핵심 요약: 조사에서 전략으로

1. 정적 탐지는 한계에 도달했습니다 (Static Detection Has Reached Its Limit)

최신 악성코드는 패킹과 난독화로 기존 시그니처 기반 방어를 쉽게 우회합니다.

2. 메모리는 악성코드의 본질을 드러냅니다 (Memory Reveals a Malware’s Essence)

실행 불변 특징(Execution Invariants)은 난독화 너머의 진실을 보여주는 신뢰도 높은 증거입니다.

3. 견고하고 지속 가능한 방어 전략입니다 (A Robust and Sustainable Strategy)

공격자 입장에서 메모리 불변 특징을 회피하는 것은 기술적, 비용적으로 매우 어렵습니다.

4. 누구나 검증하고 활용할 수 있습니다 (Accessible for Verification and Use)

`apt`와 YARA 같은 오픈소스 도구를 통해 이 접근법을 즉시 현업에 적용하고 검증할 수 있습니다.