AD(Active Directory) 시스템 악용
침해사고 탐지 스크립트 사용 매뉴얼

AD_Script_v3.1_20200130

[1. 스크립트 제공 개요]

- 최근 기업의 AD(Active Directory) 시스템 환경을 악용한 침해사고 발생 빈도 증가

- SK인포섹 침해사고대응팀 다수의 사고 분석 사례에서 축적된 DB를 기반으로 하여 유사 사고 식별을 위한 침해사고 흔적 탐지 스크립트 제작 및 배포

- 침해지표(IOC)를 식별하여 인지하지 못한 내부 공격 흔적 탐지 / 침해사고 초기 대응 및 원인 규명을 통한 재발방지 방안 마련 효과 기대

[2. 포함 프로그램]

- Microsoft LogParser 2.2

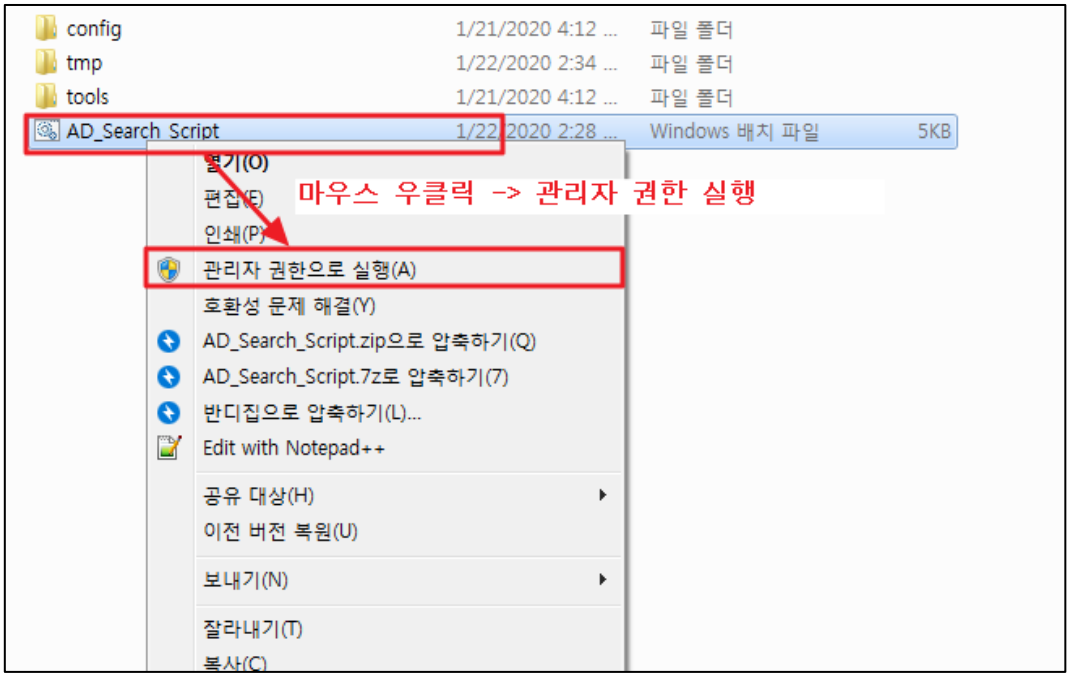
[3. 점검 대상 시스템]

- AD(Active Directory)환경으로 동작 중인 Windows 계열 서버 / PC

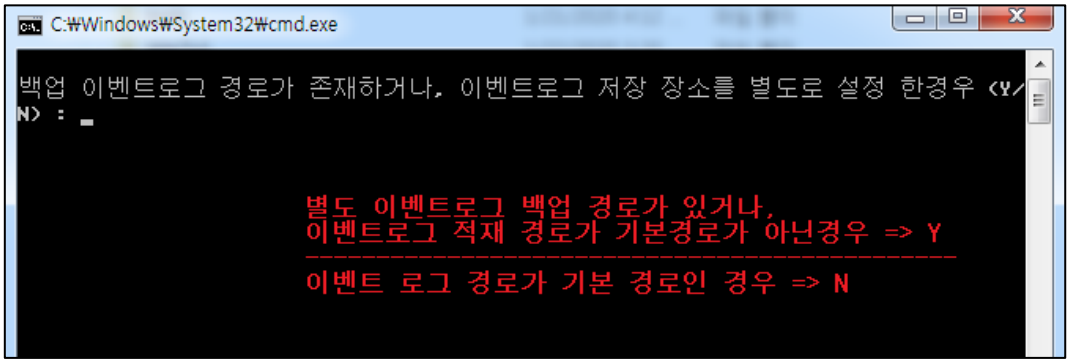
(다음 페이지 계속)

[4. 사용 방법]

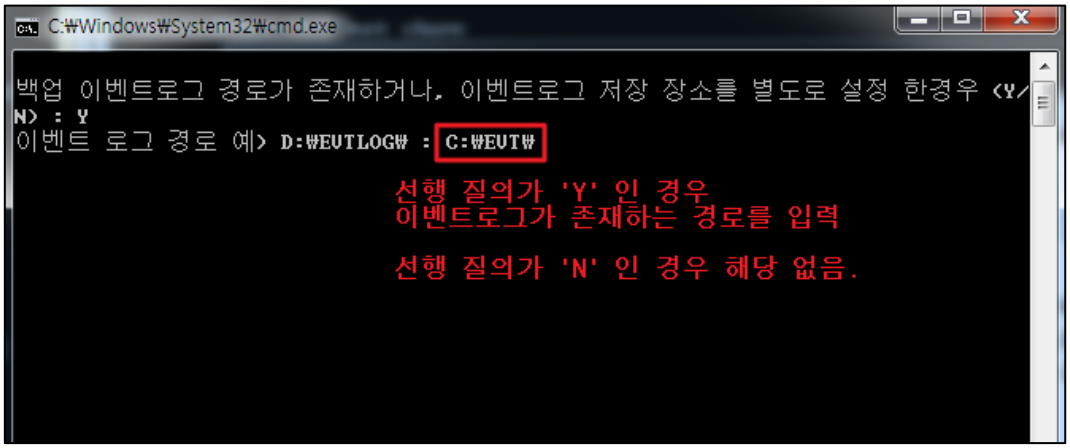
1. 다운로드 받은 첨부 파일 압축 해제 후 AD_Search_Script.bat 관리자 권한으로 실행



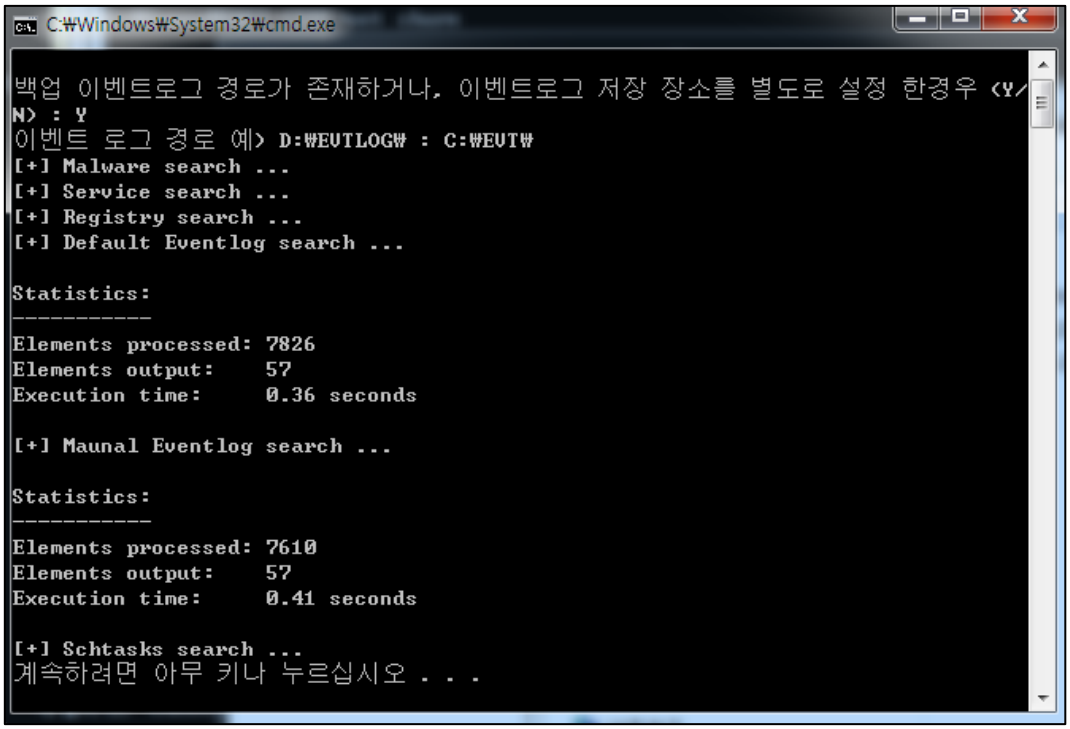
2. 이벤트로그 백업을 위한 경로가 별도 존재하거나, 이벤트로그 저장 장소가 기본경로(C:₩Windows₩System32₩winevt₩Logs₩)가 아닌 경우 Y 선택, 특이사항 없는 경우 N 선택



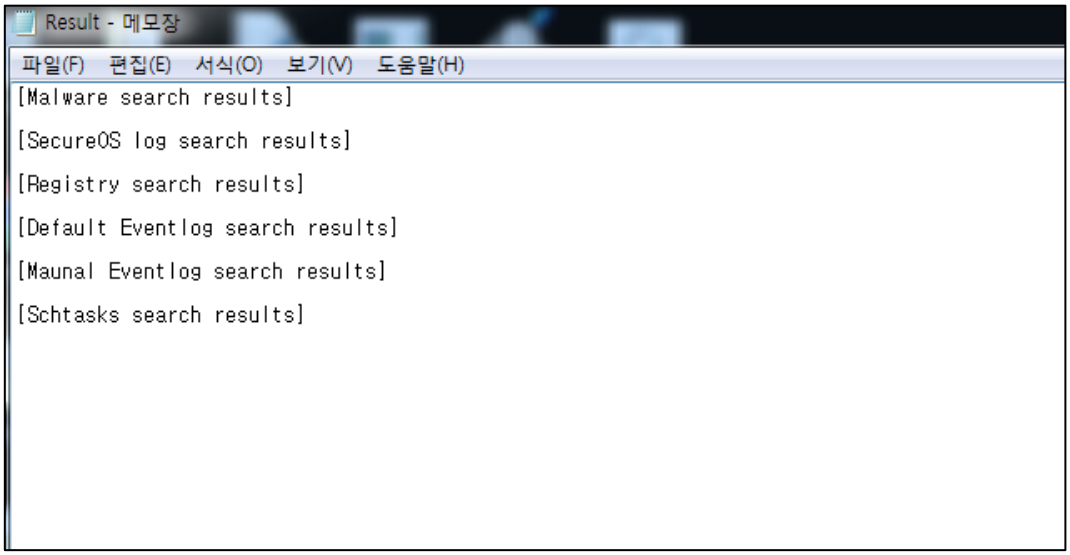
3. (2번 항목이 Y인 경우에만 해당) 이벤트로그가 존재하는 혹은 추가로 존재하는 경로 지정



4. 정상적으로 실행 완료 경우 "계속하려면 아무 키나 누르시오..." 문구 출력



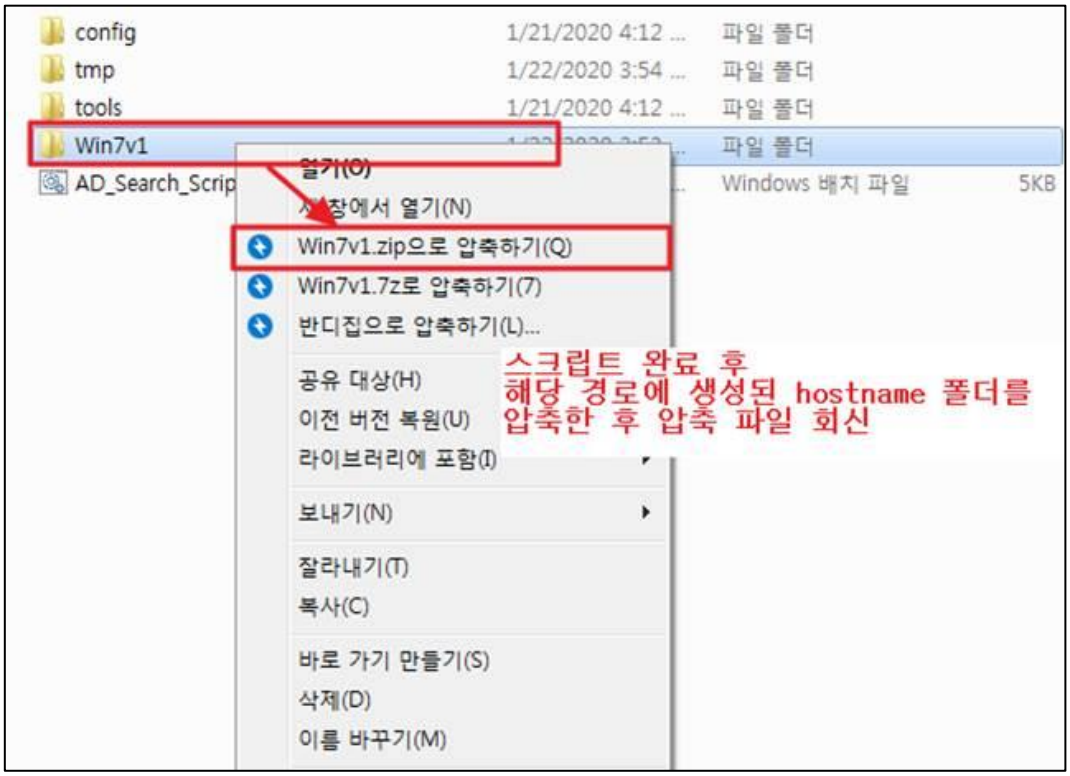
5. bat 파일을 실행한 동일 경로에 hostname 파일명 폴더 생성. 해당 폴더 내 Result.txt 파일 내 특이사항 확인



[특이사항이 존재하지 않는 경우]

[특이사항이 존재하는 경우]

6. 특이사항이 존재할 경우 아래 "**5. 정/오탐 판별방법**"을 참고하여 hostname 폴더 압축 후 침해사고대응팀으로 정/오탐 판별 및 분석 요청 의뢰



(다음 페이지 계속)

[5. 정/오탐 판별 방법]

1. Malware Search Results 항목

- "hamcore.se2" 파일 탐지 시 해당 시스템에서 Softether VPN 사용여부 확인 필요
- C:₩Windows₩System32₩dllcache₩ 항목 오탐 (v3.1_20200130 예외 처리)
- 기타 모든 탐지 내역에 대해서는 추가 확인 필요

2. SecureOS log search results, Default/Manual Eventlog search results, Schtasks search results 항목

- 정탐 예시
  : "cmd.exe /q /c echo [command] ^> ₩Windows₩temp₩filename 2^>&1 >%temp%abcd.bat & del %temp%abcd.bat" 와 유사한 형식
- cmd.exe 프로세스를 관리적인 목적으로 서비스나 스케쥴에 등록하여 사용하는 경우 탐지 가능성 존재
- Software Inventory Logging 스케쥴 오탐 (v3.1_20200130 예외 처리)
- 기타 모든 탐지 내역에 대해서는 추가 확인 필요

3. Service search results, Registry search results 항목

- 모든 탐지 내역에 대해서는 추가 확인 필요

확인이 필요한 정탐 탐지내역이 존재할 시 SK인포섹 침해사고대응팀으로 실행 결과 폴더를 **'고객사명_hostname_IP.zip'** 파일명으로 압축하여 회신 바랍니다.

[6. 회신처]

- 소속 : SK인포섹 침해사고대응팀

- 이름 : 정영하 수석

- E-Mail : yhjeong@sk.com

[7. 변경 이력]

v3.1_20200130 : 오탐 항목 예외 처리

(끝)