网站将JavaScript代码插入其网页中，以利用访问者的计算资源进行加密货币挖矿。当在浏览器中打开这些网站时，JavaScript代码会在你的计算机上运行，并使用你的CPU或GPU来进行加密货币的挖掘工作。

本次对网络连接进行分析，主要使用了wireshark和Chrome的开发者模式来进行。

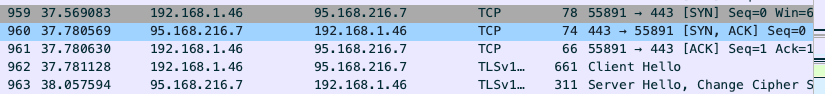
连接过程：

基本信息：

本地ip: 192.168.1.46 对端网站ip: 95.168.216.7(此ip归属地为捷克布拉格)

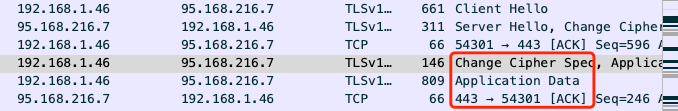
本地端口：443 网站使用端口：54891 and 54379

1. 点开网站但未运行javascript脚本



建立TCP连接--TCP三次握手，主要包含Flags[ (SYN), (SYN, ACK), (ACK) 及按照握手顺序增加的Sequence Number和Acknowledgement Number，window size 是 1448等等。

然后此时通过TLSv1.3协议（Transport Layer Security）来提供安全通信，会进行一个TLS握手的过程：client通过发送一个ClientHello消息给server，然后server从client的Hello消息中选择响应参数并发送一个ServerHello消息回应client。然后我们还会观察到这个过程中server发送了一个TCP的ACK的报文，这个“TCP ACK”用于确认客户端数据的接收，在TCP层面上建立连接确保server的消息能到达client。

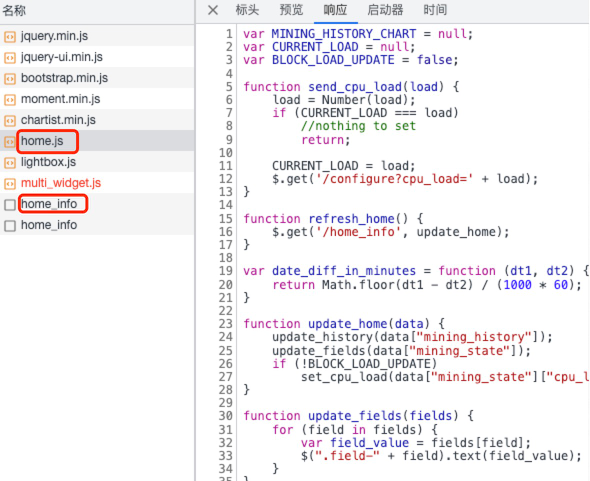
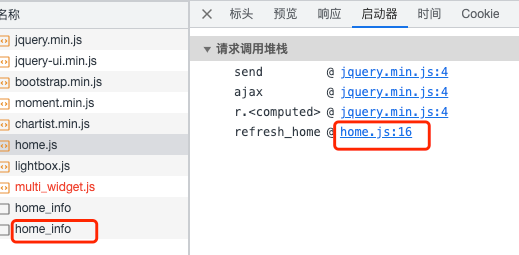


接下来在数据传输阶段TLS继续发送了“Change Cipher Spec”和“Application data”的报文，前者是通知接收方从握手模式切换到加密通信模式，后者是实际的应用的的一些数据，发送方用TLS加密他们，接收方进行解密。

1. 运行挖矿脚本开始挖矿

通过HTTP GET请求发送挖矿请求，并接收服务器（恶意网站）返回的工作信息。

从chrome浏览器可以观察到当开始执行挖矿时，从home\_info的http get请求中发现加载了一个叫home.js的脚本，点开查看响应发现是挖矿用的脚本。



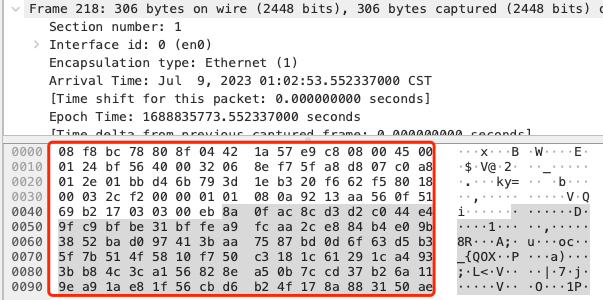
这个过程中恶意网站使用http请求与本地主机进行通行但是整个http通信过程都将在加密的TLS通道中进行因此我们只能抓到TLS加密报文。



同时，因为挖矿脚本已经被加载，因此本地主机从服务器上下载进一步的挖矿代码和配置等等，开始在本地主机进行挖矿操作（不断的向主机--矿机发送一些hash值来使用我们电脑的CPU进行计算）。

但是这些http请求使用了TLS进行了加密，因此我们无法直接看到下发的明文的hash值。只能看到经过编码的二进制数据。





在这个过程中恶意网站通过这些TLS报文向被挟持的主机下发hash值计算任务，然后主机生成相关的响应报文并发送给网站并将结果发送回恶意网站。