令隐患若被有心人利用，绝不是插播广告那么简单了。比如更改路由器管理密码，提取上网号密码，提取无线密码，开放其他权限等。
     被入侵的路由器没有绑定动态域名解析，也没有开启远端管理，那么只有“内”能更改DNS设置了。这内鬼可能是电脑上的恶意软件或网页上的脚本，或者手机上的恶意软件。它要访问网关并尝试以admin:admin登录即可。或许绝大部分家庭用户都不会更改路由器密码，因此这缺陷才会影响广泛。
     之所以会出现广告，是因为使用了恶意DNS服务器，它将网站解析到广告服务，由广告服务器请求原网站数据，并在返回时插入广告代码。有点像代理技术，只不过它是邪恶的代。这也就是所谓的DNS劫持。
     这件事提醒我们，尽管是家庭网络，终端用户绝对可信，也不能向全网暴露管能力。不要嫌麻烦，一定要改密码！！！
      最后强烈要求GFW屏蔽106.186.31.42以及p1.0817tt.com。