

Hacker hijack CoinHive DNS to dig virtual money with thousands of websites

When you heard about ransomware Bad Rabbit, did you think that was the worst thing that the security has recently received? No, here it is.

When you heard about ransomware Bad Rabbit, did you think that was the worst thing that the security has recently received? No, here it is.

CoinHive, a web service that allows the website to embed JavaScript to take advantage of the CPU of Monero peach site visitors, has been hacked. An unidentified hacker has hijacked Coinhive's CloudFlare account, allowing editing DNS servers and replacing Coinhive's JavaScript code being embedded into thousands of websites with an infected version.

`https://coin-hive[.]com/lib/coinhive.min.js`

Get the password from the data leak

Hacker reused passwords leaked from the Kickstarter leak in 2014. DNS records for coinhive.com were modified to redirect requests to coinhive.min.js to another server containing the malicious version of the JavaScript file. Thousands of pages using Coinhive's script were tricked for at least 6 hours when downloading the Monero island code for hackers.

Your website may be digging money for strangers

Coinhive received attention after the world's largest torrent download site, The Pirate Bay, was discovered using a virtual money digging tool on its browser. Since then, thousands of other websites have also started using Coinhive to utilize the visitor's CPU and dig virtual money as another way to make money.



How many Coinhive words are earned in the pocket of hackers

Even hackers use Coinhive to check money from websites they hacked by silently injecting the script. Now the company is looking for ways to compensate for losses caused by this case.

How to prevent websites from exploiting your CPU to dig virtual money

Many anti-virus software, including Malwarebytes and Kaspersky, started blocking the script to prevent the user's computer CPU from being exploited to dig virtual money.

You can also install open source browser utilities like No Coin or minerBlock to block virtual money digging tools like Coinhive.

See also: [How to block websites using your CPU to dig virtual money](#)

You finished reading the article "**Hacker hijack CoinHive DNS to dig virtual money with thousands of websites**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.