정상 도구로 위장한 공격, AhnLab EDR은 어떻게 잡아낼까

엔드포인트 공격은 악성코드 자체보다도, 실행 이후 어떤 행위가 이어지는지에 따라 피해 규모가 달라진다. 보안 담당자에게는 위협을 조기에 인지하고, 공격 흐름을 따라가며 원인을 파악할 수 있는 탐지 및 분석 기반의 대응 체계가 중요하다. 특히 정상 도구를 악용한 공격은 단순 실행 여부만으로는 위협을 식별하기 어려워, 행위 기반으로 이상 징후를 포착하는 접근이 요구된다.

이런 관점에서 AhnLab EDR은 엔드포인트에서 발생하는 의심 행위를 기반으로 위협 징후를 탐지하고, 공격 흐름을 가시화해 대응 판단을 지원한다. 이번 글에서는 AhnLab EDR이 실제 공격을 어떤 방식으로 탐지하고 가시화하는지 소개하기 위해, 최근 확인된 원격 모니터링·관리(Remote Monitoring and Management, RMM) 도구 악용 사례를 예시로 살펴본다.

EDR 기반 위협 모니터링이 필요한 이유

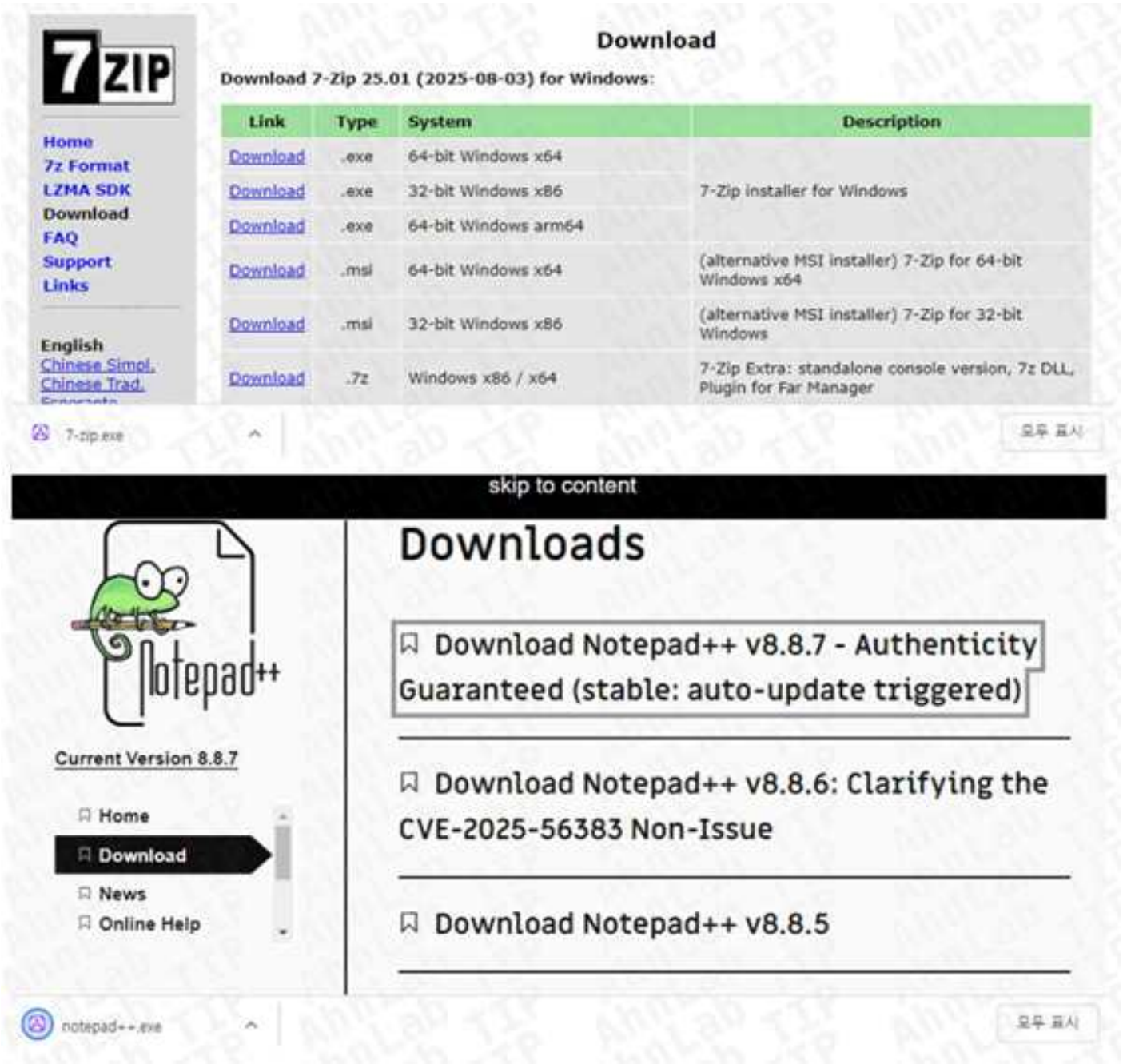
최근 공격자들은 정상 도구로도 사용되는 RMM을 악용해 감염 시스템을 원격으로 제어하거나, 추가 악성코드를 유포하는 방식으로 공격을 확장하고 있다. 문제는 이런 도구들이 업무 환경에서 활용되기도 하고, 일부는 정상 소프트웨어로 분류되는 경우가 많아 전통적인 안티바이러스(Anti-virus) 방식만으로는 위협 여부를 판단하거나 대응하기 어려울 수 있다는 점이다. 이런 이유로 조직은 특정 도구의 설치 및 실행 여부만 확인하는 방식에서 나아가, 엔드포인트에서 발생하는 의심 행위를 기반으로 실행 정황과 이후 공격 흐름까지 함께 추적할 수 있는 EDR 기반 모니터링 체계를 갖출 필요가 있다.

AhnLab EDR은 국내 유일의 행위 기반 분석 엔진을 기반으로 엔드포인트 영역에서 강력한 위협 모니터링과 분석, 대응 역량을 제공하는 차세대 엔드포인트 위협 탐지 및 대응 솔루션이다. 의심 행위에 대한 유형별 정보를 상시 수집하고, 탐지 결과를 기반으로 위협을 보다 명확하게 인지할 수 있도록 지원한다. 이를 통해 보안 담당자는 종합적인 분석을 바탕으로 원인을 파악하고, 적절한 대응 및 재발 방지 프로세스를 수립할 수 있다.

다음은 실제로 확인된 공격 흐름을 바탕으로, RMM 도구가 어떤 방식으로 악용됐는지와 함께 AhnLab EDR이 이 위협 징후를 어떻게 탐지하는지를 보여주는 대표 사례를 정리한 것이다.

사례 1. 가짜 유틸리티 다운로드 페이지 위장으로 RMM 설치 유도

2025년 11월, RMM 도구인 LogMeIn Resolve와 PDQ Connect를 악용한 공격이 확인됐다. 공격자는 Notepad++, 7-zip 등 정상 유틸리티는 물론 텔레그램, ChatCPT, OpenAI 등을 사칭한 다운로드 페이지로 사용자를 유인해 LogMeIn Resolve를 내려 받도록 한 뒤, 정보 탈취 기능을 가진 추가 악성코드를 함께 설치했다.



[그림 1] 위장 유틸리티 다운로드 페이지

LogMeIn Resolve는 원격 지원, 패치 관리, 모니터링 등의 기능을 제공하는 RMM 도구다. 사용자가 해당 프로그램을 설치하면 LogMeIn의 인프라에 등록되며, 공격자는 이를 이용해 감염 대상 시스템을 원격으로 제어할 수 있다. 공격자는 LogMeIn을 악용해 파워쉘 명령을 실행하고, 백도어 악성코드인 PatoRAT을 설치한 정황이 확인됐다.

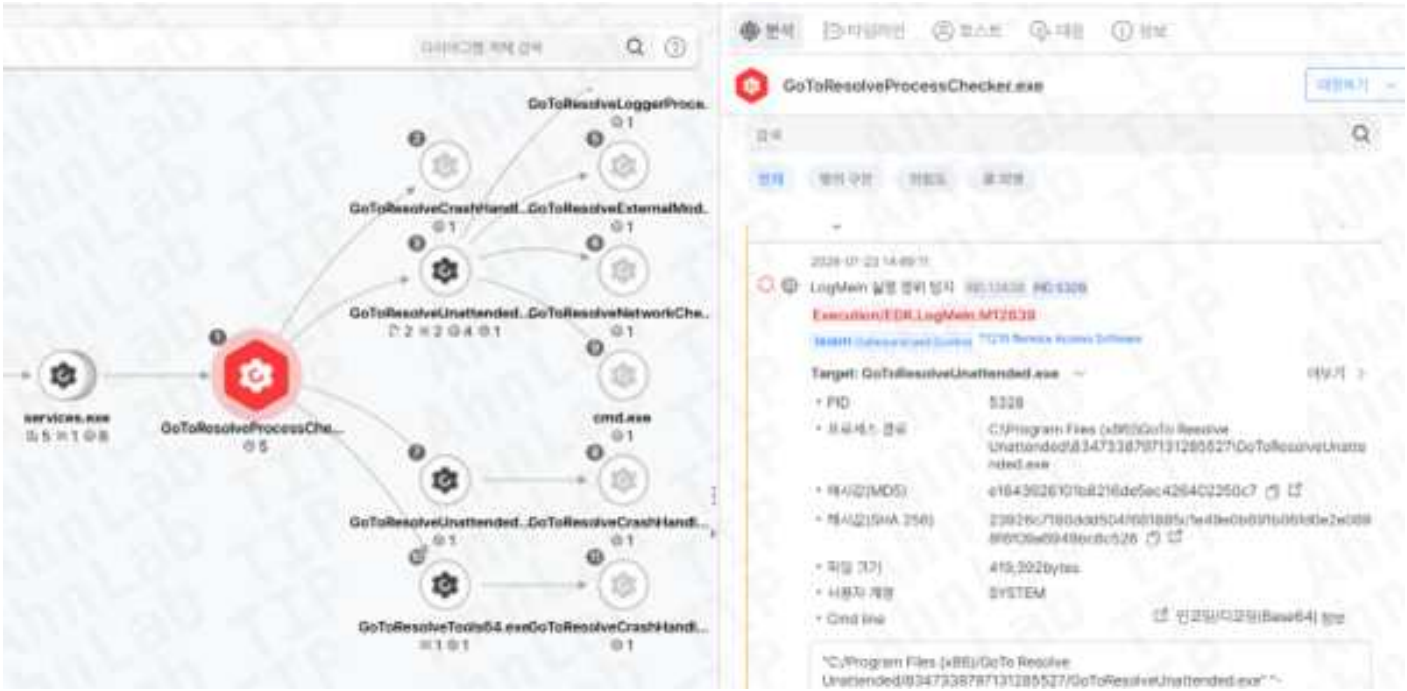
한편, PatoRAT은 LogMeIn Resolve뿐만 아니라 PDQ Connect를 통해서도 설치된 사례가 확인됐다. PDQ Connect도 LogMeIn Resolve와 유사하게 소프트웨어 패키지 배포, 패치 관리, 인벤토리, 원격 제어 기능 등을 제공하는 RMM 도구다. 공격자는 사용자의 PDQ Connect 설치를 유도한 뒤 LogMeIn Resolve와 동일한 방식으로 이를 악용해 PatoRAT을 설치한 것으로 분석된다.

Target Type	File Name	File Size	File Path
Target	webview.exe	8.41 MB	%SystemDrive%\users\%ASD%\edgeupdate\webview.exe
Current	powershell.exe	444 KB	%SystemRoot%\system32\windowspowershell\v1.0\powershell.exe
Parent	pdq-connect-agent.exe	8.98 MB	%ProgramFiles%\pdq\pdqconnectagent\pdq-connect-agent.exe

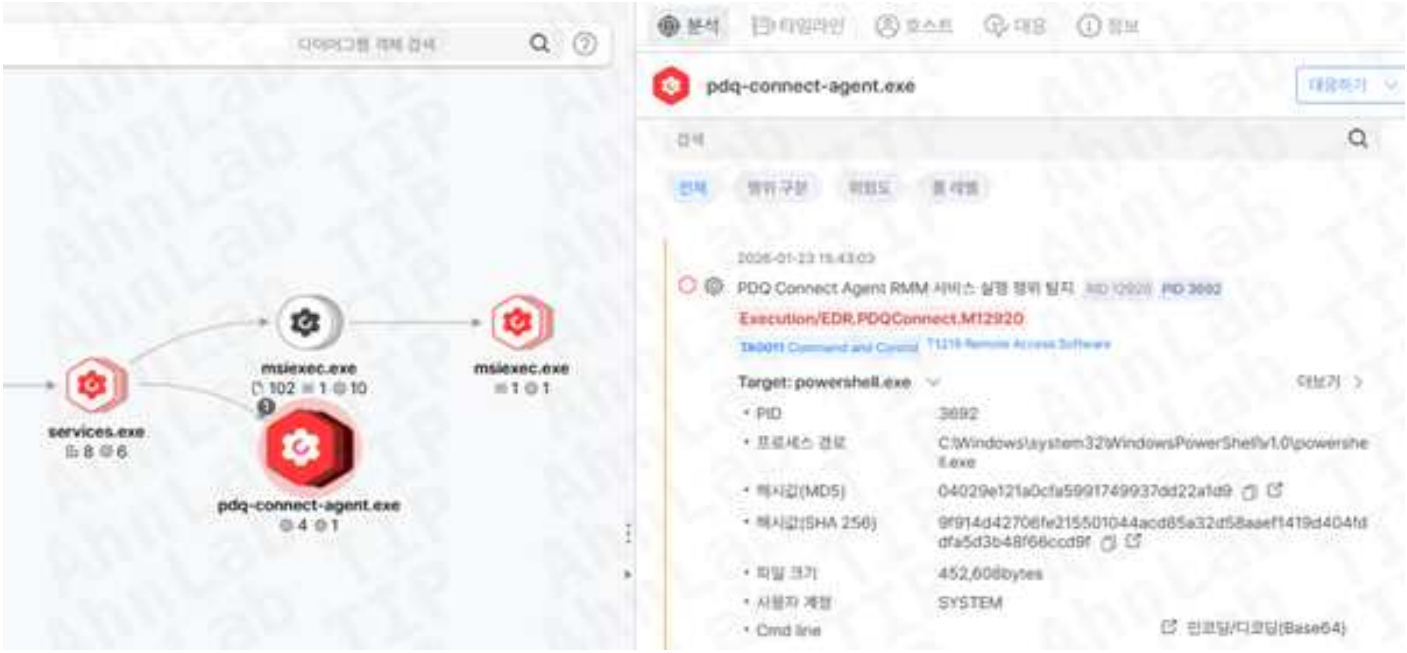
Process	Module	Target	Behavior	Data
powershell.exe	N/A	N/A	Creates executable file	webview.exe
powershell.exe	N/A	N/A	A suspicious process created a file.	N/A

[그림 2] PDQ Connect를 이용한 악성코드 설치 로그

AhnLab EDR은 LogMeIn Resolve 및 PDQ Connect가 시스템에서 실행되는 행위를 위협으로 탐지해 관리자가 해당 이상 징후를 사전에 인지하고 대응할 수 있도록 지원한다.



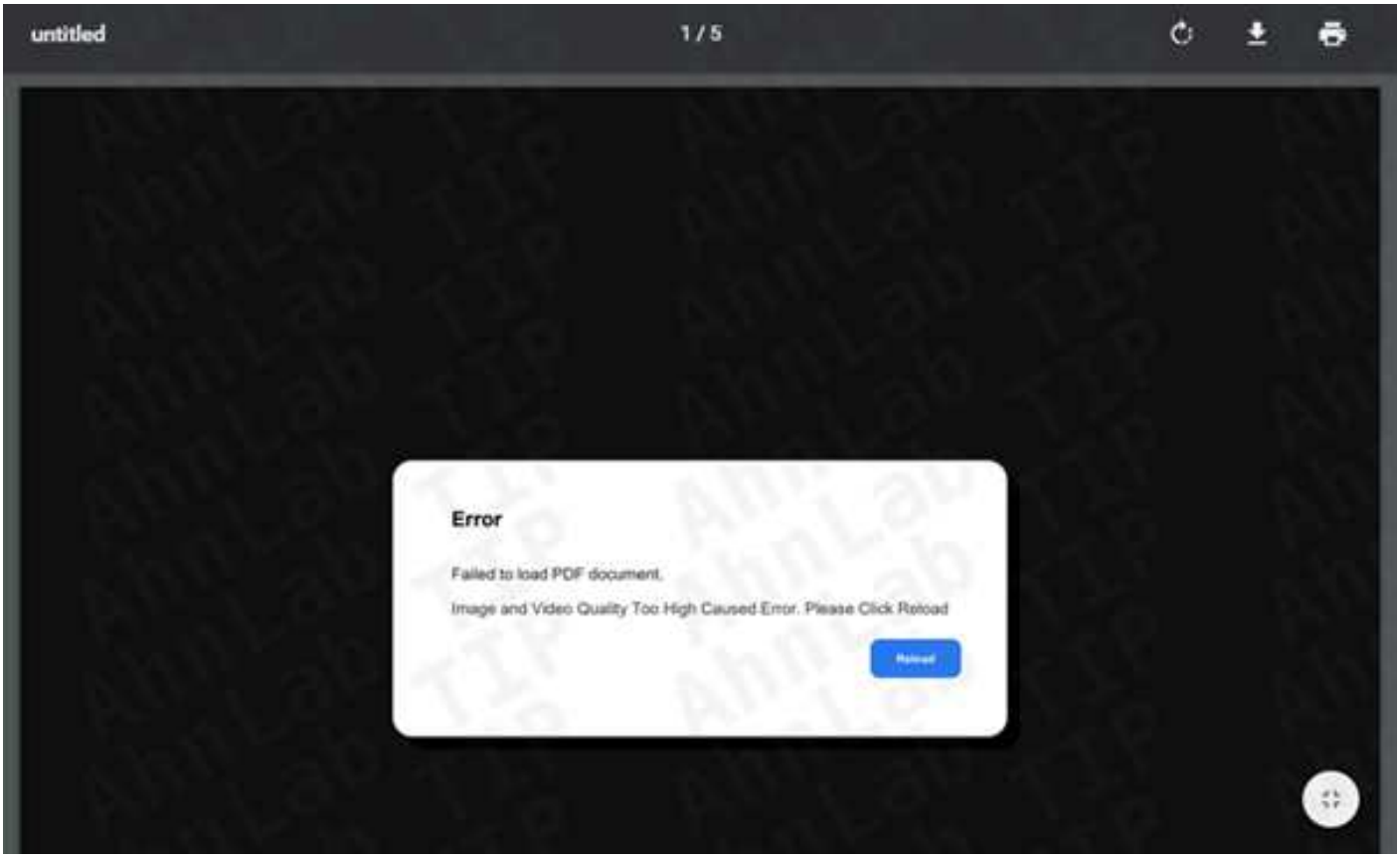
[그림 3] AhnLab EDR을 활용한 LogMeIn 실행 행위 탐지



[그림 4] AhnLab EDR을 활용한 PDQ Connect 실행 행위 탐지

사례 2. 정상 문서(PDF)로 위장한 피싱 메일 기반 RMM 유포

2026년 1월, 피싱 메일을 통해 Syncro, SuperOps, NinjaOne, ScreenConnect 등 다양한 RMM 도구를 유포한 사례가 확인됐다. 공격에 사용된 PDF 문서 파일은 “Invoce”, “Product Order”, “Payment” 등 업무 관련 키워드를 포함한 이름으로 위장해 수신자의 의심을 낮추는 방식이었으며, 실행하면 고화질로 인해 미리 보기가 불가능하다는 안내와 함께 구글 드라이브 링크 클릭을 유도하는 형태로 구성됐다.



[그림 5] 공격에 사용된 PDF 악성 문서

해당 공격을 통해 유포된 RMM 도구는 ‘Syncro’로 확인됐다. Syncro RMM은 MSP(Managed Service Provider) 및 IT 팀을 위한 원격 모니터링 및 관리 도구로, Chaos, Royal 같은 랜섬웨어 공격자들뿐만 아니라 이란 APT 위협 그룹 ‘MuddyWater’가 사용한 것으로도 알려졌다.

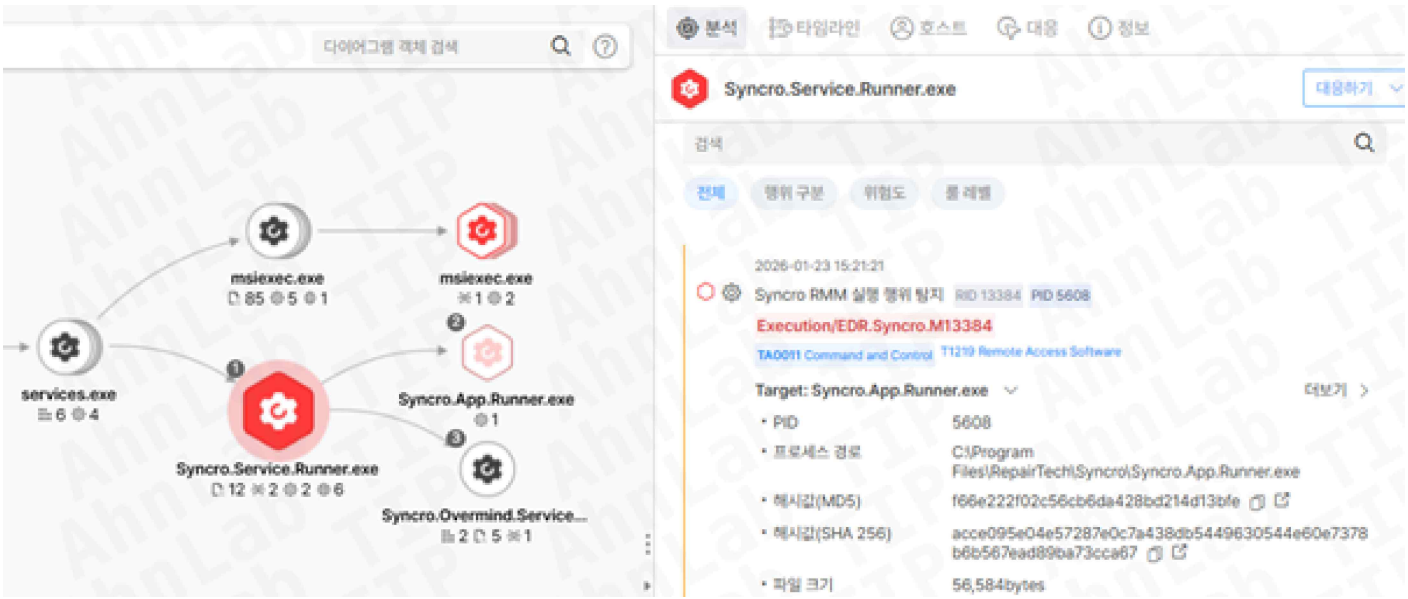
[그림 6] Syncro사 홈페이지

동일한 인증서로 서명된 악성코드들을 확인한 결과, Syncro 외에도 다양한 RMM 도구가 2025년 10월부터 악용된 정황이 확인됐다. ScreenConnect는 원격 접속과 화면 제어 기능을 제공하는 RMM/원격 지원 솔루션으로, 장애 대응이나 유지 보수 목적에 주로 활용되지만, ALPHV/BlackCat, Hive 등 랜섬웨어 공격자들에 악용된 사례도 보고된 바 있다.

[그림 7] 악성코드 서명에 사용된 인증서

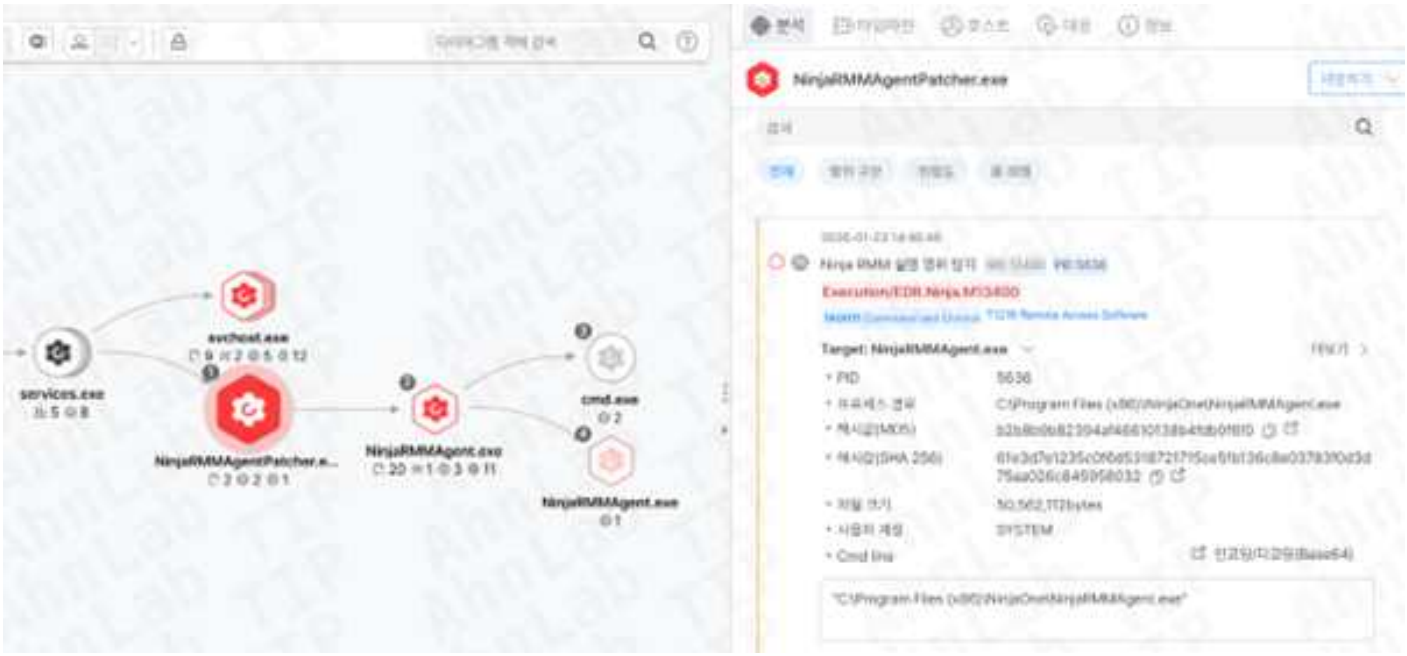
이외에도 NinjaOne과 SuperOps 역시 악용된 정황이 확인됐다. NinjaOne은 기업의 IT 인프라를 원격으로 모니터링·관리하기 위한 클라우드 기반 RMM 솔루션으로 원격 접속, 패치 및 소프트웨어 배포, 성능 모니터링, IT 자산 관리 등의 기능을 지원한다. SuperOps는 MSP를 대상으로 한 클라우드 기반 RMM/PSA 통합 솔루션으로, NinjaOne과 유사하게 원격 접속, 자산·패치 관리, 모니터링 기능을 지원한다.

AhnLab EDR은 이 RMM 도구들의 실행 징후를 위협으로 탐지해 관리자가 이상 징후를 사전에 인지하고 대응할 수 있도록 했다.



[그림 8] AhnLab EDR을 활용한 Syncro 실행 행위 탐지

[그림 9] AhnLab EDR을 활용한 ScreenConnect 실행 행위 탐지



[그림 10] AhnLab EDR을 활용한 NinjaOne 실행 행위 탐지

[그림 11] AhnLab EDR을 활용한 SuperOps 실행 행위 탐지

결론

이처럼 정상 RMM 도구를 악용한 공격 수법은 점차 다양해지고 있어, 기본적인 보안 수칙을 꾸준히 점검할 필요가 있다. 아래 4가지를 실천하면 피해 가능성을 크게 줄일 수 있을 것이다.

1) 유틸리티 다운로드 전 공식 경로 확인

- 유틸리티 다운로드 시 공식 홈페이지 여부를 먼저 확인해야 한다.
- 광고 페이지나 검색 결과 상단 링크 등은 위장 페이지일 수 있어 주의가 필요하다.

2) 다운로드 파일의 버전 정보·인증서 점검

- 내려 받은 파일의 버전 정보와 인증서를 검사해 의도한 설치 파일이 맞는지 확인한다.

3) 출처가 불분명한 이메일은 열람 전 확인

- 이메일의 발신자가 신뢰할 수 있는지 확인하고, 의심스러운 링크나 첨부 파일은 함부로 열지 않는다.

4) 운영체제 및 보안 제품 최신 상태 유지

- 운영체제와 보안 제품을 최신 버전으로 업데이트해 알려진 위협으로부터 보호해야 한다.

AhnLab EDR에 대한 보다 자세한 내용은 **안랩 홈페이지**에서 확인할 수 있다.

AhnLab

ASEC