CERT-EU Security Advisory 2017-024

Increased Use of Browser Cryptojacking

November 15, 2017 — v1.0

History:

- *15/11/2017 — v1.0 – Initial publication*

Summary

Since summer 2017 – mostly due to significant increase of the price of Bitcoin – browser-based mining services have increased their popularity [1]. By providing easy to use JavaScript libraries they allow website owners to increase their revenues by hijacking visitors' browsers for cryptocurrency mining. The browser-based mining service will then award part of the profit to the site owners.

Website owners may voluntarily add the browser-based mining services code to their pages, but malicious actors could also exploit vulnerable websites and add JavaScript code to hijack visitors CPUs [3, 4].

As cryptocurrency mining is extremely resource-consuming, it may impact the performance of the visitors' browser and operating system [1], as well as waste electricity on behalf of the owners of the infrastructure.

Technical Details

The most popular service today providing browser-based mining libraries is **Coinhive**, but other services are being created to follow the trend. Based on the Coinhive documentation [5], in order to integrate Coinhive mining on websites, the owner (or malicious actor) needs to add some JavaScript code. The first step is loading the Coinhive library:

```
<script src="https://coinhive.com/lib/coinhive.min.js"></script>
```

Then loading the Coinhive user key and starting mining:

```
<script>
 var miner = new CoinHive.Anonymous('YOUR_SITE_KEY');
 miner.start();
</script>
```

A more complex code is available for users willing to fine-tune the way visitors are mining.

In this version of Coinhive library, no permission is asked to the visitors. Coinhive also proposes another version requiring an explicit opt-in from the end-user.[1] We may assume that this option will not be the one exploited by malicious actors.

In both cases, blocking access to the domain hosting the library will prevent the mining from starting. Although Coinhive is the most popular provider at the moment, others exist. A list of other known mining domains is also available in [6]. While most of them currently do not provide infrastructure for browser-based mining, many already do. Others allow for mining with dedicated miners and may provide browser-based mining capabilities in the future.

Recommendations

Most ad-blocker plugins for browsers, as well as some of the anti-virus products, are blocking known browser-based mining services.

For large-scale network, it is recommended to block known mining domains [6], unless the users are explicitly allowed to participate in cryptocurrency mining.

References

[1] https://www.bleepingcomputer.com/news/security/coinhive-is-rapidly-becoming-a-favorite-tool-among-malware-devs/

[2] https://researchcenter.paloaltonetworks.com/2017/10/unit42-unauthorized-coin-mining-browser/

[3] https://gwillem.gitlab.io/2017/11/07/cryptojacking-found-on-2496-stores/

[4] https://blog.sucuri.net/2017/09/hacked-websites-mine-crypocurrencies.html

[5] https://coinhive.com/documentation/miner

[6] https://github.com/ZeroDot1/CoinBlockerLists

[1] `https://authedmine.com/lib/authedmine.min.js`