2022년 7월

2022년 7월에 릴리스된, Cisco 클라우드 기반 머신 러닝 전역 위협 알림에 대한 업데이트:

CCI로 마이그레이션된 SSO

고객 경험을 개선하기 위해 SSO(Single Sign-On)가 CCI(Cisco Customer Identity) 포털로 마이그레이션되었습니다. **Cisco SSO**를 클릭하고 **id.cisco.com**에 이메일과 비밀번호를 입력하여 로그인합니다.

추가 위협 탐지

다음과 같은 새로운 위협 탐지가 포트폴리오에 추가되었습니다.

- Conti
- REvil

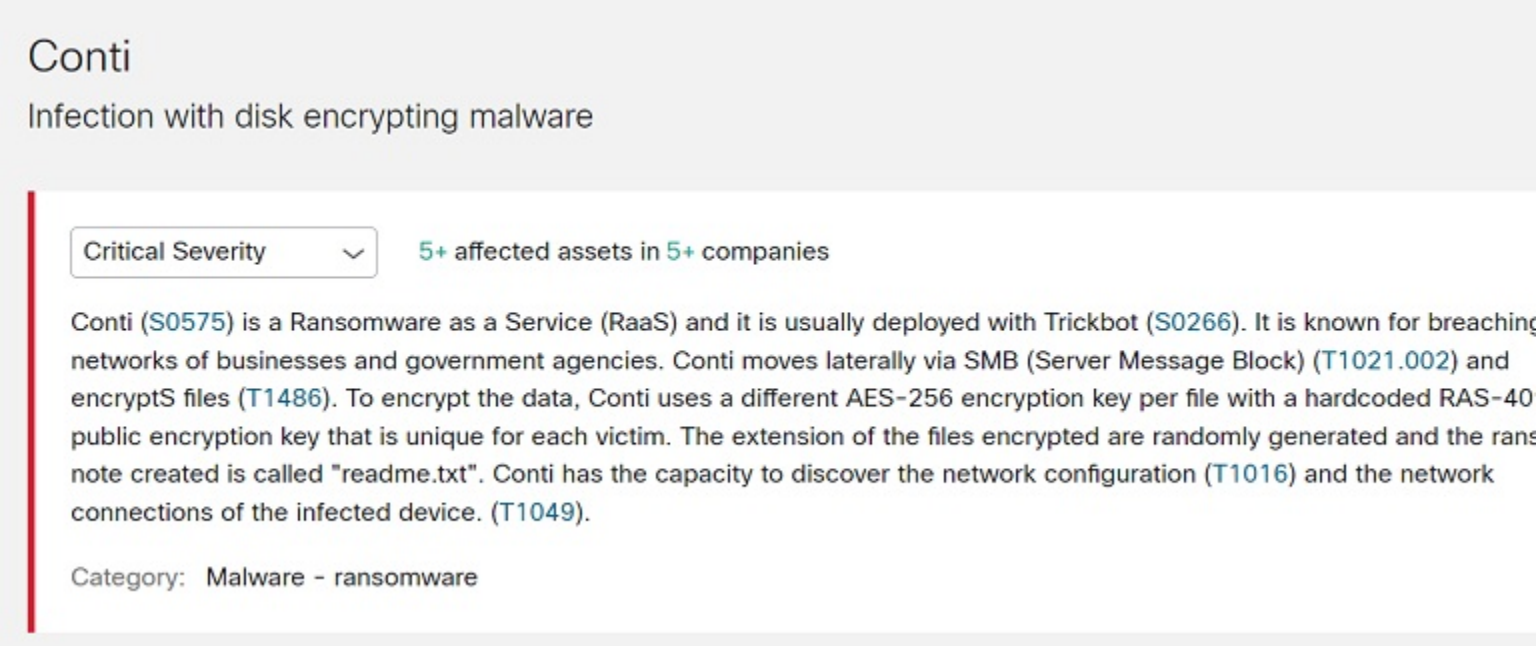
기존 위협 탐지 관련 지표도 업데이트했습니다.

Conti

Conti(S0575)는 대부분 Trickbot(S0266)을 이용해 구축되는 RaaS(Ransomware as a Service)입니다. 기업 및 정부 기관의 네트워크의 보안을 침해합니다. Conti는 SMB(Server Message Block)(T1021.002)를 이용해 수평으로 이동하고 파일을 암호화합니다(T1486). 데이터를 암호화하기 위해 Conti는 파일별로 서로 다른 AES-256 암호화 키를 사용하며, 피해자별로 고유한 하드코딩된 RAS-4096 공개 암호화 키를 사용합니다. 암호화된 파일의 확장자는 무작위로 생성되며, 생성된 몸값 요구 메시지의 이름은 "readme.txt"입니다. Conti는 감염된 디바이스(T1049)의 네트워크 컨피그레이션(T1016)과 네트워크 연결을 검색할 수 있습니다.

사용자 환경에서 Conti가 탐지되었는지 확인하려면 Conti Threat Detail(Conti 위협 세부 정보)을 클릭하여 전역 위협 알림에서 관련 세부 정보를 확인하십시오.

그림 *1:*



REvil

REvil(S0496)은 Sodinokib 및 Sodin이라고도 하는 RaaS(Ransomware as a Service)입니다. 감염은 주로 피해자가 감염된 웹사이트(T1189) 또는 악성 MS Word 첨부 파일(T1204)이 있는는 피싱 이메일(T1566)에 액세스할 때 시작됩니다. REvil은 피해자 디바이스에서 파일을 암호화(T1486)하고 파기(T1485)할 수 있습니다.

사용자 환경에서 REvil이 탐지되었는지 확인하려면 REvil Threat Detail(REvil 위협 세부 정보)을 클릭하여 전역 위협 알림에서 관련 세부 정보를 확인하십시오.

그림 *2:*