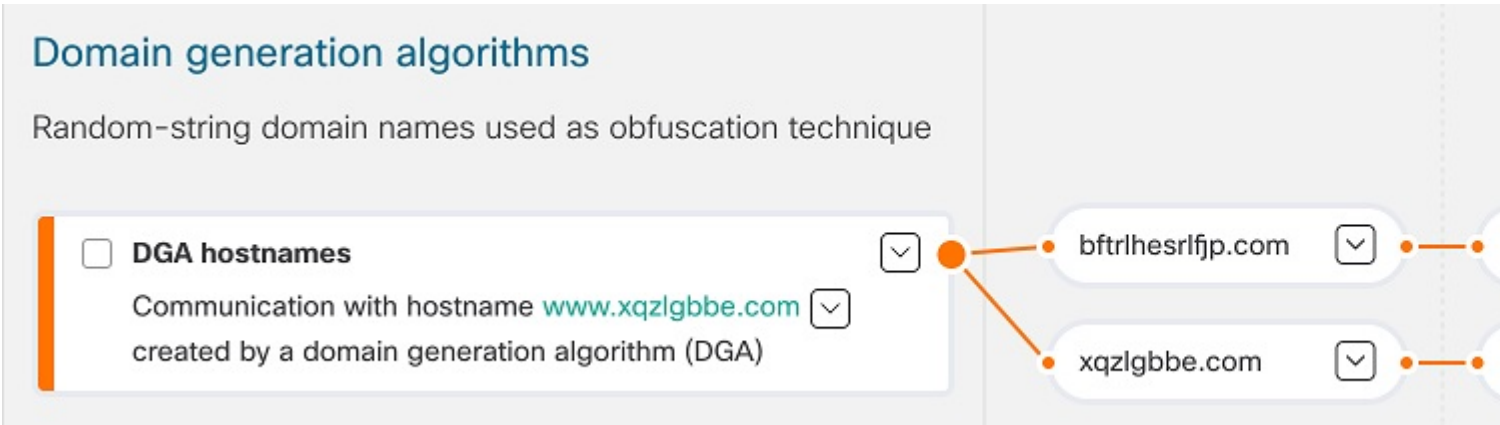
2021년 4월

2021년 4월에 릴리스된, Cisco 클라우드 기반 머신 러닝 전역 위협 알림에 대한 업데이트:

새 DGA 2.0 분류자

DGA(Domain Generation Algorithm)는 임의로 호스트 이름을 생성하여 차단 기능이 있는 보안 제품을 우회하는 용도로 공격자가 사용합니다. 이러한 알고리즘은 주로 봇넷 및 애드웨어에서의 통신에 사용합니다. 동적으로 생성되기 때문에 원래는 차단되어야 하는, 정적인 서명 기반 감시 목록에 의존하는 보안 제품을 우회할 수 있습니다.

그림 ***1:*** 예***: DGA***에 의해 난독화 차단기에 생성된 임의 문자열 도메인



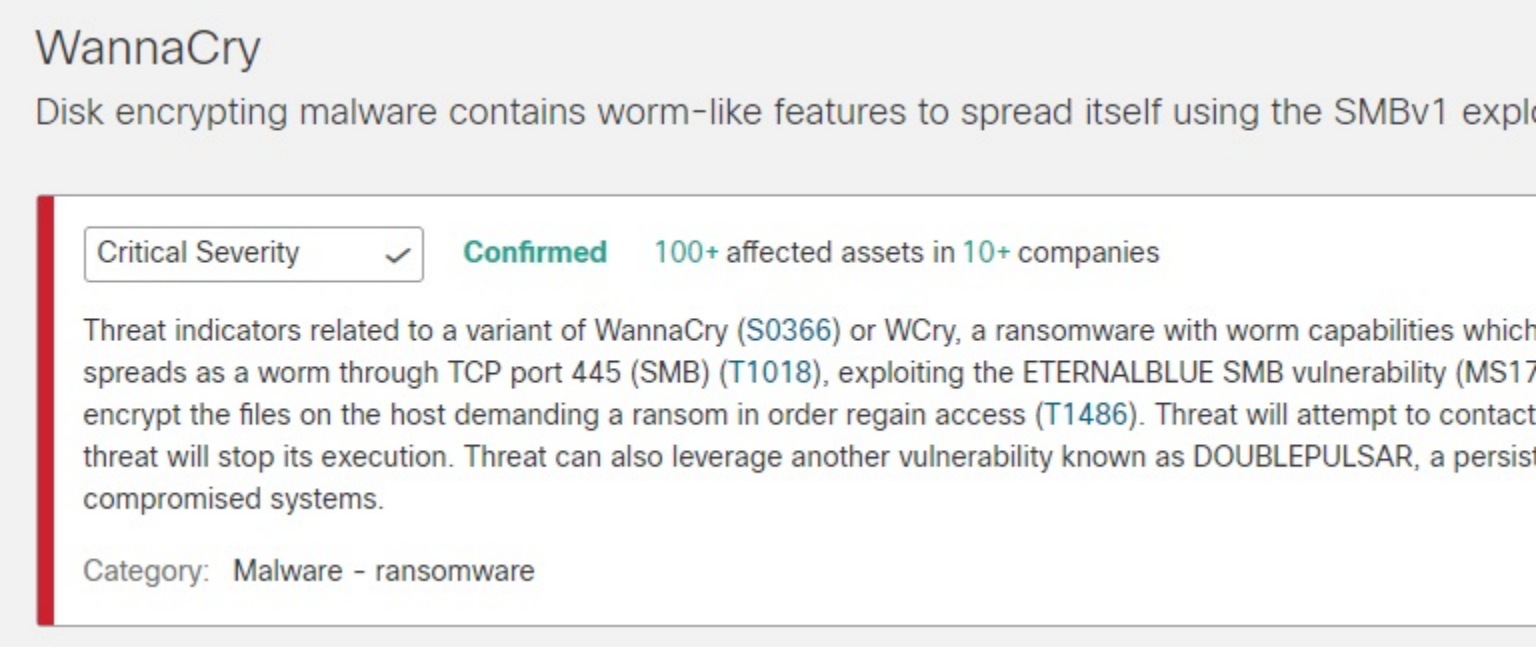
2015년부터 전역 위협 경고는 DGA 도메인 탐지를 지원했지만, DGA 2.0 분류자는 기존의 무작위 포리스트가 아닌 신경망(텍스트 처리를 위한 최첨단 솔루션)을 기반으로 구축된 새로운 모델입니다. 이러한 아키텍처 갱신과 새로 제작된 교육 집합은 오탐을 생성 하는 동안 재현율(정탐 수)을 두 배로 높이고 오탐을 줄입니다.

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

알림 설명의 새 **MITRE** 참조

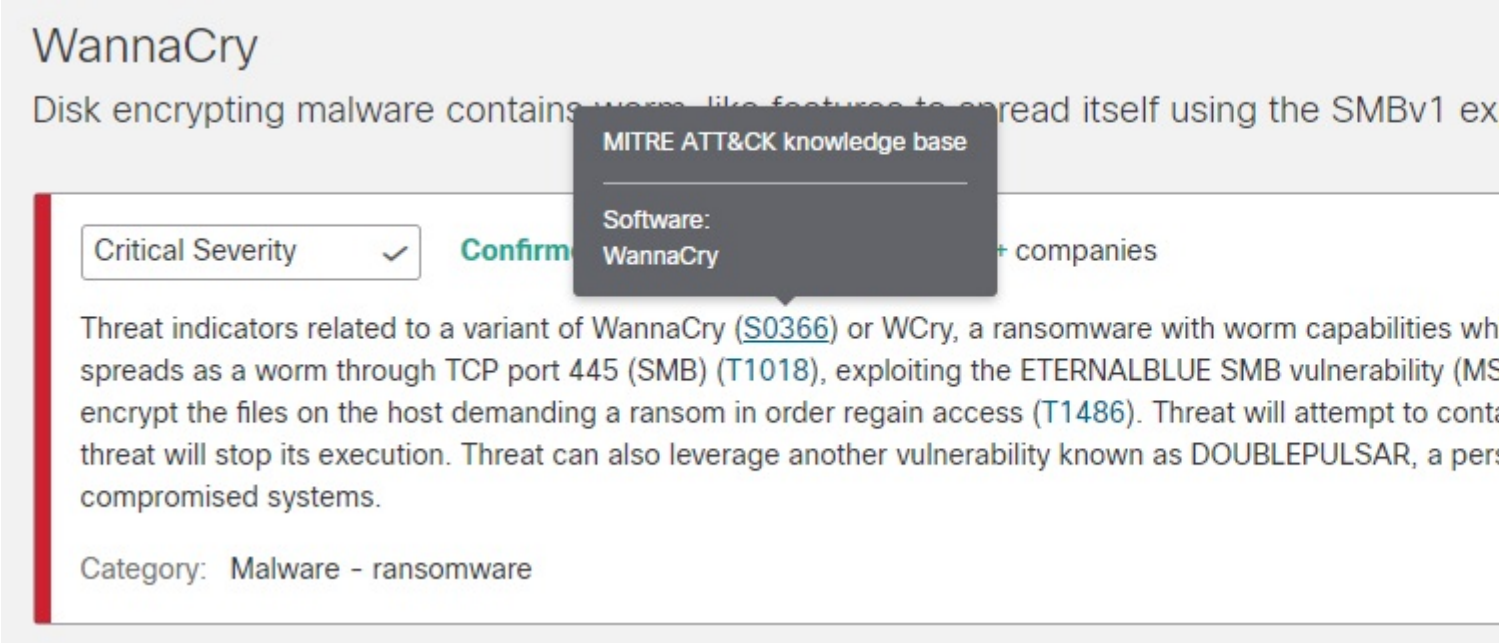
(사용 가능한 경우) 알림 설명에 MITRE 참조가 바로 추가되기 때문에 추가 정보에 편리하게 액세스할 수 있습니다.

그림 ***2:*** 예***: WannaCry*** 설명에 있는 ***4***가지 ***MITER*** 참조***(S0366, T1018, T1210, T1486)***



알림 및 알림 설명에 대한 추가 세부 정보를 찾으십니까? ID 번호를 클릭하여...

그림 *3:* 예*: S0366*에 대한 *MITRE ATT&CK* 기술 자료에 포함된 링크



...MITRE ATT&CK 기술 자료와 특정 위협에 대한 추가 정보 및 상세정보를 제공하는 새 브라우저 페이지를 여십시오.

그림 *4: S0366*에 대한 추가 정보 및 세부 정보를 제공하는 *MITRE ATT&CK* 페이지