|  |
| --- |
| 오사용으로 인한 문제 발생시 책임지지 않습니다.  SK쉴더스에서 확인된 샘플만 복호화가 가능합니다. |

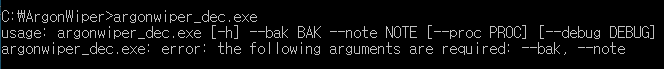
* 백업 파일과 랜섬노트 파일을 통해 키를 결정해 복호화를 수행한다. 이때 백업 파일이 생성된 시스템의 CPU 코어 수를 --proc 옵션을 통해 전달해야 하는 경우가 존재한다. (백업 파일이 생성된 시스템이 아닌 다른 곳에서 복호화 진행 시 필요하며, key 값에 따라 필요 여부가 결정된다.)
* 암호화된 백업 파일 형태

|  |  |
| --- | --- |
| 파일명 | |
| [0-9a-f]{8}eyp.bak | [0-9a-f]{8}dngi.bak |
| [0-9a-f]{8}sinar.bak | [0-9a-f]{8}ya2hsc.bak |
| [0-9a-f]{8}.{Computer name} | {Drive char}\_[0-9a-f]{12}\_jamwu.bak |
| {Drive char}\_\_[0-9a-f]{12}\_taib.bak | {Drive char}\_\_[0-9a-f]{12}\_samc.bak |
| {Drive char}\_\_[0-9a-f]{12}\_ucsi.bak | {Drive char}\_\_[0-9a-f]{12}\_wpl.bak |

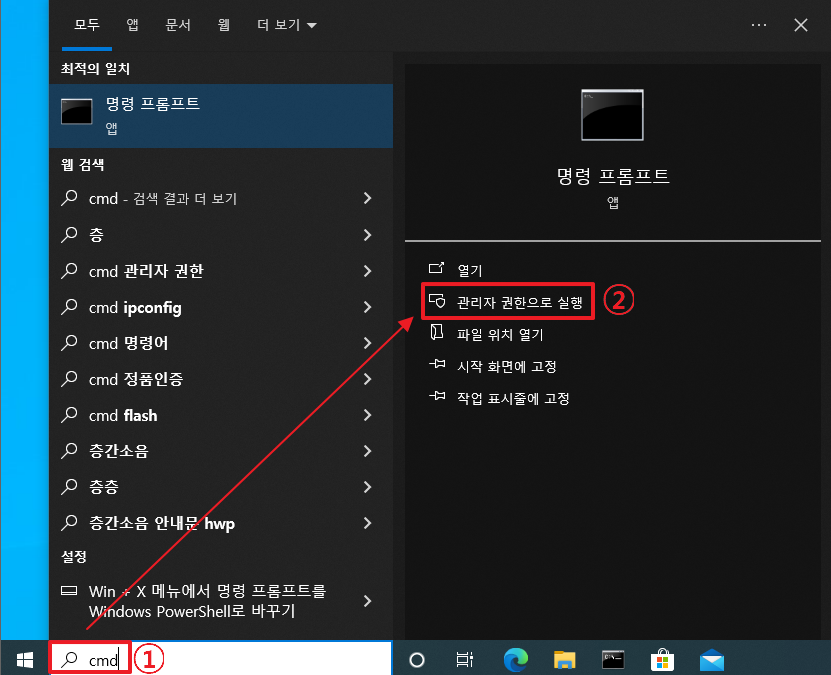
* 랜섬노트의 파일명은 backup\_log.txt, {Computer name}\_log.txt 두가지 형태
* 옵션 설명

|  |  |
| --- | --- |
| 옵션 | 설명 |
| --bak | 복호화를 진행할 \*.bak 파일의 전체 경로 |
| --note | 랜섬노트 파일의 전체 경로 |
| --proc | 백업 파일이 생성된 시스템의 프로세서 코어 개수 |
| --debug | 복호화 Block 처리 진행 출력 |

* 도움말 출력

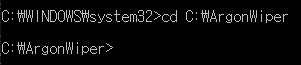


* 복호화 도구 사용법
* 우선, 명령 프롬프트를 관리자 권한으로 실행한다.



* 명령 프롬프트 실행 후 복호화 툴이 위치한 경로로 “cd” 명령어를 사용해 이동한다.

명령어: cd {복호화 툴 경로}



* 다음 예시와 같이 --bak, --note 옵션이 반드시 포함되어야 하며, 전체 경로를 입력해야 한다. 키 생성이 정상적으로 됐을 경우 복호화 과정이 진행된다.
* 만약, 키 생성이 정상적이지 않은 경우 --proc 옵션을 통해 백업 파일이 생성된 시스템의 코어 개수를 입력해 시도한다.
* 정상적으로 진행된 경우 복호화된 파일을 확인할 수 있으며, 백업 파일이 위치한 경로에 “{백업 파일명}.tar.zst” 파일로 생성된다.



* 복호화 완료 화면

