Sentinel Protocol

Security Intelligence Platform for Blockchain

초록

21세기 컴퓨터 기술의 급속한 발전은 그 역설적으로 혁신을 저해하는 정교하고 지능적인 위협이 되기도 합니다. 암호화폐의 본질은 분권화에 있는데, 보안의 관점에서 오히려 이 분권화가 때로는 암호화폐 자산 보호에 있어 가장 큰 약점이됩니다. 이는 분권화된 암호화폐 시스템의 방어기저가 보안위협에 취약하기 때문인데, 이러한 보안위협은 개인과 기업에 전적으로 부담요소가 되고 있는게 현실입니다. 이에, Sentinel Protocol은 암호화폐 시스템의 부족한 방어기저를 향상 시킴으로써, 보안 측면에서의 분권화의 단점을 극복하고자 합니다. 이를 위해 Sentinel Protocol은 분권화의 힘으로 생성된 집단 지성을 활용하며, 암호화 기능과 지능형 위협분석 알고리즘을 결합 함으로써 안전하고 혁신적인 생태계를 제공하고자 하는 바 입니다.

Uppsala Foundation

2018.04.07

Chapter 1

개요

암호화폐 기술의 주요 개념인 '분권화'는 혁신적요소와 원천적인 불안요소, 이 두가지를 모두 가지고 있습니다. 원천적인 불안요소의 근원은 자치권에 있는데, 특히 익명성이 허용된 자치권은 분권화된 시스템에 엄청난 책임을 부과하게되고, 이러한 자치권의 부작용이 분권화된 시스템을 실제로 수많은 사이버 범죄에 노출 시킨다는 것은 명백한 사실입니다. 그러나, 현재 이런 형태의 사이버 범죄를 차단하기 위한 어떠한 기본적인 방어 시스템도 아직 준비되어 있지 않은 것이 암호화폐 세계의 현실이기도 합니다.

여기서, 일반적인 암호화폐 사용자가 직면한 세 가지 보안의 주요 현안들은 다음과 같습니다. 첫째, 몇몇 사례에서도 들어나 듯이 일반적인 블록체인 어플리케이션 또는 서비스 사용자들이 해킹에 너무 쉽게 노출되어 있다는 것입니다. 둘째로, 악의적 공격자들은 공격대상들을 쉽게 식별할 수 있으나 반대로 공격대상이 되는 피해자들은 악의적 공격자들을 쉽게 식별할 수 없다는 것입니다. 마지막으로, 당연하게도 악의적 공격자들에 의해 입은 피해는 고스란히 피해자들의 몫이 되고만다는 것입니다. 이러한 근본적인 암호화폐 보안의 문제는 어떻게 해결되어야 할까요? 분권화의 자율성에 의해 발생된 원천적인 보안의 취약성은 결국 우리 스스로의 문제이자 책임으로만 치부되어야 하는 것인가요? 그렇지 않습니다. 개인들이 개별적으로 이러한 문제를 해결할 수 있는 방법을 찾긴 쉽지 않지만, 공공의 이익을 위한 집단의 노력이 있다면 이는 충분히 극복이 가능할 것입니다. 잠재적 피해자인 암호화폐 사용자들은 집단 지성을 활용하여 분산된 형태의 블록체인 기술의 철학을 그대로 유지한 채, 사이버 보안의 비즈니스 생태계를 스스로 만들고, 또 상호 이익을 위해 모두 함께 행동한다면 이를 해결할 수 있을 것입니다. 우리의 분산화된 인공지능 보안 시스템은 공격자의 알려지지 않은 공격 패턴들을 탐지하고, 집단 지성을 활용하여 생태계 전체에 악의적 공격 정보를 상호 교환 및 배포 함으로써 선의의 피해자를 보호 함과 동시에 분권화의 근본적인 자율성을 유지할 수 있게 될 것입니다.

Chapter 2

문제 진술

일반적으로, 개인과 기업 간 보안위협에 대응하는 방어 수준의 정도차이는 그와 관련된 기술 및 인적자원에 투자하는 투자금의 차이에 있다고 말 할 수 있습니다. 객관성을 높이기 위해, SANS 연구소에서 출간한 IT 보안 지출동향 보고서[1]를 참고해 보면, 2016년 보고에서 금융기관들이 IT 보안분야에 가장 많은 투자금을 집행하는데 그들의 연간 예산($500,000 ~ $1M) 중 평균 10 ~ 12%로 가장 높은 비율의 보안투자를 집행하고 있고, 그 뒤를 이어 정부기관이 연간 예산($1M ~ $10M) 대비 7 ~ 9% 비율로 보안에 투자하고 있습니다. 그외 산업군에선, 교육/헬스케어 등이 뒤를 잇는데 전반적으로 각 산업군 별 연간 예산 대비 보안 투자비용은 지속적으로 증가하는 추세입니다. 또 다른 사이버보안 시장에 대한 보고서에 따르면[2] 사이버 범죄가 기승 함에 따라 사이버 보안 시장의 규모가 2017년에서 2021년까지 $1조 달러로 성장할 것이라고 예측하기도 합니다.

기업 내 사용자들은 보안 고급 전문가와 다양한 보안솔루션을 통해 사이버 보안위협으로부터 보호를 받고 있으나 일반 개인이 스스로를 방어하는 수단들을 살펴보면, 불행하게도 고작 보안수준이 낮은 소프트웨어나 하드웨어 를 보유하는 정도이고 전문성이 결여된 보안지식 수준에서 자신의 시스템을 운영하는 정도를 크게 벗어나지 못하고 있습니다. 블록체인 기술이 발전함에 따라, 다양한 사기 기법과 사이버범죄 또한 발전하고 있는데 최근 사이버 범죄의 가장 잘 알려져 있는 분야 중 하나는 사용자의 데이터를 볼모로 삼아 비트코인을 보상금으로 요구하는 사이버 범죄의 새로운 유형인 랜섬웨어가 떠오르고 있습니다. 2021년까지 이 랜섬웨어 '시장'이 170억 달러로 성장할 것으로 예상하기도 하는데, 불행하게도 비트코인의 화폐 가치는 그 사용취지와 달리 이러한 사이버 범죄에 가장 많이 악용되는 역설적인 상황을 겪고 있기도 합니다.

2016년 DAO 해킹사례는 블록체인 시대의 첫번째 주요 보안 취약성 사고로서, 해커의 코드 취약성 공격으로 인해 이더리움 전체의 15% 정도가 악의적 공격에 노출된 사건으로 기억됩니다. 그 결과 수많은 투자자들이 재정적 손실을 입어 고통을 받게 되었고, 이 문제를 해결하기 위해 하드포크[3]를 시행하게 되는데, 그로인해 '블록체인은 불변한다.'라는 블록체인의 기술 철학적 믿음은 상처를 입은 결과를 낳게 됩니다. 결과적으로, 이는 자율성이 지나치게 강조될 경우 그로 인해 발생하는 책임은 오롯이 개인에게 부과된다는 명제가 성립되는 불행한 사고로 기억되고 말았습니다.

Chapter 3

분권화의 보안

현재 대부분의 사람들은 최소한 한 개 이상의 이메일 주소를 보유하고 있고, 이메일 주소가 기입되지 않은 명함은 상상하기도 어렵습니다. 하지만, 현대 생활의 이러한 공통적인 필요성은 또 하나의 보안 측면에서 취약성을 나타냅니다. *doc, *.xls, *.ppt 등의 문서파일에 악의적인 마크로가 삽입되어 이메일의 첨부로 수신되는 이른바 '피싱이메일'만 해도, 사실은 악의적인데도 지극히 정상적으로 보이는 문서파일이나 링크로써 많은 사용자를 감염시키고 있습니다. 2017년 7월 경, 한국의 최대 암호화폐 거래소인 '빗썸'은 31,000명의 고객 개인정보와 회사의 기밀정보를 도난 당하는 사고에 휘말렸는데, 이는 운영자가 단 하나의 감염된 파일을 오픈하면서 해킹이 된 사고로 알려져 있으며, 이 피싱 공격의 범인은 아직 밝혀지지 않고 있습니다.

피싱은 이메일에만 국한되지 않습니다. 전화를 이용한 피싱의 경우, 암호화폐 거래소의 운영자로 가장한 범죄자가 전화통화를 통해 개인정보를 얻어 내는 사기수법으로 수 많은 개인들에게 피해를 입힐 수도 있는데, 예를 들면 해커가 관리자로 가장하여 사용자에게 전화를 걸어 사용자의 계정이 해킹 당했으니 조치를 취한다는 명목으로 계정의 비밀번호를 재설정하기 위한 사용자의 개인정보를 요구할 수 있습니다. 이는 사용자의 심리적 약점을 악용하여 사용자의 주요 정보를 탈취하는 전형적인 사기 수법입니다.

또 다른 피싱 수법으로, 어떤 ICO(Initial Coin Offering)가 진행되는 동안 실제 ICO사이트의 주소를 해커가 만든 가짜 ICO사이트 주소로 바꿀 수 있도록 허위정보를 제공함으로써 투자금을 탈취하는 경우입니다.

이러한 다양한 해킹들의 사례는 희생자가 인터넷의 본질인 '개방성'으로 인해 너무나 손쉽게 해커에게 노출되기 때문에 발생한다는 것이다. 결국, 암호화폐와 인터넷 모두가 분권화를 중요한 기술적 이념으로 여길진 모르지만, 암호화폐의 기반 인프라인 블록체인이 앞서 언급한 다양한 보안위협을 완벽히 극복할 수 있는 완벽한 자치권까지 구현했다고 말하기 어려울 것이다. 개방된 상태에서의 자치권은 전적으로 개인의 책임 하에 있으며 분권화가 모든 문제의 해결책을 제시하진 못한다. 현실적으로 악의적 공격에 의한 다양한 방식의 사이버 위협이 지속 발전될수록, 분권화의 이념은 반드시 보안의 철학을 수렴하여 발전되어야 할 것이다.

Chapter 4

블록체인의 평판 시스템

비트코인의 그 근간에는 블록체인[4]이 존재하는데, 이는 중앙기관 통제 없이도 상호 신뢰가 모호한 상태에서 합의 알고리즘을 활용 해 전자 화폐 거래 체결이 가능 하도록 하는 피어-투-피어 시스템입니다. 이 블록체인의 다양한 특징과 장점으로 인해, 현재 기존 산업분야와 꾸준한 융합 시도가 이루어지고 있지만, 그 과정에서 기술 정합성 및 관련 정책 또는 규제 등의 충돌은 관련 산업발전의 저해요소로 인식되고 있습니다. 예를 들면, 블록체인과 기존 금융서비스의 융합의 경우, 모든 거래 기록을 공유하는 것이 원칙인 블록체인의 입장과 민감한 개인 자산정보 공개를 불허하는 기존 금융기관의 입장은 첨예하게 다를 뿐 아니라 블록체인의 익명성 허용이라는 기준 또한 실명제 등을 통해 본인 스스로를 확인해야 금융서비스 이용이 가능한 기존 금융기관의 입장에서 허가하기 쉽지 않은 일일 것입니다. 이에 대한 대안으로 '콘소시엄 블록체인' 등의 개념들이 대두되고 있으나, 이 또한 '공공 분권화'의 장점을 최대한 이끌어 내지 못하는 것이 현실입니다.

그렇다면 이 지점에서, 블록체인의 가장 큰 특장점인 '공공 분권화'의 기본 철학을 가장 잘 이어받아 기존 산업과 성공적으로 융합이 가능한 분야가 무엇인지 생각해 보면하게 됩니다. 또한 궁극적으로 '만약 어떠한 정보가 완전히 공개 되고 계속 축적이 된다면, 그 정보로 인한 가치는 의미가 있는 일인가'란 근본적인 질문을 하게 됩니다.

만약, 블록체인 기반의 평판 시스템과 현재 발생하고 있는 사이버범죄 정보들이 블록체인 배포 정책 하에서 함께 공유된다면, 블록체인의 '분권화'라는 철학은 다수의 시스템을 사이버범죄로 부터 보호하는데 아름답게 사용될 것입니다. 중앙 집중화된 평판 시스템 내에서 사이버 범죄 정보를 공유하는 것은 정보의 조작이나 파괴 시도가 있어 문제가 될 소지가 있습니다만, 블록체인의 이미 기록된 평판을 조작하기 위해 해킹 하는 것은 블록 체인의 데이터 무결성의 특징으로 자연스럽게 해결되는 부분이기 때문에 안전하게 운영이 가능합니다. 그러나, 특정 거래에 대한 평가가 아닌 정보의 질을 평가하는 평판 시스템에서 만약 Sybil 공격과 같은 공격이 발생할 경우 블록체인의 기본적인 특성으로는 쉽게 차단할 수 없게 되는데, 사전 조작된 정보라는 것은 거래 평판의 평가 결과와 상관없이 기록되기 때문입니다. 그러나, 이 부분은 집단 지성의 힘을 활용한다면 쉽게 해결할 수 있게됩니다.

Chapter 5

집단 지성

블록체인과 결합된 사이버 범죄 관련 평판정보는 악의적 위협 정보를 공유한다는 의미에서 수많은 모방범죄를 예방하고 보호할 수 있는 장점이 있는데, 이와 더불어 사이버 범죄를 조사하는 프레임워크를 구비 함으로써 사후 대응이 가능하다는 것이 더욱 큰 장점이 됩니다. 예를들어, 블록체인의 자율성으로 인해 암호화폐를 노리는 사이버 범죄자들이 사용자의 정보를 훔칠 수 없다는 선입견이 있는데 이는 잘못된 사실입니다.

본질적으로 블록체인은 정보를 투명하게 공유하는 시스템입니다. 모든 거래는 분산 원장에 기록되며 특별한 허가없이도 검증될 수 있고, 모든 거래는 추적 가능하게 됩니다. 사실, 사이버 범죄로 탈취된 암호화폐의 거래 흐름은 쉽게 추적 할 수 있습니다. 돈 세탁의 흔적을 없애는 가장 좋은 방법은 암호화폐 거래소와 코인 쉬프트 시스템을 이용하는 방법입니다. 돈으로 교환하지 않는다면, 코인의 현금 가치를 잃게 되는 것은 당연한 것입니다. 교환이란 것이 존재하기에 선순환이 발생하는 것입니다. BlockSci[6]와 같은 거래 추적 프로젝트와 Interactive Cooperative Framework(ICF:상호 협력 프레임웍)을 통해서 추적기능을 강화할 수 있는데 거래정보를 숨기는 Dash, Zcash, Monero와 같은 익명 거래 코인들에도 똑같이 적용됩니다. 결국, 이러한 코인들도 현금화를 위해 거래소를 필요로 하기 때문입니다.

사이버 범죄와 관련하여 암호화폐 거래소와 협력하는 것은 불가능한 것이 아닙니다. 거래소 또한 엄격한 규정에 따라 사용자를 보호하기 위해 노력 하고 있으며 그에 따라, 대부분의 암호화폐 거래소들은 사용자 비밀 보호라는 기본적인 의무를 다 하기 위해 경찰이나 정부 조사기관의 동의 없이 협력할 수 없다는 조항을 충족해야할 필요가 있습니다. 그러나, 암호화폐 규정은 전세계 나라들 사이에서 서로 다르게 운영되고 있고 지역 조사기관에 소속된 어떤 암호화폐 전문가가 존재하여 그로 부터 도움을 받는 방법은 현재 존재하지 않습니다. 더 안타까운 것은 대부분의 국가에서 암호화폐 관련 사이버 범죄를 실제 금융범죄로 취급하지 않는다는 것입니다. 결국, 법적 시스템으로 부터 보호받지 못하는 선량한 사람들만 재정적 손실을 입게되는게 암호화폐 시장의 현실입니다.

분권형 조사 시스템의 장애요소로 취급되는 현 법률 시스템의 이 엄청난 공백을 메워 줄 수 있는 도구는 바로 사이버 범죄의 존재, 발생, 의심스러운 정황들에 대한 모든 기록이 담겨 있고 그 내용이 결코 변하지 않는 블록체인 그 자체가 될 것 입니다. 모든 정보는 개인, 거래소, 프로젝트, 보안회사, 정부 등에 즉시 투명하게 전달될 수 있으며, 무엇보다 중요한 것은 전 세계의 모든 사람들이 한 시스템 내에서 사이버 범죄를 추적할 수 있다는 것입니다. 집단 지성에 의해 관리되는 평판 시스템은 매우 명쾌한데, 거래소들이 이 시스템을 활용하게 되면 이전에 사용자들이 무력감을 느꼈던 복잡한 법적 증거 확보 노력 없이도 제공되는 평판 정보만으로 선제적인 사전 조치가 가능하게 됩니다. 이렇게 되면, 암호화폐 산업 내에서 발생하는 많은 사이버 범죄를 예방하고 통제할 수 있게됩니다. 다수의 전문가들이 철저하게 검증하고 인증한 개인이나 기관들이 사이버 범죄 수사에 대한 결과를 블록체인에 업데이트 할 권한을 가지게 될 것입니다.

Chapter 6

인공 지능

인공지능의 메커니즘은 최적화된 알고리즘을 사용해 많은 수의 데이터를 모으고 그 중 양질의 데이터를 선별하여 이를 기반으로 모델링 하는 것입니다. 여기서 공격자의 공격행태를 살펴보면, 공격자는 개인, 그룹, 정부, 기업이나 조직을 대상으로 오랜 기간에 걸쳐 시스템의 취약성을 악용하기 위한 지능적인 공격을 수행하며 시스템 침투에 성공하게 되면, 이후 자신의 외부 공격용 커맨드 타워와 시스템 간 불법적인 명령 및 제어 통신을 위해 임의의 커뮤니케이션 채널을 생성하게 됩니다. 이때라면, 이미 내부 네트워크에 성공정으로 침투한 공격자의 행동을 파악하는 것은 쉽지 않은 일이되며, 공격자가 시그니처와 같은 정확한 바이너리를 만들어 외형적으로 합법적인 개체의 행위처럼 보이도록 하는데 있어 현존하는 대부분의 보안기술로는 문제제기를 할 수가 없게 됩니다. 이러한 이유로 많은 공격들이 일상적인 행위로 인식되고 기존의 보안기술로는 방어가 거의 불가능해 지게 되는것이 현재 보안기술의 이슈입니다.

위에서 언급한 공격자의 기술을 메뚜기와 연가시 관계에 빗대어 생각해 볼 수 있습니다. 연가시는 습지 환경에서 살며 번식하는 곤충이지만, 마른 땅에서도 메뚜기와 다른 곤충들을 숙주로 삼아 살아갑니다. 감염된 메뚜기는 처음에는 외관 상 감염이 되지 않은 메뚜기와 구분하기 어렵지만, 연가시가 번식할 준비가 되면 메뚜기의 행동이 바뀌기 시작하는데 화학물질의 분비를 통해 메뚜기의 인지에 영향을 주어 연가시 본인의 의지대로 습한 곳을 찾아 번식할 수 있는 환경을 찾게 하는데 그에 따라 결국 숙주인 메뚜기를 자살하게 만듭니다. 그렇게 함으로써, 연가시는 자신의 생명주기의 다음 단계를 시작하는 상황을 만들게 됩니다.

기계학습 기반의 보안 기술 핵심은 공격자의 공격에 따른 결과를 중요시 하는 것이 아니라, 공격과정에서 이상행위의 변화를 처음부터 지속적으로 추적하는데 있습니다. 앞서 언급한 연가시가 메뚜기의 두뇌를 제어하는 동안, 메뚜기의 외형은 정상적인 메뚜기와 전혀 다를 것이 없지만 습한곳을 찾아 물에 뛰어드는 이상행동을 하는 등의 정상적 활동 범위를 벗어나게 됩니다. 이를 통해 곤충학자들은 메뚜기의 이상행위를 관찰하는 것 만으로도 감염된 메뚜기를 구분해 낼 수 있게됩니다. 이를 보안에 적용하면, 외형의 변화보다는 경미한 행동변화의 상관관계 분석을 수행해 관찰되고 있는 보안 상황을 인지하고 대처할 수 있게 되어 보안위협을 제어할 수 있게 됩니다.

Sentinel Protocol이 블록체인과 인공지능을 모두 함께 사용할 수 있는 방법은 두 가지가 있습니다. 첫번째는 유저와 노드의 정보를 수집하고, 거래 패턴을 포함해 당신의 컴퓨터 사용 패턴들에 대한 정상적 행위와 같은 모든 측면의 행위들을 모델링할 수 있는 머신러닝 기반의 블록체인 보안 클라이언트 지갑을 제공하는 것이 그것입니다. 이상행위가 발생할 때, 그 보안지갑은 보안위협에 대한 가능성을 인지하고 해당 프로세스가 실행되는 것을 차단하게 됩니다. 자세한 정보는 집단지성 그룹에 보고되고 평판 시스템에 공유됩니다. 모든 정보는 API를 통해 이를 사용하기 원하는 모든 사람에게 공유되고, 세계에서 가장 정확하고 안전한 글로벌 지능형 시스템으로 확장되게 됩니다.

두 번째 방법은, 블록체인의 데이터를 활용하여 사기 탐지 시스템(Fraud Detection System)을 구성하는 것 입니다. 본질적으로, Sentinel Protocol의 이상 탐지는 합의 시스템과 연관되어 있습니다. 집단 지성 그룹이나 다수의 전문가들(또는 SIPB의 초기 단계에서는 웁살라 재단이 직접 인증할 수 있습니다.)에 의해 인증된 개인은 ‘The Sentinels’로 명명되며 ‘글로벌 사이버범죄 자경단’과 같은 역할을 하게 됩니다. The Sentinels는 보안 위협에 대한 연구 및 분석을 담당하고 평판 시스템을 업데이트 할 수 있는 특수 권한을 가지게 되며, Sentinel Protocol의 공유 경제 시스템을 통해 보상을 받게 됩니다. 또한, 내부자의 위협을 방지하기 위해서, 사기 탐지 시스템(이하, FDS)을 설치하여 일반 사용자의 비정상적 거래는 물론 집단 지성 내의 비정상적인 동작까지 모니터링하고 탐지하게 됩니다.

Chapter 7

보안 기능

블록체인을 위한 보안 지능형 플랫폼인 Security Intelligence Platform for Blockchain(SIPB 또는 Sentinel Protocol)은 다음의 보안 기능들을 보유하게 됩니다.

- 위협 평판 데이터베이스 (TRDB)
- 머신러닝(ML) 엔진 통합형 보안 지갑 (S-Wallet)
- 분산 말웨어 분석 샌드박스 (D-Sandbox)

위협 평판 데이터베이스 (TRDB)

위협 평판 데이터베이스 (TRDB)는 기존의 사이버 보안 업계에 존재하는 두 가지 문제를 해결할 수 있습니다. 첫 번째 문제는 보안 회사의 중앙 데이터베이스입니다. 위협 정보를 데이터베이스화 하여 하나의 중앙 집중식 장소에 보관하면 해당 정보는 정보 조작 및 악용에 취약 해지는데, 분명한 것은 해당 데이터베이스는 Sybil 공격 또는 서버 해킹 및 서비스 중단의 분명한 타겟이 된다는 것입니다. 이는 인터넷에 존재하는 중앙 집중식 '클라이언트 - 서버'모델의 근본적인 문제인데, 예를 들어, 2017 년 10 월 러시아 해커들은 잘 알려져 있는 안티바이러스 제공 회사 인 카스퍼스키의 바이러스 백신 소프트웨어를 사용하여 미국의 NSA 자료를 훔쳤습니다. 이는 기본적으로 해커들이 공격 대상의 취약성을 찾기 위해서 해당 시스템을 보호하고 있는 보안 솔루션을 이용했다는 점에서 보안 솔루션 또한 더 이상 안전하지 않다는 아이러니한 사건으로 알려져 있습니다. 블록체인의 분권화는 불변성으로 인해 데이터를 변경하는 것 자체가 어렵기 때문에 이러한 문제를 해결할 수 있습니다. 이렇게 하면 데이터를 제공하는 서버의 보안 안정성을 향상 시킬 수 있게 됩니다.

또 다른 문제는 보안 업체들 간에 보안 정보 공유가 부족하다는 것입니다. 수집된 위협 정보는 많으면 많을수록 사이버범죄를 예방할 가능성이 높아지게 되지만, 각 보안 업체들은 해당 위협 정보를 공유 하더라도 자신들에게 돌아올 이득이 없기 때문에 포괄적인 관련 정보를 취합하고 서로 동기화할 이유가 없으며 자신들만 보유한 보안 정보가 있다면 이를 '승자독식'의 논리로 생각하여 공개를 꺼려하는게 현실입니다. 가트너의 안톤 추바킨 리서치 부사장은 "악의적 해커들이 서로간에 데이터, 속임수, 방법들을 유기적으로 공유하는 것에 비해 선한 의지를 가진 사람들이 그에 대해 효과적으로 대응하지 못하는 것은 정말 화가 나는 일입니다."라며 기존 보안업계의 보안위협 대응에 대한 엄청난 비효율성을 비판하기도 했습니다. 이에 Sentinel Protocol은 11장에서 설명될 인센티브 제도를 활용하여 보안 전문가들과 업체들을 참여 및 독려하고 보안위협에 공동 대응할 수 있는 합의 메커니즘, 참여자의 피드백 또는 Delegated Proof of Stake(DPOS) 기반 하에 위협 데이터베이스(TRDB)를 구축하고자 합니다. 이러한 집단 지성을 통해, TRDB는 가장 효과적이고 효율적으로 해커의 지갑주소, 악의적 URI, 피싱 주소, 말웨어 해쉬 등을 수집할 수 있습니다.

오탐(false positives) 처럼 계통적인 오류들을 제거하기 위한 TRDB 업데이트 권한은 반드시 보안 전문가들에게만 제공됩니다. 그에 반해 일반 사용자들은 자동보고 및 수동보고의 두 가지 방법으로 참여할 수 있습니다. 사용자가 자동보고를 허용하면, 머신러닝 기반의 보안 지갑을 통해 검출된 알려지지 않은 보안위협들은 자동으로 데이터베이스에 업데이트 됩니다. 또한, 수동보고를 통해 나중에 커뮤니티를 통해 검증될 위험 정보를 보고할 수도 있습니다. TRDB는 API를 통해 제공되기 때문에, 어떠한 개인이나 조직(예를 들어, 암호화폐 지갑 프로젝트들, 암호화폐 거래소들, 그리고 보안 업체들)도 이렇게 구축된 데이터베이스의 정보를 이용할 수 있게 됩니다.

머신러닝 엔진 기반, 통합 보안지갑 (S-Wallet)

S-Wallet이 기존 바이러스 백신 소프트웨어와 유사한 기능이 있으나, 근본적인 차이점을 보이는 것은 기존 바이러스 백신 소프트웨어는 모든 새로운 알려진 시그니처에 대해 중앙 서버를 통해 최신 업데이트를 수시로 수신 해야만 새로운 위협에 잘 대처할 수 있다는 것입니다. 이 접근법은 인간이 생성한 시그니처 업데이트가 존재하지 않으면 제로데이 공격 처럼 알려지지 않은 위협에 대응하기 어려운 단점이 있습니다. 반면 S-wallet은 이러한 위협의 경향 및 기록들을 분석하는 방법으로 위협이나 제로데이 공격에 있어 시그니처 업데이트 없이 사전 대응할 수 있습니다. 따라서, 이러한 비지도 머신러닝 방법을 통해 랜섬웨어[7] 와 같은 위협에 대해 특히 효과적 입니다. S-wallet은 연결된 TRDB의 집단 지성을 활용, 다음 정보에 대한 기본적인 차단 서비스를 제공합니다:

- 암호화폐 지갑의 주소 필터링
- URL/URI 필터링
- Data 필터링
- 사기 검출 시스템(Fraud Detection System)

Sentinel Protocol의 머신러닝 기술이 블록체인의 모든 분산원장 사기 탐지 시스템 FDS(Fraud Detection System)에 개입하며, 도난으로 의심되는 거래를 식별함으로써 2차 피해를 예방한다는 점에서도 의미가 있다 하겠습니다.

말웨어 분석용, 분산 샌드박스 (D-Sandbox)

샌드박스는 응용프로그램이나 호스트에 어떠한 위해 없이 테스트 되지 않거나 확인되지 않은 프로그램 또는 코드를 별도의 가상 컴퓨터에서 실행하여 무결성을 검증하는 보안 메커니즘입니다. D-Sandbox는 티켓 시스템을 통해 제출된 잠재적 위협을 집단 지성을 통해 분석하는 보안 기능 입니다.

D-Sandbox에는 두 가지 뛰어난 장점이 있습니다. 첫째, 상당히 비용 효율적 입니다. 분산 시스템을 통해 무한 확장이 보장됩니다. 일반적인 샌드박스 보안 어플라이언스는 가상 머신을 통한 실행이 권고사항인데, 아무리 고가의 보안 어플라이언스라도 이런 방식으로 멀웨어를 분석하는 데 매우 제한적입니다. 또한 일반 샌드박스 시스템은 높은 처리량, 높은 대역폭, 예상보다 높은 사용량과 같은 고성능이 보장되지 않는다면, 상당히 불안정하게 동작하게 되게 됩니다. 이로 인해 시스템 성능 저하 및 오작

동이 발생하여 결국 사용자 경험에 해를 끼칠뿐만 아니라 최악의 경우 악성코드 감염을 차단하지 못하는 결과도 초래하게 됩니다.

두 번째 장점은 D-Sandbox는 작업 증명(PoW)에서 소요되는 컴퓨팅 성능의 낭비를 해결할 수 있고, 더 나은 보안 생태계를 구축 할 수 있다는 것입니다. 실제로 해시 값을 생성하는데 사용 되는 컴퓨팅 성능은 낭비입니다. Sentinel Protocol의 네트워크에 참여하는 노드는 자신의 컴퓨팅 파워를 사용하여 말웨어를 추가로 분석 할 수 있습니다. 결국, 분산 시스템의 장점은 그들의 유휴 자원이 필요한 곳에 활용 될 수 있다는 것입니다. 개별 사용자들은 가상머신을 통해 적당한 샌드박스의 공급계획을 세움으로써 전반적인 보안 생태계를 강화하는데 기여하게 되고, 결과적으로 보안위협에 대응할 수 있는 도움을받을 수 있게 됩니다.

Chapter 8

Sentinel Protocol 생태계

다음은 블록체인 보안 지능형 플랫폼(Security Intelligence Platform for Blockchain : 이하, SIPB 또는 Sentinel Protocol) 생태계의 사용자 사례에 대해 설명합니다.

상호 협력 프레임웍 (ICF, or Sentinel Portal)

암호화폐 업계의 비즈니스 연속성에 가장 큰 장애물 중 하나는 보안입니다. 고객 해킹 사건 및 그와 관련된 비용은 최근 엄청나게 증가했지만 적절한 보안 조치는 아직 마련되지 않고 있습니다. 업계가 급속도로 성장하는 경우 보안요소들을 모두 다루기는 어렵지만 이와 관련된 보안 사고에 있어 변명의 여지는 있어서는 안됩니다. 일부 암호화폐 거래소의 플랫폼은 초기 시스템 설계에서 전체 운영에 이르기까지 보안 전문성이 부족하다 말할 수 있습니다. 거래소 고객서비스 전문가는 사이버 보안전문가는 아니지만 현재로서는 두가지 임무를 모두 수행할 수 밖에 없는 상황입니다. Sentinel Protocol은 신뢰할 수 있는 암호화폐 보안 전문가와 집단 지성에 의해 실행되는 필수 프레임워크를 제공함으로써이 문제를 극복합니다. Sentinel Protocol 커뮤니티에 가입함으로써 암호화폐 사용자는 모든 보안 문제에 대한 지식과 지원을 쉽게 얻을 수 있습니다. 또한 Sentinel Protocol이 제공하는 보안 솔루션을 활용할 수 있습니다. 기업 및 개인은 모두 비효율적인 비용에 대한 부담을 덜게 될 것입니다. 이 프레임워크는 암호화폐 세계의 전반적인 보안을 강화하고 블록체인의 기술 철학인 분권화의 기본 원칙을 철저히 준수하며 발전합니다.

베타버전은 홈페이지에서(https://www.sentinelprotocol.io) 공지 될 예정입니다.

도난 방지 시스템

암호화폐를 위한 실생활의 응용프로그램이 매일 만들어 지고 있지만, 암호 자산의 보안측면에서 무결성을 입증할 수 있는 시스템은 거의 없는 것이 현실입니다. 즉, 도난 당한 암호 자산을 해커가 텀블링과 믹싱을 통해 분할 한다면, 충분히 상용 서비스 지불에 악용할 수 있다는 의미입니다. 이를 방지하기 위해 Sentinel Protocol은 카드 회사가 도난당한 신용 / 직불 카드의 사용을 차단하는 현실 세계의 경우와 마찬가지로, 도난 당한 모든 암호화폐를 추적하여 이 정보를 암호화폐 관련 서비스 공급자에게 알려줍니다. 그러면 이 도난 당한 암호 자산은 현실 세계의 현금으로 바꾸거나 사용 할 수 없게 되고, 이 보호 체계는 규제 제한 하에 암호화폐 더욱 안전하게 유지할 수 있게 될 것입니다.

거래 오류 방지

사기로 등록 된 주소 및 관련된 모든 파생 주소들은 블록 체인의 특성으로 인해, Sentinel Protocol 커뮤니티 내에 실시간 공유되고, Sentinel Protocol이 적용되어 있는 한 피해 확산은 방지

됩니다. ICO가 진행되는 과정을 예를 들면, 일반적으로 수천 명의 투자자가 참여하는 ICO의 피투자자 지갑 주소도 훼손 되어 악용 될 가능성이 있는데, 만약 해커가 ICO관련 주소를 변경 하더라도 모든 사용자들에게 원래의 정상 주소와 새로 변경된 주소를 자동으로 알리게 되어 안전하게 됩니다. 이렇게 되면, 이전까지는 이렇게 작동하는 확실한 보안 플랫폼이 없었기에 관련 보안 업계의 패러다임을 완전히 바꿀 수 있게 됩니다. 지금까지는 수천 명의 개별 사용자가 공격 사실을 통보 받고 동시에 피해 확산을 방지 할 수있는 체계적인 방법은 없었습니다.

알려지지 않은 위협 차단 사례 (유저 시나리오)

해커로 활동하는 Malloy는 유명한 암호화폐 온라인 커뮤니티에 본인이 만든 채굴소프트웨어를 업로드하게 됩니다. 해당 소프트웨어는 위협 검사 웹사이트 중 평판이 좋은 'VirusTotal' 이나 안티 바이러스 어플리케이션에서 조차 탐색되지 않는 소프트웨어로 만들어 졌습니다. 시간이 흘러, Alice를 비롯한 수십 명의 커뮤니티 사용자가 이 겉보기에 평범해 보이는 채굴소프트웨어를 다운로드합니다. (불행히도, 해당 소프트웨어를 다운로드한 대부분의 사용자는 md5, sha 등을 통해 원본 파일의 무결성을 검사하는 방법 조차 모릅니다.) Malloy는 해당 소프트웨어(백도어)가 사용자의 기기에 다운로드 되었다는 것을 인지하는 순간, 해당 소프트웨어를 무결하고 정상적으로 보이는 파일로 변경합니다. 이러한 상황에 이르면, 이미 첫 번째 채굴 소프트웨어(백도어) 사용자는 이미 감염이 된 상태가 되고, 모든 정보는 Malloy에게 전송됩니다. 즉, 지갑의 개인 키의 암호문과 암호화폐 거래소의 증명서 모두 Malloy에게 전송된 상태란 의미입니다. 하지만 불행하게도, 이런 상황에서 단순 일반사용자인 Alice는 이 사이버 범죄를 조사하는 데 필요한 조사 기술이나 도구를 가지고 있지 않기 때문에 시스템이 어떻게 감염 되었는지 조차 확인하기 어려운 상황에 놓이게 됩니다.

한편, 동일한 온라인 커뮤니티 사용자 인 Bob은 Sentinel Protocol의 S-wallet을 사용합니다. Bob 역시 Malloy에 의해 손상된 채굴 소프트웨어를 다운로드합니다. 그러나, S-wallet 내의 머신러닝 엔진은 다운로드한 채굴 소프트웨어가 매우 의심 스럽다는 것을 감지합니다. 해당 소프트웨어가 잘 알려지지 않은 공격이고 따라서 지금까지 'VirusTotal'이나 바이러스 백신 소프트웨어로도 탐지되지 않은 경우라 할지라도 S-wallet의 머신러닝 엔진은 해당 소프트웨어의 실행을 차단하게 됩니다. 해당 소프트웨어의 실행이 차단되자 마자 위협 관련 정보는 자동으로 Sentinel Protocol에 제출되게 됩니다. 그후, 신뢰할 수있는 보안 전문가 그룹 인 The Sentinels가 위협의 근본 원인을 분석합니다. 이 분석 된 정보는 TRDB (Threat Reputation Database)에 등록되며 해당 소프트웨어가 처음 발견 된 온라인 커뮤니티에도 이 정보가 공유가 되고 해당 소프트웨어가 업로드된 시간 기록 등의 정보와 업로더에 대한 자세한 분석을 통해 Malloy는 해커로 확인됩니다. 한편, Malloy는 Sentinel Protocol 위협정보 데이터베이스가 실시간으로 모든 곳에서 사용 되고 있기 때문에, 자신의 채굴 소프트웨어를 악의적으로 배포할 수 없다는 것에 좌절하게 될 것입니다.

거래 추적 (유저 시나리오)

해커로 활동하는 Malloy는 많은 사람들로부터 해킹하여 훔친 코인의 지갑을 가지고 있습니다. 이 코인들을 현금화 하기 전에, 그는 추적을 피하기 위해 여러 하위 주소에 코인을 분배하게 되고 이러

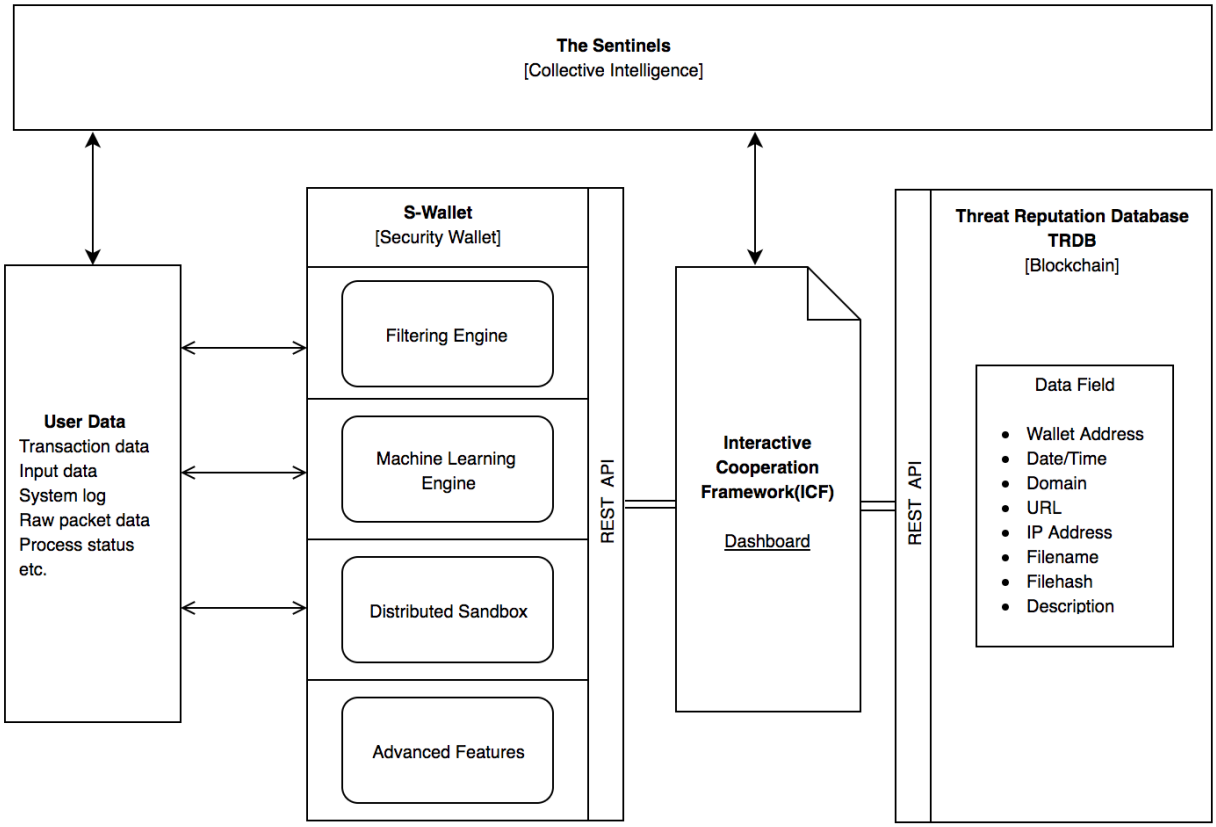
한 과정은 암호화폐 지갑의 특성 상 가능한게 현실입니다. Alice는 Malloy의 희생자 중 하나입니다. Alice가 동전을 도난당한 것을 알게되자, 그 사실은 Sentinel Protocol에 사례 정보로 보고 됩니다. 신뢰할 수있는 보안 전문가 그룹 인 The Sentinels는 사건을 확인하고 사례 정보를 TRDB (Threat Reputation Database)에 등록합니다. Sentinel Protocol은 등록 된 원래 주소에서 파생 된 모든 하위 주소를 자동으로 추적하게 되고, 이 정보는 Sentinel Protocol과 통합된 거래소들을 포함 모든 암호화폐 서비스들에 공유됩니다. 이러한 사실을 모르고 있는 Malloy가 현금 전환을 시도하게 되고, 이미 우선 순위가 높은 경보를 수신한 거래소 및 암호화폐 서비스의 시스템들은 해커인 Malloy가 훔친 코인을 사용할 수있는 기회를 차단하게 됩니다. 하지만 이렇게 된다 하더라도, Alice는 도난당한 코인을 되찾기 어렵습니다. 왜냐하면, 불행하게도 유럽에 거주하는 Alice가 미국에 있는 거래소에서 발생된 해킹 사건으로 발생된 금전적 손해를 현재의 사법제도 체제 아래에서 보상 받을 길은 없기 때문입니다. 실의에 빠진 Alice가 적극적으로 자신의 사례를 전파 함과 동시에 Sentinel Protocol 사용의 이점을 널리 알리게 된다면, 머지 않은 미래에 Sentinel Protocol은 해킹 신고 및 처리를 위해 인터폴이 요구하는 각종 복잡한 문서 및 법적 신원 확인 요청을 대체하는 역할과 사명을 감당하고 있을것입니다.

Chapter 9

아키텍쳐

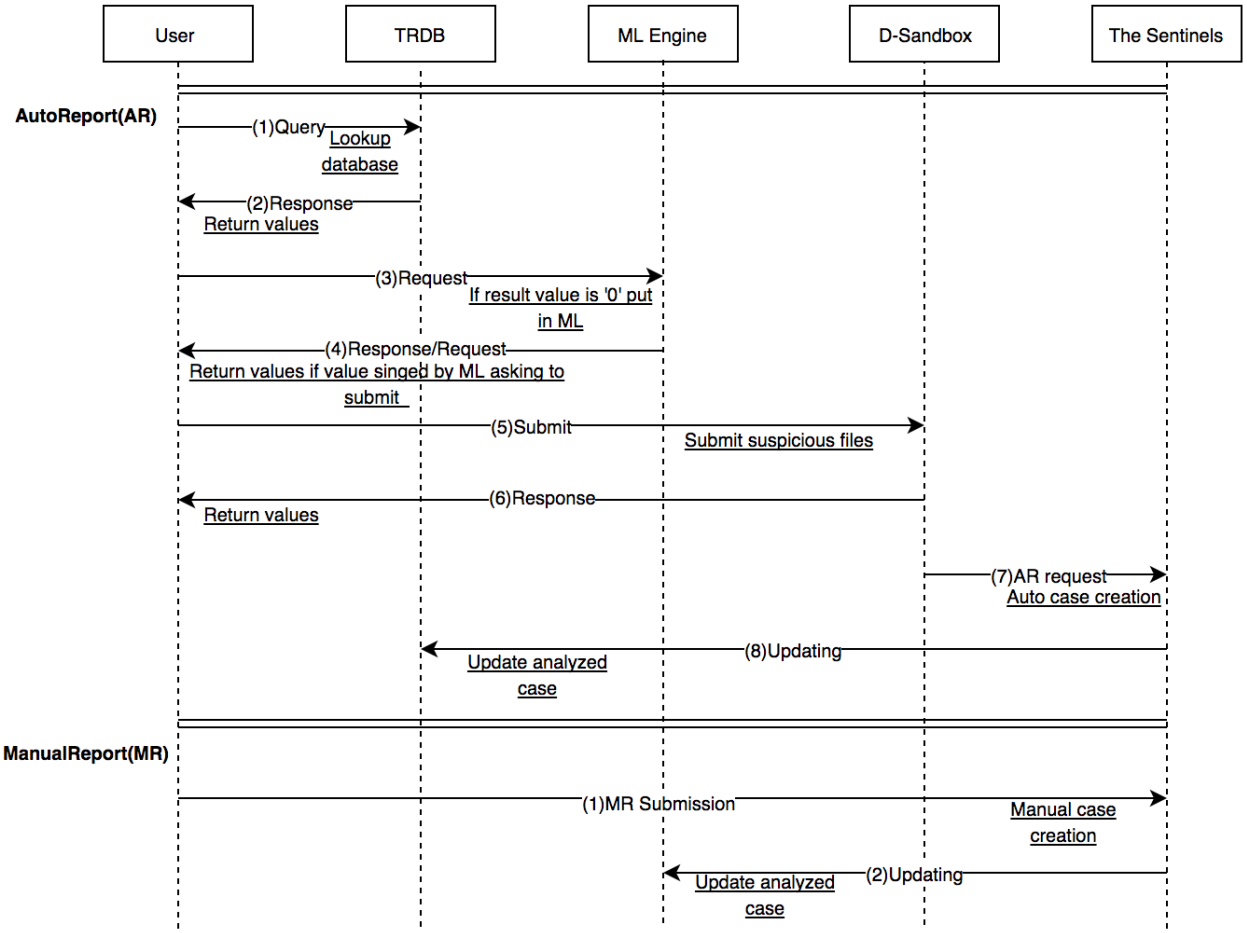
Sentinel Protocol은 자체 통합된 보안 지갑을 통해서 모든 보안 서비스들을 제공되지만, 이와 함께 각각의 서비스들이 제3자가 개발한 어플리케이션(또는 서비스 등)과 협업 가능하도록 설계된 API도 제공될 것입니다. 기본적으로, Senitinel Protocol의 통합 보안지갑은 보안 위협신고를 위해 '자동 보고' 및 '수동 보고' 두가지의 기능이 제공됩니다.

[Technology Architecture: Security Intelligence Platform for Blockchain]



- S-Wallet : 통합 보안 지갑
- User Data : 유저가 입력 데이터, 거래 데이터, 시스템 로그, 그리고 패킷 데이터
- Filtering Engine : 암호화폐 주소, 사기성 도메인 주소, URL, IP, 그리고 파일에 대한 필터링 용 엔진
- Machine Learning Engine : 이상 행위 분석을 위한 로컬 머신러닝 엔진
- Distributed Sandbox : 말웨어 분석용 분산 샌드박스
- Threat Reputation DB : 사이버범죄 정보가 저장된 지능형 데이터베이스
- Plugin Features : VPN, 제3자 통합 암호화폐 지갑과 같은 기능 강화 보안솔루션은 추후 개발
- The Sentinels : 보안 분야 전문성을 인증 받은 집단 지성 그룹 및 개인
- Interactive Cooperation Framework(ICF) : 전 세계에서 발생하는 보안위협 행위에 대한 근본 원인 분석과 보안사고 분석 및 대응 정보가 담겨 있는 Sentinel Protocol 포탈의 대시보드로서, 권한을 소유한 The Sentinels들이 활용

[Security Intelligence Platform for Blockchain (SIPB) Process Flow]



Sentinel Protocol의 S-Wallet(이하, 보안지갑)이 실행되는 동안, 특정 도메인, URL, 암호화폐 지갑 주소, 파일 다운로드 관련된 링크나 경로재설정 행위가 감지될 경우 다음의 상황이 발생됩니다 :

자동 보고 (Auto Report)

자동 리포트는 알려지지 않은 위협분석을 위한, 최적화된 지능형 프레임워크입니다.

1. Query : Threat DB를 통해, 보고된 정보의 잠재된 사기나 피해 여지가 있는지에 대한 조사를 수행합니다.
2. Response : Threat DB를 통해, 등록된 정보의 데이터 필드를 제공합니다.
3. Request : 사기나 피해로 확인된 주소에 대한 문의가 들어올 경우 이 주소는 우선 차단 되며, 심지어 새로운 주소나 처음 다운로드된 파일 그리고 새로운 프로세스가 시작된다 하더라도 머신러닝 엔진이 사기나 피해 등의 위협요소가 없는지 분석하고 확인하게 됩니다.
4. Response/request : 머신러닝 엔진은 알려지지 않은 위협을 파악하기 위해 파일들이나 프로세스들의 이상행위를 분석하고 차단하고 사용자들에게 이 정보를 보고 할것인지에 대해 질의하게 됩니다.
5. Submit : 사용자가 승인 옵션(on 또는 off 선택가능)을 가동할 경우, 해당 정보는 말웨어 검사 및 분석을 위해 Distributed Sandbox로 전달되게 됩니다.
6. AR Request : 자동 보고된 사례는 ICF 대시보드에 생성되고 공유됩니다.

7. Analysis response : The Sentinels는 샌드박스나 추가적인 보안도구들을 활용하여 알려지지 않은 보안 위협을 분석하게 됩니다.
8. Updating : Threat DB로 송신된 위협정보는 항상 최신으로 업데이트됩니다.

수동 보고 **(Manual Report)**

사용자는 수동으로 사기성 정보에 대한 보고를 할 수 있습니다.

1. MR Submission : 의심스러운 Domain, URL, 사기성 주소 및 파일들에 대한 정보는 The Sentinels에 직접 보고할 수 있습니다.
2. Updating : 사기성 정보에 대한 검증 후, 관련된 정보는 Threat DB에 최신으로 업데이트됩니다.

Chapter 10

합의 시스템

작업 증명(Proof of Work : 이하, PoW) 알고리즘의 기본 구조는 그 결과가 채굴을 통해 주어진 목표 난이도에 도달하면, 블록을 생성할 권한과 그 수고에 대응하는 혜택을 제공하는 것입니다. 그런데, 그 결과를 찾는 과정에 많은 시행착오가 발생하게 되고 그에 따른 광범위한 계산작업이 필요하게 되어 전문 채굴자에 의해 많은 자원의 낭비가 일어나고 있습니다. 따라서, 이 복잡한 계산을 성공적으로 수행한 개체가 과반수를 대표하는 권리를 갖게 됩니다. 그런데 문제는 이 과정에서 많은 전력 낭비 등의 비효율성이 대두 되었고, 그래서 탄생한 것이 지분증명(Proof of Stake : 이하, PoS)입니다. 이 PoS 알고리즘은 지분을 보유한 양이 많을수록 대표자가 될 확률이 높아지는 방식으로 잘 알려져 있습니다. 그러나, 상기 두 가지 알고리즘 모두 대표자가 좋은 의도가 있는지 악의적 의도가 있는지 구분할 수 없기에 '51% 공격'(100개의 노드 중 51개만 내 편으로 만들면 거래장부의 위조가 가능한 공격이론)에서 100% 자유롭지 못한 한계를 여전히 드러내고 있습니다.

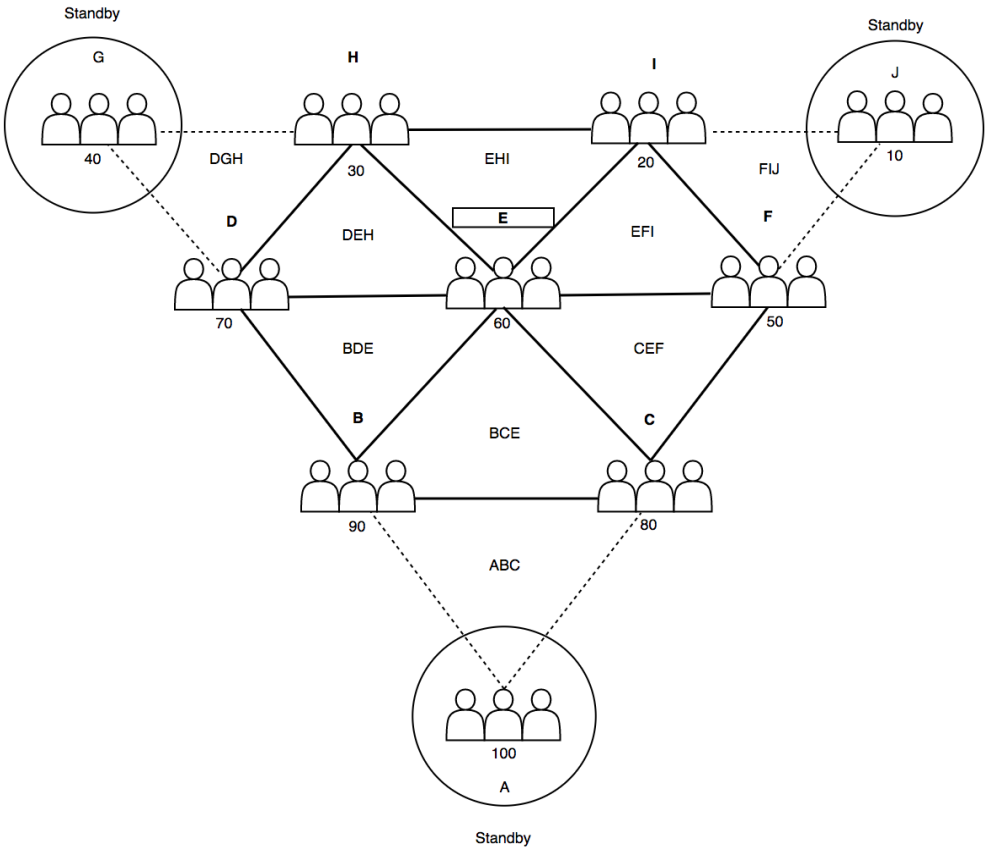
Sentinel Protocol의 합의는 본질적으로 다니엘 라리머가 개발하여, BitShares에서 소개한 위임 지분 증명(Delegated Proof of Stake) [8]의 개념을 사용합니다. 웁살라 재단이 위임 한 The Sentinels는 암호화폐 거래소의 보안 팀, 글로벌 사이버 보안 연구 회사 또는 화이트 해커 그룹 또는 개별 화이트 해커 등과 같이 충분한 자격을 갖춘 검증된 기관, 개인 그리고 그룹이 될 수 있습니다. 그들 모두는 자신의 사회적 지위와 평판을 이미 스스로 입증 한 전문가 들이기 때문에 실제로 부정을 저지를 위험요소는 상당히 줄어들게 되고 합의는 최선의 선택이 될 것입니다. 그럼에도 불구하고, 사회공학적 관점과 그 합의 알고리즘 사이에 어느 정도의 간극이 존재하게 될 것입니다. 이 문제를 해결하기 위해, 그들의 평판은 Sentinel Point(SP) 점수로 평가 되고, 부여 받은 Sentinel Point는 순환 통화인 UPP과 연계 해 그들에게 혜택으로 돌아가게 될 것입니다. Sentinel Point는 The Sentinels의 일원으로 행동함으로써 얻을 수 있게 됩니다. 예를 들어, 자동보고와 수동보고에 등록 된 사례를 분석하고 관련 정보를 위협 데이터베이스(TRDB)에 기록한 다음 해당 데이터를 기반으로 생태계에 많은 도움을 주는 경우가 그에 해당할 것입니다. 또 다른 방법은 성과에 따라 사람들이 실제로 그들의 평판에 투표 하는 과정을 통해서도 Sentinel Point를 얻을 수 있게 됩니다. 이 합의 시스템은 Sentinel Protocol의 Proof of Protection(PoP)로 정의된 평판점수를 획득 하는 방식으로 대표자 위임되는 시스템입니다. 만약 부정직한 The Sentinels의 구성원이 Sentinel Protocol을 부적절하게 활용해 예를 들어, Sybil 공격이나 블록체인 포킹과 같은 해를 끼치는 상황이 된다면, 그는 그의 평판을 스스로 잃게 될 것이며 평판 점수 또한 잃게 되고 심지어 The Sentinels의 자격조차 잃을 수 있는 상황이 오게 될 것입니다. 이더리움 [9]의 Slasher와 마찬가지로, 명성과 자격의 상실은 곧 대표자의 위치를 잃게 되는 것과 같은 의미라 할 수 있습니다.

본 평판 시스템의 장점은 개인이 자신의 전문 분야에서 쌓아 온 신뢰를 기반으로 대표성을 나타내는 구조이기 때문에 결코 스스로 악당이 될 가능성은 상당히 낮게 됩니다. 엄밀히 말해, 이 신뢰 구조에서는 많은 수의 대표로 위임된 Sentinels는 필요 없습니다. 이는 합의를 확보하기 위한 무작위성을

높이고 불필요한 지연을 추가하는 역할을 담당하게 됩니다. 따라서, Sentinel Protocol의 합의 구조에는 트랜잭션 유효성 검사, 블록 생성 및 위협 데이터베이스 업데이트로 청구되는 단 7 명의 Sentinel 중 작은 그룹만 있게 됩니다. 명성 랭킹에 따르면 총 10 명의 Sentinel이 선택되며, 7 명은 Active로 지정되고 3 명은 Standby로 지정됩니다. 3명의 Sentinel은 네트워크 대기 시간과 지연을 줄이기 위해 필요로 하지 않는 한 Standby 상태를 유지하게 됩니다. 중요한 네트웍의 단편화, 대규모 DDoS 공격 또는 대다수의 The Sentinels가 서로 통신을 잃게 만드는 예기치 않은 이벤트의 경우 PoP 동기 알고리즘과 비동기식 비잔틴 장애대응책(BFT)[10]이 장애대처를 위한 합의 알고리즘으로 지원되게 됩니다.

Sentinel Protocol의 Proof of Protection(PoP)는 지연, 확장과 신뢰성 측면에서 간편하고 효율적으로 설계되었습니다.

[High Level Consensus Diagram]



- 위임된 10명의 Sentinels 들은 상기 다이어그램과 같이, 역 피라미드 구조를 가지게 됩니다.
- 다이어그램에 있는 그룹의 사람들은 The Sentinels입니다. (개인 또는 조직)
- 각 그룹 아래의 점수는 그들의 기여로 얻은 센티널 포인트를 나타냅니다.
- A, G, J는 엔드포인트로서 대기(Standby) 상태입니다.
- 6각형의 노드들은 무작위로 블록을 생성할 권한을 가지고 있습니다.
- 브로드캐스트를 최소화하기 위하여 작은 삼각 구조의 멀티캐스트 그룹을 지정합니다.
- 최초의 합의는 고정된 7개의 노드들로 구성됩니다.
- BFT를 활성화 하기 위해 ‘n=3f+1’구조가 되어야 하는데 최대 10개의 노드가 활용가능하며 3개의 잔여 노드는 standby가 되며 그리고 E노드는 마스터 노드가 됩니다.

- Standnby 노드는 DoS 저항성을 가지기 위한 고가용성 노드들로 A,G, J는 각 피어 노드의 백업을 담당하게 됩니다. 안정화된 네트웍 보안환경을 위해 The Sentinels 노드는 노드 보안에 관련한 최적의 방안을 구성해야 합니다.

Chapter 11

인센티브 시스템

Sentinel Protocol은 중앙 집권화된 지침이나 조직을 필요로하지 않고, 참여자가 스스로 공헌도를 높이고 기여도에 따라 보상받는 자급자족 형태의 사이버 보안 생태계 유지를 지향 합니다. Sentinel Protocol은 실효성 있는 사이버 보안 생태계로서, 보안 위협에 대응 가능한 최적의 도구 또는 서비스를 제공하게 되고 그에 따른 직접 지불을 위해 교환 가능한 암호화폐를 필요로 합니다. 더불어, 사이버 보안 생태계를 지속 향상시키기 위해서는 개인별 기여도를 나타내는 독립적 인 가치도 필요하게 됩니다. 그에 따라, Sentinel Protocol은 Security Intelligence Platform for Blockchain(SIPB) 보안 도구와 서비스 사용을 위해 UPP(Uppsala)이라고 명명한 순환 암호화폐를 발행하게 되고, Sentinel Protocol 생태계에 참여하는 개인 또는 그룹의 공헌도에 따른 명성 가치를 보상하기 위해 Sentinel Points(SP)를 제공하게 됩니다.

초기에 높은 공헌을 하는 개인이나 그룹에게는 보다 많은 양의 인센티브가 제공됩니다. Sentinel Protocol이 초기 상태를 벗어나 일정 수준의 보안 인텔리전스를 갖추거나 일정 기간이 지난 때에는, 초기 공헌자에게 혜택을 더 많이 제공하기 위해 다른 공헌자를 위해 할당된 보상금의 양은 상대적으로 줄어들게 됩니다. 본 인센티브 시스템은 사이버 보안 전문가들로 부터 도움이 필요한 사람들과 이 시스템에 참여할 전문가들(개인 또는 조직) 모두를 독려하기 위해 설계되었습니다.

[UPP Point (Uppsala)]

- UPP은 SIPB에 의해 제공되는 보안 도구 및 서비스를 위해 사용되는 통화로서, 보안지갑의 고급 보안 기능들을 사용할 때 활용됩니다.
- UPP은 또한 상세한 사이버 포렌식 서비스, 컨설팅, 취약성 평가, Sentinel Protocol의 도움이 필요한 기타 활동 등에 대한 의뢰 요청 시에도 활용됩니다.
- 사용료는 카이버 네트웍과 같은 DEX (분산 거래소) 플랫폼에서 스마트 계약으로 수집됩니다.
- 초기 단계의 사이버 보안 커뮤니티 빌더들을 위해, 초기 500,000,000 개의 UPP이 생성되고 배포됩니다.
- 하기에 명시되어있는 인플레이션률에 따라서 Proof of Protection을 통하여 Sentinel Protocol을 발전시킨 사용자에게20회에 걸쳐서 추가적인 UPP이 생성되고 배포됩니다.
- 초기 기여자에게 더 많은 인센티브를 주기위하여 초기 인플레이션률은 3~7%사이로 정해지며 이후 인플레이션률은 0%에 수렴할때까지 로그함수감소를 따릅니다.
- 재단의 UPP 수입원인 고급기능 사용료, 케이스 처리 수수료, 그리고 추후 추가될 기능들로 모여진 수입의 30%는 인플레이션과 별도로 커뮤니티의 기여자들을 보상하기 위하여 추가 배포 됩니다.
- UPP의 배포(vesting) 주기는 Sentinel Point가 설정된 값에 도달하였거나, 특정 주기의 주간(week)중 선도래를 기준으로 합니다. 자세한 계획은 추후 공지 될 예정입니다.
- 초기 UPP의 15%는 Uppsala Foundation을 위해 배정됩니다.

- 비즈니스 개발, 개발 자금, 법률 자금, 어드바이저 인센티브, 기타 자금을 필요로 하는 조직 활동 등을 돕기 위해 초기 UPP의 15%가 배정됩니다.
- 어드바이저 인센티브를 위해 초기 UPP의 2%가 배정됩니다.
- 예기치 않은 비즈니스 활동을 대비하여 초기 UPP의 8%가 배정됩니다.
- UPP(초기 UPP의 60% 정도)의 나머지는 Sentinel Protocol 초기 공헌자, 사용자, 공헌자, 후원자 등을 위해 시장에 배포합니다.
- 초기 UPP 환율은 공식 홈페이지에 게시 됩니다.

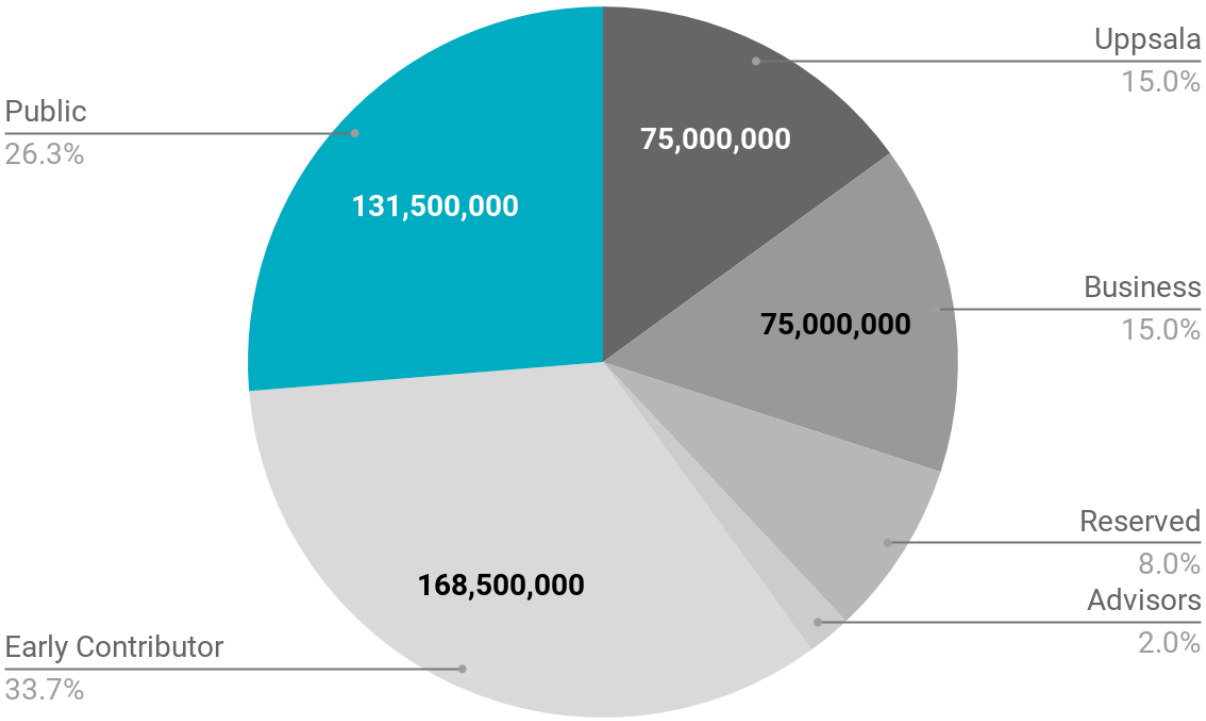
[Sentinel Point]

- Sentinel Point는 Proof of Protection(이하, PoP)에 의해서만 획득 할 수 있습니다.
- PoP는 사기 주소, IP, 웹 사이트, 보고서 검증, 사건 해결 케이스 등의 보고 활동과 같은 다양한 사이버보안 활동을 포함합니다.
- 합법적 보고는 The Sentinels에 의해 검증됩니다.
- S-wallet 소지자는 D-Sandboxing 계산을 통해 PoP를 수행 할 수 있습니다.
- Sentinel Protocol 커뮤니티를 위한 기타 간접적 기여 방법으로는 사이버 보안 문제에 대한 대중의 관심을 끄는 기사를 작성하거나 그 기사를 다른 언어로 번역하는 활동 등이 해당됩니다.
- The Sentinels들은 보고서 분석 및 사용자의 평판 투표에 따라 Sentinel Points를 획득합니다.
- Sentinel Point 소지자는 앞서 설명한 UPP으로 교환이 가능합니다. 커뮤니티의 발전을 위해 수행된 PoP를 통해, 생성된 총 Sentinel Point 수에 상대 비례 하여 교환 가능한 양이 정해지게 됩니다. 자동화된 교환이 적용될 수도 있습니다.

[초기 UPP 분배 제도]

Rounds	UPP 개수	비고
Uppsala Foundation	75,000,000 (15% of 초기 UPP)	-
사업 개발	75,000,000 (15% of 초기 UPP)	-
예약된 할당	40,000,000 (8% of 초기 UPP)	-
어드바이저	10,000,000 (2% of 초기 UPP)	-
초기 기여자	168,500,000 (33.7% of 초기 UPP)	-
퍼블릭 기여자	131,500,000 (26.3% of 초기 UPP)	2018년 04~05월

[초기 UPP 분배]



[펀드 사용 계획]

	비율
연구 개발	50%
사이버 보안 장비	10%
세일즈 & 마케팅	20%
운영 전반	10%
회계, 법, 컴플라이언스	10%

설명:

- 연구 개발: 로드맵에 있는 대로 제품 개발을 하기 위한 비용
- 사이버 보안 장비: 최신의 정보보안 기술에 발 맞추고 보안 팀을 운영하는 비용
- 세일즈 & 마케팅: 글로벌 브랜드 구축을 위한 온라인 및 오프라인 마케팅 비용
- 운영 전반: 사업체의 하루 하루 운영 비용
- 회계, 법, 컴플라이언스: 기준을 충족하고 투명한 비즈니스 운영을 위한 비용

Chapter 12

로드맵

웁살라 재단 설립과 동시에 다음과 같은 활동이 이루어지고 있습니다:

Phase 1 – Sentinel Protocol of The Cryptocurrency World

18 Jan	HQ R&D center open in Singapore, APAC
	HQ R&D center security researchers integrate cybercrime, scam information existing in history, indexing into blockchain scheme Threat Reputation Database (TRDB)
	Regional R&D center developing Interactive Cooperation Framework (ICF) interface
18 Feb	SIPB prototype beta test
18 Mar	SIPB testnet launch with token issuance

Phase 2 – Proof of Protection

18 Jun	Public SIPB best release : The Sentinel Protocols serviced by sentinel protocol collective portal
18 Jul	Mainnet launch (The manual report of TRDB feature enabled into mainnet)

Phase 3 – Self Purification

18 Nov	Machine learning engine beta test
18 Dec	Machine learning engine feature release (auto report applied) beta
	Distributed sandbox (D-sandbox) release

Phase 4 – Self Evolution

2019	Machine learning based Fraud Detection System (FDS) release into mainnet

Chapter 13

결론

Sentinel Protocol은 현재의 사이버 보안 생태계, 특히 본질적으로 감독기능이 부족한 암호화폐 보안 산업을 지원하는 가장 효과적인 플랫폼입니다. 날로 진화하는 새로운 공격 유형에 대한 선제적 대응은 머신러닝을 활용하는 것이 효과적이라는 것은 이미 입증된 사실입니다. 그러나 확률을 근거로한 보안 위협 식별의 불명확함은 여전한 도전 과제입니다. Sentinel Protocol의 블록체인용 보안 지능 플랫폼은 블록 체인의 집단 지성을 활용하여 암호화폐의 보안 문제를 해결함으로써 가장 효율적이고 합리적인 솔루션을 제공합니다. 또한 현재는 진입 장벽이 높다고 알려진 암호화폐 시장도 곧 관련 보안업체들의 진출이 예상되고 이를 통해, 현재 법적으로는 보호 받을 수 없는 다수의 암호화폐 거래소, 지불 시스템 회사, 지갑 회사들의 보안 문제를 해결하는데 있어 희소식이 될 것입니다. 이에, Sentinel Protocol은 블록체인의 분권화된 보안을 책임질 새로운 플랫폼으로서, 적절한 기술을 갖춘 참여자들에게 최적의 기회가 될 것을 확신합니다.

참고 문헌

[1] SANS Institute InfoSec Reading Room /IT Security Spending Trends
: https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697
[2] Cyber security market report: https://cybersecurityventures.com/cybersecurity-market-report/
[3] Hard Fork Completed: https://blog.ethereum.org/2016/07/20/hard-fork-completed/
[4] bitcoin: https://bitcoin.org/bitcoin.pdf
[5] Rep on the block: A next generation reputation system based on the blockchain
: http://ieeexplore.ieee.org/document/7412073/
[6] BlockSci Traces Transactions Performed With Dash, ZCash, and Other Currencies
https://themerkle.com/blocksci-succesfully-traces-transactions-performed-with-dash-zcash-and-other-currencies/
[7] A behavioural-based approach to ransomware detection
:https://labs.mwrinfosecurity.com/assets/resourceFiles/mwri-behavioural-ransomware-detection-2017-04-5.pdf
[8] Bitshares: https://bitshares.org/technology/delegated-proof-of-stake-consensus/
[9] Proof of Stake FAQ: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ
[10] Practical Byzantine Fault Tolerance: http://pmg.csail.mit.edu/papers/osdi99.pdf