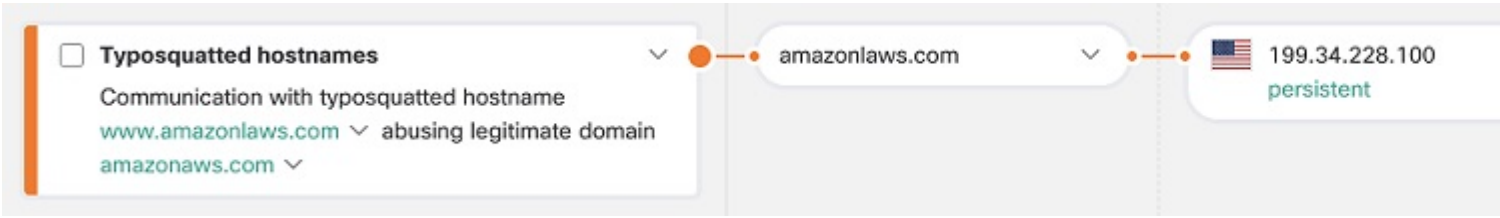
2021년 3월

Cisco 클라우드 기반 머신 러닝 전역 위협 알림에 대해 2021년 3월에 릴리스된 업데이트:

새 타이포스쿼팅 분류자

타이포스쿼팅은 URL 하이재킹의 한 형태로, 사용자가 웹 브라우저에 URL을 입력할 때 발생하는 오타(타이포)를 이용합니다. 그 결과 사용자는 공격자 소유의 대체 웹사이트에 연결됩니다. 타이포스쿼팅 URL은 다음과 같이 합법적인 URL과 유사하게 보입니다.

그림 *1:* 예*:* 다른 문자가 추가된 타이포스쿼팅한 호스트 이름



타이포스쿼팅 URL은 대부분 온라인 스캠으로 연결됩니다. 대표적인 예는 광고를 통해 수익을 창출하는 광고 페이지나 사용자의 정보를 훔치는 데 사용하는 피싱 페이지입니다.

그림 *2:* 예*: Amazon AWS*로 이동하려는 사용자를 노리는 광고 페이지

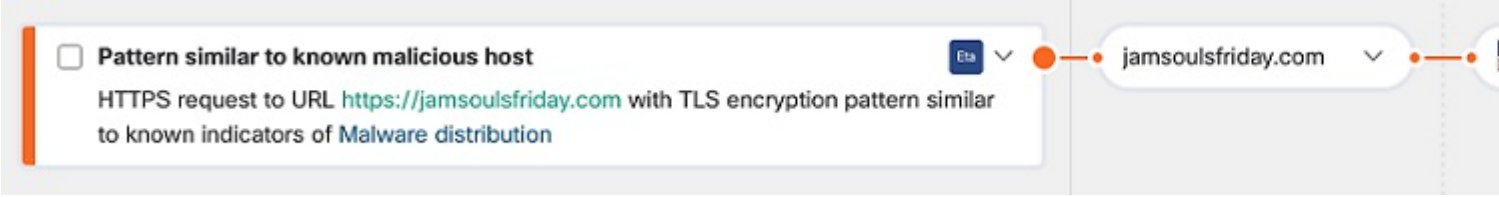
새로운 분류자의 목적은 가장 많이 사용하는 도메인을 대상으로 하는 타이포스쿼팅 도메인으로부터 사용자를 보호하는 것입니다. 분류자는 도메인의 유사성을 계산하여 가장 인기 있는 도메인과 유사한 도메인을 효과적으로 식별합니다. 그런 다음 분류자는 타이포스쿼팅 도메인 나이와 같은 추가 매개변수를 기반으로 위협의 심각도를 결정합니다.

Alert(알림**)** > **Alert detail(**알림 세부 정보**)** > **Security events(**보안 이벤트**)**에서 확인할 수 있습니다.

새 **TLS** 패턴 분류자

새 분류자는 TLS(Transport Layer Security) 핑거프린팅 기술을 이용해 구축됩니다. 분류자는 ETA(Encrypted Traffic Analytics)의 TLS 헤더와 추가 전역 및 로컬 상황별 기능을 고려하여, TLS 공간을 기반으로 의심스러운 애플리케이션과 악성 애플리케이션을 탐지합니다. 분류자는 암호화된 통신을 분석하여, HTTP를 이용해 통신하는 위협을 대상으로 하는 모델의 기능을 확장합니다.

그림 *3:* 예*:* 악성으로 알려진 호스트와 유사한 *TLS* 패턴



Alert(알림**)** > **Alert detail(**알림 세부 정보**)** > **Security events(**보안 이벤트**)**에서 확인할 수 있습니다.