Rseligm2 - Russell Seligmann
Roatis2 - Michael Roatis
Jasondv2 - Jason Vo

Fake Wikipedia CryptoJacker

https://github.com/jasonvooo/cs460-project

Our idea was to create a Fake Wikipedia with a Cryptominer running in the background. The cryptominer mines cryptocurrency using a percentage of the visitors CPU. The fact that we do not ask visitor permission to use their CPU is why it is considered CryptoJacking. The aim of the project was to make the website seem as close to the actual Wikipedia as possible, so that users would not leave the page under suspicion that they were on a malicious website and therefore stay on ours for as long as possible.

To create a fake version of Wikipedia, we decided to buy an available domain that was very similar in spelling, called typosquatting, hoping that users would land their on accident. We chose to buy www.wikpdia.org for $12 off of GoDaddy. Our next move was to try to replicate the real Wikipedia as closely as possible. For this, we developed a webscraper to extract all of the html and css off of a webpage, and copy into our own file. The issue with this, however, was that after attaching the new html files to our website, the url ended in ".html". To us, this seemed like a relatively obvious give away to a visitor that the website was not what it seemed. Our work around to this was to make a script that packed the entire html file as a string, then saved it as a Javascript file. The reasoning for this was we could now implement our website using React, and thus relieve the ".html" dilemma.

Our project was not finished at just the home page. We webscraped the top 100 visited pages on Wikipedia, and added those routes to our project. This provided plenty of content for users to stay on the website for long lengths of time while we mined cryptocurrency using their CPU. In order to highlight our webscraped pages, we webscraped Wikipedia's top 100 searched pages article, and used that as our homepage. We then routed the links on our homepage to redirect to all the pages we had just made.

One of our last issues was that obviously Wikipedia has more than 100 pages, what happened if a user clicked any of the links that took them to a less common page? For this, we webscraped Wikipedia's 404 not found page, and had any links not pointing to our top 100 pages link to that 404 page. The only options on the 404 page took us back to the home page.

Lastly, we attached a mining tool called Coinimp to the root of our project. Due to reacts DOM, we only had to include the script once at the root in order for it to trickle down to all the pages and components. Attached below is our wallet after running for about 24 hours. Although we cannot post a link to the wallet dashboard for you to see the current balance, you should still see a very noticeable decrease in computing power while on the website. Our throttle down is at 70% meaning the mining is using up to 30% of the visitor CPU. This website was made purely for educational purposes, but it shows how easily a website could be using just a small percentage of your CPU without you knowing.

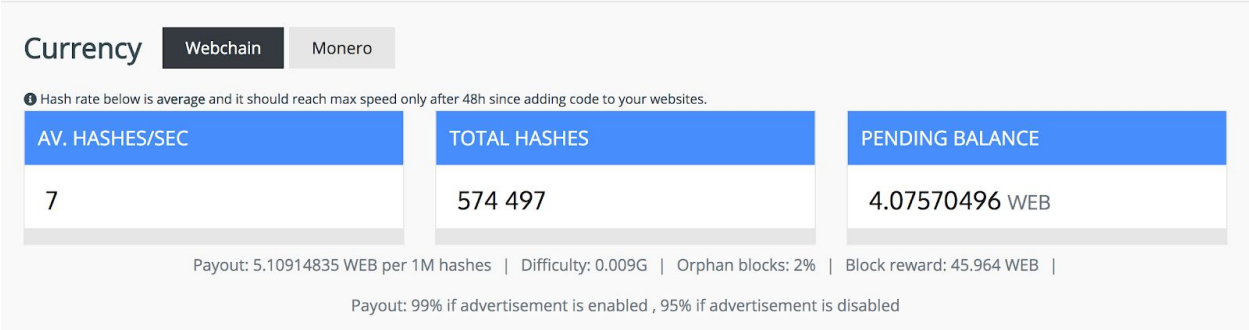

Figure 1: CoinImp balance after about 24 hours. After just 24 hours, we can see that we have accumulated many hashes from visitors. Since Webchain is almost worthless at the moment, we calculated at 70% throttle down, it would take 1000 visitors spending 24 hours a day on the page in order to see a revenue of around $1. This is not an impressive number, but imagine if a website like Youtube that gets millions of daily visitors was using just a small percentage.