보안 이슈

AhnLab 보안 전문가의 심층분석! 보안 이슈 정보를 전해드립니다.

AhnLab EDR, 실전에서는 이렇게 활용한다

AhnLab 2023-06-02

국내 기업 및 기관들을 노리는 사이버 위협이 고도화를 거듭하고 있다. 해커들은 다양한 기법과 경로를 통해 공격을 감행하고 있으며, 이들의 활동은 우리가 체감하는 것보다 훨씬 가까이 와있다.

공격자들이 구사하는 최신 공격 기법에 효과적으로 대응하기 위해서는 차단을 넘어 위협을 종합적으로 탐지해 대응할 수 있는 역량을 갖춰야 한다. 안랩은 자사 EDR 솔루션 AhnLab EDR을 통해 의심스러운 행위에 대한 정확한 탐지부터 수집 및 분석, 대응, 지속적인 모니터링과 통합 관리까지 지원하고 있다. 이번 글에서는 AhnLab EDR로 프로세스 할로잉을 수행하는 닷넷 패커와 록랫 악성코드의 공격 기법을 탐지하고 분석한 사례를 소개한다.

1. 프로세스 할로잉 악성코드 추적

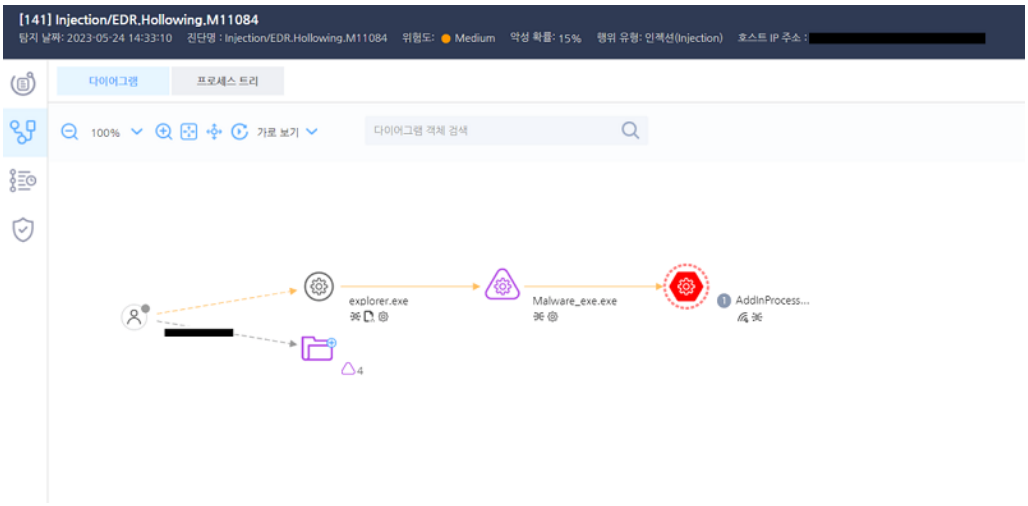
최근 닷넷(.NET)으로 만들어진 패커가 국내외에서 대거 확인되고 있다. 닷넷 패커는 대부분 패커를 통해 감추고 있는 EXE 형태의 악성 실행 파일을 로컬에 생성하지 않고, 정상 프로세스에 악성코드를 주입해 실행한다.

닷넷 패커 자체에 대한 심층 분석 내용은 ASEC 블로그를 통해 게시한 분석 보고서에서 확인할 수 있다.

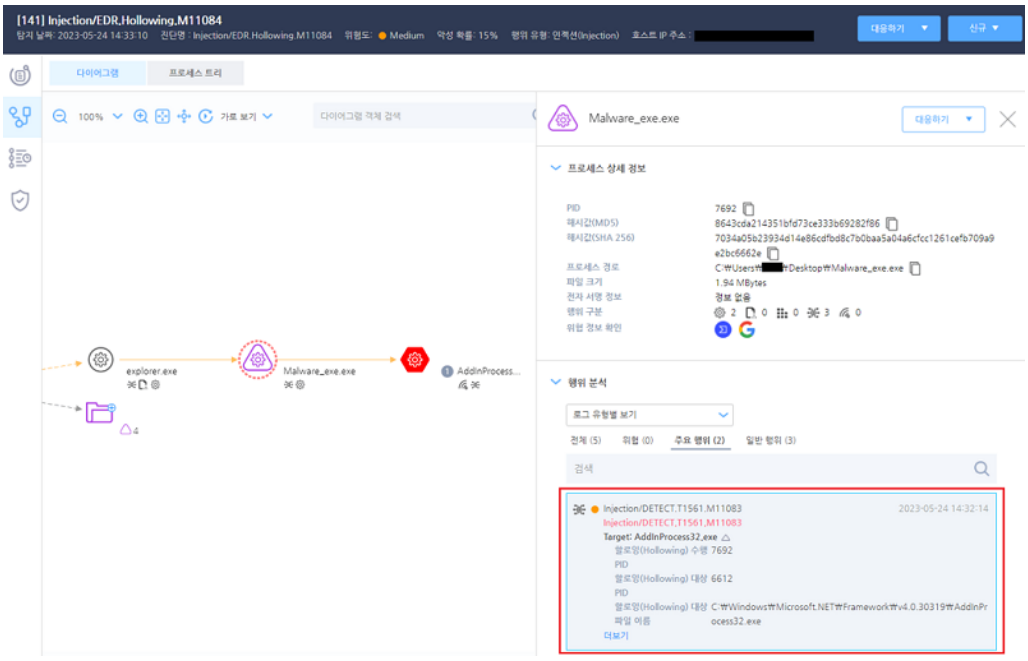
닷넷 패커는 렘코스(Remcos), 폼북(FormBook), 스크럽크립트(ScrubCrypt), 에이싱크랫(AsyncRAT) 등의 다양한 악성코드를 유포할 때 주로 최초 유포 파일 또는 중간 단계의 로더(Loader) 역할을 수행한다. 닷넷 패커에 숨겨진 악성 파일이 C2 서버의 명령에 따라 제어되는 백도어(Backdoor) 유형일 경우, 탐지하기 어렵다. 백도어가 명령을 전달받지 않은 휴면 상태일 때 C2 통신 외에는 별다른 행위를 수행하지 않기 때문이다.

하지만 AhnLab EDR에는 닷넷 패커가 사용한 악성코드가 프로세스 할로잉(Process Hollowing)을 수행한 행위 기록이 남아있다. AhnLab EDR은 이 정보를 활용해 침해를 인지하고 추적해 C2 서버를 확보하는 등의 조치로 추가 피해를 방지한다. 프로세스 할로잉이란 시스템에 정상적인 프로세스를 실행한 후 원본 프로세스의 데이터를 악성코드 데이터로 변경하는 일종의 코드 인젝션 기법을 의미한다.

[그림 1]은 AhnLab EDR이 프로세스 할로잉을 수행하는 닷넷 패커를 탐지한 화면이다. 내부에 렘코스 악성코드르 포함한 해당 닷넷 패커(Malware_exe.exe)는 할로잉 기법을 사용해 정상 프로세스인 'AddinProcess32.exe'를 실행했다. 이로 인해 렘코스 악성코드는 사용자 환경에서 파일로 생성되지 않고 AddinProcess32.exe에서 동작했다.

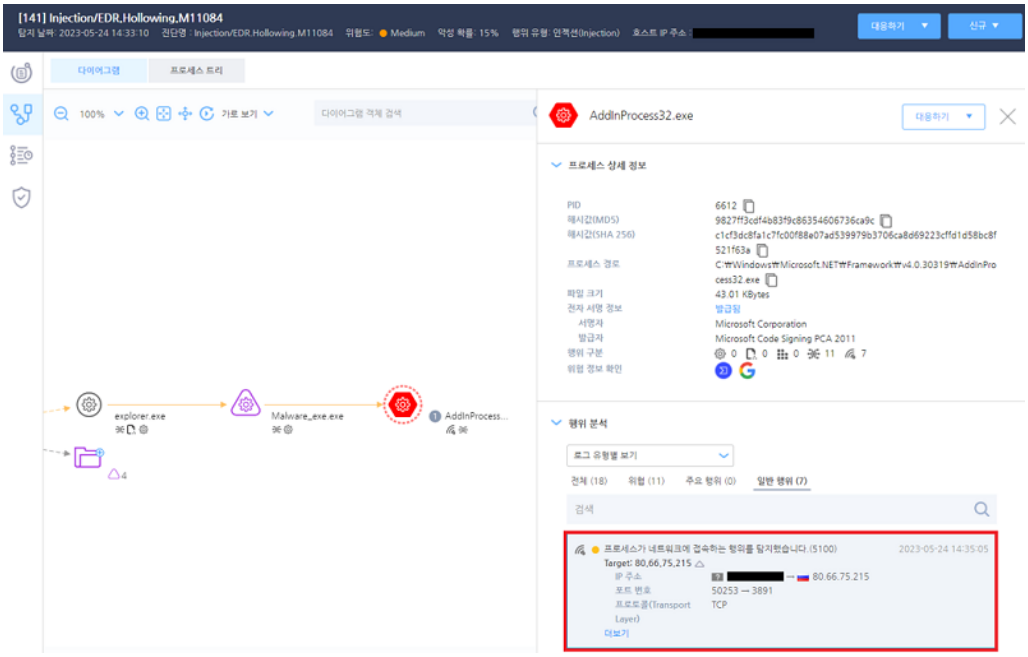


[그림 1] AhnLab EDR 탐지 다이어그램



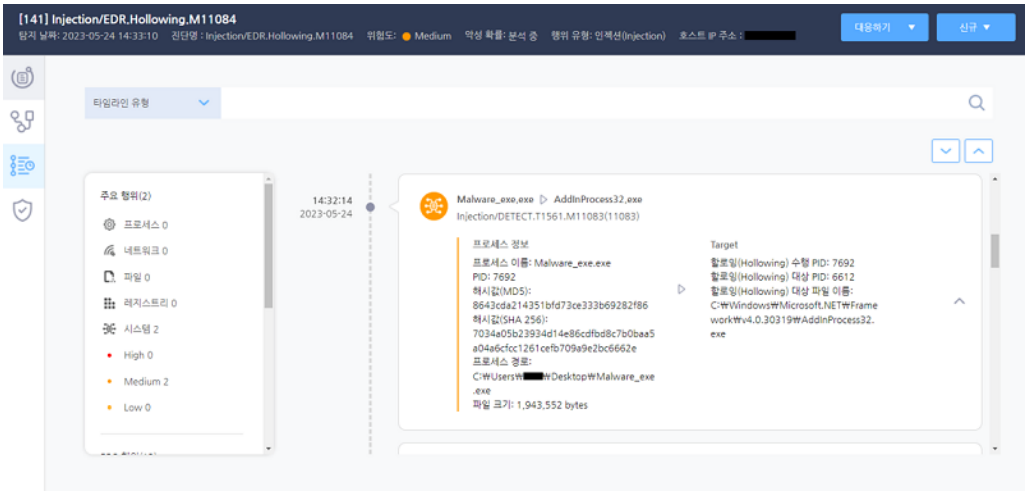
[그림 2] AhnLab EDR 탐지 다이어그램 (프로세스 할로잉)

AhnLab EDR은 [그림 3]과 같이 AddinProcess32.exe에서 동작한 렘코스가 C2 통신만 수행한 것을 보여주며, 동시에 침해가 발생한 사실을 인지한다.

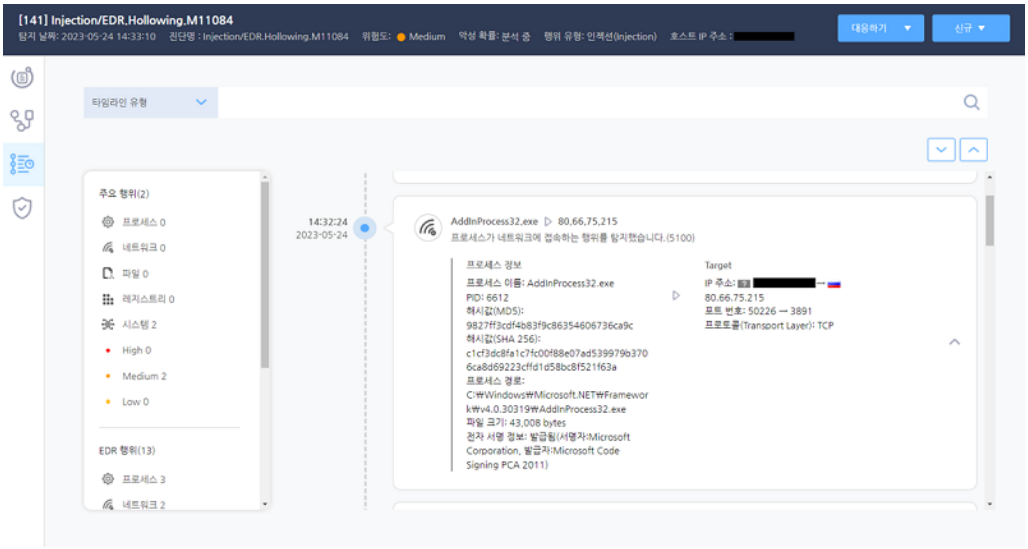


[그림 3] AhnLab EDR 탐지 다이어그램 (C2 통신)

AhnLab EDR 탐지 시점의 타임라인에서도 할로잉 및 C2 통신에 관한 정보를 확인할 수 있다. 또한, [그림 4]와 같이 닷넷 패커 악성코드의 할로잉 주체 및 대상도 알 수 있다. [그림 5]는 할로잉된 정상 프로세스(AddinProcess32.exe)에서 동작하는 렘코스 악성코드의 C2 통신을 보여주는 화면이다.



[그림 4] AhnLab EDR 탐지 타임라인 (프로세스 할로잉)



[그림 5] AhnLab EDR 탐지 타임라인 (C2 통신)

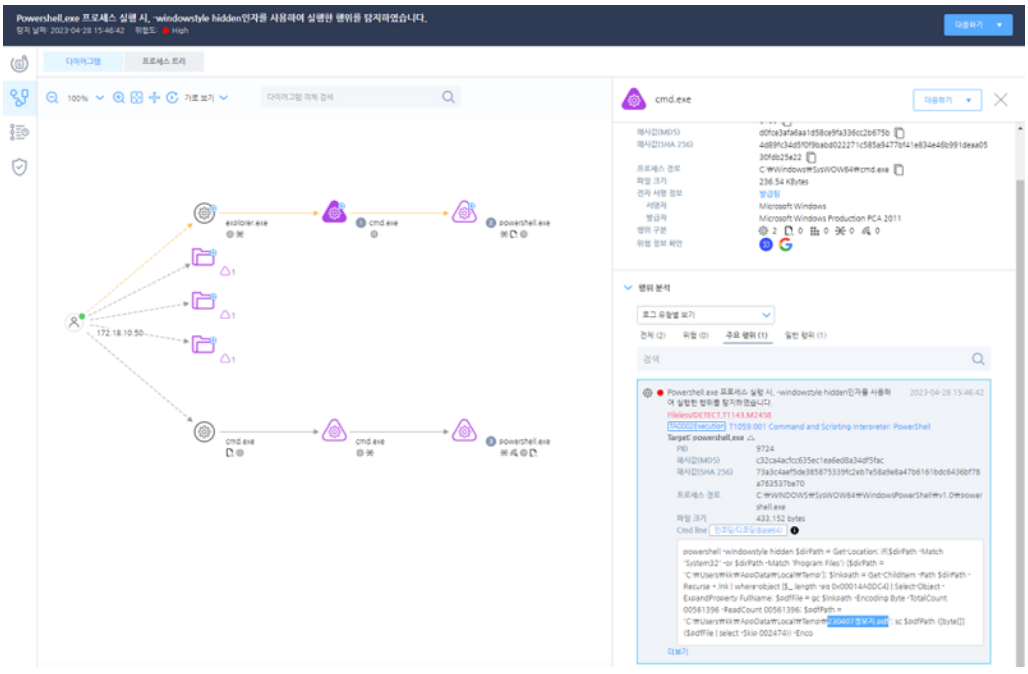
이처럼, AhnLab EDR을 활용하면 탐지가 어려운 고도화된 위협과 공격 기법도 탐지해 선제적으로 대응하여 피해를 최소화할 수 있다.

2. 악성 링크 파일 탐지 및 분석

안랩은 지난 4월, ASEC 블로그를 통해 레드아이즈(RedEyes) 공격 그룹(APT37 혹은 ScarCruft)이 링크 파일(*.lnk)을 통해 유포하는 'RokRAT 악성코드' 관련 내용을 공유한 바 있다. 해당 공격 역시 AhnLab EDR을 통해 상세한 탐지 및 분석이 가능하다.

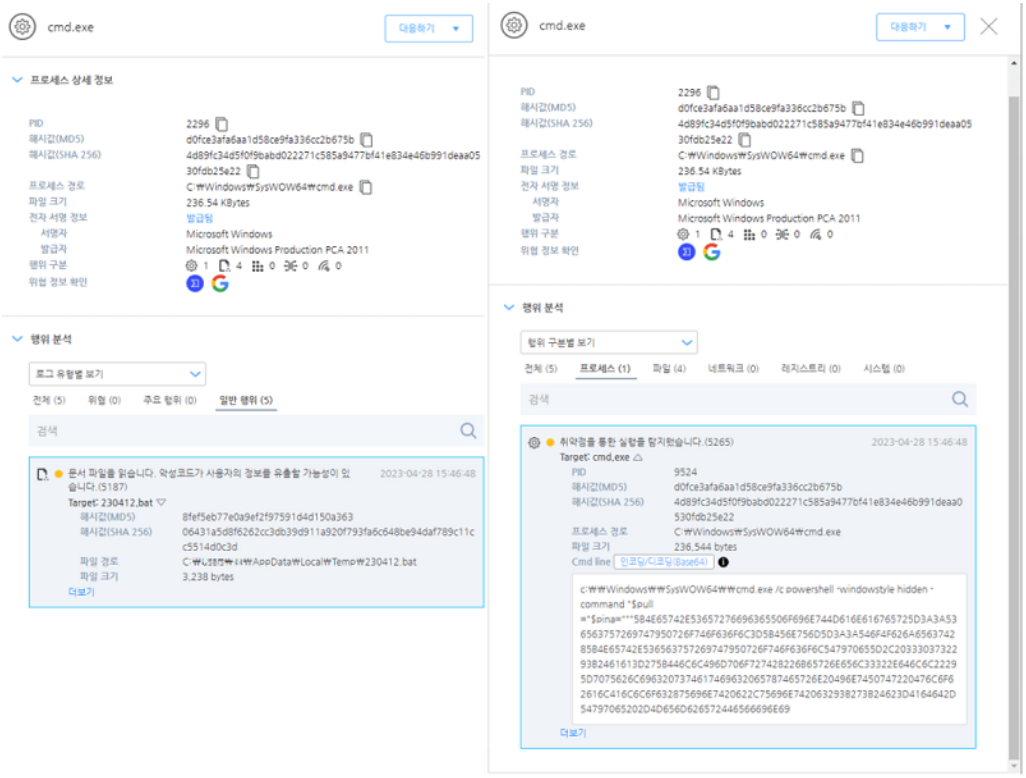
우선, 레드아이즈가 록랫 악성코드를 유포하는데 사용한 링크 파일은 "temp" 경로에 정상 파일과 함께 스크립트 파일을 생성 및 실행해 악성 행위를 수행하는 파워셸(PoweShell) 명령어를 포함한다.

AhnLab EDR은 악성 링크 파일이 사용자 시스템에 유입돼 실행되면 [그림 6]과 같이 의심스러운 파워셸의 실행을 탐지한다.

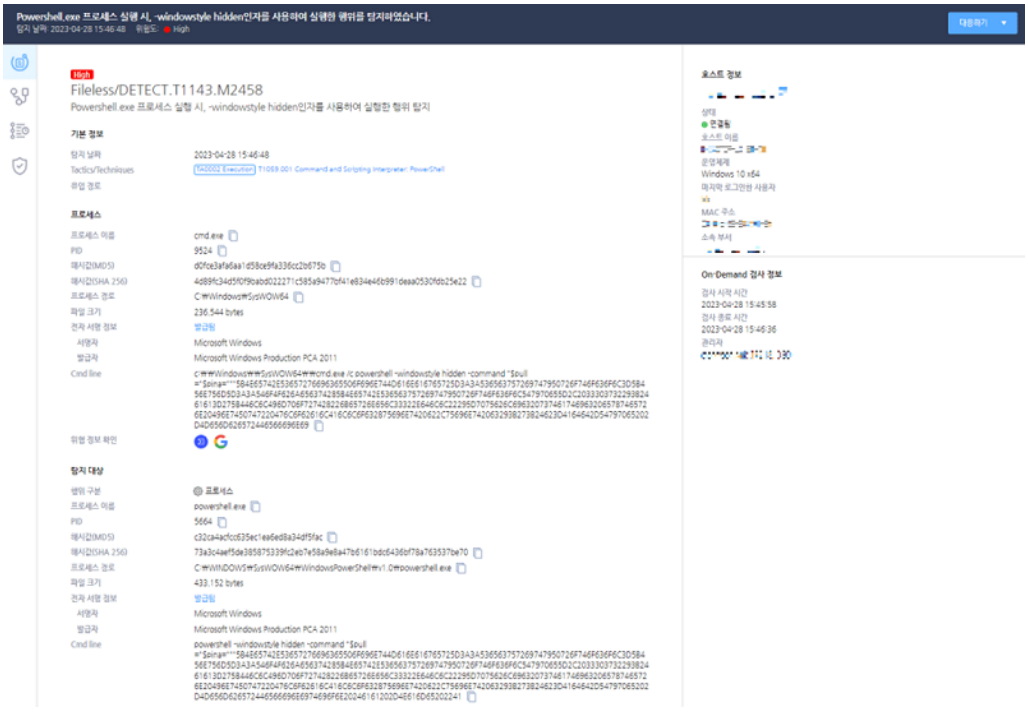


[그림 6] 의심스러운 PowerShell.exe 프로세스 실행 탐지

[그림 6]에서 "cmd.exe"를 클릭하면 [그림 7]과 같이 배치 파일(*.bat)의 실행 이력과 명령어를 확인할 수 있다.

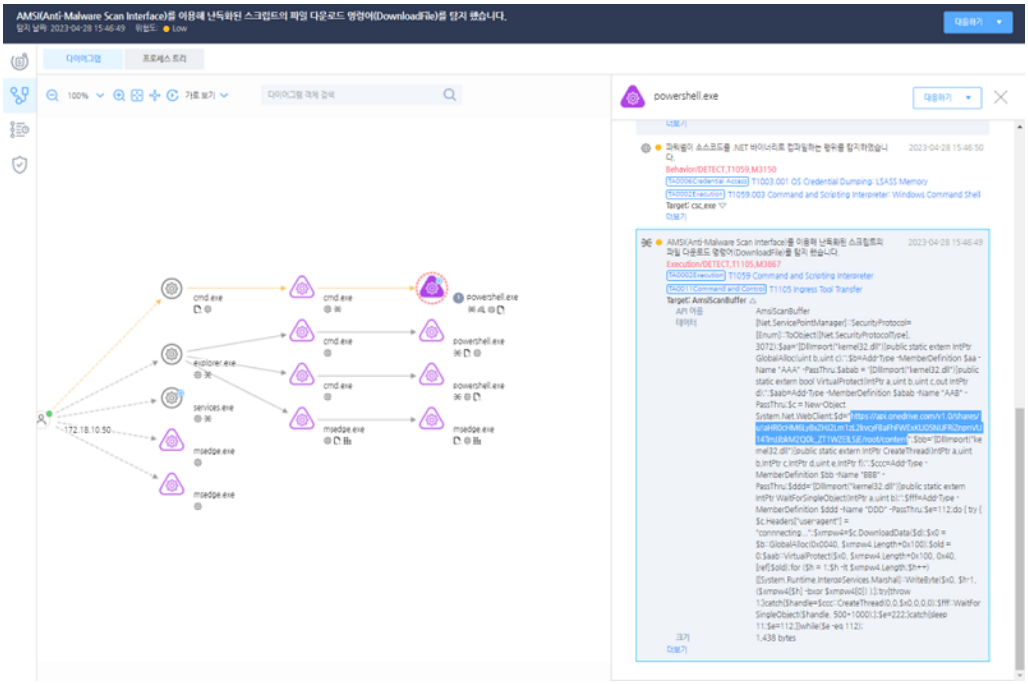


[그림 7] 배치 파일 실행 내역과 명령어



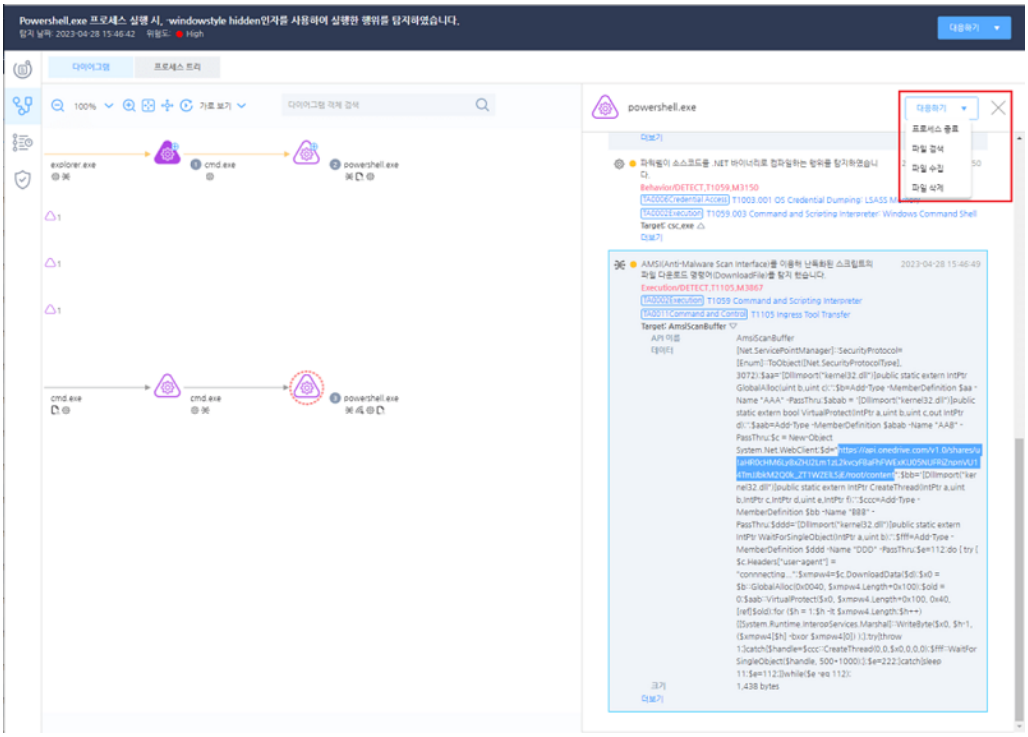
[그림 8] 배치 파일에 의해 실행된 파워셸 탐지 화면

AhnLab EDR이 배치 파일에 의해 실행된 파워셸 명령어를 탐지하면 오른쪽 상단의 호스트 정보를 통해 어떤 시스템에 누가 로그인을 해서 해당 명령어가 실행된 것인지 파악할 수 있다. 또, 해당 PC를 조사하는 과정에서 [그림 9]와 같이 악성코드 다운로드 URL 주소도 확인이 가능하다.

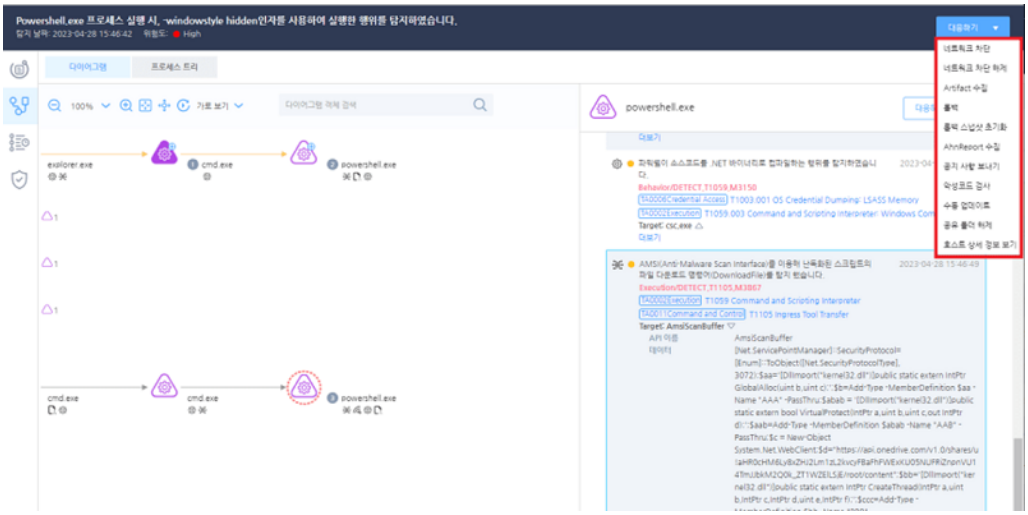


[그림 9] 악성코드 다운로드 URL

의심스러운 로그가 확인되면 보안 담당자는 [그림 10] 및 [그림 11]과 같이 AhnLab EDR에 탑재된 프로세스 종료, 해당 시스템의 네트워크 격리 등의 기능으로 대응할 수 있다.



[그림 10] AhnLab EDR의 프로세스 종료 기능



[그림 11] 의심스러운 시스템에 대한 대응(네트워크 차단, 악성코드 검사)

결론적으로, 사용자는 AhnLab EDR을 활용해 공격 단계별 다차원 분석과 지속적인 모니터링, 통합 관리로 정교화된 위협에 대한 선제적 대응이 가능하다. 더 나아가, EDR과 V3(안티바이러스), MDS(샌드박스)를 상호 연계하면 더 강력한 시너지 효과를 낼 수 있다.

AhnLab EDR에 대한 보다 자세한 정보는 안랩 홈페이지를 통해 확인할 수 있다.
▶**AhnLab EDR 제품정보페이지 바로가기**

AhnLab 콘텐츠기획팀 서보경 사원