랜섬웨어 방지를 위한 블록체인 활용 모델에 대한 설계

안정현 · 김기천*

건국대학교

Design of Blockchain Model for Ransomware Prevention

Jung-hyun An · Ki-chun Kim*

Konkuk University

E-mail :aa9922@konkuk.ac.kr, kckim@konkuk.ac.kr*

요 약

금전적 수확 등의 목적으로 네트워크 사용자들의 컴퓨터 및 파일을 잠근 후 금품을 요구하는 악성 프로그램 랜섬웨어(Ransomware)의 진화가 계속될 전망으로, 메일 시스템에서 업무정보를 주고 받는 기업의 생존권에 있어 랜섬웨어는 위협적인 존재이다. 이러한 위협에 있어, 분산원장(Distributed Ledger) 기술인 블록체인(Blockchain)을 활용하여 랜섬웨어 이상징후 데이터로써 자동 생성되는 블록을 기업 내 보안정책에 바로 연계되도록 하여 메일 시스템에서의 랜섬웨어를 사전방지하는 블록체인 모델을 설계한다.

ABSTRACT

Ransomware, a malicious program that requires money and then locks computers and files on network users for financial harvesting, will continue to evolve. Ransomware is a threat in mail systems that send and receive business information. By using Block Chain, Distributed Ledger technology, it is designed to be a safe mail system in which the automatically generated Ramsomware symptom data is directly linked to the security policy in the enterprise.

키워드

Blockchain, Ransomware, Distributed Ldeger, Security Policy, Prevention

Ⅰ. 서 론

사용자의 PC를 암호화하여 몸값을 요구하는 랜섬웨어가 금전적 및 개인적 목적에 따라 심화되고 있어, 전세계적으로 랜섬웨어에 의한 피해와 위험이 계속될 전망이다. 그중 특정 기업을 목적으로 이메일을 통하여 랜섬웨어를 유포하는 방법은, 업무처리를 위해 기업 메일 시스템을 이용하는 직원들의 부주의가 바로 기업의 중요 데이터 유출로 이어지며 기업의 생존을 좌우하기 때문에 치명적인 위협이 된다.

이에 네트워크 참여자가 협력적으로 데이터를 수집한 후 공유하는 데이터 기술인 블록체인을 활용하여 랜섬웨어 이상징후 데이터를 수집하여 랜섬웨어를 방지하는 맞춤형 보안 기법을 제안하고자 한다. 기업 이메일 시스템을 사용하는 사용자들에게 수신되는 외부메일에서 추출되는 '랜섬웨어 이상징후 데이터'로 구성된 '랜섬웨어 이상징후 블록체인'은 데이터기술로써 방화벽 및 IDS/IPS, ESM 등 보안 솔루션에서의 보안 정책 설정에 있어 의사결정을 지원함으로써 랜섬웨어를 방지한다.

2절에서는 관련 연구로써 메일 보안 솔루션 및 블록체인에 대한 개념에 대해 설명한다. 3절에서는 본 논문에서 제안하고자 하는 랜섬웨어 이상징후 블록체인과 적용방안을 설명한다. 마지막으로 4절에서는 결론을 설명한다.

Ⅱ. 관련 연구

2.1 메일 보안 솔루션

기존 기업 내 메일 보안 솔루션에서는 메일서버를 거치기 전에 동작하여 기업 메일 시스템 사용자들에게 악성 메일 등이 걸러진 메일을 수신

하도록 하고, 기업 메일 시스템 사용자가 외부인에게 메일을 발송할 때는 정보 유출을 막기 위해 특정 내용의 메일 및 첨부파일 발신을 막는다. 이러한 메일 보안 솔루션에서 악성 메일을 탐지하기 위한 데이터로서 수집하는 보안 이벤트 항목들은 아래 표 1과 같다.

표 1. 보안 이벤트 항목[1]

발생시간, 발생장비, 근원지 IP, 목적지 IP, 수신자 메일주소, 메일제목, 첨부파일명, 제품명, 발생횟수

메일 보안 솔루션은 주로 Flume, Scribe 등의 로그 수집 도구를 활용하여 보안 이벤트를 수집하고, 설정해둔 룰(rule)을 기준으로 Snort, Snorby, NTop 등의 트래픽 분석 도구를 이용하여 악성 메일을 걸러낸다.

그러나 랜섬웨어는 개인의 심리를 이용하는 사회공학적 기법을 사용하기 때문에 보안 이벤트를 수집하여 필터링 하는 메일 보안 시스템에서 쉽게 해결되지 않아 기업 내 각 메일 사용자에게 각별한 유의가 권고되고 있다.

2.2. 블록체인

분산원장 기술(Distributed Ledger Technology)이라고 불리는 블록체인은 중앙 서버에 저장하지 않고, 네트워크 내에서 공동으로 데이터를 검증하고 기록·보관하여 공인된 제3자 없이 데이터의 무결성 및 신뢰성을 확보할 수 있는 기술이다[2]. 블록체인의 원리는 아래와 같다[3].

① 블록체인은 블록체인의 참여자들의 새로 생성되는 데이터가 서로에게 전송이 되어 검증을 수행한다.
② 검증된 데이터는 생성 주기마다 취합이 되어 블록을 생성한다.
③ 블록들은 고유의 해쉬값을 가지고, 이전 블록의 해쉬값을 같이 소유함으로써 연결되어 링크드 리스트(linked list) 구조의 블록체인을 형성한다.
④ 형성된 원본 블록체인은 생성된 블록을 각 참여자들에게 다시 전송해 재검증을 수행한다.
⑤ 완전히 검증된 블록은 각 참여자들의 블록체인으로 전송되어 원본 블록체인과 참여자의 블록체인은 동일한 데이터를 공유한다.

특정 시스템에 블록체인 기술을 활용함에 앞서, 블록체인이 다수의 참여자가 합의 및 공유함으로써 동작하는 특징을 가지고 있기 때문에, 먼저 시스템과 블록체인의 활용 목적·활용 환경·활용 범위가 적합한지 고려해야 한다. 이후 참여자 범위 및 접근 권한 등에 따라 분류되는 블록체인의 유형을 설정하는 것이 필요하다. 아래 표 2에서 블록체인의 유형의 특성을 상세히 나타낸다.

표 2. 블록체인 유형[4]

	퍼블릭 블록체인	컨소시엄 블록체인	프라이빗 블록체인
관리주체	모든 참여자	컨소시엄 참여자	기관의 관리자
거버넌스	법칙 변경 어려움	컨소시엄 내 합의에 따라 법칙 변경	관리자의 의사결정에 따라 법칙 변경
거래속도	느림	빠름	매우 빠름
데이터 접근	누구나 접근가능	허가받은 사용자만 접근가능	허가받은 사용자만 접근가능
식별성	익명성	식별 가능	식별 가능
활용사례	비트코인	R3 CEV	나스닥의 비상장 주식거래소

이러한 블록체인을 활용함으로써 신뢰성 있는 데이터를 무결성을 유지하며 확보할 수 있으며, 기존 중앙 집중식 거래환경에 상대적으로 경제성과 효율성, 확장성을 가질 수 있는 장점이 있다. 특히 거래 절차에서 많은 번거로움과 비용이 소모되는 금융 거래에서 이상적인 기술로 꼽히고 있어, 현재 블록체인은 가상화폐 및 해외 송금서비스 등 금융 분야에서의 활용을 중심으로 활발히 진행되고 있다. 더불어 여러 분야에서의 블록체인 활용의 필요성 또한 대두되고 있다.

Ⅲ. 랜섬웨어 이상징후 블록체인

3.1 구성

본 논문에서 제안하는 랜섬웨어 이상징후 블록체인은 프로토타입으로써 표 1과 같이 각 기업 내 메일 사용자의 메일 시스템에서 수집되는 보안 이벤트 데이터를 중심으로 설계되었다. 랜섬웨어 이상징후 블록체인 구성은 아래 표 3와 같다.

표 3. 랜섬웨어 이상징후 블록체인 구성

	랜섬웨어 이상징후 블록체인
블록체인 유형	프라이빗 블록체인
관리자	기업 보안 담당자
참가자	기업 메일 시스템 사용자
법칙관리	담당자에 따라 법칙 관리
데이터 항목	외부 메일 주소, 첨부파일, 링크, 악성 IP, 특정 문구

그중 랜섬웨어 이상징후를 추출하기 위한 수집 보안 이벤트 데이터는 ‘외부 메일, 첨부파일, 링크, 악성 IP, 특정문구’ 항목으로 선정했다. 랜섬

웨어는 주로 외부 메일 주소를 가진 외부 발신자가 보낸 외부 메일의 링크 및 첨부파일을 통해 감염되기 때문에 외부 메일 주소에 대한 데이터를 필수적으로 블록체인으로 구성하도록 한다. 이외 첨부파일 링크, 악성 IP, 특정 문구 등의 항목과 독립적 혹은 AND・OR 논리로 조합한 조건에 맞는 데이터로 구성한다. 이러한 방식으로 수집된 보안 이벤트 데이터는 이후 '랜섬웨어 이상징후 데이터'라 하며, 분(min)단위의 블록 생성 주기마다 취합되어 랜섬웨어 이상징후 블록을 생성한다.

3.2 동작

랜섬웨어 이상징후 블록체인은 다음과 같이 동작한다.

① 블록체인 참가자인 기업 메일 시스템 사용자들의 외부 수신 메일에서의 보안 이벤트 데이터를 수집한다.
② 수집된 보안 이벤트 데이터가 랜섬웨어 이상징후 데이터로써 추합되어 블록을 형성한다.
③ 형성된 블록은 원본 블록체인에 엮여지고, 각 참가자 블록체인에도 똑같이 공유된다.
④ 랜섬웨어 이상징후로 의심되는 데이터를 가지고 있는 랜섬웨어 이상징후 블록체인이 의사결정을 지원한다.

3.3 적용

본 논문에서 제시하는 랜섬웨어 이상징후 블록체인을 보안정책에 적용하는 구조는 아래 그림 1과 같다.

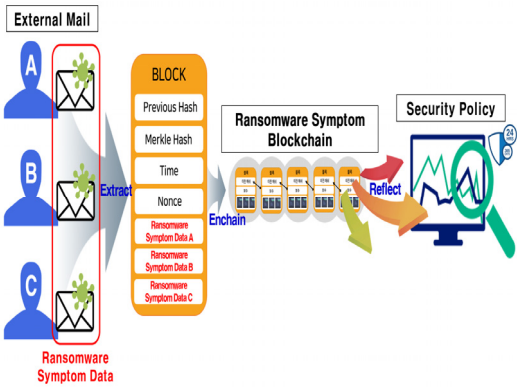

그림 1. 랜섬웨어 이상징후 블록체인 적용구조

해당 블록체인은 기업 메일 시스템에 랜섬웨어 이상징후 데이터를 해당 블록체인에 의해 추출하고 엮는 데이터 관리 기술이자, 기업의 방화벽 및 IPS/IDS, 메일 보안 솔루션 등에 연계되는 보안정책 설정에 있어 의사결정을 지원하는 기술로 작동한다.

Ⅳ. 결론

본 논문에서는 제시한 랜섬웨어 방지를 위한 블록체인을 설계하고 그에 대한 활용방안을 소개하였다. 해당 블록체인 및 활용방안은 주로 금융분야에서 활용되는 블록체인을 정보보호・보안분야에 활용한 사례이다. 또한 전세계적으로 심화되고 있는 사이버위협에서 대두되고 있는 협력적 정보 수집의 필요성을 충족시키는 방안이자, 기업의 보안 솔루션의 보안정책 설정에 대한 의사결정을 즉각적으로 지원할 수 있는 방안으로 응용될 수 있다.

향후 연구에서는 해당 블록체인의 엔진 및 데이터베이스 등 세부적인 프레임워크를 구축하기 위한 설계를 수행하고, 세부적으로 연계될 수 있는 추가 랜섬웨어 이상징후를 선정하고자 한다. 해당 블록체인의 엔진 및 데이터베이스 프레임워크를 설계함으로써 향후 실제적인 정보보호 기술로서 구현을 목적으로 한다.

ACKNOWLEDGEMENT

이 논문은 2017년도 정부재원(미래창조과학부 여대학(원)생 공학연구팀제 지원사업)으로 미래창조과학부, 한국연구재단과 한국여성과학기술인지원센터의 지원을 받아 연구되었습니다.

참고문헌

[1] 최대수, 이용균(2007), "ESM에서 보안이벤트 분석기술에 관한 연구", 한국정보과학회 학술발표논문집, 34(1D), 21-24
[2] BNK 금융연구소, "블록체인의 발전 전망과 금융기관의 대응 현황", 2016
[3] Nakamoto Satoshi(2008), "Bitcoin: A peer-to-peer electronic cash system",28
[4] 성신여자대학교, "블록체인기술 금융분야 도입방안을 위한 연구", 금융위원회 연구용역, 2016