

2019년도
한국정보보호학회

학술발표대회 논문집

- 일시 : 2019년 2월 14일(목)
- 주최 : 한국정보보호학회 영남지부/충청지부
- 주관 : 부산가톨릭대학교
- 후원 : (주)오픈링크시스템
(주)대신정보통신 (주)아이티센
- 장소 : 부산가톨릭대학교

행 사 일 정

■ 행 사 장 : 부산가톨릭대학교 정보공학관

□ 2월 14일(목요일)

시 간	행 사 내 용					
12:00- 13:30	등 록					
	부산가톨릭대학교 정보공학관					
	2층 202호	2층 205호	2층 206호	3층 302호	3층 305호	3층 306호
13:30- 14:30	A- 1 IoT/CPS /클라우드 보안	B- 1 IoT/CPS /클라우드 보안	C- 1 블록체인 /금융 보안	D- 1 인공지능 보안	E- 1 컴퓨터보안	F- 1 정보보호관리/정책 기타정보보호
14:30- 15:00	휴 식					
15:00- 16:00	A- 2 IoT/CPS /클라우드 보안	B- 2 모바일 보안 디지털포렌식	C- 2 블록체인 /금융 보안	D- 2 인공지능 보안	E- 2 컴퓨터보안	F- 2 컴퓨터보안
16:00- 16:30	휴 식					
16:30- 18:00	□초청강연: 2019년 보안 트렌드 (장소: 대학본부관 103호 대강의실) - 강 사: 이호웅 안랩 CTO □한국정보보호학회 영남지부 총회 및 폐회					

손현민, 박민규, 최현택, 이현철 (대신정보통신) -----	36
• 복합체 기반 폴딩 Sbox 구현 최병준, 박종선 (고려대) -----	39
• 비트 시리얼 구조를 적용한 ARIA 암호화 하드웨어 조정훈, 김보훈, 박종선 (고려대) -----	42

Session B-2 모바일 보안 디지털포렌식 (정보공학관 205호)

15:00 ~ 16:00 좌장 : 이만희 (한남대)

• 역전파 신경망 기반의 안드로이드 악성코드 탐지 시스템 Afifatul Mukaroh, 강효은, 김호원 (부산대) -----	48
• 전자 영수증 어플리케이션의 보안 취약점 분석 Afifatul Mukaroh, 강효은, 김호원 (부산대) -----	51
• 디지털 포렌식 관점의 Windows 10 Sticky Notes 연구 on a Crypto Hardware 채진희 (순천향대), 허원석 (고려대) -----	55
• 스마트 기기의 디지털 증거 훼손 방지 방안에 대한 연구 (생체인증 방식이 적용된 단말을 중심으로) 황혜성 (서울여대), 이세영 (경북대), 허원석 (고려대) -----	59

Session C-1 블록체인/금융 보안 (정보공학관 206호)

13:30 ~ 14:30 좌장 : 신상욱 (부경대)

• 블록체인 기반의 분산 EHRs 저장소 프라이버시 보호에 관한 연구구현 Sandi Rahmadika, 이경현 (부경대) -----	66
• 블록체인 프라이버시 보호 프로토콜 동향 강원태, 이상현, 김호원 (부산대) -----	69
• 탈중앙화 데이터 마켓플레이스의 접근제어 기법에 대한 연구 김혜빈, 박지선, 신상욱 (부경대) -----	72
• 탈중앙화된 데이터 거래 플랫폼의 연구 동향 분석 노시완, 이경현 (부경대) -----	75

Session C-2 블록체인/금융 보안 (정보공학관 206호)

15:00 ~ 16:00 좌장 : 이종혁 (상명대)

• 식품 추적 시스템에서의 블록체인 솔루션 Cho Nwe Zin Latt, 이경현 (부경대) -----	82
• 크립토재킹 공격 유형 및 동향 분석 김의진, 김득훈, 박진 (아주대) -----	85
• 수정·삭제를 위한 Hybrid Blockchain 기반의 XGS (XOR Global State) 인젝션 기술에 관한 연구 라경진, 이임영 (순천향대) -----	88
• 기업 블록체인 거버넌스와 위험 통제 프레임워크 설계 이경모, 이경현 (부경대) -----	91

Session D-1 인공지능 보안 (정보공학과 302호)

13:30 ~ 14:30 좌장 : 최대선 (공주대)

• 딥러닝 기반 의료분야 인공지능 기술 동향 조사 김도완, 최대선 (공주대) -----	99
• CNN기반 악성코드 이미지화 및 분석 시스템 김용수, Le Thi Thu Huong, 김호원 (부산대) -----	102
• 확률적 분석을 통한 Feature Selection 및 머신러닝 기반 악성코드 탐지 박승수, 이만희 (한남대) -----	105

Session D-2 인공지능 보안 (정보공학과 302호)

15:00 ~ 16:00 좌장 : 신 원 (동명대)

• Intrusion Detection Classifier Using Feature Selection and Recurrent Neural Network Thi-Thu-Huong Le, 김용수, 김호원 (부산대) -----	112
• 딥러닝 기반 얼굴인식 기술의 동향 권대용, 최대선 (공주대) -----	116
• 인공지능 시스템 보안 위협과 대책 박호성, 최대선 (공주대) -----	119
• 딥러닝 기반 악성 PowerShell 스크립트 탐지 방안 송지현 (과학기술연합대학원대학교), 최선오, 김종현, 김익균 (ETRI) -----	122

Session E-1 컴퓨터보안 (정보공학과 305호)

13:30 ~ 14:30 좌장 : 서화정 (한성대)

크립토재킹 공격 유형 및 동향 분석

김의진*, 김득훈**, 곽진***

*,**,*아주대학교 사이버보안학과

**정보보호응용및보증연구실, 아주대학교 컴퓨터공학과

*dmlwls0403@ajou.ac.kr, **dhkim.isaa@gmail.com, ***security@ajou.ac.kr

Types and Trends Analysis of Cryptojacking Attack

Eui-Jin Kim*, Deuk-Hun Kim**, Jin Kwak***

*,**,*Department of Cyber Security, Ajou University

**ISAA Lab., Department of Computer Engineering, Ajou University

요 약

블록체인은 분산원장 플랫폼을 이용해 익명성과 거래의 무결성을 보장하는 기술이다. 블록체인기술이 주목받으면서 이로부터 생성되는 가치가 존재하는 암호 화폐에 대한 관심도 증가하였다. 암호 화폐의 가치가 높아짐에 따라 암호 화폐 채굴 방식도 다양해졌으며, 이 중에서도 브라우저 기반 암호 화폐 채굴 방식이 큰 주목을 받고 있다. 그러나 브라우저 기반 채굴의 취약점을 악용한 크립토재킹(Cryptojacking)이 등장하면서 공격자는 실질적 이익을 볼 수 있게 되었다. 이를 대비하기 위해 본 논문에서는 대표적인 크립토재킹 공격 유형인 피싱, Malvertisement, 파일 공유 사이트를 이용한 공격 유형 및 동향 분석과 이에 대한 대응방안을 제시한다.

I. 서론

블록체인은 분산원장 플랫폼을 이용하여 익명성과 거래의 무결성을 보장함에 따라 향상된 보안성을 제공하는 기술이다[1]. 블록체인에 의해 획득 가능한 암호 화폐에 대한 가치가 높아지면서, 암호 화폐와 더불어 암호 화폐 채굴에 대한 관심이 증가하고 있다.

암호 화폐 채굴에는 CPU(Central Processing Unit), GPU(Graphics Processing Unit), ASIC(Application Specific Integrated Circuit)등의 채굴 방식이 있다. CPU와 GPU 채굴 방식은 전력 소모량에 비해 낮은 채굴 효율성을 가지며, ASIC는 주문형 반도체를 이용하며 CPU와 GPU 채굴 방식보다 빠르지만, 가격이 비싸다는 단점이 있다[2].

초기에는 브라우저 기반 암호 화폐 채굴 방식이 존재하였으나 암호 화폐의 가치가 낮아 주목받지 못하였다. 그러나 암호 화폐 가치 상승으로 브라우저 기반 암호 화폐 채굴 방식이 재주목을 받게 되었다[3]. 브라우저 기반 암호 화폐 채굴 방식인 Coinhive는 웹 사이트를 통해 사용자의 PC 자원을 사용자에게 허가받은 후 채굴을 진행한다. 웹 관리자들은 소규모의 스크립트를 추가함으로써 웹 사이트에 암호 화폐를 채굴 할 수 있다.

그러나 브라우저 기반 채굴 방식의 취약점을 이용한 악의적인 공격이 발생하고 있으며 이를 크립토재킹(Cryptojacking)이라 한다[3].

본 논문에서는, 2장에서 브라우저 기반 암호 화폐 채굴 사이트인 Coinhive와 이에 대한 취약점을 악용한 크립토재킹에 대해 설명하고, 3장에서 크립토재킹 공격 유형과 동향을 분석한 뒤 4장에서 이에 대응하기 위한 브라우저 기반 애플리케이션을 분석하고, 마지막으로 결론을 맺는다.

이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2017 R1E1A1A01075110).

II. 관련 연구

2.1 Coinhive

2017년 9월 브라우저 기반 암호 화폐 채굴 사이트인 Coinhive가 등장하였다. Coinhive는 CPU를 기반으로 한 CryptoNight 알고리즘으로 만들어진 모네로라는 암호 화폐를 채굴한다[4].

Coinhive는 웹 사이트 수익 창출을 위한 광고의 대안으로 제시되었다. 해당 과정은 웹 사이트에 소규모의 스크립트만 추가하면 되며, 이는 사용자의 컴퓨팅 파워를 이용해 해시값을 알아내고 암호 화폐를 지급한다[5].

[그림 1]은 Coinhive를 통해 웹 사이트 채굴을 위한 코드를 나타낸다.

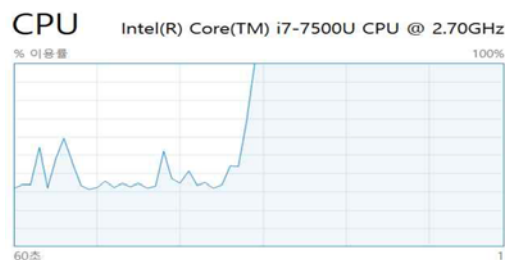
사용자의 컴퓨팅 파워를 이용하기 위해서는 사용자의 자원 활용 허가를 먼저 받아야 한다. 그러나 공격자에 의한 다양한 크립토재킹 공격을 통해서 사용자의 컴퓨팅 파워를 악용하는 공격이 가능하다는 문제가 존재한다.

```
<script src = "https://authedmine.com/lib/authedmine.min.js"></script>
<script>
var miner = new Coinhive.Anonymous('<YOUR PUBLIC SITE KEY>', {throttle: 0.5});
// 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 80] Coinhive 스크립트

2.2 크립토재킹

크립토재킹이란 암호 화폐(CryptoCurrency)와 하이재킹(Hijacking)의 합성어로 사용자의 허가 없이 컴퓨팅 파워를 통해 암호 화폐를 채굴하여 공격자의 지갑으로 보내는 것이다. 사용자의 PC를 대상으로 수행되는 공격이므로 CPU 채굴 또는 GPU 채굴을 활용하여 수행된다.



[그림 81] 크립토재킹에 의한 개인 PC 사용량

크립토재킹은 사용자의 자원을 사용하는 것

외에는 다른 피해가 없는, 채굴을 위한 마이너(Miner) 악성코드로 분류된다. 그러나 크립토재킹 공격은 장기적으로 사용자 기기의 수명 및 성능 저하의 원인이 된다. 최근에는 개인 PC의 고성능화로 인하여 개인 PC를 목표로 한 공격이 이뤄지고 있으며, 기업용 PC 또는 산업 기반시설을 목표로 한 크립토재킹 공격 또한 증가하고 있다. 기업의 서버와 같이 고사양의 시스템이 암호 화폐 채굴에 효과적이기 때문인데, 이는 기업 전체·산업 기반시설 및 국가 경제에 악영향을 줄 수 있다[6].

III. 크립토재킹 공격 유형 및 동향 분석

3.1 피싱과 악성 메일

크립토재킹의 주요 공격 방법 중 하나인 피싱(Phishing)은 불법적인 경로를 통해 얻은 사용자의 개인정보 또는 이메일을 이용하는 방법으로 정상 파일로 위장한 악성 메일 혹은 지인으로 위장한다. 이후 파일을 다운로드하면 암호 채굴 스크립트 또는 프로그램이 사용자의 허가 없이 컴퓨터에 다운로드되어 사용자의 자원을 악용하는 크립토재킹이 수행된다.

3.2 Malvertisement

Malvertisement는 악성코드(Malware)와 광고(Advertisement)의 합성어이다. 이러한 악성광고는 사용자가 볼 수 없는 아이프레임(iframe)을 통해 취약점 공격사이트로 재접속 하는데, 이 때 Exploit Kit이 사용된다. Exploit Kit은 사용자 PC의 취약점을 분석하며, 사용자의 PC에 취약점 패치가 되어 있지 않다면 취약점을 이용해 악성코드를 다운로드할 수 있는 셸 코드(Shell Code)가 실행된다[7].

[표 1]은 Exploit Kit을 통한 크립토재킹에 악용되는 취약점이다[6].

[표 47] 크립토재킹에 악용되는 취약점

취약점 유형	설 명
CVE-2018-8174	VBScript 원격코드 실행 취약점
CVE-2016-0189	JScript와 VBScript 원격코드 취약점
CVE-2018-4878	허상포인터(Dangling Pointer) 취약점

3.3 파일 공유 사이트

파일 공유 사이트는 P2P 프로토콜을 사용하여 사용자들끼리 파일을 주고받을 수 있다. 파일 공유 사이트의 증가로 인해 해커들의 악의적인 파일 유통도 증가하였다. 예를 들어 게임 크랙으로 위장한 악성코드의 경우 백신 프로그램이 크랙을 악성코드로 인식하는 점을 이용해 백신 프로그램 종료를 유도한다[8]. 이와 같은 상황을 악용하여 공격자는 사용자 PC에 쉽게 접근하여 정상 파일로 위장한 악성코드를 사용자 PC에 설치한 후 크립토재킹을 수행한다.

3.4 크립토재킹 동향

IoT 기기의 증가에 따라 크립토재킹의 대상이 PC에서 IoT 기기로 향하고 있다. 인기 유료 앱에 악성코드를 심은 뒤 불법적 경로로 무료 배포를 하는 수법을 사용되는데, 무료 배포된 앱 안의 공유된 APK파일을 설치할 경우 크립토재킹 공격을 받기 쉬우며 앱 실행 시 정상 작동하는 것처럼 보이나 백그라운드에서 암호 화폐를 채굴한다.

공격자들은 IoT 기기의 자원을 적정량만 사용하여 사용자들이 인지하지 못하게 접근하는 새로운 방법을 제시하고 있다. 또한 충전할 때에만 암호 화폐를 채굴하거나 모바일 환경에서 악성 프로그램 설치 시 와이파이를 이용하여 데이터 사용량을 최소화하는 방법을 이용하는 등 공격이 지능적으로 발전하고 있으므로 이에 대한 대응방안이 필요하다.

IV. 대응방안 분석

4.1 NoCoin 기술

NoCoin은 암호 화폐 채굴 웹 사이트가 blacklist.txt에 저장된 블랙리스트 기반 애플리케이션이다. NoCoin은 인터넷 익스플로러나 크롬에서 확장 프로그램으로 이용이 가능하며, 현재 버전 0.4.14 기준으로 사용자가 직접 자신의 화이트리스트를 추가할 수 있다[9].

4.2 Miner Block 기술

Miner Block 기술은 블랙리스트 기반

애플리케이션이다. Miner Block은 버전 0.4.0을 기준으로 사용자가 직접 추가할 수 있으며 특정 경로를 필터링할 수 있는 화이트리스트 기능이 추가되었다[10].

V. 결론

본 논문에서는 Coinhive의 등장으로 웹 브라우저 기반 암호 화폐 채굴이 알려졌고, 이를 통한 암호 화폐 채굴 시 취약점을 악용하는 크립토재킹에 대한 동향을 분석하였다. 최근에는 모바일을 기반으로 사용자가 인지하지 못하는 새로운 방법을 이용하는 지능적인 크립토재킹이 등장하고 있으며, 개인 PC뿐 아니라 IoT 기기도 위협 대상이 되고 있다. 따라서 웹 브라우저 기반 대응방안뿐만 아니라 모바일, IoT 기기에도 적용할 수 있는 선제적 대응방안이 필요하다.

[참고문헌]

- [01] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008.
- [02] 최원석, 김형식, 이대화, "크립토재킹 연구 동향", 정보보호학회지 28권 3호, Jun 2018.
- [03] Symantec, "Cryptojacking : A Modern Cash Cow", Symantec ISTR, Sep 2018.
- [04] 고동현, 정인혁, 최석환, 최윤호, "크립토재킹 사이트 탐지를 위한 동적 분석 프레임워크", 정보보호학회논문지 28권 4호, Aug 2018.
- [05] Coinhive, "Coinhive monetize your business with your users cpu power". <https://coinhive.com/>, 2017.
- [06] Ahnlab, "월간 安 201810호", Ahnlab, Oct 2018.
- [07] Trend Micro, "Rig Exploit Kit Now Using CVE-2018-8174 to Deliver Monero Miner", 2018.
- [08] Ahnlab, "월간 安 201809호", Ahnlab, Sep 2018.
- [09] Keramidas, "R. NoCoin Browser Extension", <https://github.com/keraf/NoCoin>
- [10] Belkacim, "I. MinerBlock Browser Extension", <https://github.com/xd4rker/MinerBlock>