정 보 보 호 학 회 지
제28권 제3호, 2018. 6

크립토재킹 연구 동향

최 원 석*, 김 형 식**, 이 대 화***

요 약

암호 화폐가 다양해지면서 암호 화폐를 채굴하는 방법 또한 다양한 방향으로 생겨났다. CyptoNote라는 프로토콜을 이용한 암호 화폐 중 하나인 모네로를 채굴할 때 메모리를 중점적으로 사용하도록 되어 있다. Coinhive는 광고 없이 수익을 내기위한 방법으로 웹브라우저를 이용한 모네로를 채굴하는 API를 만들었다. 하지만 본래의 목적과 다르게 API를 악의적으로 사용하여 웹브라우저 방문자의 동의 없이 채굴하는 공격인 크립토재킹이 증가하게 되었다. 이러한 공격을 막기 위해 브라우저 확장 어플리케이션이 등장하였으나, 공격자는 이를 우회하기 위해 자바스크립트 난독화를 사용하고 있다. 본 논문에서는, 크립토재킹에 대한 연구동향을 분석하고자 한다.

Ⅰ. 서 론

2009년 비트코인이 등장하면서 거래에 대한 익명성 보장을 내세우며 암호 화폐는 급진적으로 증가하기 시작하였다. 암호 화폐 거래가 이루어지기 위해서는 채굴자(miner)가 채굴(mining)이라는 것을 해야 한다. 채굴을 성공하면 암호 화폐 거래가 이루어지고, 채굴자는 그에 따른 보상을 받게 된다. 채굴로 얻는 수익이 상당하기 때문에 많은 사람들이 채굴을 위한 장비를 구하기 시작했다. 비트코인의 초기 채굴 장비는 CPU이었으나, 전기 소모량에 비해 채굴량이 많지 않기 때문에 GPU로 채굴하는 채굴자들이 많아졌고, GPU 또한 효율이 좋지 않기 때문에 최종적으로 반복적인 작업을 수행하는데 있어 최적화된 ASIC을 이용한 채굴로 넘어가게 되었다. CryptoNote라는 프로토콜을 사용하는 모네로는 비트코인과 다르게 CryptoNight라는 CPU 기반의 알고리즘을 사용한다. 이런 특징 때문에, 모네로는 특별한 장비 없이 CPU만 있으면 쉽게 채굴을 할 수 있다는 장점이 있다. Coinhive는 이런 모네로의 장점을 이용해 누구나 쉽게 모네로를 채굴할 수 있게 웹브라우저를 이용한 채굴 API 제공한다. 홈페이지 관리자는 Coinhive가 제공하는 자바스크립트 코드를 넣으면 광고의 수익없이 방문자를 통해서 모네로 채굴로 인한 수익을 얻을 수 있다. 하지만 본래 의도와 다르게 공격자가 사용자들이 많이 방문하는 사이트를 해킹하여 모네로 채굴 스크립트를 웹페이지에 심어 넣어, 방문자들의 동의 없이 공격자를 위해 모네로를 채굴하는 크립토재킹이 증가하기 시작했다. 웹페이지 방문자는 인식하지 못한 채 본인의 CPU를 사용하여 남을 위해 채굴을 하게 되는 것이다. 웹브라우저에서의 크립토재킹을 막기 위해 NoCoin, Minerblock같은 브라우저 확장 어플리케이션이 등장했으나, 현재는 단순히 하드코딩 된 스크립트를 탐지하는 기술뿐이라서 자바스크립트 코드를 난독화하면 쉽게 우회 할 수 있는 단점이 있다.

본 논문에서는 우선, 암호 화폐를 채굴하기 위해 사용되는 여러 장비들에 대해 특징을 설명하고 각 채굴 방식에 따른 장점과 단점을 2장에서 설명한다. 다음으로, 3장에서는 웹브라우저를 이용한 채굴에 대해 설명하고 웹브라우저 채굴에 적합한 모네로(monero)라는 암호 화폐에 대하여 설명한다. Coinhive에 대해서 설명하고 Coinhive를 이용해 웹페이지 방문자 동의 없이 방문자의 자원을 이용해 채굴을 하는 공격인 크립토재킹에 대하여 정리한다. 4장에서는 크립토재킹을 막기 위해 사용하는 브라우저 확장 어플리케이션에 대해 설명

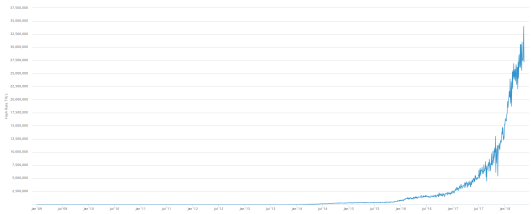
이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2017-0-00545, 암호화된 데이터상의 기계학습 라이브러리 설계 및 활용기법 연구)
* 성균관대학교 전자전기컴퓨터학과 보안공학연구실 (wschoi93@skku.edu)
** 교신저자, 성균관대학교 전자전기컴퓨터학과 보안공학연구실 (hyoung@skku.edu)
*** 기타 공저자, 성균관대학교 전자전기컴퓨터학과 보안공학연구실 (dhwa1206@skku.edu)

하고, 이것을 회피하기 위해 사용하는 자바스크립트 난독화에 대해 설명한다.

Ⅱ. 암호 화폐 채굴의 진화

암호 화폐에서 중요한 역할로 자리 잡고 있는 것 중 하나는 바로 암호 화폐 채굴(mining)이다. 채굴자(miner)는 채굴을 하여 암호 화폐 트랜잭션을 성사시켜 줄 때 수수료를 받으면서 별도로 그에 따른 보상도 받게 된다. 올해 기준으로, 채굴자가 비트코인을 채굴에 성공하면 12.5 비트코인과 약간의 수수료를 얻게 된다. 이는 한화 가격으로 1억 정도의 수익이기 때문에 채굴자들 사이에서 채굴 경쟁이 치열해 질 수 밖에 없다. 채굴자들은 보다 빠른 채굴을 위해 컴퓨터의 성능을 높이는데 관심을 가지게 되었고, 점차 채굴을 하는데 사용하는 장비를 바꾸기 시작하였다. 장비는 채굴을 위해 최적화 되었고, 그 결과 비트코인의 경우 한 블록을 생성하는데 필요한 해시 속도가 급격하게 증가하였다.

본 장에서는 각 장비를 이용한 채굴에 대한 특징과 장단점에 대해서 조사를 진행하였다.



〔그림 1〕 2018년까지의 비트코인 채굴에 필요한 해시파워

2.1. CPU 기반 채굴 방식

초기에 비트코인을 채굴을 할 수 있는 유일한 방법은 자신의 Central Processing Unit(CPU)와 비트코인 코어 지갑을 사용하는 방법뿐이었다. 비트코인 코어 지갑은 CPU 자원을 사용하여 비트코인을 채굴을 할 수 있게 구현되어서 채굴하는 방법이 굉장히 쉽다. CPU를 통한 채굴은 자신의 컴퓨터 외에 다른 특별한 하드웨어를 필요로 하지 않는다는 장점이 있다. 하지만, CPU 채굴은 사용자가 사용하는 전기 사용량만큼의 채굴량이 나오지 않기 때문에 CPU를 이용한 채굴은 더 이상 이익이 되는 방법이 아니다.

2.2. GPU를 이용한 채굴 방식

처음으로 Graphics Processing Unit (GPU)를 이용한 채굴 방법은 201년 6월 18일 ArtForz라는 사람이 시작했다. 해시를 반복적으로 하는 일에 있어서, GPU는 CPU보다 높은 효율을 갖기 때문에 많은 채굴자들이 GPU를 이용한 채굴 도구를 만들었다. GPU 또한 거의 모든 데스크톱에 있으므로 채굴을 이해하는데 유용하지만, CPU와 마찬가지로, 갈수록 GPU를 이용해서 채굴을 하는 전기 값이 수익을 넘어서기 때문에 효율적인 채굴방법이 아니다.

2.3. FPGA를 이용한 채굴 방식

Filed Programmable Gate Array(FPGA)는 특별한 목적의 소프트웨어를 프로그래밍 한 기술이다. 예를 들어, FPGA 채굴이 진행되는 동안 채굴 소프트웨어는 필요한 작업을 생성하고 FPAG 해시들은 가능한 해결책을 찾는다. 따라서 요구되어지는 업무에 대하여 하드웨어를 최적화 시킬 수 있기 때문에, GPU보다 성능이 더 빠르다는 이점이 있다.

2.4. ASIC를 이용한 채굴 방식

Application Specific Integrated Circuits (ASIC) 은 한 목적을 위해 만들어진 마이크로프로세서이다. 비트코인 채굴의 경우 비트코인에서 사용되어지는 SHA-256 해시함수를 수행하기 위해 만들어졌다. ASIC은 다른 하드웨어 채굴보다 명확한 이점을 가지고 있다. ASIC은 후보 블록의 해싱을 반복하기 위해 특별하게 설계되었다. ASIC은 CPU, GPU, FPGA 보다 빠르게 채굴을 할 수 있기 때문에 가격이 비싼 단점이 있지만, 채굴자들 사이에서 가장 많이 사용되고 있다.

Ⅲ. 브라우저를 이용한 암호 화폐 채굴

3.1. CryptoNote Protocol

CryptoNote[4]는 개인 정보 보호를 지향하는 암호 화폐 프로토콜로 발신자의 공개키를 여러 다른 공개키와 그룹화 하여 함께 보내는 방식을 통해 익명성을 보

장한다. CryptoNote는 CryptoNight라는 알고리즘으로 Proof of Work를 수행하여 새로운 블록을 생성한다. CryptoNight 알고리즘은 Proof-of -Work를 수행할 때 64바이트의 새 블록을 만들기 위해서 이전의 모든 블록에 대한 정보가 있어야하기 때문에 메모리가 중점적으로 사용될 수밖에 없다. CryptoNight 는 한번 알고리즘이 실행될 때 2Mb 크기의 용량을 필요로 한다[5]. 메가바이트의 메모리 사용은 ASIC pipeline에 맞지 않기 때문에 ASIC 방식보다는 Memory-on-chip 방식을 갖춘 CPU에서 높은 성능을 보인다. CryptoNote 프로토콜 기반의 대표적인 암호 화폐는 2014년 개발된 모네로이다[6].

3.2. Coinhive

Coinhive[3]는 웹브라우저를 이용하여 모네로의 Proof of Work를 수행하여 새로운 블록을 생성하는 API를 제공한다. 웹브라우저에 방문하는 시간에 비례하여 Proof of Work를 수행하며 초기 광고 없이 수익을 내기위해 만들어졌다. 자바스크립트 코드로 사용되는 Coinhive API는 단 4줄만으로도 모네로를 채굴할 수 있다.

또 다른 방법인 CAPTCHA용 Coinhive API는 웹브라우저 로그인 시 CAPTCHA 버튼을 눌러 일정시간만 Proof-of-Work를 수행하게 한다. 현재 Coinhive의 Hashrate는 Intel i7 CPU 기준 90h/s 가 최대로 Native의 Hashrate인 140h/s에 도달하기 위해 현재도 개발 진행 중이라고 한다.

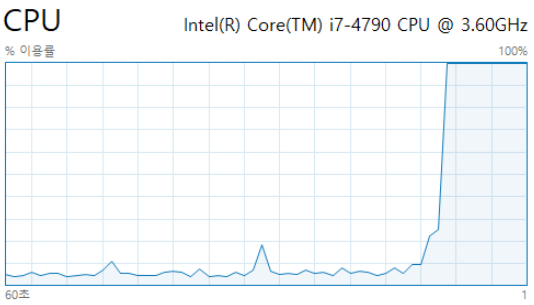
```
<script src="https://authedmine.com/lib/authedmine.min.js"></script>
<script>
    var miner = new CoinHive.Anonymous('YOUR_SITE_KEY', {throttle: 0.3});

    // Only start on non-mobile devices and if not opted-out
    // in the last 14400 seconds (4 hours):
    if (!miner.isMobile() && !miner.didOptOut(14400)) {
        miner.start();
    }
</script>
```

〔그림 2〕 coinhive API 자바스크립트 코드 예시

3.3. 크립토재킹

크립토재킹[7]이란, 암호 화폐(cryptocurrency)와 납치(hijacking)의 합성어로, 암호 화폐의 가치가 상승하면서 새롭게 등장한 사이버 공격이다. 크립토재킹은 사용자의 동의 없이 사용자의 컴퓨터 자원을 이용하여 암호 화폐를 채굴하는 행위이다. 기존의 암호 화폐 채굴과는 다르게 브라우저를 접속하기만 해도 CPU를 사용하여 암호 화폐를 채굴할 수 있다. 모네로 암호 화폐가 생기면서, 브라우저를 이용한 채굴방식이 급속도로 증가하기 시작했다. 이에 따라서, 홈페이지 관리자가 방문자의 동의 없이 페이지에 채굴하는 스크립트를 넣어 방문자의 CPU를 악의적으로 이용하는 사례도 생겨났다. [그림 3]과 같이 CPU의 사용량이 급격하게 증가하는 것을 볼 수 있다. 홈페이지 방문자는 아무것도 모른 채 홈페이지 관리자를 위해 채굴을 하게 되는 것이다. 게다가, 악성 공격자는 사용자들이 많이 방문하는 웹브라우저를 공격하여 본인의 주소로 채굴하는 스크립트 코드를 넣는 공격도 많이 생겨났다.



〔그림 3〕 채굴 스크립트가 삽입된 웹브라우저를 접근할 때 급격하게 증가하는 CPU 사용량

Ⅳ. 크립토재킹 방어 솔루션 및 회피기법

웹브라우저 방문자가 웹브라우저를 방문했을 때, 이 웹브라우저가 채굴 자바스크립트 코드가 있는지 확인하기는 어렵다. CPU사용량을 웹브라우저 방문할 때마다 확인할 수 없기 때문에 방문하려는 웹브라우저가 크립토재킹을 시도하는지 안하는지 검사해주는 크립토재킹 방어 솔루션이 필요하다. 본 장에서는 크립토재킹 웹사이트를 검사하는 대표적인 브라우저 기반 확장 어플리케이션들을 소개한다.

4.1. 크립토재킹 방어 솔루션

NoCoin[1]은 개발자들이 스스로 블랙리스트를 만들

어서 암호 화폐 채굴을 막는 브라우저 확장 어플리케이션이다. 현재 크롬, 파이어 폭스, 오페라에서 제공되고 있고, GitHub에 오픈소스로 소스코드를 찾을 수 있다. NoCoin은 개발자들이 만든 블랙리스트를 blacklist.txt에 저장 후 리스트에 있는 URL을 사용하는 웹브라우저에 대하여 차단한다. NoCoin은 채굴 스크립트가 존재하는 3,311개의 웹사이트를 발견했다.

Minerblock[2]은 NoCoin과 같이 개발자들이 블랙리스트를 만들어 웹브라우저를 차단하는 브라우저 확장 어플리케이션이다. 크롬, 파이어 폭스, 오페라에서 사용할 수 있고, 3,235 개의 웹사이트가 채굴 스크립트가 있는 것을 발견했다.

Mining Hunter[8]는 웹페이지에서 웹 소켓 트래픽을 검사하는 크롬 개발자 도구 프로토콜 기반으로 만들었다. 정적으로 분석하는 위의 두 어플리케이션과 다르게, Mining Hunter는 동적으로 분석하기 때문에 난독화 같은 크립토재킹 방어솔루션 회피기법에 대한 탐지율이 좋다.

4.2. 크립토재킹 방어솔루션 회피기법

악성 채굴자가 여러 웹브라우저에 채굴 스크립트 코드를 넣어 사용자의 컴퓨터 자원을 탈취하는 것을 막기 위해 NoCoin이나 Minerblock 같은 브라우저 확상 어플리케이션이 등장했다, 그러나 이러한 어플리케이션은 단순히 하드코딩 되어있는 스크립트를 감지하는 데에만 신경을 쓰기 때문에 약간의 변조만 하면 쉽게 탐지를 우회할 수 있다. 현재 사용하고 있는 난독화 기법으로 onload, eval과 같은 자바스크립트 이벤트 함수를 이용한 코드 실행과 [그림 4]과 같이 문자열 인코딩으로 자바스크립트 코드를 난독화하는 기법이 있다. 최근에는 난독화에서 복호화를 어렵게 만들기 위해 암호화키를 서버에 별도로 저장하거나 자신만의 인코딩 함수를 만들어서 사용하는 방법도 있다. 또한, Phoenix, Exploit Toolkit, NeoSploit Exploit Toolkit 같은 자바스크립트 난독화 전용 도구도 있어 별도의 자바스크립트를 난독화 하는데 사용된다[9].

```
eval(function(p,a,c,k,e,r){e=function(c){return c
    .toString(a)};if(!''.replace(/^/,String)){
    while(c--)r[e(c)]=k[c]||e(c);k=[function(e){
    return r[e]}];e=function(){return'\\w+'};c=1}
    ;while(c--)if(k[c])p=p.replace(new RegExp('\\
    b'+e(c)+'\\b','g'),k[c]);return p}('4.8=9(
    a){1 b=e f();1 c=4.g("*");5(1 i=0;i<
    c.6;i++){2(c[i].3.h(" ")>=0){1 d=c[i].3.k("
    ");5(1 j=0;j<d.6;j++){2(d[j]==a){b.7(c[
    i])}}}}1 2(c[i].3==a){b.7(c[i])}}m b}',23,23,'
|var|if|className|document|for|length|push|getEle
mentsByClassName|function|||||new|Array|getElemen
tsByTagName|indexOf|||split|else|return'.split('|
    '),0,{}))
```

〔그림 4〕 난독화 된 자바스크립트 코드

Ⅴ. 결 론

본 논문에서는 암호 화폐를 채굴하기 위한 여러 장비에 대하여 분석하였다. 모네로의 등장에 Coinhive라는 웹브라우저를 이용한 채굴 방법이 생겼고, 이를 악용한 크립토재킹을 분석하였다. 후에 크립토재킹을 막기 위한 브라우저 기반 어플리케이션을 분석했지만, 단순히 자바스크립트 코드를 감지하는 단점 때문에 자바스크립트 난독화를 이용하면 쉽게 회피할 수 있는 결론을 얻을 수 있었다. 따라서 향후에 자바스크립트 난독화를 한 크립토재킹을 감지하기 위한 솔루션이 요구 되고, 단순히 자바스크립트 코드를 감지하는 것이 아닌 네트워크 단위의 분석으로 크립토재킹을 방어하는 연구가 요구된다.

참 고 문 헌

[1] Keramidas, R. NoCoin Browser Extension. https://github.com/keraf/ NoCoin.

[2] Belkacim, I. MinerBlock Browser Exten- sion. https://github.com/xd4rker/Miner Block.

[3] Coinhive. Coinhive monetize your business with your users cpu power. https://coinhive.com/, 2017.

[4] CryptoNote Technology. An open-source technology and concepts for the cryptocurrencies of the future. https://cryptonote.org/whitepaper.pdf

[5] Seigen, Jameson, M., Nieminen, T., Neocortex, and Juarez, A. M. CryptoNight Hash Function, 2013. https://cryptonote.org/cns/cns008.txt.

[6] Monero. MONERO private digital currency. https://getmonero.org/

[7] European Union Agency for Network and Information Security (ENISA). Cryptojacking -

Cryptomining in the browser, 2017. https://www.enisa.europa. eu/publications/info-notes/cryptojackingcryptomining-in-the-browser.

[8] Julian, R., Sebastian, S., Tobias, D., Robert, L., Damjan, B., Gerhard, P and Hyoungshick, K. The Other Side of the Coin: A Framework for Detecting and Analyzing Web-based Cryptocurrency Mining Campaigns. In *International Conference on Availability, Reliability and Security (2018)*, Hamburg, Germany.

[9] 지선호, 김휘강. 난독화된 자바스크립트의 자동 복호화를 통한 악성코드의 효율적인 탐지 방안 연구. 정보보호학회논문지 (2012). 22(4), 869-882.

〈저 자 소 개〉

최 원 석 (Won Seok Choi)
학생회원

2018년 2월 : 성균관대학교 소프트웨어학과 학사 졸업
2018년 3월 : 성균관대학교 전자전기컴퓨터공학과 석사과정
관심분야 : Blockchain, Security Engineering, Usable Security

이 대 화 (Daehwa Rayer Lee)
학생회원

2017년 8월 : 용인대학교 컴퓨터과학과 학사
2018년 3월~현재 : 성균관대학교 전자전기컴퓨터공학과 석사과정
관심분야 : Blockchain, Usable Security, Security Engineering

김 형 식 (Hyoungshick Kim)
종신회원

1999년 2월 : 성균관대학교 정보공학부 학사
2001년 2월 : KAIST 컴퓨터 과학과 석사
2012년 2월 : University of Cambridge 컴퓨터공학과 박사
2013년 3월~현재 : 성균관대학교 전자전기컴퓨터공학과 조교수
관심분야 : Security Engineering, Usable Security. Social Computing