AppCheck 안티랜섬웨어

- 캅(CARB)엔진 동작 확인 방법 -

CHECKMAL

AppCheck 안티랜섬웨어의 캅(CARB)엔진을 통해 파일 훼손 행위 차단 여부를 사용자가 직접 확인할 수 있는 테스트입니다.

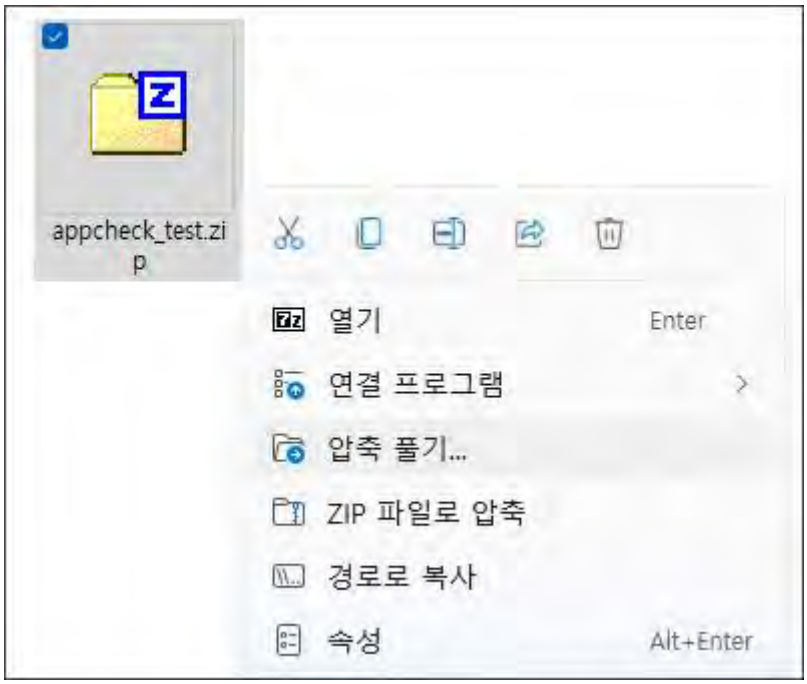
해당 테스트 방법은 시스템에 아무런 위협을 주지 않으므로 안심하시기 바랍니다.

<사전 준비물>

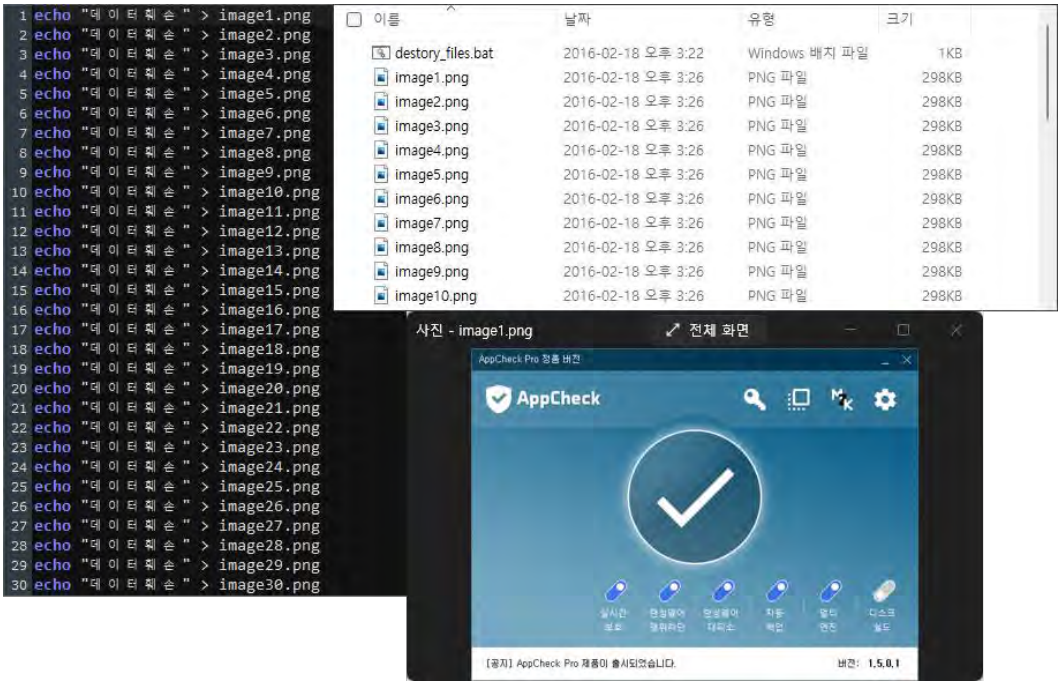
- ✓ **AppCheck 안티랜섬웨어 :** https://www.checkmal.com/download/appcheckv3.0/AppCheckSetup.exe
- ✓ **테스트 파일(appcheck_test.zip) :** https://www.checkmal.com/download/appcheck_test.zip

1. AppCheck 안티랜섬웨어 설치 파일을 다운로드하여 설치를 진행하시기 바랍니다.

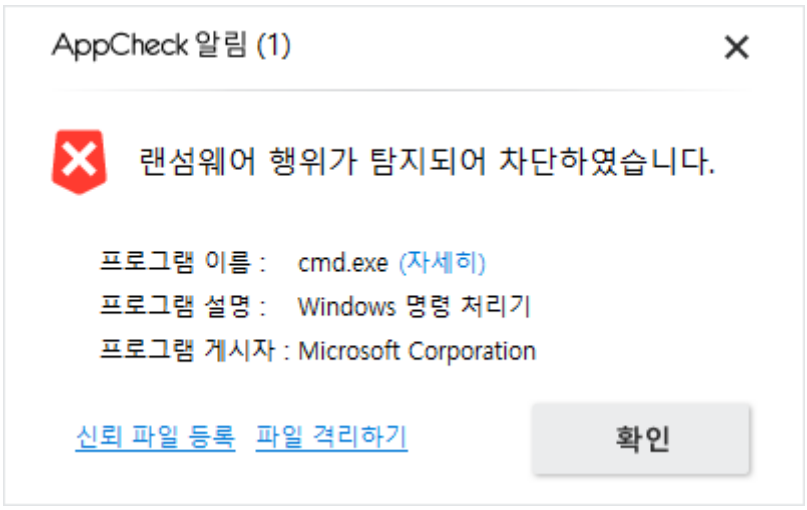
2. 테스트 파일(appcheck_test.zip)을 임의의 폴더에 다운로드 후 압축 해제하시기 바랍니다.



3. 압축 해제된 폴더에는 PNG 그림 파일(30개)과 destory_files.bat 배치 파일이 존재하며, destory_files.bat 파일은 echo의 redirect 명령을 통해 30개의 PNG 그림 파일을 훼손할 목적으로 제작되었습니다.

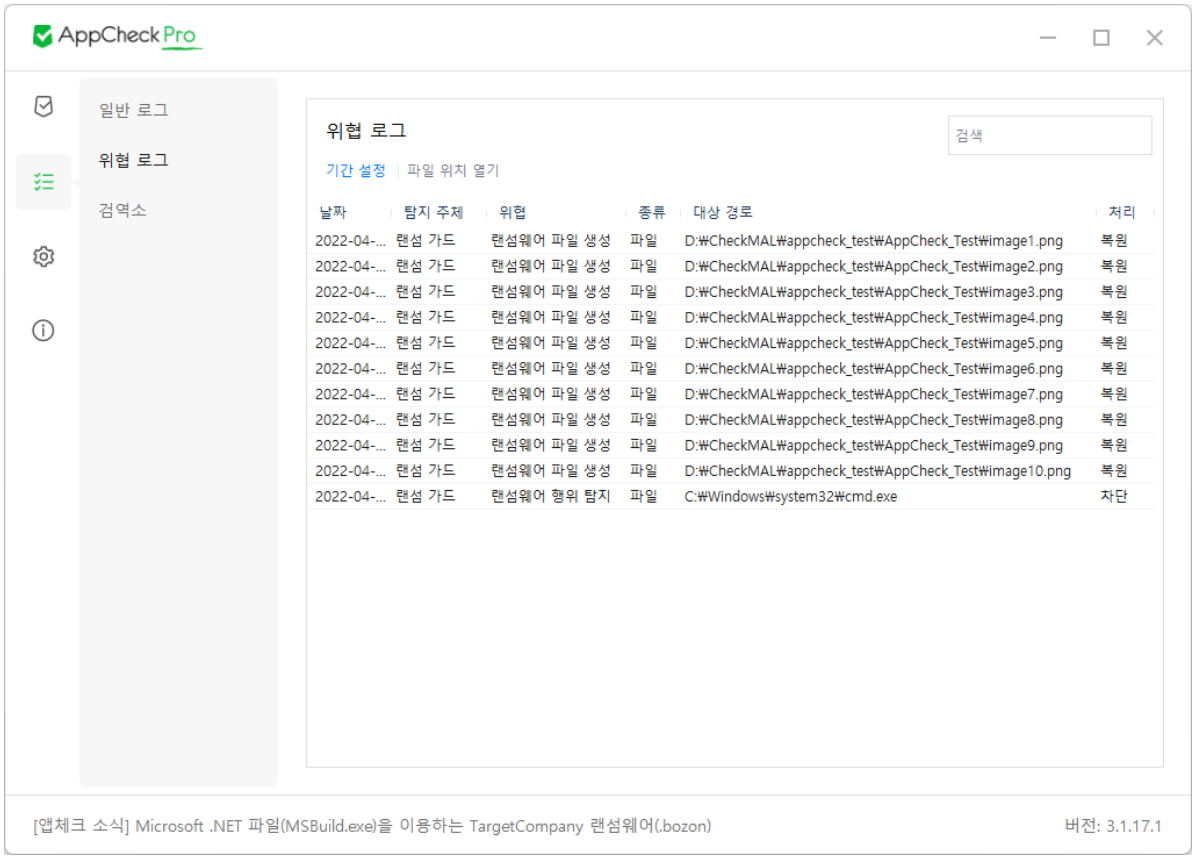


4. destory_files.bat 파일을 클릭하여 실행하면 자동으로 30개의 PNG 그림 파일에 대한 데이터 훼손 행위가 진행되며, 이 과정에서 AppCheck 안티랜섬웨어는 **"랜섬웨어 행위 탐지"** 알림창을 생성하여 파일 훼손 행위를 차단합니다.



파일 훼손 행위가 발생하는 파일(.png 그림 파일)의 복사본은 실시간으로 랜섬웨어 대피소 폴더(기본값 : C:₩ProgramData₩CheckMAL₩AppCheck₩RansomShelter)에 임시 백업되며, 랜섬웨어 행위 탐지를 통해 차단이 이루어질 경우 랜섬웨어 대피소 폴더에 임시 백업된 파일을 이용하여 자동 복원을 진행합니다.

5. AppCheck 도구의 **"위협 로그"** 메뉴를 통해 랜섬웨어 행위 탐지를 통해 차단된 프로세스(파일) 및 일부 훼손된 파일이 자동 복원된 상세한 정보를 확인할 수 있습니다.


AppCheck Pro
일반 로그
위협 로그
검역소
위협 로그
검색
기간 설정 | 파일 위치 열기
날짜 탐지 주체 위협 종류 대상 경로 처리
2022-04-... 랜섬 가드 랜섬웨어 파일 생성 파일 D:₩CheckMAL₩appcheck_test₩AppCheck_Test₩image1.png 복원
2022-04-... 랜섬 가드 랜섬웨어 파일 생성 파일 D:₩CheckMAL₩appcheck_test₩AppCheck_Test₩image2.png 복원
2022-04-... 랜섬 가드 랜섬웨어 파일 생성 파일 D:₩CheckMAL₩appcheck_test₩AppCheck_Test₩image3.png 복원
2022-04-... 랜섬 가드 랜섬웨어 파일 생성 파일 D:₩CheckMAL₩appcheck_test₩AppCheck_Test₩image4.png 복원
2022-04-... 랜섬 가드 랜섬웨어 파일 생성 파일 D:₩CheckMAL₩appcheck_test₩AppCheck_Test₩image5.png 복원
2022-04-... 랜섬 가드 랜섬웨어 파일 생성 파일 D:₩CheckMAL₩appcheck_test₩AppCheck_Test₩image6.png 복원
2022-04-... 랜섬 가드 랜섬웨어 파일 생성 파일 D:₩CheckMAL₩appcheck_test₩AppCheck_Test₩image7.png 복원
2022-04-... 랜섬 가드 랜섬웨어 파일 생성 파일 D:₩CheckMAL₩appcheck_test₩AppCheck_Test₩image8.png 복원
2022-04-... 랜섬 가드 랜섬웨어 파일 생성 파일 D:₩CheckMAL₩appcheck_test₩AppCheck_Test₩image9.png 복원
2022-04-... 랜섬 가드 랜섬웨어 파일 생성 파일 D:₩CheckMAL₩appcheck_test₩AppCheck_Test₩image10.png 복원
2022-04-... 랜섬 가드 랜섬웨어 행위 탐지 파일 C:₩Windows₩system32₩cmd.exe 차단
[앱체크 소식] Microsoft .NET 파일(MSBuild.exe)을 이용하는 TargetCompany 랜섬웨어(.bozon)
버전: 3.1.17.1