국내 암호화폐 거래소 보안위협 및 대응방안 제시

박현성, 서정택

순천향대학교 정보보호학과

A Proposal of Security Threats and Countermeasures for the Internal Cryptocurrency Exchange

Hyeon-Seong Park, Jung-Teak Seo

Division of information security, Soonchunhyang University.

요 약

최근 암호화폐에 대한 관심과 거래가 증가함에 따라 암호화폐 거래소가 급증하였다. 탈중앙화 분산장부 기술인 블록체인을 활용한 암호화폐의 공급과 수요가 나날이 증가하고 있으며 그에 따라 화폐와 가상화폐를 거래해주는 암호화폐 거래소의 거래량이 증가하였다. 점차 암호화폐 거래소를 목표로 하는 사이버 공격이 증가하였고 더불어 보안의 중요성이 나날이 커지고 있다. 하지만 국내 거래소에서는 거래 서비스의 보안적 측면을 고려하지 않았으며, 이로 인한 거래소 대상 사이버 공격이 주기적으로 발생하였고 큰 피해를 입는 사고가 발생하였다. 따라서 본 논문에서는 암호화폐 거래소의 사이버 공격 사례와 공격시나리오를 바탕으로 사이버 공격에 대한 대응방안을 제시한다.

I. 서론

국내 암호화폐 거래소는 2013년 '코빗'을 시작으로 현재의 주요 암호화폐 거래소인 고팍스, 빗썸, 업비트, 코빗, 코인원 등 약 20여개의 거래소가 설립되어 운영 중이다[1]. 그에 따라 세계 1위의 암호화폐의 거래량을 달성했으며 약 2조원의 거래가 하루 평균 발생하고 있다.

암호화폐 거래소(Cryptocurrency exchange)는 암호화폐와 화폐를 환전해주는 거래소로 달러나 엔화를 원화로 환전해주는 외환 거래소와 비슷한 역할을 한다.

하지만 이러한 거래소들은 해커들의 타겟이 되어오고 있으며, 거래소를 통한 거래가 매우 활발하게 이루어지고 있고 금융과 관련된 분야이기 때문에 이에 따른 피해 규모가 심각하다고 볼 수 있다[2]. 더욱이 사용자의 개인정보와 계좌정보, 암호화폐 보유량 등 개인정보와 금전정보를 수집하고 관리하고 있기 때문에 막대한 경제적 피해와 2차 피해까지 이어질 수 있다. PC와 모바일을 통한 암호화폐 거래가 활발하게 이루어지는 만큼 정부가 앞장서서 보안 강화를 요구하고 있으나 계속해서 피해가 속출하고 있다.

본 논문에서는 과거 국내 암호화폐 해킹 사례를 통해 국내 거래소 보안위협 및 공격 시나리오를 도출하고, 그에 따른 대응방안을 제시하여 국내 암호화폐 거래소 보안을 강화하는데 일조할 수 있을 것으로 사료된다.

본 논문의 구성은 다음과 같다. 2장에서 국내 암호화폐 거래소의 해킹 사례들을 살펴보고, 3장에서 국내 암호화폐 거래소 보안 위협에 대해 분석하며 4장에서 국내 암호화폐 거래소 사이버 공격 시나리오를 도출한다. 5장에서는 국내 암호화폐 거래소 사이버 공격 대응방안과 마지막으로 6장의 결론으로 논문을 마무리한다.

II. 국내 암호화폐 거래소 해킹 사례

국내 암호화폐 거래소를 대상으로 한 주요 사이버 공격 사례는 [표 2]로, 매년 수십억 가량의 경제적 피해가 발생하였다.

발생일시	피해내역
16.07.26.	3억 원 상당의 가상통화 부정인출
17.04.22.	55억 원 상당의 가상통화 부정인출
17.06.28.	70억 원 상당의 가상통화 부정인출 약 3.6만여 건 개인정보 유출
17.09.23.	21억 원 상당의 가상통화 부정인출
17.12.19.	259억 원 상당의 가상통화 부정인출
18.06.10	530억 원 상당의 가상통화 부정인출
18.06.19	350억 원 상당의 가상통화 부정인출

[표 2] 암호화폐 거래소 해킹 사례(경찰청)

2.2 암호화폐 거래소 '빗썸' 2차례 해킹

이메일 피싱을 통한 악성코드로 업무용 PC가 감염되었고, 고객정보가 저장되어 있는 데이터베이스를 목적으로한 공격으로 인해 약 3만 6천여건의 고객정보가 유출되었다[3]. 해커에게 유출된 고객정보는 접속 인증 우회 및 고객에게 2차 피싱등을 통하여 계정에 접근할 수 있었고, 본인 계좌가 아닌 다른 계좌로 인출되는 사고가 발생하였다[4].

1차 해킹을 통해 개인정보 유출과 부정인출로 인한 피해가 발생한 후, 해당 업체는 보안솔루션을 도입하여 보안을 강화하였다. 그럼에도 불구하고 2018년 6월, 350억 원의 암호화폐의 부정인출과 금전적 피해가 발생하였다.

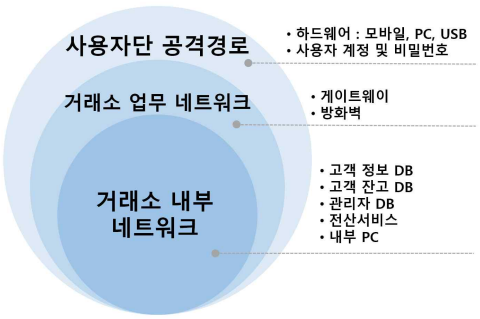
2.3 국내 암호화폐 거래소 보안 점검 결과

A사	· 망 분리 및 시스템 접근통제 관리 미흡 · 가상통화 지갑관리 미흡(보안정책 운영 등) · 정보보호시스템(방화벽 등) 구축 미흡 · 관리자 PC 설치프로그램에 대한 보안관리(유해사이트 접속 차단 등) 미흡
B사	· 망 분리 및 시스템 접근통제 관리 미흡 · 관리자 PC 설치프로그램에 대한 보안관리(유해사이트 접속 차단 등) 미흡 · 외부 개인PC에서 인터넷망을 통해 내부시스템 접근 기능 등 보안사고 우려
C사	· 망 분리 및 시스템 접근통제 관리 미흡 · 가상통화 지갑관리 미흡(보안정책 운영 등) · 정보보호시스템(방화벽 등) 구축 미흡 · 침해사고 대응 절차, 지침 등 미흡 · 주요데이터 백업관리 체계 미흡
D사	· 망 분리 및 시스템 접근통제 관리 미흡 · 정보보호시스템(방화벽 등) 구축 미흡 · 주요데이터 백업관리 체계 미흡
E사	· 망 분리 및 시스템 접근통제 관리 미흡 · 가상통화 지갑관리 미흡(보안정책 운영 등) · 정보보호시스템(방화벽 등) 구축 미흡 · 주요데이터 백업관리 체계 미흡
F사	· 망 분리 및 시스템 접근통제 관리 미흡 · 침해사고 대응 절차, 지침 등 미흡
G사	· 방화벽 등 기본적인 보안시스템은 있으나, 보안정책관리 등 미흡
H사	· 망 분리 및 시스템 접근통제 관리 미흡 · 침해사고 대응 절차, 지침 등 미흡 · 정보보호시스템(방화벽 등) 구축 미흡 · 주요데이터 백업관리 체계 미흡
I사 (폐업)	· 계정관리정책 수립이 되어있지 않음 · 관리자PC가 지정되어 있지 않으며, 노트북과 무선 인터넷을 사용하여 관리수행(망 분리 권고)
J사	· 관리자 PC 설치프로그램에 대한 보안관리(유해사이트 접속 차단 등) 미흡 · 침해사고 대응 절차, 지침 등 미흡

[표 3] 암호화폐 거래소 보안 점검 결과
(과학기술정보통신부, 한국인터넷진흥원)

III. 국내 암호화폐 거래소 보안 위협

급격한 사용자 증가에 따라 확대된 사이버 공격동기 및 공격벡터를 통한 내부 네트워크 불법 침투의 가능성이 증가하였다[5]. 보안 설계가 미흡한 내부 네트워크 특성은 백도어, 스푸핑 및 위·변조 데이터 주입 등 공격 탐지의 취약점이 노출되어 있다.



[그림 1] 국내 암호화폐 거래소 구성(예시)

3.1 사용자단 보안위협

거래소를 이용하는 사용자의 모바일 및 PC는 대중화되어 외부 인터넷에 노출되어 있으므로 비밀번호 유출, 인증서 유출, 펌웨어 감염 및 악성 어플리케이션 설치 등 다양한 공격에 취약하다.

거래소 SW 및 거래소 웹사이트의 취약점으로 인한 보안 위협이 존재한다. 또한 사용자에게 페이크 사이트(Fake Site)의 접속을 유도하는 공격도 가능하다.

3.2 거래소 업무 네트워크 보안위협

외부 인터넷에 연결된 업무용 PC의 사용으로 인한 악성코드의 유입이 가능하다. 방화벽의 접근제어 취약점을 이용하여 정상적인 경로를 통해 공격이 이루어질 수 있다. 또한 주요 전산서버와 연결되어 있는 경우 SQL Injection등과 같은 취약점을 이용하여 데이터베이스로의 접근이 가능하다.

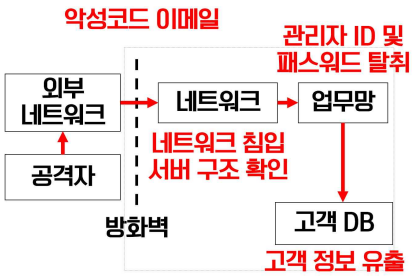
3.3 거래소 내부 네트워크 보안위협

업무망과 내부망의 망 분리 및 주요 자산 시스템에 대한 접근통제 관리 미흡으로 인한 외부 인터넷 연결을 통한 공격이 가능하다.

IV. 국내 암호화폐 거래소 사이버 공격 시나리오

4.1 개인정보 유출 시나리오

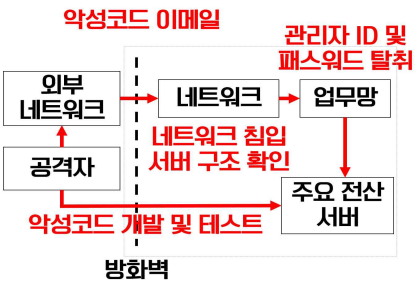
업무용 메신저 주소의 유출이나 직원 계정 탈취를 통하여 악성코드 프로그램이 담긴 이메일을 통한 스피어피싱이 발생한다. 거래소 업무망 내 PC에 접근한 공격자는 네트워크 스캔을 통해 서버 구조를 확인하고 관리자 ID 및 패스워드를 탈취한다. 관리자 계정으로 접속 가능한 고객의 개인정보가 저장된 데이터베이스에서 개인정보를 유출한다.



[그림 2] 개인정보 유출 시나리오 다이어그램

4.2 거래소 서버 장악 시나리오

거래소의 업무망과 전산망(내부망)이 연결되어 있는 PC를 찾기 위해 네트워크 스캔을 통해 해당 구간을 탐색한다. 관리자 권한을 가진 PC를 통해 주요 전산 서버를 장악하고 해당 공격 벡터와 C&C서버를 연결하여 내부망 내의 PC에서 악성코드를 개발하거나 테스트한다. 이 과정에서 업무망의 모든 네트워크 패킷들이 유출된다.

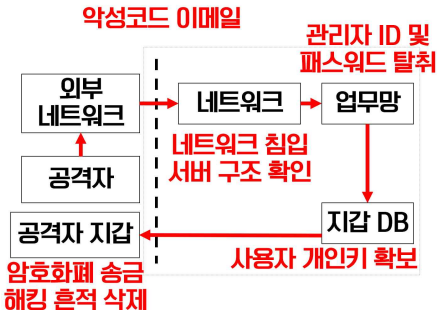


[그림 3] 서버 장악 시나리오 다이어그램

4.1 비대칭키 유출 및 지갑 탈취 시나리오

고객의 계좌에 해당하는 지갑정보가 저장되어 있는 데이터베이스에 접근하여 고객의 개인키를 확보하게 되면, 마지막으로 공격자는 자신의 암호화폐 지갑에 암호화폐를 송신하여 개인 자산을 유출한다. 이와 같은 과정이 모두 끝나

면 자신의 해킹 흔적을 은닉하거나 삭제하여 해킹의 흔적이나 유무를 쉽게 발견할 수 없도록 한다.



[그림 4] 비대칭키 유출 및 지갑 탈취 시나리오 다이어그램

V. 국내 암호화폐 거래소 사이버 공격 대응 방안

5.1 망 분리

업무망과 내부망의 망 분리를 통해 고의적이거나 비고의적인 실수와 오류로부터 주요 자산을 보호하고 체계적인 접근제어가 필요하다. 더욱이 자산의 식별과 관리가 효율적으로 이루어질 수 있도록 망 분리 시 고려해야하는 부분과 함께 망 분리가 이루어져야한다.

5.2 주요 데이터 암호화

주요 자산 및 데이터의 접근이나 사용함에 있어서 데이터를 암호화시킴으로써 높은 레벨을 통한 접근권한에서의 자산 관리가 필요하다. 특히 고객 개인정보와 같은 경우, 사용되지 않고 있는 계정의 개인정보는 암호화되어 저장되거나 암호화 백업을 통해 보호되어야한다.

5.3 구간별 보안 강화

주요 데이터의 가용성과 무결성의 침해 위협으로부터 보호하거나 유출되는 정보의 기밀성을 유지하기 위한 보안 기술이나 장치를 추가해야한다.

5.4 ISMS 및 ISMS-P 인증

정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 인터넷진흥원 또는 인증기관이 증명하는 제도로 대부분의 국내 거래소는 인증 의무 대상에 포함되어 있다. 이에 따라 적합한 보안 관리체계 수립 및 운영과 보안 기술 적용, 개인정보의 보호조치가 이루어져야한다.

VI. 결론

본 논문에서는 국내 암호화폐 거래소에 대한 보안 위협과 공격 시나리오를 도출하였다. 또 그에 따른 대응 방안을 제시하였다. 가상화폐와 화폐를 교환하고 거래하는 서비스의 보안은 금융서비스의 보안만큼 중요성이 크다. 더불어 개인정보를 통한 거래가 이루어지기 때문에 악의적인 해커에 의해 발생하는 해킹이 매우 큰 금전적 피해를 가져올 수 있어 심각성이 크다고 할 수 있다. 이미 국내 암호화폐 거래소의 시스템 구성의 취약점을 이용하여 과거 수차례의 해킹이 발생하였고, 그에 따른 보안 조치가 이루어지지 않는다면 앞으로도 큰 피해가 발생할 것으로 판단된다. 이러한 공격은 거래소의 보안 관리가 금융서비스와 유사한 방식의 적절한 보안 조치가 필요할 것으로 보인다. 그렇기 때문에 거래소 시스템 구성에 있어서 구조적인 취약점을 방어할 방법을 연구하고 강화해나가야 할 것이다.

[참고문헌]

[1] 송지환, “비트코인 거래소, 해커와 절도범으로부터 안전한가”, 월간SW중심사회 2018년 10월호, 소프트웨어정책연구소, pp.36-43

[2] Financial Security Institute , “BlockChain Technology and Security Considerations", August, 2017.

[3] 한국인터넷진흥원, 2017년 3분기 사이버 위협 동향 보고서, 2017

[4] igloosecurity, Monthly Security Report, Feb. 2018

[5] 정용식, 차재상. (2018). 블록체인 기반 가상화폐 거래의 보안 위험 및 대응방안. 한국정보전자통신기술학회 논문지, 11(1), 100-106.