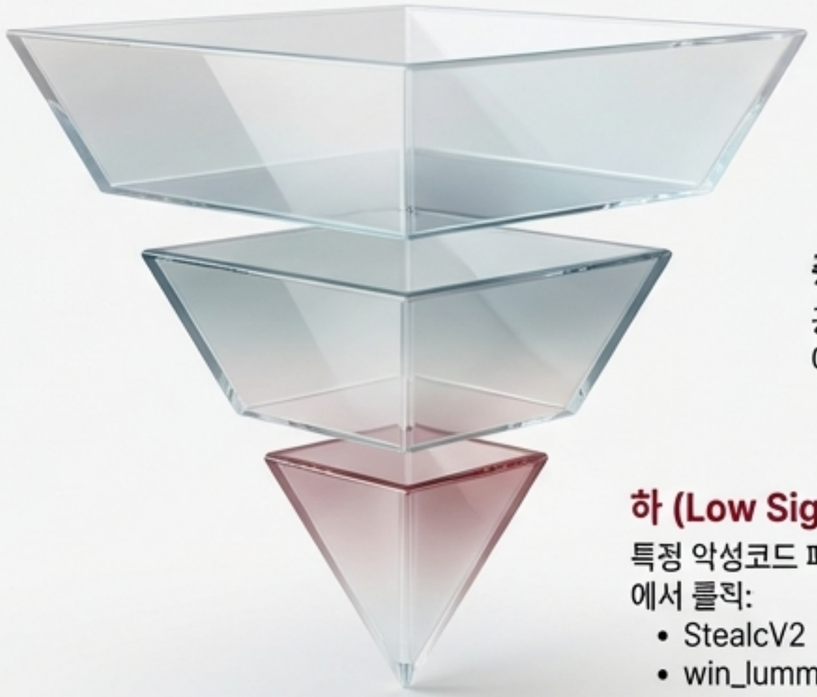
탐지를 넘어 프로파일링으로: 메모리 신호의 이해

YaraHub 룰셋을 활용하면 단순 탐지를 넘어, 메모리의 "성격"을 프로파일링할 수 있습니다.
모든 룰이 같은 의미를 갖는 것은 아닙니다.



상 (High Signal) - 행위의 단서 (Behavioral Clues)

로더/언패커 등에서 공통적으로 나타나는 일반적인 악성 행위의 흔적.

- meth_get_eip
- pe_detect_tls_callbacks
- DetectEncryptedVariants

중 (Mid Signal) - 도구의 흔적 (Tooling Artifacts)

공격 프레임워크(에: Cobalt Strike)나 특정 캠페인에서 사용된 도구의 흔적.
에서 흔적:

- cobalt_strike_tmp01925d3f
- RANSOMWARE

하 (Low Signal) - 패밀리 확증 (Family Confirmation)

특정 악성코드 패밀리를 높은 신뢰도로 확증할 수 있는 고유한 시그니처.
에서 를직:

- StealcV2
- win_lumma_generic

메모리 분석은 "이것이 악성코드인가?"라는 질문뿐만 아니라,
"이 악성코드는 어떤 종류의 행위를 하는가?"에 대한 깊이 있는 답변을 제공합니다.