AhnLab

eBook

마이터 어택 평가 라운드 6
탁월한 위협 탐지 & 분석 역량 입증

안랩은 비영리 연구개발 단체 '마이터(MITRE)'가 실시한 '마이터 어택 평가 엔터프라이즈 부문 라운드 6(MITRE ATT&CK® Evaluations Enterprise Round 6)에 참가해 95%의 탐지율을 기록하며, 탁월한 위협 탐지 및 분석 역량을 입증했다.

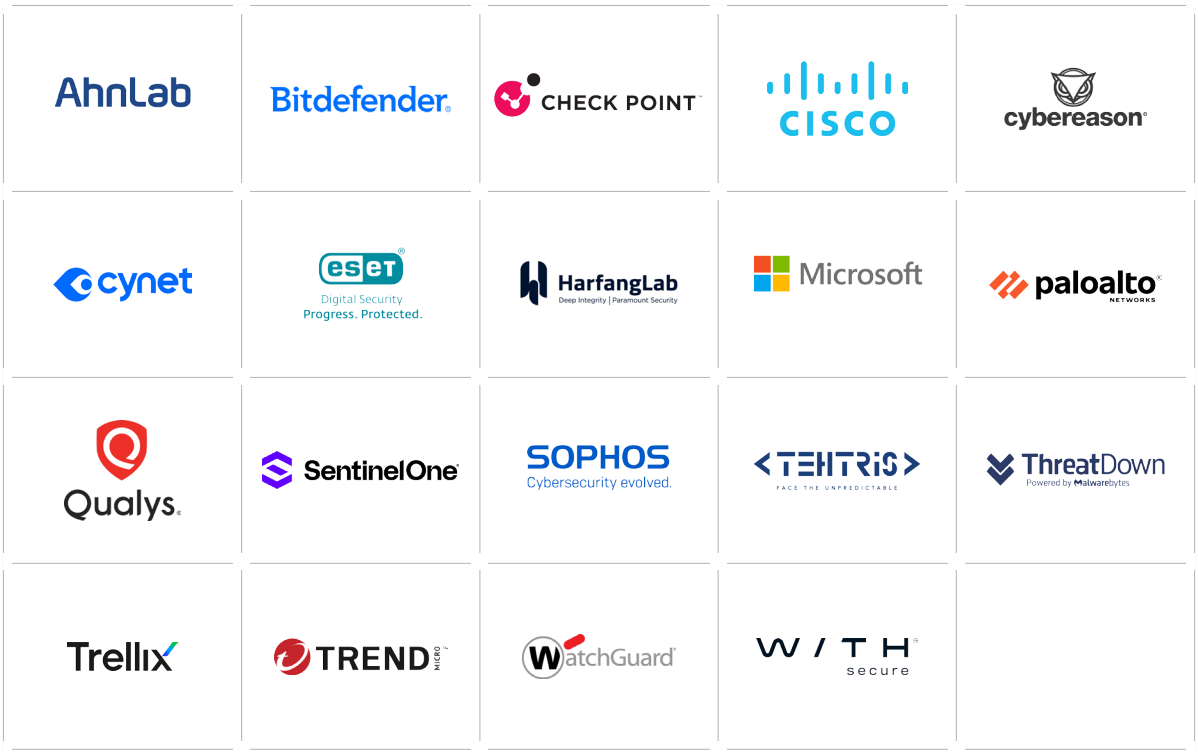
이번 마이터 어택 평가와 안랩의 결과가 어떤 의미를 갖는지 알아보자.

마이터 어택 평가 소개

먼저, 마이터 어택 평가를 주관하는 마이터(MITRE)는 국가 보안을 위해 미국 정부 지원을 받아 연구를 수행하는 비영리 조직으로, 정부, 민간, 학계 등과 협력하여 공익적인 R&D 사업을 진행한다. 사이버 보안 업계에서는 마이터 어택 프레임워크(MITRE ATT&CK Framework)를 통해 공격자들의 전술(Tactics), 기술(Techniques) 및 절차(Procedures)를 리서치 및 정의하는 것으로 잘 알려져 있다.

'마이터 어택 평가'는 마이터가 실시하는 글로벌 보안 제품 평가로, 알려진 공격 그룹들의 행위에 대한 대응 및 기술 역량을 중점으로 평가를 시행한다. 주요 공격 그룹이 사용하는 최신 공격 기법을 구현해 각 공격 단계에서 보안 솔루션의 탐지 여부와 탐지 증적 및 맥락 제공 여부, 차단 여부 등을 테스트한다. 각 솔루션에 대한 순위 책정이나 경쟁을 위한 분석이 아닌 MITRE ATT&CK®의 지식기반을 중심으로 각 보안업체가 위협 탐지에 접근하는 방식을 보여주는 데 초점을 맞추고 있다.

올해로 6회차를 맞은 마이터 어택 평가는 실제 공격 그룹들이 사용하는 기법과의 유사성, 위협 시나리오의 완성도 등 여러 측면에서 전 세계적으로 가장 공신력 있는 보안 제품 테스트 중 하나로 인정받고 있다. 이번 라운드 6에는 총 19개 글로벌 보안 기업이 참가했다. 안랩은 한국 기업으로는 유일하게 라운드 3부터 4회 연속 평가에 참여하고 있다.



[그림] 마이터 어택 평가 라운드 6 참가 기업

평가 구성

마이터 어택 평가는 큰 틀에서 사이버 위협 시나리오(Scenario)를 구성하는 단계(Step)와 각 단계들을 구성하는 세부 단계(Substep)로 구성된다. 해당 구조를 토대로 마이터 측에서 위협 시나리오를 모의 수행하여 참가사 솔루션의 보안 역량을 평가한다.

사이버 위협 탐지 및 분석 역량을 평가하는 '탐지(Detection)' 부문은 각 세부 단계 별로 수집한 증적들의 맥락과 정보를 종합해 다음 [표]와 같이 등급을 부여한다. 탐지 등급은 None부터 General, Tactic, Technique 순으로 탐지 및 식별한 위협 정보가 정확하고 상세해지는 것으로 이해하면 된다.

카테고리	설명
N/A	평가에 반영되지 않는 경우
None	세부 단계에 대한 증적이 없거나 요건에 부합하지 않는 경우
General	악성, 의심, 비정상 행위가 발생했는지 설명 가능한 수준의 증적
Tactic	특정 행위의 배경과 잠재적 의도 등 전술적인(Tactic) 맥락을 제공하는 증적
Technique	특정 행위의 전술(Tactic)을 넘어 방법과 세부 내용 등 기법(Technique)에 대한 맥락까지 제공하는 증적

[표] 마이터 어택 평가 탐지 부문 평가 등급

이번 라운드 6부터는 분석 정보 없이 남기는 기초적인 증적에 대해 부여되는 'Telemetry' 등급이 제외되었다. 사이버 위협의 맥락을 유추할 수 없는 정보는 의미있는 증적으로 인정하지 않겠다는 의미이며, 높은 수준의 위협 탐지 및 분석 역량과 정확성을 요구했음을 알 수 있다.

공격 그룹 시나리오

마이터 어택 평가 라운드 6는 특정 공격 그룹의 기법들을 모의 수행했던 과거 라운드들과 달리 다양한 공격 그룹들의 기법들을 조합하여 시나리오를 구성했다. 이번 평가의 시나리오는 윈도우(Windows)와 리눅스(Linux)에서의 랜섬웨어 그룹(LockBit & CL0P) 및 맥OS(macOS)에 대한 북한 공격 그룹(DPRK)의 실제 위협 행위를 기반으로 구성되었다.

각 시나리오에 대한 설명은 다음과 같다.

랜섬웨어
라운드 6에서는 록빗(LockBit)과 클롭(CL0P) 랜섬웨어의 행위를 모의수행했다. 전 세계에서 가장 많이 배포된 랜섬웨어 변종 중 하나인 록빗(LockBit)은 정교한 도구 사용과 윈도우 및 리눅스 시스템을 이중 타겟팅 하는 것으로 알려져 있다. 클롭(CL0P)은 TA505 그룹과 관련된 랜섬웨어 패밀리로, 다양한 지역과 산업에서 데이터를 탈취, 암호화 및 유출하는 전략을 활용한다.

북한 공격 그룹(DPRK)
북한은 핵 능력 발전을 위해 글로벌 금융, 방위, 기술 부문을 표적으로 사이버 위협을 가하고 있으며, macOS 대상 공격을 확대해 민감 시스템 침투 능력을 갖추게 되었다. 라운드 6에서는 합법적인 macOS 유틸리티를 악용하고 민감한 데이터를 수집 및 유출하는 모듈식 멀웨어를 기반으로 시나리오를 구성했다.

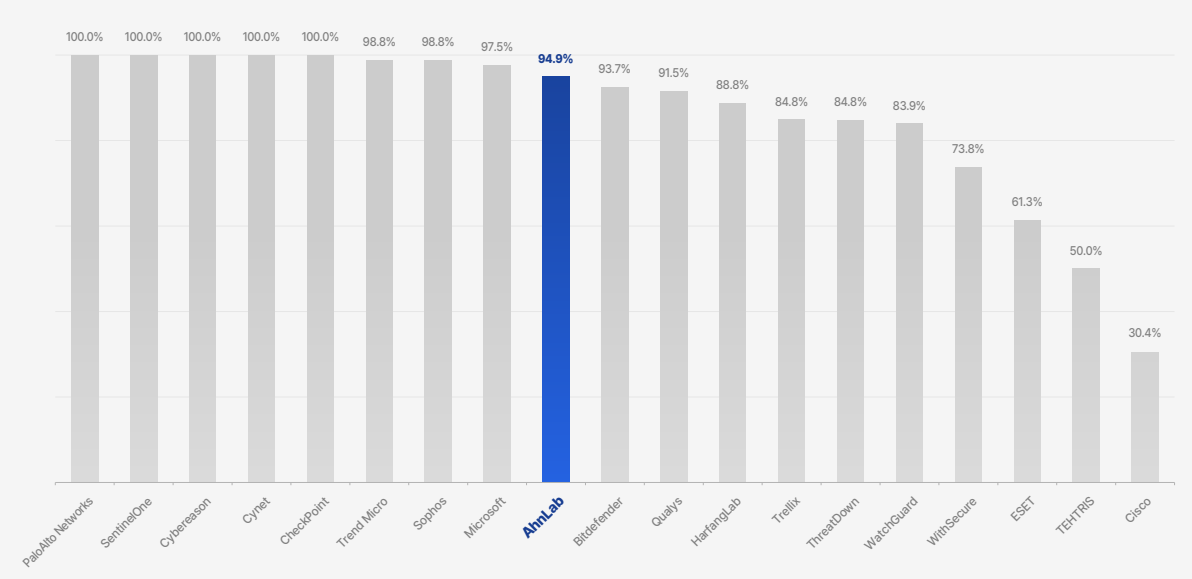
탐지율 95%! 안랩의 결과가 특별한 이유

안랩은 자사 △차세대 엔드포인트 탐지 및 대응 솔루션 'AhnLab EDR' △엔드포인트 보안 플랫폼 'AhnLab EPP' △SaaS형 보안 위협 분석 플랫폼 'AhnLab XDR'로 이번 평가의 '탐지(Detection)' 부문에 참가해 '랜섬웨어' 영역에서 95%의 탐지율을 기록했다.

사용자 입장에서 안랩의 이번 평가 결과는 다음 관점에서 주목할만하다.

#1. 고도화된 위협에 대한 탁월한 탐지 및 분석 역량

안랩은 탐지 부문의 랜섬웨어(Ransomware) 영역에서 윈도우와 리눅스에 걸쳐 구성된 59개 세부 단계(Substep) 중 56개를 탐지하며 95%의 탐지율을 기록하고, 이에 대한 상세 증적과 공격 분석 정보를 제시했다. 아래 [그림]을 보면, 안랩의 탐지 결과는 전 세계 참가 기업들 중에서도 경쟁력 있는 수준임을 알 수 있다.



[그림] 마이터 어택 평가 라운드 6 참가사 별 탐지율

**위 [그림]은 안랩이 자체적으로 분석한 결과로 마이터는 참가사 순위를 산정하지 않음*

특히, 안랩은 탐지한 56개 세부 단계 중 49개에서 최고 등급인 Technique을 받았다. 이는 사용자가 자사 제품 증적 정보를 통해 위협 행위에 대한 '맥락(Context)'을 포괄적으로 이해할 수 있다는 방증이다. 사이버 위협이 고도화를 거듭하는 가운데, 맥락을 이해한 탐지(Context-Aware Detection)는 최적화된 위협 대응(Optimal Threat Response)의 열쇠와 같다. 위협 대응이라는 관점에서 안랩의 탐지 결과는 자사 솔루션을 사용하는 고객들에게 큰 의미가 있다.

#2. 제품의 지속적인 발전

안랩은 지난 라운드 5 탐지 부문에서 82%의 탐지율을 기록했다. 이번 라운드 6부터 탐지 등급에서 Telemetry가 제외되며 평가 난이도와 기준이 높아진 점을 고려했을 때, 탐지율 95%를 기록한 이번 평가 결과는 자사 솔루션에 획기적인 발전이 있었음을 시사한다.

실제로 안랩은 지난 세 번의 마이터 어택 평가 참여를 통해 최신 위협에 대한 제품 역량을 검증하고 개선점을 파악해 보완하는 작업을 진행하여 현재에 이르렀다. 또한, 솔루션의 백엔드와 프론트엔드에 AI와 같은 신기술을 적극적으로 적용해 솔루션을 발전시키고 있다. 앞으로도 해당 작업을 지속하여 고도화되는 사이버 위협을 정확하게 탐지 & 대응하는 동시에 고객들의 제품 사용성(Usability)을 높이기 위한 연구 개발에 박차를 가할 계획이다.

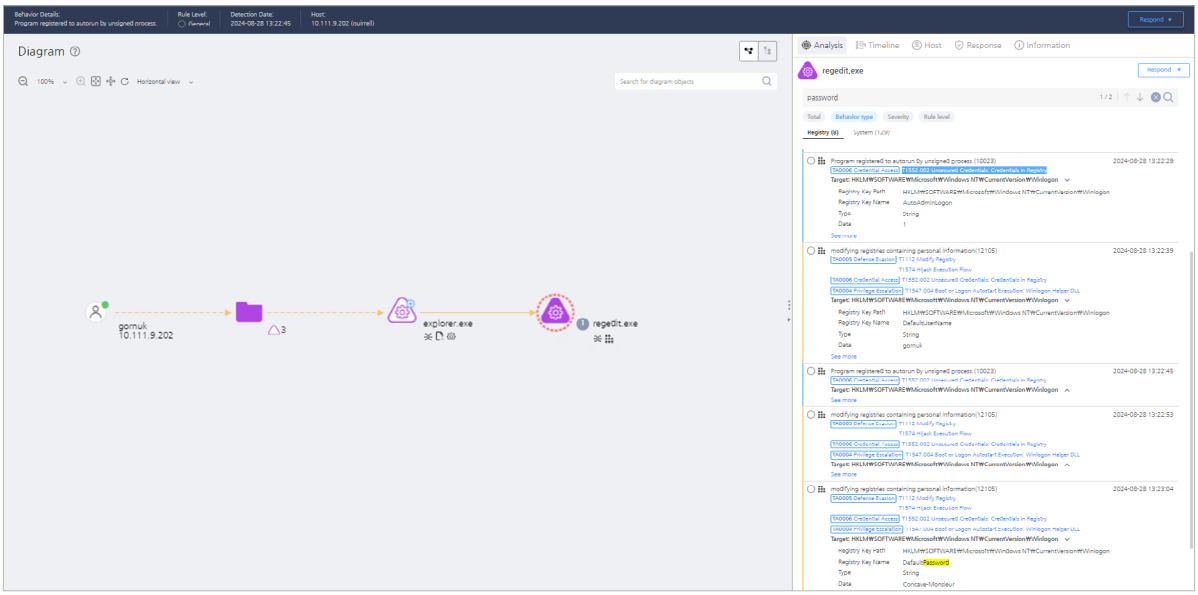
실제 평가 위협 탐지 내역

마지막으로 이번 라운드 6에서 자사 솔루션이 랜섬웨어 그룹의 기법들을 어떻게 탐지했는지 랜섬웨어 LockBit 시나리오에서의 예시를 통해 살펴보도록 하자.

1. Substep 11.01 – 자동 로그인 활성화

랜섬웨어 그룹 록빗(LockBit)의 공격 기법을 모의수행한 시나리오의 Step 11을 보면, 공격자는 서버 quirrell(10.111.9.202)에서 지속성 유지를 위해 서브키를 변경하고 자동 로그인을 활성화한다.

이를 위한 세부 단계로 Substep 11.01에서 사용자 GORNUK(공격자)는 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon 경로의 서브키를 변경해 자동 로그인을 활성화하는 행위를 발현했다.



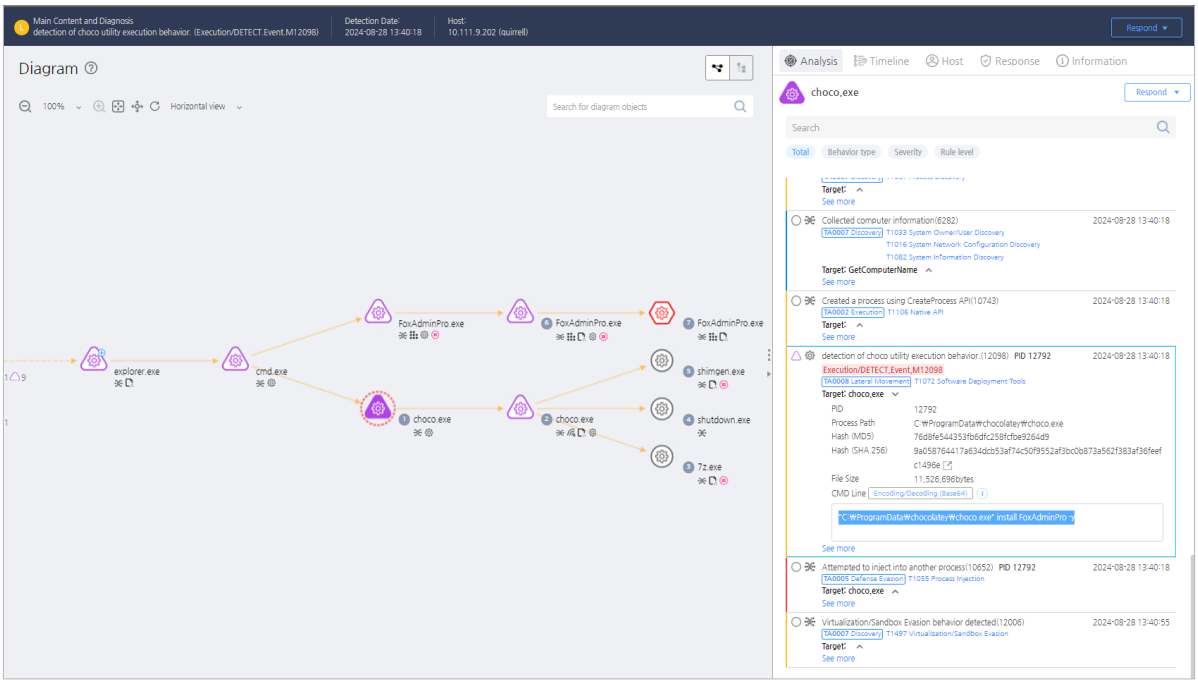
[그림] Substep 11.01 탐지 화면

AhnLab EDR은 GORNUK이 자동 실행(autorun)을 위해 서명되지 않은 프로세스를 활용하여 프로그램을 레지스터한 흐름을 행위 다이어그램으로 제시했다. 레지스트리 키 경로와 이름(AutoAdminLogon)을 정확하게 탐지하고, 이에 부합하는 TID(TA0006 Credential Access / T1552.002 Unsecured Credentials: Credentials in Registry)를 제공해 방어자가 공격자의 자동 로그인 활성화를 위한 서브키 변경 행위를 상세하게 이해할 수 있도록 했다.

2. Substep 12.01 – 정상 툴 활용 패스워드 덤핑

이어지는 Step 12는 공격자가 초콜릿리(Chocolatey)를 활용해 파이어폭스(FireFox) 브라우저의 패스워드를 덤핑하고 도메인 관리자 권한을 회복시켜 리눅스 KVM 서버에 접근한다.

이를 위해 세부 단계인 Substep 12.01에서는 먼저 cmd.exe가 choco를 실행하고 FoxAdminPro를 설치한다.

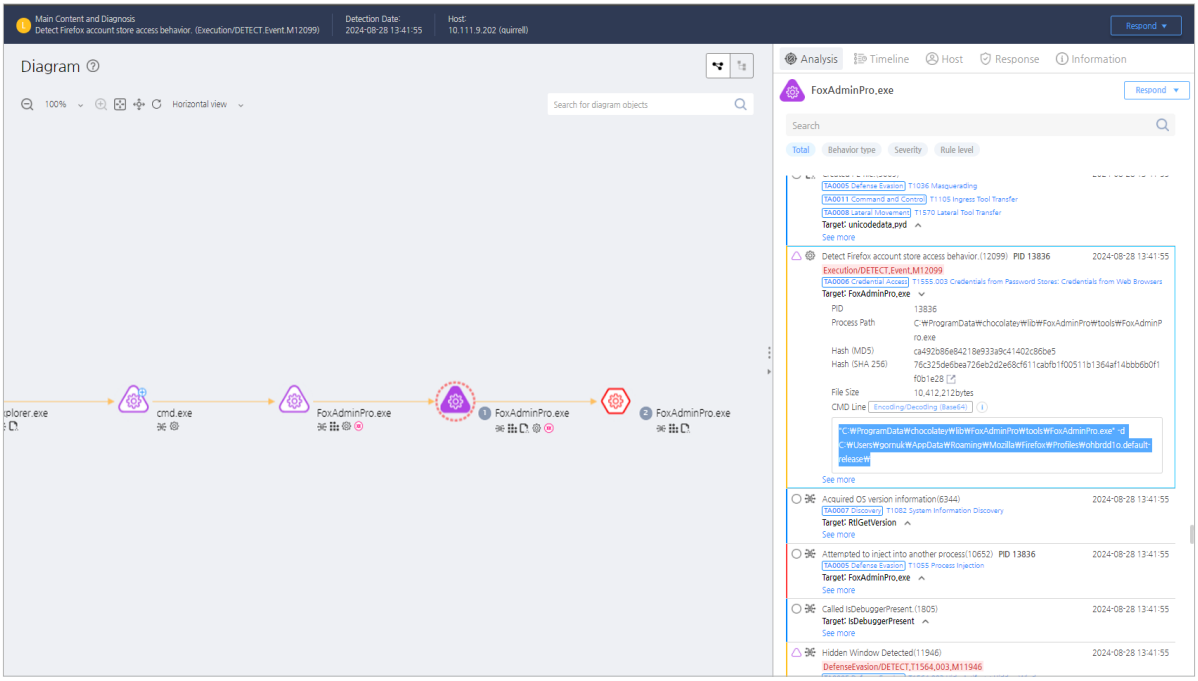


[그림] Substep 12.01 탐지 화면

AhnLab EDR은 cmd.exe.가 FoxAdminPro를 설치하기까지의 과정을 행위 다이어그램으로 나타내고, choco 실행에 관한 경로, TID(T1072 Software Deployment Tools) 및 상세 정보를 제공해 사용자가 행위의 흐름을 포괄적으로 이해할 수 있도록 했다.

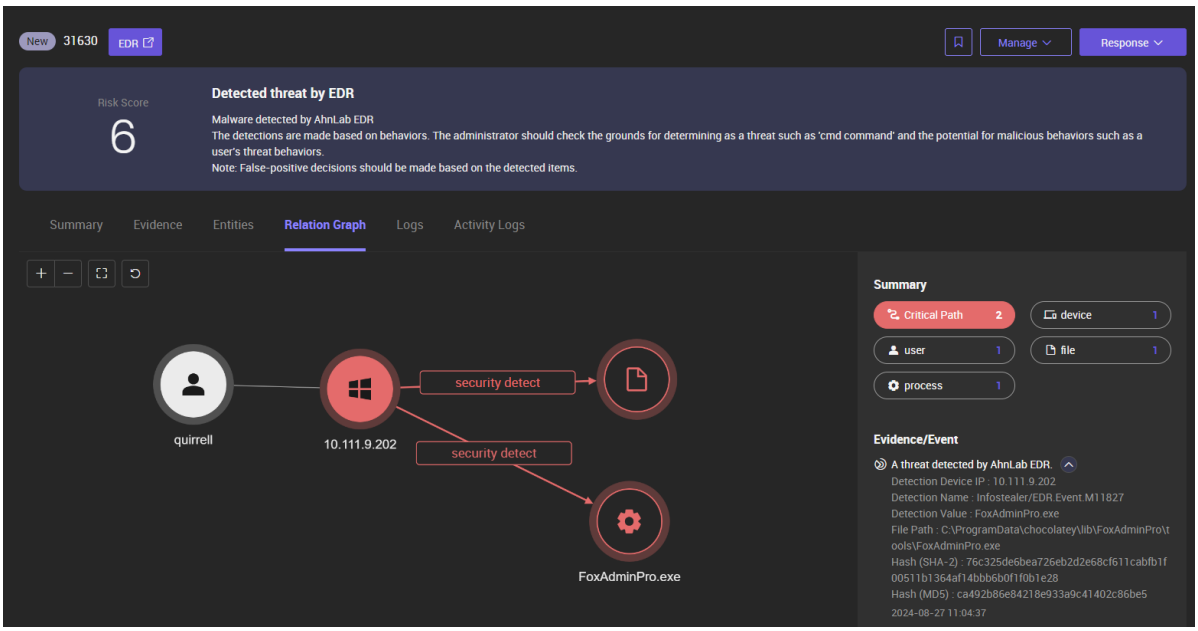
3. Substep 12.03 – 웹 브라우저 크리덴셜 저장소 접근 시도

다음으로 공격자는 cmd.exe를 통해C:\Users\gornuk\AppData\Roaming\Mozilla\Firefox\Profiles\ohbrdd1o.default-release\ 경로에 FoxAdminPro를 설치해 웹 브라우저 크리덴셜 저장소에 접근해 접근 권한을 획득하려 했다.

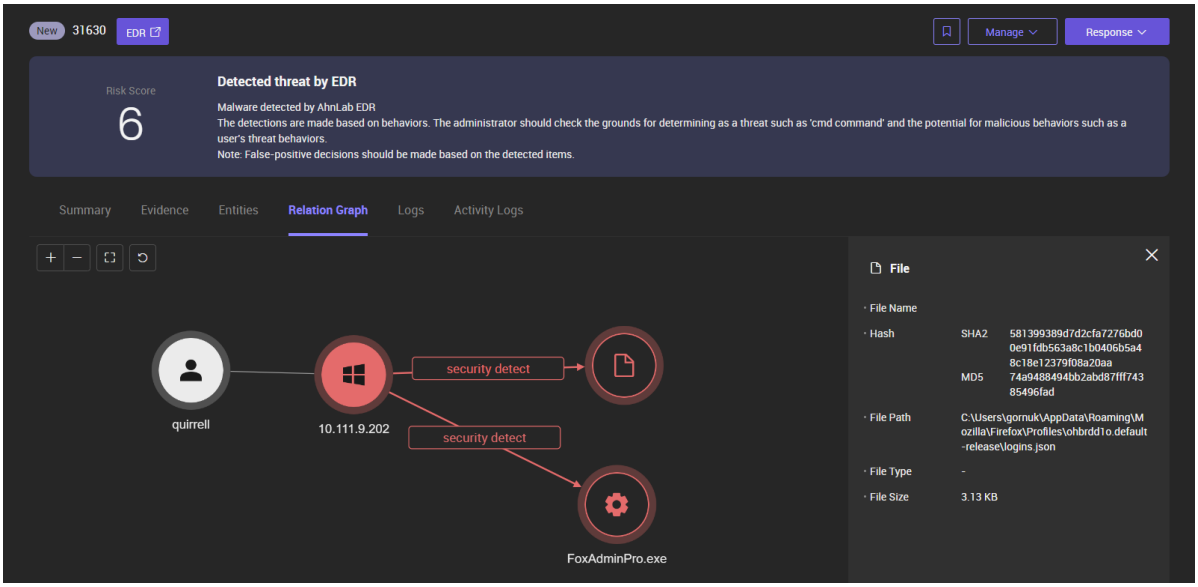


[그림] Substep 12.03 탐지 화면 (1)

AhnLab EDR은 FireFox의 크리덴셜 저장소에 접근하는 행위를 탐지하고 이에 관한 상세 정보, TID(TA0006 Credential Access / T1555.000 Credentials from Web Browsers) 및 행위 수행을 위한 CMD 명령어 등을 제공했다.



[그림] Substep 12.03 탐지 화면 (2)



[그림] Substep 12.03 탐지 화면 (3)

AhnLab XDR 역시 이 행위에 대한 다이어그램, 탐지명, 파일 정보 및 기타 상세 정보들을 제공해 사용자가 위협을 보다 깊이 이해할 수 있도록 했다.

안랩은 이번 평가에서 위 세 개 Substep 모두 최고 등급인 Technique을 받았다. 하지만, 개별 탐지 결과보다 중요한 것은 사용자들로 하여금 '자동 로그인 활성화 > 웹 브라우저 패스워드 덤핑 > 웹 브라우저 크리덴셜 저장소 접근'으로 이어지는 실제 위협 행위의 맥락을 이해할 수 있도록 했다는 것이다. 이 정보들을 연계해 분석하면 실제 환경에서 공격자들이 발현하는 행위와 그 의도를 이해하고 대응 및 예방할 수 있다는 점에서 큰 의미가 있다.

마이터 어택 평가 라운드 6 결과는 마이터 홈페이지에서 확인할 수 있다. 본 평가에 참여한 안랩 제품에 대한 자세한 정보는 안랩 홈페이지에서 확인 가능하다.

▶ AhnLab EDR 더 알아보기

▶ AhnLab XDR 더 알아보기

▶ AhnLab EPP 더 알아보기

AhnLab

경기도 성남시 분당구 판교역로 220 (우)13493
홈페이지: www.ahnlab.com
대표전화: 031-722-8000 팩스: 031-722-8901