2022년 6월

2022년 6월에 릴리스된, Cisco 클라우드 기반 머신 러닝 전역 위협 알림에 대한 업데이트:

추가 위협 탐지

다음과 같은 새로운 위협 탐지가 포트폴리오에 추가되었습니다.

- AutoKMS HackTool
- Raspberry Robin
- UNC2447 활동

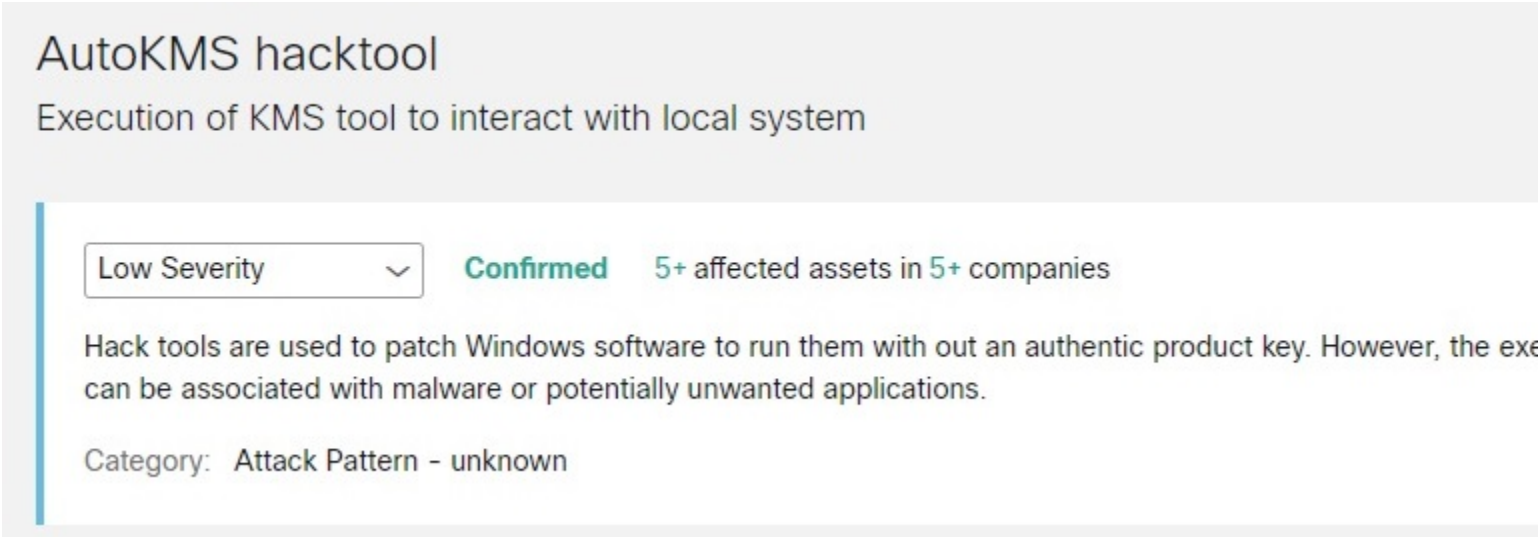
기존 위협 탐지 관련 지표도 업데이트했습니다.

AutoKMS HackTool

해킹 툴은 Windows 소프트웨어를 패치하여 정품 제품 키 없이 실행하는 용도로 사용됩니다. 그러나 이 툴의 실행은 악성코드 또는 원치 않는 애플리케이션과 관련이 있을 수 있습니다.

사용자 환경에서 AutoKMS HackTool이 탐지되었는지 확인하려면 AutoKMS HackTool Threat Detail(AutoKMS HackTool 위협 세부 정보)을 클릭하여 전역 위협 알림에서 관련 세부 정보를 확인하십시오.

그림 *1:*

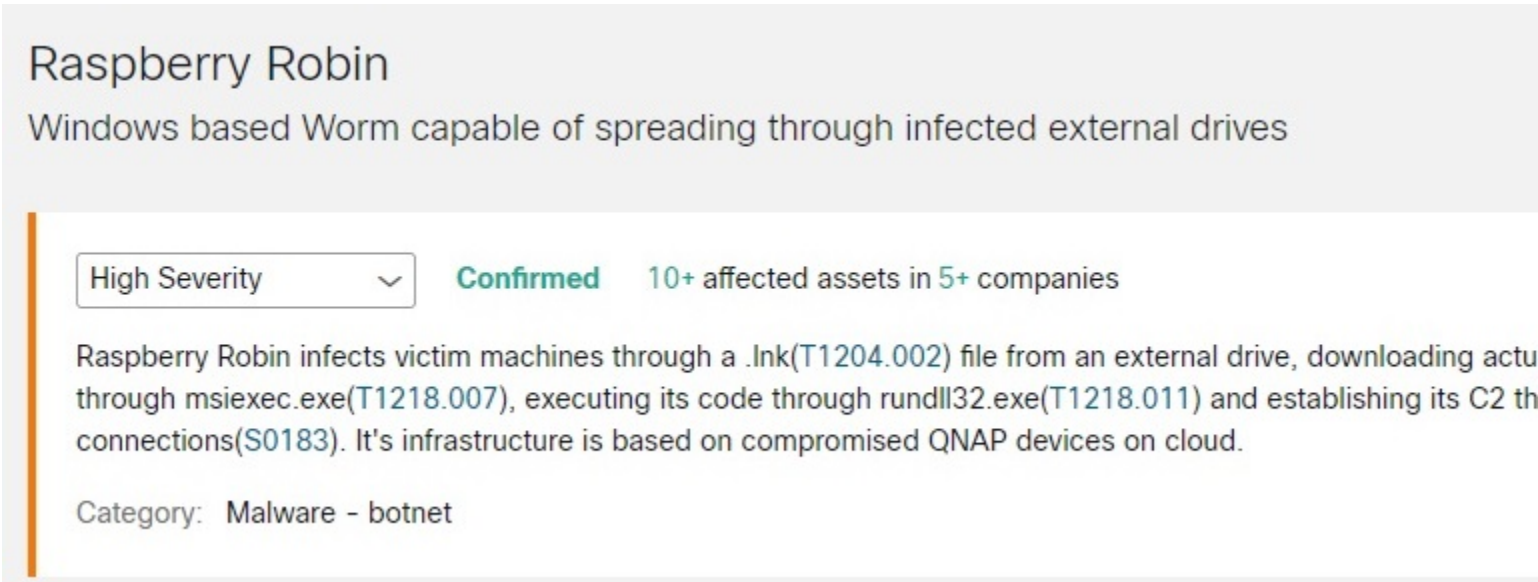


Raspberry Robin

Raspberry Robin은 외부 드라이브에서 .lnk(T1204.002) 파일을 통해 시스템을 감염시키고, msiexec.exe(T1218.007)를 통해 실제 페이로드를 다운로드하고, rundll32.exe(T1218.011)를 통해 코드를 실행하고, TOR 연결(S0183)을 통해 C2를 구성합니다. 인프라는 보안이 침해된 QNAP 디바이스를 기반으로 합니다

사용자 환경에서 Raspberry Robin이 탐지되었는지 확인하려면 Raspberry Robin Threat Detail(Raspberry Robin 위협 세부 정보)을 클릭하여 전역 위협 알림에서 관련 세부 정보를 확인하십시오.

그림 *2:*



UNC2447 활동

UNC2447은 랜섬웨어를 사용하여 데이터를 가져오는 그룹으로, 피해자의 데이터를 포럼에 유출합니다. 이 그룹은 SOMBRAT(S0615)과 FIVEHANDS(S0618) 같은 다양한 RATS 및 랜섬웨어 제품군을 사용하는 것으로 알려져 있습니다. 이 그룹에서 사용하는 대표적인 툴은 ADFIND(S0552), BLOODHOUND(S0521), MIMIKATZ(S0002), PCHUNTER, RCLONE, ROUTERSCAN, S3BROWSER, ZAP, 7ZIP(T1560.001)입니다. 이 그룹은 TeamViewer나 LogMeIn 같은 원격 액세스 애플리케이션(T1219)도 사용합니다.

사용자 환경에서 UNC2447 활동이 탐지되었는지 확인하려면 UNC2447 Activity Threat Detail(UNC2447 활동 위협 세부 정보)을 클릭하여 전역 위협 알림에서 관련 세부 정보를 확인하십시오.

그림 *3:*