从俄罗斯黑客 SEO 回顾启明星辰官网安全隐患问题

混习科论坛的小伙伴们大概都知道，最近论坛又迎来一只俄罗斯的黑阔小伙伴，这只小伙伴主要是做 SEO 优化的黑客，我们在文中简称黑客 I 吧。

其实这位黑客在注册习科论坛以前就已经和习科技术人员 Email 联系很久了。

这个黑客做 SEO 大多挑一些流量大的网站搞。毕竟大多数的网站都是越大防护做的越好，黑客也不是万能的。黑客 I 对这些网站的下手方式就很有意思了。小编带大家看看是怎么个有意思。

小伙伴们觉得小编这样说很没有亮点，没关系，小编刚好找到了一篇 2014 年 8 月份去美国黑帽前，上报给北京启明星辰的一篇安全报告，比较符合这种 SEO 方式的入侵手法，不同的地方在于习科毕竟不混黑产，我们想到的利用方式是挂马，但是一些专业的黑产哥就不一定了。。

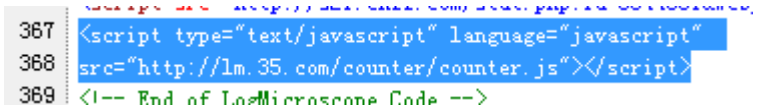
下面就来看看这篇报告的正文。

启明星辰官方网站域名：venustech.com.cn，点击百度的搜索结果进入启明星辰的官方网站，可以看到启明官方的风格，简洁不失高雅，简约而又有逼格 balabala...

有一件事情看起来好像是很诡异，明明网页已经加载完毕，但是 IE 的标题处还有有个小圈圈在不停的转呀转， 这显然是页面中有某个（些）元素没能成功加载。

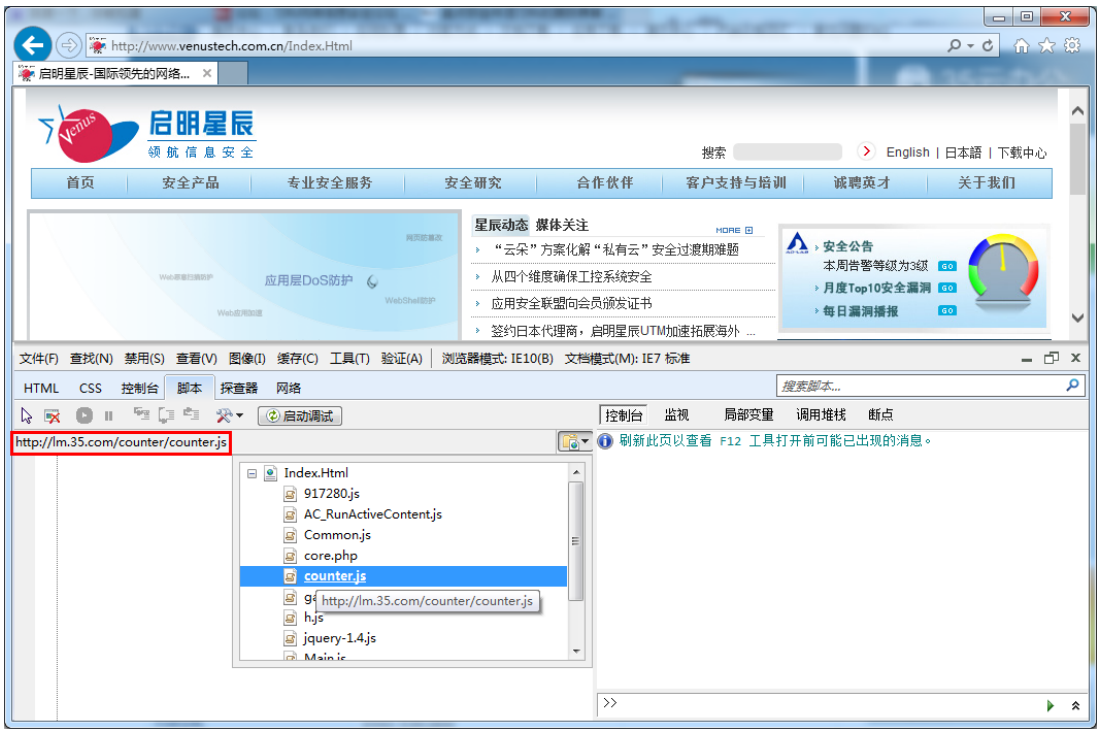
浏览器所能展现给我们的就是 HTML 内容而已，查看 HTML 源码分析网页加载的元素。由于启明官方的首页比较简洁，几秒内就可以扫一遍，特别留意了一下通过 src 引用的页面元素，发现只有一个从外部引用的 js 可能出现问题。

另外的 cnzz 和 tongji.baidu.com 的外部 js，这类统计专用的 js 一般不会出现不能加载的问题，所以这一类统计 js 忽略不算。那么也就是说，只有前面提到的外部元素是唯一有可能造成浏览器小圈圈不断转的。如下图：

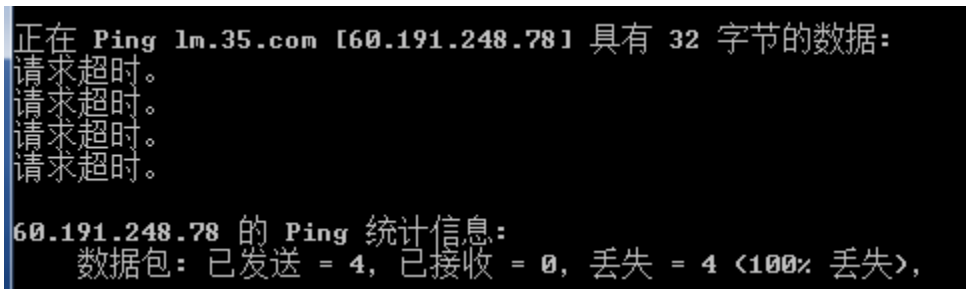


在也只是一个推断。进一步确认这个 js 文件到底是不是加载不出来，是通过 IE 的 F12 调试模式发现这个 JS 的确是加载不出来的。

如下图：



这是三五互联的二级域名，ping 了一下这个外部地址 lm.35.com，发现这个域名有解析，但没有返回 ping 响应，导致看起来整个 IP 似乎是死的(后来证实就是死的)》。



暂且先不管为什么启明官方网站会引用这样一个外部 js，从安全的角度来说，或许我会更关心我是不是能够控制这个 js 的内容？如果能够控制页面中的一个 js，那么就相当于控制了整个页面：通过 JS 文件中的代码完全可以操作各种自己想要的 HTML 和 javascript，比如页面的跳转，或者对 dom 的操作，甚至嵌入恶意挂马代码。

那么重点来了，如何控制这个 js 的内容呢？经过测试发现 lm.35.com 这个地址其实并没有提供 WEB 服务，也就是说除了域名解析到了这个 IP 以外，没有发现明显的可以利用的地方。

访客通过浏览器访问 lm.35.com/counter/counter.js 来加载页面 javascript 元素，只要让 lm.35.com/counter/counter.js 这个 WEB 地址返回我们想要的伪造内容就算达到目的。

刚才说过 60.191.248.78 这个 IP 想要直接下手入侵，恐怕有点出力不讨好。但是对于业界的小黑来说，这个时候第一时间想到的是 ARP 入手。这种欺骗方式对黑客来说屡试不爽。通过在子网中伪造网关，来达到改变数据流向的问题。通过入侵同子网的机器并进行 ARP 攻击，使全部发送往 lm.35.com（60.191.248.78）的请求全部都发送到子网中被入侵的特定机器上。然后让被入侵的子网机器反馈期望的 counter/counter.js 这个元素，这样就完美的达到了“血洗”启明星辰官网的可能。

理论看起来是很美好的，最后事实也证明确实可以这样做。查询了一下 60.191.248.x 这个 IP 段，发现大多数 IP 都提供了 WEB 服务，并且可以通过域名反查工具查到同 ip 网段的域名。

通过 60.191.248.100 这个 IP 上网站的 SQL 注入漏洞，很容易就得到了这台服务器的控制权。通过查看服务器的 IP 配置等信息，发现这台服务器很理想，而且也在同一个网段下。这就意味着可以通过 ARP 攻击欺骗网关达到将.100 服务器伪造成.78 的目的。

报告到此结束了。

其实劫持同网关的机器达到劫持页面的攻击手法已经出现很长时间了，其中也不乏很多经典案例。大多数的同网关机器劫持都是黑客挂黑页的案例，极少出现劫持站外第三方文件来挂马或者做 SEO 的案例。

论坛中的老毛子跟习科技术人员交流的时候我们曾表示他想要挂 SEO 链接的站点费力不讨好，但是他提供他经常使用的手法着实让我们醉了。果然国内和国际还有有很多区别的，无论是技术还是黑色产业。

小编写在最后

本文绝不是教唆大家参与黑色产业链，但是文中案例告诉我们，常在河边走，不可大意，还是多多提防为好。