AhnLab

eBook

마이터 어택 평가 라운드 7 차단율 100% 기록!

안랩은 비영리 연구개발 단체 '마이터(MITRE)'가 실시한 '마이터 어택 평가 엔터프라이즈 부문 라운드 7(MITRE ATT&CK® Evaluations Enterprise Round 7)에 참가해 '보호(Protections)' 부문에서 100%의 차단율을 기록했다. 이를 통해, 세계 최고 수준의 보안 역량을 입증했다.

마이터 어택 평가에 대하여

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 7회차를 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 7에는 총 11개 글로벌 보안 기업이 참가했다. 안랩은 한국 기업으로는 유일하게 라운드 3부터 5회 연속 평가에 참여하고 있다.

[그림 1] 마이터 어택 평가 라운드 7 참가 기업

평가 시나리오 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.

이전 라운드들 대비 가장 큰 변화는 기존 온프레미스(윈도우/리눅스) 환경에 클라우드 환경을 추가한 것이다. 최근 공격자들이 온프레미스와 클라우드를 넘나들면서 공격을 수행하는 점을 감안해 실제 위협과 유사한 형태로 평가를 고도화했다.

시나리오 관점에서 마이터 어택 평가는 크게 ▲탐지(Detections) ▲보호(Protections)로 구성된다.

1. 탐지(Detections)

사이버 위협 탐지 및 분석 역량을 평가하는 '탐지(Detection)' 부문은 각 세부 단계 별로 수집한 악성 이벤트 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 1] 마이터 어택 평가 탐지 부문 평가 등급 – 악성 이벤트

그리고, 악성 이벤트 뿐만 아니라 정상 이벤트에 대한 오탐(False Positives) 여부도 확인한다. 시나리오에는 악성 이벤트와 정상 이벤트가 섞여 있으며, 솔루션이 악성과 정상을 정확하게 구분하는지를 함께 확인한다.

카테고리	설명
N/A	평가에 반영되지 않는 경우
Reported	정상 행위이지만 악성으로 탐지해 알림을 보낸 경우
Not Reported	정상 행위를 올바르게 탐지해 알림을 보내지 않은 경우

[표 2] 마이터 어택 평가 탐지 부문 평가 등급 – 오탐(False Positives)

2. 보호(Protections)

'보호(Protections)' 부문에서는 솔루션이 사이버 공격이 시스템에 영향을 미치지 전 차단하는지 여부를 평가한다. 시스템이 피해를 입기 전 방어했는지 합격/불합격(Pass/Fail) 형태로 테스트를 진행한다.

카테고리	설명
N/A	평가에 반영되지 않는 경우
Protected	악성 행위 발현 전 차단
Not Blocked	악성 행위 발현 허용

[표 3] 마이터 어택 평가 보호 부문 평가 등급

공격 그룹 설명

마이터 어택 평가 라운드 7은 지난 라운드 6와 마찬가지로 다양한 공격 그룹들의 기법들을 조합하여 시나리오를 구성했다. 모의수행한 공격 그룹은 크게 ▲금전을 노린 사이버 공격 그룹(Financially-Motivated Cybercriminal Collective) ▲ 중국 배후 사이버 스파이 그룹(People's Republic of China (PRC) Cyber Espionage Group)으로 구성된다.

각 공격 그룹에 대한 설명은 다음과 같다.

1. Scattered Spider: 금전을 노린 사이버 공격 그룹

마이터는 사회공학 기법, 원격 접근 도구 설치, 다중 인증(MFA) 우회에 능숙한 공격 그룹 'Scattered Spider'의 기법을 모의 수행했다. 공격자는 피해자의 클라우드 자원을 지속적으로 노리며, 거점을 확보하고 네트워크 및 디렉터리 정찰을 수행한 뒤, 민감 시스템과 데이터 저장소에 접근한다. 공격 전개 속도가 굉장히 빠르고, 대량의 데이터에 신속하게 접근해 유출시킨다.

2. Mustang Panda: 중국 배후 사이버 스파이 그룹

또한, 마이터는 해킹 역량과 도구를 계속해서 발전시키는 중국 배후 사이버 스파이 그룹 'Mustang Panda'도 모의 수행했다. 공격자는 사회공학 기법과 합법적인 도구 및 서비스를 악용하여 맞춤형 악성코드를 배포한다. 알려진 행위와 도구 중 다수는 중국의 사이버 공격 생태계 전반에서 널리 사용된다. 예를 들면, LOTL(Living off the Land) 기법, 맞춤형 악성코드, 클라우드 기반 인프라 공략 등이 있다.

차단율 100%! 업계를 선도하는 안랩의 평가 결과

안랩은 자사 △차세대 엔드포인트 탐지 및 대응 솔루션 'AhnLab EDR' △엔드포인트 보안 플랫폼 'AhnLab EPP' △SaaS형 보안 위협 분석 플랫폼 'AhnLab XDR'로 이번 평가에 참가했다. 보호(Protections) 평가에서 100%를 기록한 것을 비롯해 온프레미스-클라우드를 아우르는 위협 가시성 및 탐지 정확성 측면에서도 주목할만한 성과를 거뒀다.

사용자 입장에서 안랩의 이번 평가 결과는 다음 관점에서 주목할만하다.

1. 100% 위협 차단! 업계 최고 수준의 보안 역량 입증

안랩은 보호(Protections) 부문에서 악성 행위를 100% 차단하며 평가 환경의 시스템을 안전하게 보호했다. 마이터 어택 평가, 글로벌 인증, 실제 고객 환경 등 다방면에서 검증 받아 온 업계 최고 수준의 보안 역량을 다시 한 번 입증했다.

특히, 이번 보호 평가에서는 악성 이벤트 뿐만 아니라 '정상 이벤트로만' 구성된 테스트도 있었다. 안랩은 해당 항목에 대해서는 정상으로 판별해 차단을 수행하지 않음으로써 차단의 정확도까지 증명했다. 쉽게 말해, 차단해야 할 악성 이벤트만 차단하고 정상 이벤트는 허용해 실제 사용자 환경에서 강력한 보안과 실용성을 동시에 제공하는 것이다.

2. 온프레미스와 클라우드를 아우르는 포괄적인 위협 가시성

앞서 설명한 바와 같이 이번 라운드 7은 온프레미스(윈도우/리눅스)와 클라우드를 혼합한 시나리오로 구성되었다. 안랩의 솔루션들은 OS를 넘나드는 고도화된 공격 기법들에 대한 상세한 증적과 분석 정보를 제시했다. 이를 통해, 사용자가 증적 정보를 통해 위협 행위에 대한 '맥락(Context)'을 포괄적으로 이해할 수 있도록 했다.

올해부터 새롭게 도입된 클라우드 시나리오에서는 자사 XDR 솔루션 'AhnLab XDR'을 평가 환경 클라우드 리소스와 연동해 탐지 체계를 구축했다. 유연한 연동 기반 '오픈 XDR'을 표방하는 AhnLab XDR은 공격자가 클라우드를 넘나들며 수행하는 악성 행위를 효과적으로 탐지해 맥락 정보를 제공했다. 이를 통해, 기존 온프레미스 뿐만 아니라 클라우드에서도 탁월한 탐지 역량을 입증했다.

3. 정탐(False Positives) 90% & 탐지 지연 '제로'

탐지 정확도와 품질을 평가하기 위해 구성한 정상 이벤트에 대해서는 약 90%의 정확도를 기록했다. 해당 결과는 '정상 행위에 대해서는 위협 알림을 보내지 않았다'는 것으로 이해하면 된다. 이를 통해, 자사 솔루션들이 정확한 탐지 역량을 바탕으로 실제 고객들이 보안을 운영하면서 어려움을 호소하는 과탐 이슈를 해결할 수 있음을 보여줬다.

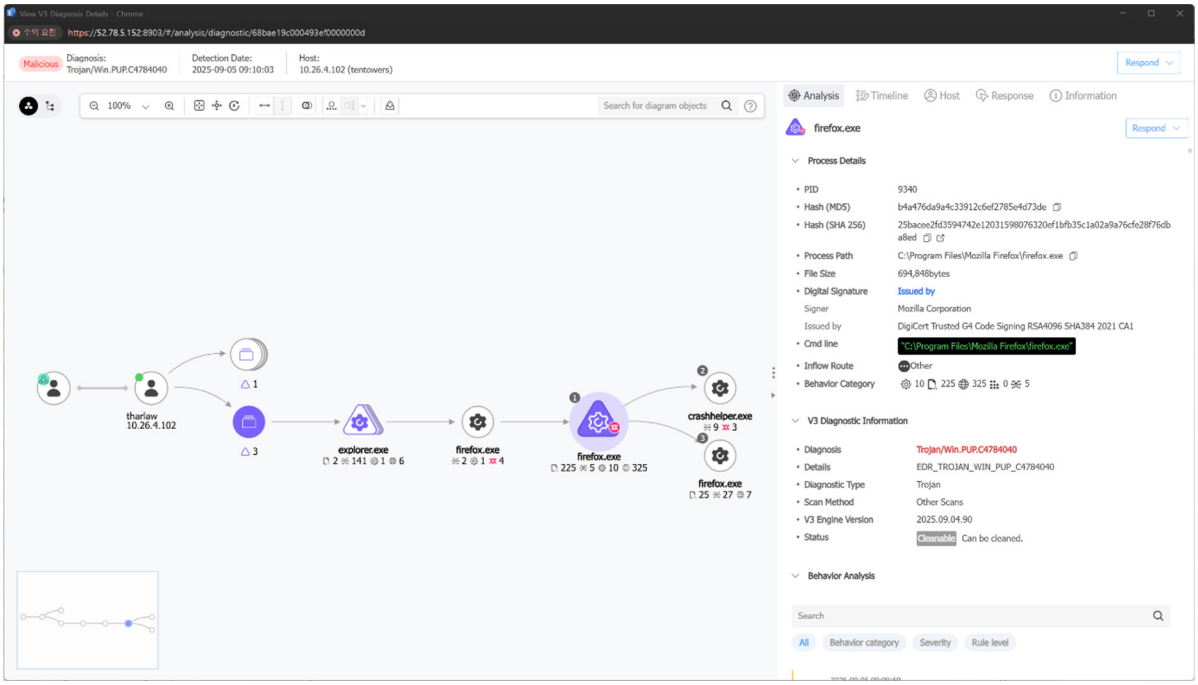
이 밖에, 마이터 어택 평가는 탐지 알림에 지연(Delay)가 있었는지 여부도 함께 확인한다. 실제 사용자들이 탐지 결과를 즉각적으로 위협 대응에 활용해야 하기 때문이다. 안랩 솔루션들은 모든 탐지 결과를 실시간으로 제공하여 '지연 없는 탐지(Zero Delay)'를 달성했다.

실제 평가 위협 탐지 내역

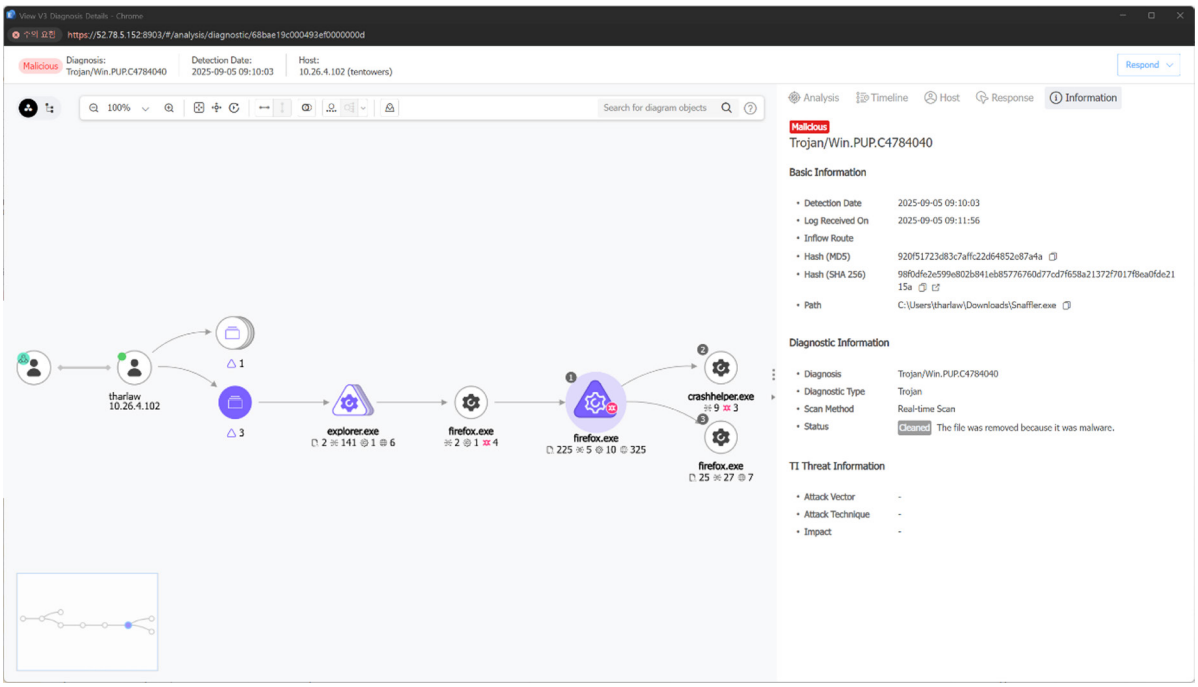
이번 라운드 7에서 안랩의 솔루션들은 윈도우, 리눅스 및 클라우드에 걸쳐 탁월한 탐지 & 차단 역량을 선보였다. 그 과정이 구체적으로 어떻게 이뤄졌는지 실제 예시를 통해 살펴보도록 하자.

1. 보호(Protections): Test 1

피해자 환경에 침입한 공격자는 tharlaw라는 사용자 계정으로 파일 서버에서 Snaffler.exe라는 실행 파일을 다운로드하였다. 공격자는 Snaffler.exe 다운로드와 함께 로컬 드라이브 및 네트워크 공유 상태를 검색하는 행위를 발현했다.



[그림 2] Protections: Test 1 – 파일 다운로드 증적

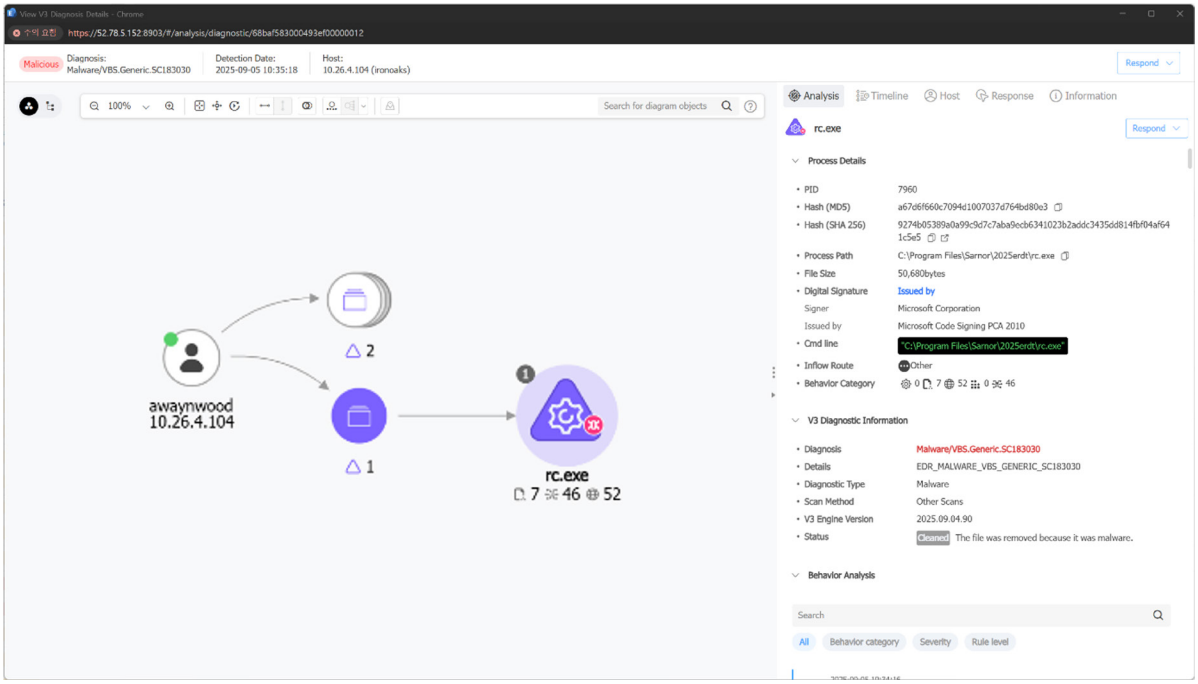


[그림 3] Protections: Test 1 – 파일 차단 증적

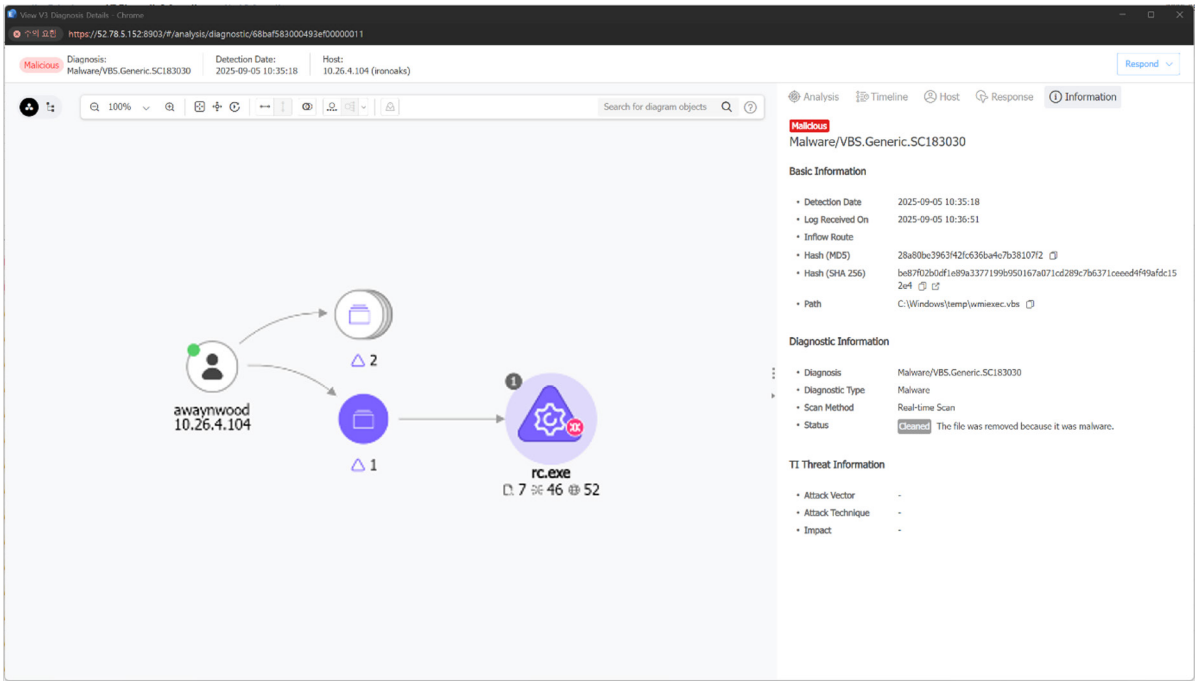
AhnLab EDR은 외부에서 다운로드된 실행 파일 Snaffler.exe가 악성 시그니처를 포함하고 있음을 탐지했다. 이에 대해, 자사 안티바이러스 솔루션 AhnLab V3와 연계하여 실행 파일을 Trojan/Win.PUP.C4784040로 진단해 차단하여 악성 행위 발현을 사전에 막았다. 단순히 악성 파일을 차단한 것을 넘어, EDR과 안티바이러스 연계를 통해 구체적으로 어떤 맥락에서 차단이 이뤄졌는지 사용자들이 이해할 수 있도록 했다는 점에서 큰 의미가 있다.

2. 보호(Protections): Test 5

감염된 환경에 침입한 공격자는 awaynwood라는 사용자 계정으로 원격 명령 실행 도구를 통해 wmiexec.vbs를 C:\Windows\Temp 경로에 다운로드 했다. 이후, 해당 스크립트를 활용하여 파일 서버 heartshome(10.26.3.106)에 네트워크 공유를 생성했다.



[그림 4] Protections: Test 5 – 파일 다운로드 증적

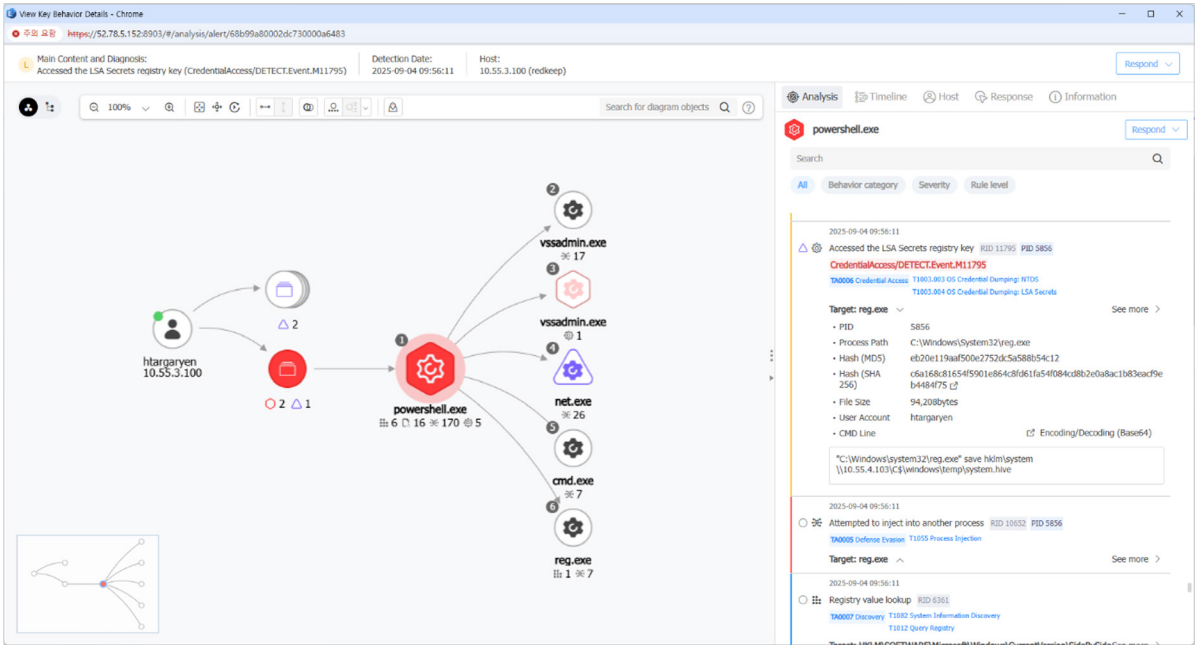


[그림 5] Protections: Test 5 – 파일 차단 증적

위 Test 1과 유사하게 AhnLab EDR은 외부에서 C:\Windows\Temp 경로에 다운로드된 실행 파일 wmiexec.vbs가 악성 시그니처를 포함하고 있음을 탐지했다. 이에 대해, AhnLab V3를 활용해 Malware/VBS.Generic.SC183030로 진단하고 파일을 차단했다.

3. 탐지(Detections): Substep 7.5 – 온프레미스

공격자는 htargaryen이라는 사용자 계정으로 도메인 컨트롤러 redkeep(10.55.3.100)에서 NTDS를 활용한 자격 증명 덤프를 통해 NTDS 파일을 추출하고 오프라인 크래킹을 수행했다. 이를 위한 세부 단계로 redkeep(10.55.3.100)에서 reg.exe를 실행해 시스템 하이브를 원격지인 harrenhal(10.55.4.103)의 Windows\Temp\system.hive 경로로 저장하려 했다.



[그림 6] Detections: Substep 7.5 – 시스템 하이브 유출 행위 탐지

AhnLab EDR은 공격자가 도메인 자격 증명 탈취를 위해 서명되지 않은 reg.exe를 활용해 시스템 하이브를 원격지에 저장하려는 흐름을 행위 다이어그램으로 제시했다. 레지스트리 하이브 경로(HKLM\SYSTEM)와 원격 UNC 저장 위치(\10.55.4.103\C$\Windows\Temp\system.hive)를 정확하게 탐지하고, 이에 부합하는 TID(TA0006 Credential Access & T1003.002 OS Credential Dumping: Security Account Manager)를 제공했다. 이를 통해, 공격자의 자격 증명 탈취를 위한 시스템 하이브 유출 행위를 상세하게 이해할 수 있도록 했다.

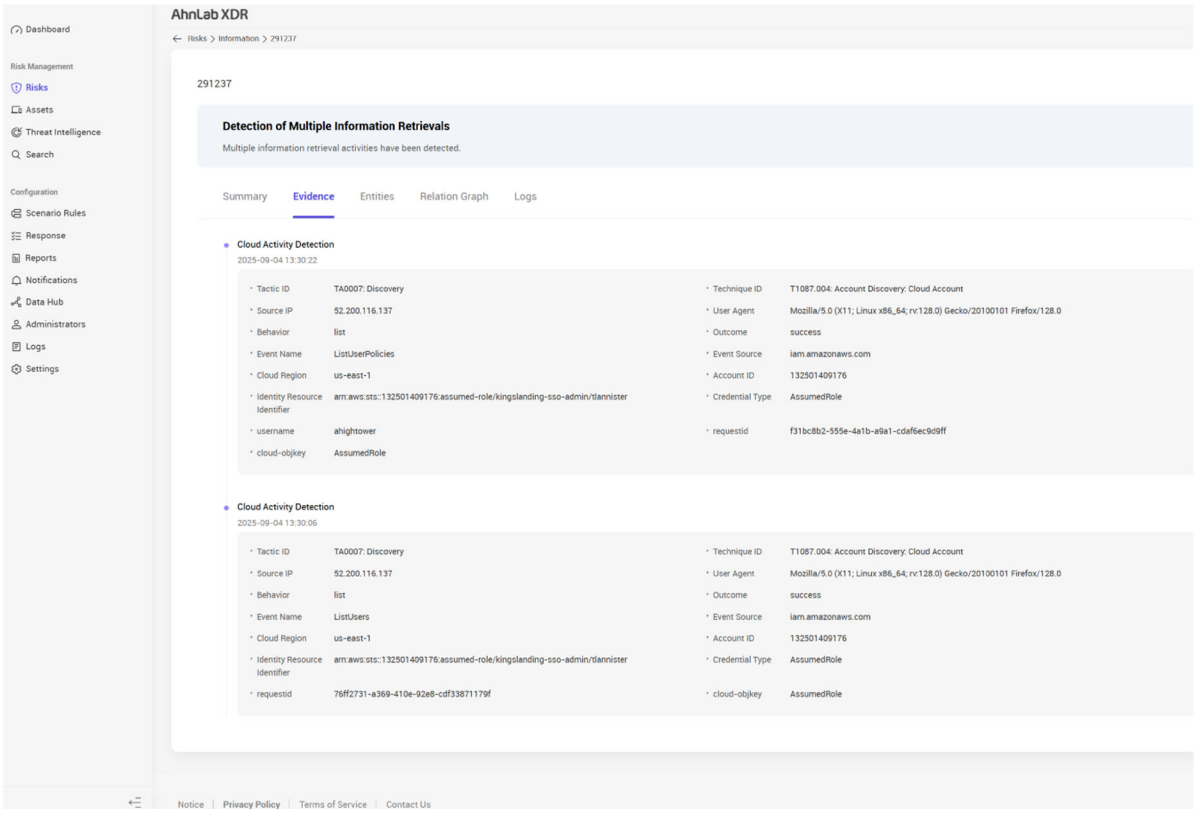
4. 탐지(Detections): Substep 7.2 – 클라우드

마지막으로, 클라우드 영역에서 공격자는 tlannister라는 사용자 계정으로 ahightower라는 AWS 계정을 생성하였다. 여기서, 정상 사용자로 위장하기 위해 피해자 환경의 기존 네이밍 체계를 조회했고 해당 체계에 따라 ahightower 계정을 생성했다.

AhnLab XDR은 공격자가 기존 네이밍 체계 조회를 위해 사용자 목록을 가져온 뒤 계정을 생성한 것을 확인했다. 네이밍 체계는 왕좌의 게임에 등장하는 가문 이름에 하나의 알파벳을 추가한 형태였다.

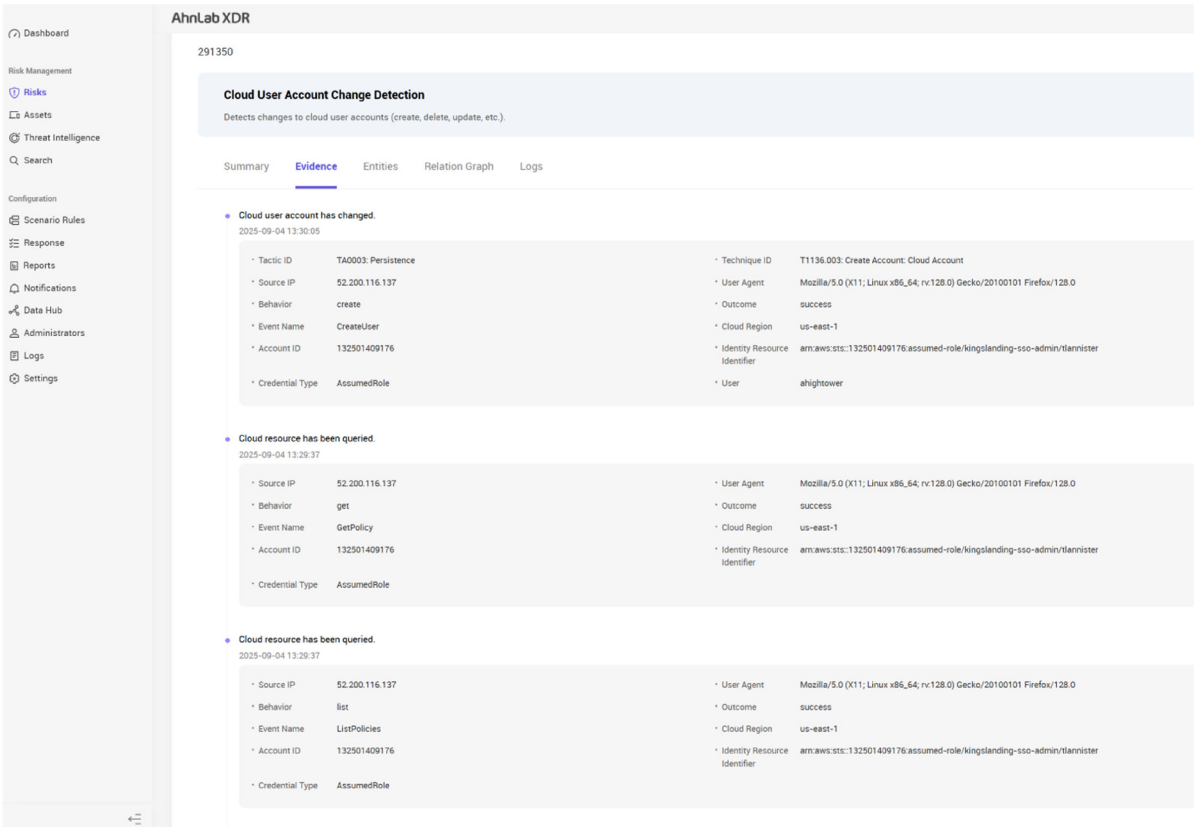
- a + targaryen
- t + lannister
- j + mormont
- a + hightower

자세히 살펴보면, AhnLab XDR은 먼저 tlannister(공격자)가 ListUserPolicies 및 ListUsers 이벤트를 통해 기존 사용자 목록 및 정책을 가져오는 행위를 탐지하였다.



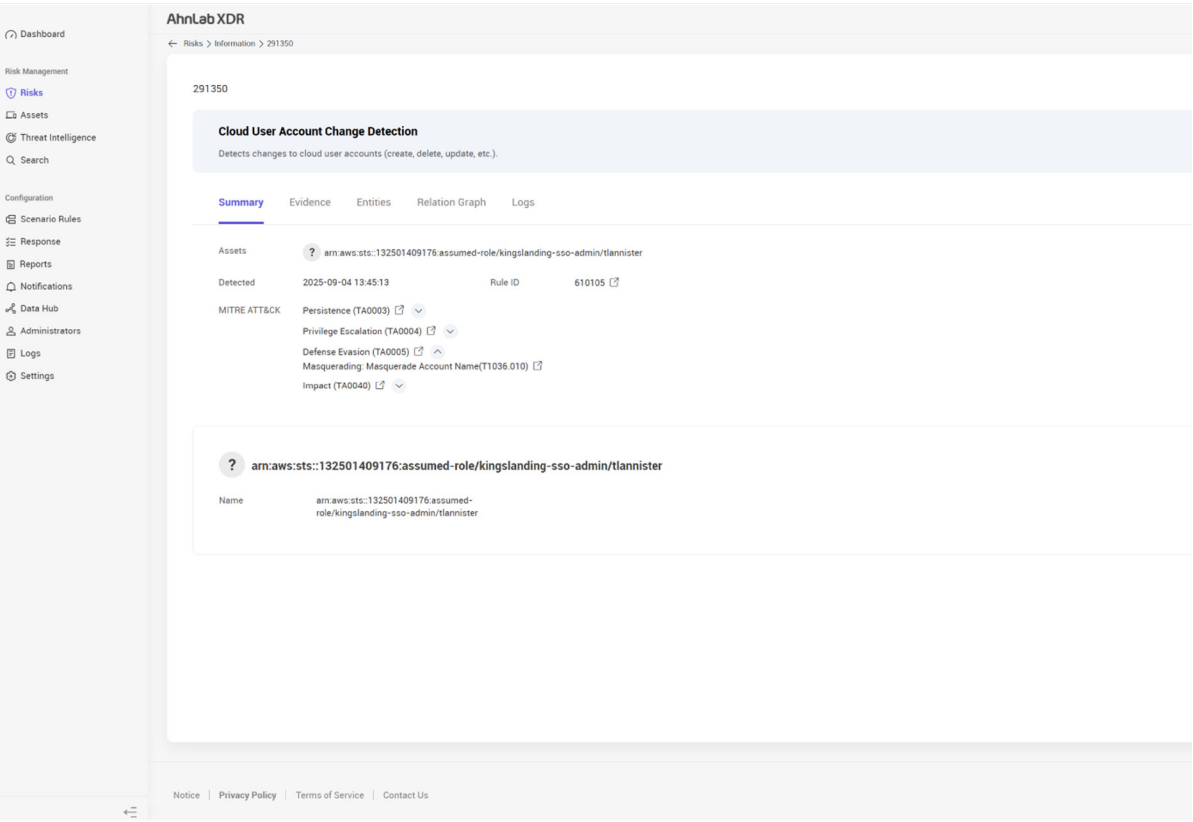
[그림 7] Detections: Substep 7.2 – 사용자 목록 및 정책 가져오기

그리고, tlannister(공격자)가 CreateUser 이벤트를 통해 ahightower를 생성하는 과정을 탐지했다.



[그림 8] Detections: Substep 7.2 – ahightower 생성

AhnLab XDR은 해당 행위에 대해 Defense Evasion (TA0005)과 Masquerading: Masquerade Account Name(T1036.010)라는 적합한 TID와 설명을 제공했다.



[그림 9] Detections: Substep 7.2 – 적합한 TID 제공

정리하면, 공격자가 탐지 회피를 목적으로 계정 이름을 위장하여 정상적인 계정처럼 보이게 하는 행위를 수행했음을 명확히 이해할 수 있도록 했다.

결론: 검증된 기술력으로 고객들을 안전하게

마이터 어택 평가는 전 세계적으로 공신력을 인정 받는 평가로 실제 위협들과 유사한 정교한 기법들로 구성되어 있다. 안랩은 본 평가에서 온프레미스와 클라우드에 걸쳐 강력한 차단, 포괄적인 위협 가시성 및 정확한 탐지 역량을 입증했다. 더 나아가, 해당 평가에 5년 연속으로 참가해 객관적인 검증을 지속하는 동시에 끊임 없는 솔루션 고도화를 통해 고객들의 신뢰를 높이고 있다는 점에서 큰 의미가 있다.

마이터 어택 평가 라운드 7 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