

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

{ *saykim0727, ahnmoo, sjh8563, s.jeong* } @ *kaist.ac.kr*

Abstract—As a cryptocurrency comes in, a lot of people started a cryptocurrency mining by using mining program in their computers. But if a user execute a mining program in local computers, his computers are overloaded excessively using CPU, GPU and so on. So, Many people thought a way how to do mining without damaging to their computers. As services like CoinHive are made, many sites have consisted of web-based mining codes to use a visitor computer resource. To use the 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 use visitors's computer resource to mine a cryptocurrency in visitors computer. Because Some people thought that the web mining services were morally problematic, several program are made to detect and prevent these situations. However most of the program detect javascript mining code based on blacklists that have some specific domain. This way is practically impossible to prevent mining codes because most of web admin can bypass the anti programs. So we suggest a practical anti program to prevent mining code on web browser and a way to detect malware mining code with a analysis of mining code.