# Proposal; Detecting Mining Script on Web Browser

Hyunki Kim, Junghwan Park, Juhyung Song, Seonyong Jeong

Graduate School of Information Security
Korea Advanced Institute of Science and Technology
Yuseong, Daejeon
$\{$ *saykim*0727, *ahnmo*, *sjh*8563, *s.jeong* $\}$ @ *kaist.ac.kr*

***Abstract*—As a cryptocurrency comes up, a lot of people started the cryptocurrency mining by using a mining programs in their computers. However, if a user executes the mining programs in his local computers, his computers are overloaded by using CPU, GPU and so on. So, many people thought a way how to mine without damaging their computers. As services like CoinHive are made, many sites have consisted of web-based mining codes to use a visitor's computer resources. Using these services, web administrator involved a javascript mining code instead of advertisement or hide a javascript mining code to run in background. Visitors can't know that the web administrator uses their computer resources to mine the cryptocurrency in visitors computer. Because some people thought that the web mining services were morally problematic, several programs are made to detect and prevent these services from mining. However, most of the programs detect javascript mining code based on blacklist which have some specific domain. This way is practically impossible to detect mining codes, because most of web administrators can bypass a anti mining programs. So we suggest a practical programs to prevent mining code from working on web browser and a way to detect malicious codes by analyzing them.**

## I. Introduction

From long ago, people get users personal secret information by hacking and get profits by selling them. For example, in 2016, Mirai botnet that composed primarily of embedded and IoT devices infects others IoT devices and performs DDOS attack. and a number of botnet is made like Mirai[1-2]. On the other hand, some people get a profit by lending their botnet to someone who need them[1-3]. Also, Ransomware, which has been a hot issue in recent years such as Trojan.Gpcoder in 2005 and recent 2017 WannaCry or Scarab, break users computer down or encrypt all files and get a profit from users by decrypting encrypted files.[1-1] In recent years, the cryptocurrency has become an issue, so they foucs on the cryptocurrency.

Starting with Bitcoin of Satoshi Nakamoto in 2009, many the cryptocurrency is made by programer like Ethereum, Ripple, Litecoin, and so one. Th cryptocurrency is electronic currency mined by algorithms using blockchain based on cryptology. The mining process is called Proof-of-work. The goal of 'proof-of-work' is finding nonce value which makes required zero-bits after hashing. By incrementing nonce in the block, they calculate iteratively to find the value gives the block's hash the required zero bits. the cryptocurrency is a platform supporting electronic transactions without relying on trusted third party. All transactions are announced to the public, all users guarantee validation of transaction. So users can transact all over the world with minimize a fee and the speed of transaction get fast[2-1]. Besides, the cryptocurrency wallet has advantage, against general bank account. Bank account directly linked to the owner's physical identity but the cryptocurrency wallet can be generated anytime. So, it is difficult to find real owner from digital wallet[2-2]. As the cryptocurrency become popular for this reason, many people have mined the cryptocurrency by using the mining programs to make a progit in their computers. However, their computers have a problem while the mining programs working with a computer resources which are CPU, GPU, and so on. Because a heat which is made by the computer resources have a bad effect on a computers like IC damage or processing speed down[3]. Therefore some computer expert give a warning that people should not mine the cryptocurrency in desktop or labtop. After taking the advice, the people found ways to do mining without the problems. For these reason, a web-based javascript mining codes which mine the cryptocurrency using visitor computer resources on website are developed.

The first javascript mining codes were Jsminer and Bitcoinplus In 2011. they were developed to mine the cryptocurrency instead of advertisement, but they were not used often because they were slow[7]. CoinHive, which was developed In 2017, is suitable for CPU because it mines Monero. Thus, it has been used by many people on their website to mine Monero using visitor resources. Actually, it is illgal that web administrator mines cryptocurrency using visitor's computer resources without their agreement. However. most of sites cheat visitors to mine using clickjacking or mine in background secretly.

To detect these sites, several anti mining programs were developed like Nocoin[4], MinerBlock[5], Coin-Hive Blocker[6]. these programs are extension in Chrome or Firefox and detect malicious mining sites based on blacklist which have at least 100 domain urls in real-time. MinerBlock not only domains blacklist, but also checks DOM element to detect mining sites. Also Coin-Hive Blocker check CPU usage. However, these extensions have problems to detect mining sites. They basically check the mining site based on the blacklist, so some computer experts can bypass them simply by using a domain that is not in the blacklist. Also, the experts can bypass the Dom blacklist and CPU usage inspection. So we will explain in detail in chapter 3 To prevent a lot of sites from mining, we will develop Chrome extension with domains blacklist that we collected. Also, our extension will check DOM elements with dynamic analysis and monitor if CPU usage is exceeded. As a result, we propose more powerful extension than existing others.