

이제 당신의 차례입니다: `apt` 툴킷으로 직접 확인하십시오

- 본 발표에 사용된 모든 워크플로우와 스크립트는 공개된 GitHub 리포지토리에서 사용할 수 있습니다.
- 직접 이 실험을 재현하고, 탐지율을 검증하고, 여러분의 YARA 룰을 테스트해보십시오.
- **주요 기능:**
 - 악성코드 샘플 및 메모리 덤프의 자동 수집
 - 안전한 Docker 격리 환경 내에서 YARA 스캔 수행
 - 탐지 결과 및 통계 자동 생성



github.com/windshock/apt