J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

비트코인 네크워크에서의 암호화된 봇넷 C&C 통신기법☆

An Encrypted Botnet C&C Communication Method in Bitcoin Network

김 기 범[1] 조 영 호[1*]
Kibeom Kim Youngho Cho

요 약

봇넷은 금전적인 요구부터 국가적 위협에 이르는 다양한 목적을 위해 악용되어왔으며 사이버보안 분야에서 가장 위협적인 공격 유형 중 하나이다. 봇넷은 초창기 중앙집중식 구조로 출현한 이후 P2P 구조로 발전되어 왔다. 비트코인은 2008년 Satoshi Nakamoto가 발표한 최초의 블록체인 기술 기반의 온라인 암호화폐로 전 세계에서 가장 널리 통용되고 있는 암호화폐이며 비트코인 사용자가 증가함에 따라 비트코인 네트워크는 더욱 확장되고 있다. 이에 따라, 비트코인 네트워크를 C&C 채널로 사용하는 봇넷이 등장했으며 최근에는 다양한 연구가 수행되고 있다. 본 연구에서는 비트코인 환경에서 암호화된 봇넷 C&C 통신 메커니즘과 기법을 제안하고 비트코인 테스트넷에서 실제로 구축한 후 다양한 실험을 통해 성능평가를 해봄으로써 제안 기법의 유효성을 확인하고 궁극적으로는 비트코인 네트워크에서의 봇넷 위협의 가능성과 대응 필요성을 알리고자 한다.

☞ 주제어 : 비트코인 네트워크, 봇넷 C&C 통신, 암호화, 사이버위협

ABSTRACT

Botnets have been exploited for a variety of purposes, ranging from monetary demands to national threats, and are one of the most threatening types of attacks in the field of cybersecurity. Botnets emerged as a centralized structure in the early days and then evolved to a P2P structure. Bitcoin is the first online cryptocurrency based on blockchain technology announced by Satoshi Nakamoto in 2008 and is the most widely used cryptocurrency in the world. As the number of Bitcoin users increases, the size of Bitcoin network is also expanding. As a result, a botnet using the Bitcoin network as a C&C channel has emerged, and related research has been recently reported. In this study, we propose an encrypted botnet C&C communication mechanism and technique in the Bitcoin network and validate the proposed method by conducting performance evaluation through various experiments after building it on the Bitcoin testnet. By this research, we want to inform the possibility of botnet threats in the Bitcoin network to researchers.

☞ keyword : Bitcoin Network, Botnet C&C Communication, Encryption, Cyber Threat

1. 서 론

봇넷은 1990년대 등장이후 현재까지 가장 큰 사이버 위협 중 하나로 인식되고 있다[1]. 봇넷의 구조는 네트워크 기술의 발전에 따라 진화하고 있다. 등장 초기에는 중앙집중형 구조를 띄었으나 이후 P2P 구조로 진화하였으며, 최근에는 블록체인 네트워크에서 봇넷의 구축하고자 하는 움직임이 포착되고 있다[2, 3].

블록체인 기술은 분산원장 기술의 한 형태로 한 번 블록체인에 기록된 데이터는 수정과 제거가 불가능한 특징을 가지고 있다[4]. 블록체인 기술은 등장 초기에는 화폐 기능만을 지원하기 위해 사용되었지만 최근에는 신원인증 및 각종 보안영역에 응용되며 4차 산업혁명을 선도하는 핵심기술로 자리매김하고 있다[5].

최근에는 이러한 블록체인 기술을 봇넷의 C&C 통신에 활용하고자 하는 연구가 수행되었는데, S. T. Ali 등[3]은 비트코인 네트워크를 활용해 봇넷의 C&C 메시지를 전달하는 개념을 제시하였다. 이 연구에서 저자는 봇넷 C&C 메시지를 비트코인 트랜잭션의 출력 필드에 OP_RETURN 명령어를 사용하여 압축된 C&C 메시지를 전달하는 방식을 제시함으로써 전송 효율성을 확인한 바 있으나, 별도의 암호화 과정 없이 수행하여 쉽게 탐지될 수 있다는 단점이 있었다.

따라서, 본 연구에서는 기존 연구의 한계를 극복하기 위해 비트코인의 OP_RETURN 스크립트를 활용하는 암

1 Department of Defense Science(Computer Engineering Major), Graduate School of Defense Management, Korea National Defense University, Nonsan, Korea.
* Corresponding author (youngho@kndu.ac.kr)
[Received 27 August 2022, Reviewed 17 September 2022(R2 14 October 2022), Accepted 17 October 2022]
☆ 본 논문은 2021년 KSII 추계 학술대회에서 발표한 논문인 "블록체인 기반 봇넷의 위험성 연구"를 확장한 것이다.

호화된 봇넷의 C&C 통신기법을 제안한다.

본 논문의 공헌은 다음과 같다. 첫째, 기존 비트코인 기반 봇넷 연구에서 구현하지 않았던 암호화 과정을 추가하여 비트코인 네트워크에서의 봇넷 C&C 통신기법을 보완하였다. 둘째, 실제 비트코인과 거의 동일한 환경인 비트코인 테스트넷(Testnet)에서 제안 기법을 실험하여 검증하였다. 이를 통해, 비트코인을 통한 암호화된 봇넷 통신의 위험성을 알리고 향후 대응방안을 연구하고자 한다.

이후 논문의 구성은 다음과 같다. 2장에서는 봇넷의 C&C 통신 구조와 비트코인에 대해 소개하고, 3장에서는 제안기법을 설명하고 설계한다. 4장에서는 제안 기법을 비트코인 테스트넷에서 구축하여 실험하고, 5장에서 향후 연구방향을 제시하고 결론을 맺는다.

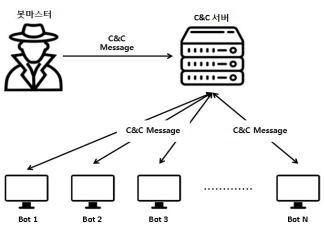
2. 배경지식 및 관련연구

2.1 봇넷의 C&C 구조

봇넷은 봇마스터가 특정 목적을 위해 조종하는 감염된 봇들의 네트워크이며, 봇넷의 C&C 통신구조에 따라 중앙집중식, P2P 방식, SNS 기반 방식 등이 있다[6].

2.1.1 중앙집중식 봇넷

중앙집중식 C&C 구조는 그림 1과 같이 서버-클라이언트 모델과 유사하다. 이러한 구조를 가진 대표적인 봇넷에는 IRC 및 HTTP 기반 봇넷이 있으며, 봇넷이 등장한 초창기에 많이 사용되는 방식이었다. 중앙집중식 봇넷은 구현이 쉽고 지연 시간이 짧아 봇마스터가 봇넷을 쉽게 모니터링을 할 수 있다. 반면에, 중앙서버가 중단되면 전체 봇넷 통신이 중단된다는 단일 장애 지점이 있으며 보안 관계자가 C&C 서버를 특정하여 무력화하면 봇넷 전체가 무력화된다는 단점이 있다[6].

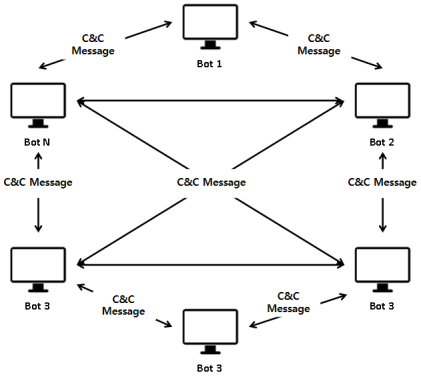


(그림 1) 중앙집중식 봇넷 구조[6]
(Figure 1) Centralized Botnet Structure[6]

2.1.2 P2P 봇넷

P2P 봇넷은 그림 2와 같이 각각의 봇 들이 클라이언트와 C&C 서버의 역할을 동시에 수행하는 형태의 봇넷이다. P2P 프로토콜의 분산 기능을 기반을 이용하여 봇마스터는 C&C 서버의 실제 주소를 숨기고 단일 장애지점 문제를 효과적으로 해결할 수 있다[7].

하지만 P2P 봇넷 또한 기술 자체의 특성에 기인한 단점이 존재한다. 우선, Storm[8]과 같은 P2P 기반 봇넷은 피어 노드를 찾기 위해 봇 내부에 하드코딩된 피어 목록이 존재하는데, 이러한 피어 목록을 오염시키는 오염공격(Poisoning Attack)과 가짜 노드를 생성하여 전체 P2P 네트워크를 장악하는 시빌 공격(Cybil Attack)에 취약하며 이러한 방식을 통해 전체 봇넷의 규모를 쉽게 파악할 수 있다는 단점이 존재한다. 또한, P2P 봇넷은 네트워크를 구성하기 위해 봇 들은 피어 봇을 네트워크에서 탐색 부트스트랩 단계를 거치는데, 이 단계로 인해 봇넷이 탐지될 가능성이 증가 된다는 단점이 있다[9].



(그림 2) P2P 봇넷 구조[6]
(Figure 2) P2P Botnet Structure[6]

2.1.3 SNS 기반 봇넷

최근에는 봇마스터가 트위터나 카카오톡과 같은 SNS 공간에 유통되는 멀티미디어 메시지에 스테가노그래피 기술을 사용하여 C&C 명령을 은닉한 후 봇에게 전달하는 SNS 기반 봇넷이 등장하였다[10, 11].

이러한 방식의 주요 이점에는 봇마스터가 자체 C&C 채널을 구축할 필요가 없다는 것과 봇과 봇마스터 사이에 교환되는 메시지가 정상적인 트래픽과 구분이 어렵다는 것 등이 있다.

2.2 비트코인 기반 봇넷

2.2.1 비트코인 네트워크

비트코인은 블록체인 기술을 기반으로 특정 기관이나 개인에 의해 통제되지 않으며, 비트코인의 모든 거래는 탈 중앙화된 글로벌 비트코인 블록체인 네트워크를 통해 검증되고 유통된다[4]. 비트코인은 탈 중앙화된 거래를 구현하기 위해 이전 거래의 정보를 참조하여 다음 거래 정보를 생성하는 사슬처럼 이어진 구조의 트랜잭션 데이터 구조를 채택하였다. 비트코인에서의 트랜잭션은 거래 내역 정보를 나타내는 데이터로, 각각의 트랜잭션은 식별을 위한 고유값인 TXID를 가지는데 이 값은 이전 트랜잭션 출력의 해시값을 참조하여 생성된다.

각각의 트랜잭션은 하나 이상의 입력과 출력으로 구성되며 입력 필드는 필드는TXID와 송신자의 서명, 공개키 값으로 구성된 ScriptSIG 등으로 구성되며 출력 필드는 송금 화폐를 나타내는 Value 값과 출력에 사용되는 화폐의 소유권을 증명할 수 있는 조건을 나타내는 ScriptPubkey 등으로 구성된다. 비트코인의 트랜잭션은 블록이라는 형태로 묶여서 저장되며 각각의 블록은 이전에 생성된 블록의 해시값을 포함하여 생성되기 때문에 한번 생성된 블록은 수정이나 제거가 불가능하다[12].

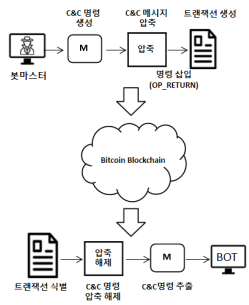
비트코인 네트워크에 참여하는 컴퓨터를 풀 노드라고 하며, 비트코인 풀 노드로 참여하기 위해서는 Bitcoin Core 프로그램을 설치하여 참여할 수 있다.

비트코인의 풀 노드는 트랜잭션 생성, 트랜잭션 검증, 블록 생성과 저장 등 크게 4가지 임무를 수행한다. [13]에 따르면 2022년 8월 기준 비트코인의 풀 노드 수는 전 세계 약 13,000여개 가량 분포되어 있다.

2.2.2 비트코인 기반 봇넷: Zombiecoin

비트코인 네트워크를 봇넷의 C&C 채널로 활용하는 연구는 S. T. Ali 등의 연구[3] Zombiecoin에서 최초로 제안되었다. 이 연구는 비트코인의 표준 트랜잭션 스크립트 중 하나인 OP_RETURN 스크립트를 이용하여 트랜잭션에 봇넷의 C&C 메시지를 삽입 후 전달하는 개념을 제시하였다.

OP_RETURN은 2014년 3월, Bitcoin Core 클라이언트 버전 0.9부터 도입되었으며 사용자가 트랜잭션에 최대 80 Byte의 임의의 16진수 데이터를 삽입할 수 있는 기능이다. 이 기능을 사용하여 비트코인 블록에 기록된 데이터는 영구적으로 수정이나 삭제가 불가하며 하나의 트랜잭션에는 하나의 OP_RETURN 데이터만 삽입이 가능하다[14].



(그림 3) Zombiecoin 개념[3]
(Figure 3) Concept Of Zombiecoin[3]

Zombiecoin은 그림 3과 같이 비트코인 네트워크에 C&C 메시지를 삽입하는 가장 직접적인 방법으로 이 OP_RETURN 명령어를 사용하는 것을 제시하였다. Zombiecoin의 주요 개념은 다음과 같다.

- 봇 마스터는 봇소프트웨어(봇SW)에 C&C 명령의 생성자가 봇마스트임을 식별하기 위한 봇마스터의 공개키를 포함하여 배포한다.
- 봇 마스터는 OP_RETURN 명령어를 이용하여 C&C 명령을 삽입하여 트랜잭션을 생성한다. C&C 명령은 OP_RETURN의 80 Byte 크기 제한에 맞추기 위하여 Huffman 코딩 방식을 이용하여 압축하여 삽입한다.
- 봇이 비트코인 네트워크를 통해 C&C 명령을 수신하면 봇은 봇마스터의 명령에 따라 대상을 공격한다.

2.3 기존 연구의 제한사항

Zombicoin은 C&C 메시지를 OP_RETURN의 80 Byte 크기에 맞도록 압축하여 전달하는 데에 초점을 맞추어 메시지를 암호화 후 전달하는 개념에 대해서는 다루지 않았으며, 실제 비트코인 네트워크를 통해 메시지를 전파하고 전파된 메시지를 추출하는 과정에 대해서는 구체적으로 다루지 않았다는 한계가 있었다.

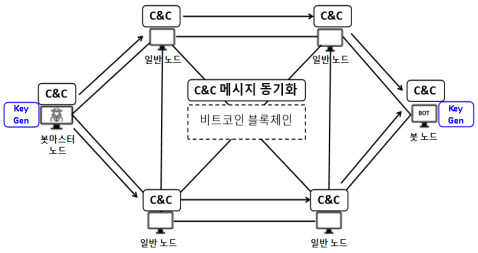
봇넷의 C&C 메시지를 암호화하지 않고 비트코인과 같은 퍼블릭 블록체인에 전파할 경우 다음과 같은 문제점이 발생할 수 있다. 우선 비트코인과 같은 퍼블릭 블록

체인에서 생성된 트랜잭션 데이터는 전 세계에 공개되기 때문에 C&C 메시지가 암호화되지 않으면 누구나 식별이 가능해진다. 이로 인해 봇 마스터는 쉽게 추적될 수 있으며, C&C 메시지가 사전에 파악되어 공격이 쉽게 무력화될 수 있다. 따라서 비트코인과 같은 퍼블릭 블록체인을 봇넷의 C&C 매개체로 활용하기 위해서는 메시지를 암호화하는 과정이 더욱 중요하다.

3. 제안기법: 비트코인 기반 암호화된 봇넷 C&C 통신기법

3.1 제안 모델 및 동작절차

그림 4에서 보는 것과 같이 제안 모델은 4가지 주요 구성요소(봇마스터, 봇, Key Generator, 비트코인 네트워크)를 갖고 있으며, 2단계 동작을 통해 봇넷 C&C 메시지를 송수신한다. 이때, 봇마스터와 봇은 풀노드이며 비트코인 네트워크에 참여하며 블록 데이터가 실시간으로 동기화된다. 또한, 봇마스터는 봇소프트웨어 C&C 명령의 생성자가 봇마스트임을 식별하기 위한 봇마스터의 공개키와 암호화된 C&C 메시지를 해독하는데 필요한 비밀키 생성기(Key Generator)를 포함시킨후 봇을 감염시켜 봇 SW를 사전에 설치 배포한 것을 가정한다.

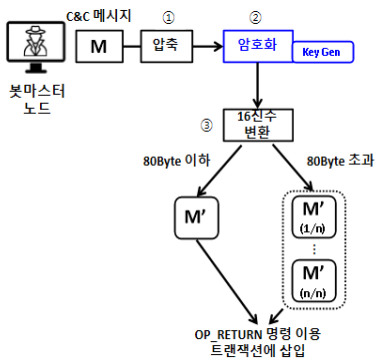


(그림 4) 비트코인 기반 암호화된 봇넷 C&C 통신 모델
(FIgure 4) Proposed Model: Bitcoin-based Encrypted Botnet C&C Communication Model

- **(1단계) 암호화된 C&C 메시지 생성:** 봇마스터는 봇에게 보낼 C&C 메시지를 작성하고 이 메시지를 압축과 암호화 과정을 거쳐 OP_RETURN에 최대 삽입 가능한 데이터 크기인 80 Byte 단위로 분할 후 이 데이터를 OP_RETURN 트랜잭션 내부에 포함시켜 비트코인 네트워크에 배포한다.

그림 5는 봇마스터가 암호화된 C&C 메시지가 포함된 트랜잭션을 생성하는 절차를 세부적으로 나타낸다.

① 봇마스터는 C&C 명령 M을 작성 후 이를 압축한다. 예를 들어, Huffman Coding 압축 알고리즘은 알파벳의 출현 빈도에 따라 부호의 길이를 다르게 할당하여 데이터를 압축한다.
② 압축된 데이터는 대칭키(DES, 3DES, AES 등) 방식의 암호화 알고리즘을 이용하여 암호화한다. 이때, 암호키는 봇과 동기화된 Key Generator을 통해 생성한다. 예를 들어, DES 암호화 알고리즘의 경우 64 Bit(패리티 체크를 위한 8 Bit 포함) 암호키를 생성하여 암호화를 진행한다.
③ 암호화된 데이터를 16진수 값으로 변환하여 OP_RETURN 트랜잭션을 생성한다. 이때, 암호화된 메시지가 80 Byte를 초과하는 경우 80 Byte 단위로 분할시켜서 여러 개의 트랜잭션을 생성한다.

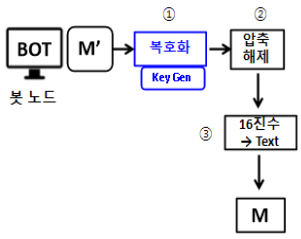


(그림 5) 암호화된 C&C 메시지 생성 절차
(Figure 5) Generation of Encrypted C&C Message

이후, 봇마스터가 생성한 암호화된 C&C 메시지가 포함된 트랜잭션은 블록의 형태로 모든 비트코인 네트워크의 노드의 저장소에 배포되어 동기화된다.

- **(2단계) 암호화된 C&C 메시지 추출:** 봇은 비트코인 네트워크를 통해 동기화된 블록 데이터 속에서 봇 마스터의 공개키를 검색하여 봇 마스터가 생성한 트랜잭션을 식별하고 식별된 트랜잭션 내부의 OP_RETURN 명령어를 통해 삽입된 데이터에서 암호화된 C&C 메시지 데이터를 추출하고 복호화하여 C&C 메시지를 추출한다.

그림 6은 봇이 메시지를 추출하는 단계를 세부적으로 나타낸다.



(그림 6) 암호화된 C&C 메시지 추출 절차
(Figure 6) Extraction of C&C Message from Encrypted C&C Message

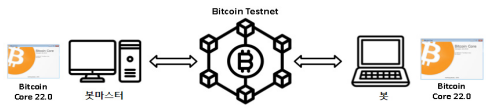
① 봇은 봇 마스터와 동기화된 Key Generator를 이용하여 메시지를 복호화 하기 위한 암호키를 생성하고, 이 암호키를 이용하여 암호화된 데이터를 복호화한다.
② 압축 데이터는 역압축 과정을 통해 압축을 해제한다. (예: Huffman 방식).
③ 압축 해제된 16진 값의 데이터를 Text 형태로 변환하여 C&C 메시지를 최종 추출한다.

이후, 복호화 과정을 통해 추출한 C&C 메시지의 공격지령을 수령한 봇들은 공격지령에 따라 DDoS 공격, 악성코드 유포, 개인정보 유출 등 다양한 2차 공격을 수행하게 된다.

4. 실험 결과

4.1 실험의 목적과 방법

실험의 목적은 제안기법이 비트코인 네트워크에서 구축 및 동작되는 지를 확인하고 검증하는 것이다. 즉, 실험을 통해 비트코인 네트워크에 봇마스터가 삽입한 암호화된 C&C 메시지가 봇 노드에 정상적으로 전달되고 공격메시지가 정상적으로 추출된다면 제안된 기법이 유효하다고 본다.



(그림 7) 실험 환경
(Figure 7) Experiment Environment

실험 환경은 그림 7과 같이 구성한다. 봇마스터 역할을 구현하기 위한 봇마스터 노드는 Bitcoin Core 클라이언트가 설치된 데스크탑(Intel Core I7 10700, RAM 16GB)을 사용하였고, 봇 노드는 Bitcoin Core 클라이언트가 설치된 노트북 PC(Intel Core I5 5500U, RAM 8GB)를 사용하였다. 실험용 비트코인 블록체인 네트워크로 실제 비트코인 네트워크인 메인넷과 동일한 환경의 비트코인 테스트넷(Testnet)을 사용하였다. 비트코인 테스트넷은 비트코인 어플리케이션 개발자들에게 개발 환경을 제공하기 위한 테스트 블록체인 네트워크로 비트코인 메인넷과 동일한 알고리즘과 프로토콜로 운영되어 실제 환경과 큰 차이없이 실험이 가능한 실험용 네트워크이다[15].

실험용 메시지는 Python의 dahuffman, DES 모듈을 이용하여 압축 및 암호화하여 생성하였다. 생성한 테스트 메시지는 표 1과 같다.

(표 1) 실험 메시지 생성
(Table 1) Generating An Experimental Message

구분	데이터	크기
평문	This message is test message for the BTC test net This message is test message for the BTC test net This message is test message fo	135 byte
압축후	052016FB35B561287425CADC5D2CA2D1545A6CF73CE35C5BFB6E9AE4BE0B7F6DD1287898A3B97097C1FB0CE35C5BFB6E9AE4BE0B7F6DD1287898A3B97097C1FB0CE35C5BFB6E9AE4BE0B7F6DD128	78 Byte
MODE : ECB / Key: qzclGHVh		
DES 암호화	17CD6B956651D9576ABF7CB56BB509C391A75BC6DA56F54C9A3A5F05B472DC8A7D644E12BE7349F4CCAFCAE76B44AA956DA75AD022AD2C60744AADD00ACFEF3D489BD5DC10EA1ECDE7A617A1E159B8E7	80 Byte

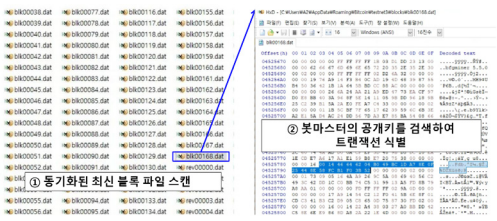
생성된 메시지를 바탕으로 그림 9과 같이 Bitcoin Core 프로그램의 콘솔을 이용하여 OP_RETURN 트랜잭션을 생성하였다.

(그림 8) 실험용 트랜잭션 생성 과정
(Figure 8) Generation of Experimental Transaction

4.2 실험 결과

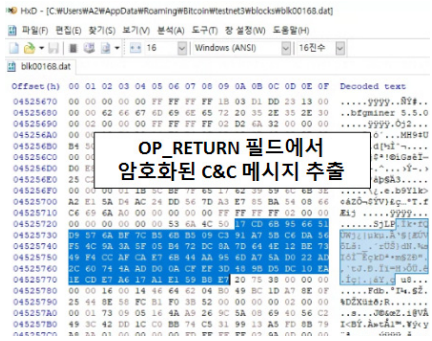
실험 수행 결과 봇마스터 노드가 생성한 암호화된 C&C 메시지는 비트코인 네트워크를 통해 봇 노드에게 성공적으로 전달되었으며, 실험 단계에 따른 수행 결과는 다음과 같다.

- **C&C 메시지가 포함 된 트랜잭션 식별 단계:** 봇 노드는 마스터가 생성한 트랜잭션을 찾기위해 블록 데이터 폴더에서 최신 블록 파일을 스캔하고 봇마스터의 트랜잭션을 봇마스터의 공개키 정보를 활용하여 식별하였다. 그림 9는 메시지를 식별하는 세부 절차를 나타낸다. 봇 노드(실험 노트북)에 자동으로 동기화된 블록 데이터는 특정 폴더(C:\Users\Appdata\Roaming\Bitcoin) 내에 DAT 포맷의 형태로 저장된다. 본 실험에서는 “blk00168.dat” 파일이 최신 블록파일이었으며, 이 파일을 HEX 에디터 프로그램을 통해 실행하여 블록 내 데이터(봇마스터의 공개키 정보)를 확인할 수 있었다.



(그림 9) 암호화된 C&C 메시지가 포함 된 트랜잭션 식별
(Figure 9) Identification of Transaction Including Encrypted C&C Message

- **식별된 트랜잭션으로부터 메시지 추출 단계**



(그림 10) 메시지 추출
(Figure 10) Extraction of C&C Message

식별된 OP_RETURN 트랜잭션에서 데이터를 추출한 결과 봇 마스터 단말기에서 작성한 것과 동일한 암호화된 16진수 데이터(80Bytes)가 추출되었다. 그림 10은 OP_RETURN 명령에서 검색한 16진수 형태의 암호화된 데이터이다. 추출된 데이터는 표 2와 같으며, 암호키를 이용하여 해독한 결과 원문과 동일한 데이터가 추출된 것을 확인할 수 있었다.

(표 2) 실험 메시지 추출 및 해독 결과
(Table 2) The Result of Test Message Extraction and Decryption

구분	데이터
추출 데이터	17CD6B956651D9576ABF7CB56BB509C391A75BC6DA56F54C9A3A5F05B472DC8A7D644E12BE7349F4CCAFCAE76B44AA956DA75AD022AD2C60744AADD00ACFEF3D489BD5DC10EA1ECDE7A617A1E159B8E7
복호화 / 암축해제 결과	This message is test message for the BTC test net This message is test message for the BTC test net This message is test message fo
	복호화 MODE : ECB / Key : qzclGHVh 압축하제 알고리즘 : Huffman Coding

위의 두 단계를 실험을 통해 확인함으로써 제안 기법이 비트코인 네트워크에서 구축 및 동작이 가능함을 검증하였다.

다음은 제안기법의 봇넷 C&C 채널을 운영에 소요되는 비용을 간략히 분석한 결과이다. 비트코인 트랜잭션 수수료는 트랜잭션의 데이터 크기에 따라 산정되며, [16]에 따르면 최근 3년 간 비트코인의 평균 트랜잭션 수수료는 0.00000013 BTC/byte인 것으로 분석되었다. 따라서 OP_RETURN에 80 Byte 데이터를 삽입한 전체 트랜잭션의 데이터는 약 240 Byte 정도이며, 이를 비트코인 평균 트랜잭션 수수료를 대입하여 계산한다면 0.0000312 BTC이며 이는 2022년 8월 24일 기준의 비트코인 가격을 고려하면 약 0.67$ 정도의 비용이 필요함을 알 수 있다. 다시말해, 봇마스터가 80Byte의 공격메시지를 비트코인 네트워크를 통해 유포하는데 필요한 비용은 0.79$(=900원)이라는 의미이며 큰 비용이 아님을 알 수 있다.

5. 결론 및 향후 연구

본 연구에서는 기존 비트코인 기반 봇넷 C&C 연구의 개념을 발전시켜 비트코인에 임의의 데이터를 삽입할 수 있는 80Byte의 한정된 공간에 C&C 메시지를 암호화하여 트랜잭션 내에 은닉하여 생성하고, 그것이 블록체인 네트워크를 통해 동기화되어 봇에게 정상적으로 전달되어

메시지가 추출되는 과정을 실험을 통해 증명하였다.

향후 연구 계획은 다음과 같다. 우선 본 연구에서는 암호화 알고리즘에 대칭키 암호화 알고리즘인 DES 방식만을 사용하여 실험하였으나, 향후 연구에서는 AES, 3DES 등 다양한 암호화 알고리즘을 적용하여 그 성능차이를 비교할 것이다. 더불어 본 연구에서는 OP_RETURN의 80 Byte라는 한정된 공간으로 인해 C&C 메시지를 은닉할 수 있는 다양한 기법을 적용하기 제한되었다. 향후 연구에서는 OP_RETURN 이외의 더 큰 용량의 데이터를 비트코인 트랜잭션을 통하여 전송할 수 있는 방법을 연구하고 이를 통해 스테가노그래피 등 다양한 은닉 기법과 암호화 알고리즘을 적용한 봇넷 C&C 통신 메커니즘을 연구하여 테스트 넷에서 구현 가능성을 실험할 것이며, 이를 통해 더욱 효율적이고 식별이 어려운 비트코인 기반 봇넷의 C&C 메커니즘의 구현 방안을 연구할 예정이다.

참고문헌(Reference)

[1] Sergio S.C. Silva, Rodrigo M.P. Silva, Raquel C.G. Pinto, Ronaldo M. Salles, “Botnets: A survey”, Computer Networks, Vol. 57, No. 2, pp. 378-403, 2013. https://doi.org/10.1016/j.comnet.2012.07.021

[2] L. Bock, N. Alexopoulos, E. Saracoglu, M. Muhlhauser and E. Vasilomanolakis, “Assessing the Threat of Blockchain-based Botnets”, 2019 APWG Symposium on Electronic Crime Research (eCrime), pp. 1-11, 2019. https://doi.org/10.1109/eCrime47957.2019.9037600

[3] Ali, S.T., McCorry, P., Lee, P.HJ. et al., “ZombieCoin 2.0: managing next-generation botnets using Bitcoin” International Journal of Information Security, Vol. 17, No. 4, pp. 411-422, 2018. https://doi.org/10.1007/s10207-017-0379-8

[4] Nakamoto Satoshi, “Bitcoin: A peer-to-peer electronic cash system”, Decentralized Business Review, 2008.

[5] Korea 4th Industrial Revolution Committee Resolution, “「Blockchain Technology Expansion Strategy」 for a hyper-connected and non-face-to-face trust society”, 2020. https://www.4th-ir.go.kr/article/detail/1142

[6] G. Vormayr, T. Zseby and J. Fabini, “Botnet Communication Patterns”, IEEE Communications Surveys & Tutorials, Vol. 19, No. 4, pp. 2768-2796, 2017. http://dx.doi.org/10.1109/COMST.2017.2749442

[7] M. Bailey, E. Cooke, F. Jahanian, Y. Xu and M. Karir “A Survey of Botnet Technology and Defenses”, 2009 Cybersecurity Applications & Technology Conference for Homeland Security, pp. 299-304, 2009. https://doi.org/10.1109/CATCH.2009.40

[8] B.H, Kang, et al., “Towards complete node enumeration in a peerto-peer botnet”, Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, pp. 23–34, 2009. https://doi.org/10.1145/1533057.1533064

[9] S. Chang, L. Zhang, Y. Guan and T. E. Daniels, “A Framework for P2P Botnets”, 2009 WRI International Conference on Communications and Mobile Computing, pp. 594-599, 2009. https://doi.org/10.1109/CMC.2009.268

[10] Jaewoo Jeon, and Youngho Cho, “Construction and Performance Analysis of Image Steganography-Based Botnet in KakaoTalk Openchat”, Computers, 8(3), 61, 2019. https://doi.org/10.3390/computers8030061

[11] Kwak, Minkyung, and Youngho Cho, “A novel video steganography-based botnet communication model in telegram sns messenger”, Symmetry, 13(1), 84, 2021. https://doi.org/10.3390/sym13010084

[12] V. Vallois and F. A. Guenane, “Bitcoin transaction: From the creation to validation, a protocol overview, 2017 1st Cyber Security in Networking Conference (CSNet), pp. 378-403, 2017. https://doi.org/10.1109/CSNET.2017.8241988

[13] https://bitnodes.io/

[14] Bartoletti, M. and Pompianu, L., “An Analysis of Bitcoin OP_RETURN Metadata”, International Conference on Financial Cryptography and Data Security, pp. 218-230, 2017. https://doi.org/10.1007/978-3-319-70278-0_14

[15] Franzoni, F., Abellan, I., Daza, V, “Leveraging Bitcoin Testnet for Bidirectional Botnet Command and Control Systems”, International Conference on Financial Cryptography and Data Security, pp. 3-19, 2020. https://doi.org/10.1007/978-3-030-51280-4_1

[16] https://bitinfocharts.com/comparison/bitcoin-transactionfees.html

◐ 저 자 소 개 ◑

김 기 범(Kibeom Kim)
2012년 해군사관학교 졸업(학사)
2021년~현재 국방대학교 관리대학원 컴퓨터공학과(공학석사)
관심분야 : 블록체인, 봇넷, 네트워크 보안, 디지털 포렌식 등
E-mail : kibeomkim@mnd.go.kr

조 영 호(Youngho Cho)
1998년 공군사관학교 졸업 (학사)
2006년 연세대학교 졸업 (공학석사)
2013년 University of Maryland, College Park, USA 졸업 (공학박사)
현재 국방대학교 국방관리대학원 국방과학학과 컴퓨터공학/사이버전협동전공 부교수
관심분야 : 네트워크 보안, 스테가노그래피 봇넷, 신뢰 메커니즘, 블록체인, 디지털 포렌식, AI 보안 등
E-mail : youngho@kndu.ac.kr