머신러닝을 활용해 복잡하고 정교한 발신자 속임수 기법을 탐지하는 이메일 보안 기법

이메일 보안분야 세계 No1. 시스코의 머신러닝 보안 솔루션
Advanced Phishing Protection (APP)

사이버 공격자들은 계속해서 당신의 네트워크에 침투하기 위한 새로운 방법을 찾고 있습니다. 스푸핑, 랜섬웨어, 피싱, 제로 데이 공격 그리고 비즈니스 이메일 속임수(BEC)는 공격자들이 성공적으로 조직을 침입하기 위해 신분 기만을 사용하는 새로운 방법의 일부에 불과합니다. FBI 조사에 따르면 CEO 나 임원들을 사칭하여 의심하지 않는 직원들을 속이는 능력은 회사들로 하여금 전세계적으로 53 억 달러의 손해를 입혔다고 합니다. 조직에서는 위협 발신자로부터 사용자를 보호하기 위해 더 많은 계층의 보호가 필요하며, 시스코는 이에 대한 최신 기법으로 Cisco® Advanced Phishing Protection 을 제안합니다. 세계 1 위의 시스코 이메일 보안에서 사용하는 발신자 인증 및 BEC 탐지 기능을 특별히 강화한 솔루션입니다. 향상된 머신러닝 기법, 실시간 행위 분석, 연계 모델 및 텔레메트리를 통해 사용자 인증 기반의 위협을 차단합니다. 다양한 인텔리전스를 적용하여 실시간으로 메일 발신자를 이해하고 이를 통해 침해사고에 대한 보호를 향상시킵니다.

머신러닝 기법

시스코 APP 가 활용하는 머신러닝 모델링 기법

- 이메일을 발송 중인 사용자 ID 를 식별합니다.
- 해당 ID 의 평소의 발신 행위를 분석하여, 이상 행위 여부를 탐지합니다.
- 평소의 메일 발송 행위를 수신자들의 관계와 연관해서도 판단합니다. 예를 들어 동료와 같이 가까운 관계의 이메일의 경우 스푸핑 공격이 일어날 경우 피해가 높기 때문에 더 엄격한 임계치 값을 설정합니다.

방어 가능 공격

- 위협파일이나 URL 없는 BEC 공격 기법
- 속임수 계정이나 사회공학적 기법
- 피싱(phishing)
- 랜섬웨어(Ransomware)
- 제로데이공격(zero-day attacks)
- 스푸핑(spoofing)

구축 장점

- 기존의 이메일 환경을 보다 효과적으로 보호하기 위한 방어 단계를 추가로 제공합니다.
- 실시간으로 이메일 발송자를 분석, 이해하고 학습하여 이메일 ID 인증 및 행동 분석을 통한 공격을 방어합니다.
- 사용자의 수신함에서 자동으로 악성 이메일을 제거하고, ID 인식 기술을 활용하여 이상 행위나 최신 공격을 방어합니다.
- 모든 이메일 공격 활동에 대한 가시성을 확보합니다.
- 기존 이메일 보안 솔루션에 추가로 피싱, BEC 탐지 및 방어기능을 향상시킬 수 있습니다.
- 기존 솔루션에 영향 없는 동작 방식으로 침해 사고에 대한 머신러닝, AI 를 통한 추가적인 이메일 보호 기능을 제공하는 솔루션입니다.

동작 방식

시스코 APP 는 작은 용량의 센서를 클라우드나 구축형으로 설치하여 동작합니다.

- 센서는 이메일 보안 게이트웨이로부터 안전하다고 판단된 메일 중 일부 정보를 수집합니다.
- 수집 된 메일들의 악성 여부를 ML, AI 를 통해 분석합니다.
- 사전에 설정된 정책에 따라 해당 메일을 바로 차단하거나 추가 분석을 위해 전달(Redirect)합니다.

* 시스코 APP 는 GDPR 을 포함한 개인정보 관련 법률을 준수하며 개인정보, 민감정보를 수집하지 않습니다.

적용 된 첨단 기술

- 매일 3 억개 이상의 업데이트를 기반으로 한 인공지능 예측 기술을 사용하여 신뢰할 수 있는 모델링
- Rapid DMARC, 향상된 사용자 이름 보호, 유사 도메인 탐지 기법을 통한 동급 최고의 BEC 공격 방어 능력
- 공급 파트너를 모델링하고 자동으로 생성하며, 지속적인 정책을 업데이트하여 협력사 이상 행위를 방어하는 협력사 기만 방지
- 머신 러닝을 통해 손상되거나 감염된 이메일 계정에서 오는 공격을 효과적으로 차단
- 지능형 콘텐츠 검사는 AI 기반의 의인화 분석, URL 과 파일 분석을 결합하여 SEG(Secure Email Gateway)를 회피하는 악성 컨텐츠를 탐지
- 이메일 포렌직 및 강제 정책 기능을 통해 운영팀에서 조치를 취하거나 악의적인 활동을 확인 할 수 있는 정책을 제공 할 수 있도록 자동화 된 경고 또는 API 제공