AppCheck 안티랜섬웨어 : 캅(CARB)엔진 동작 확인 방법

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

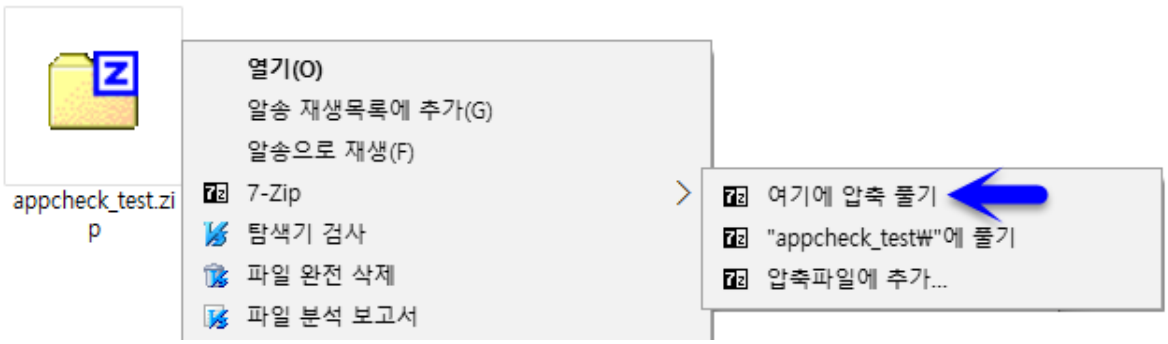
해당 테스트 방법은 시스템에 아무런 위협을 주지 않으므로 안심하시기 바랍니다.

<사전 준비물>

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

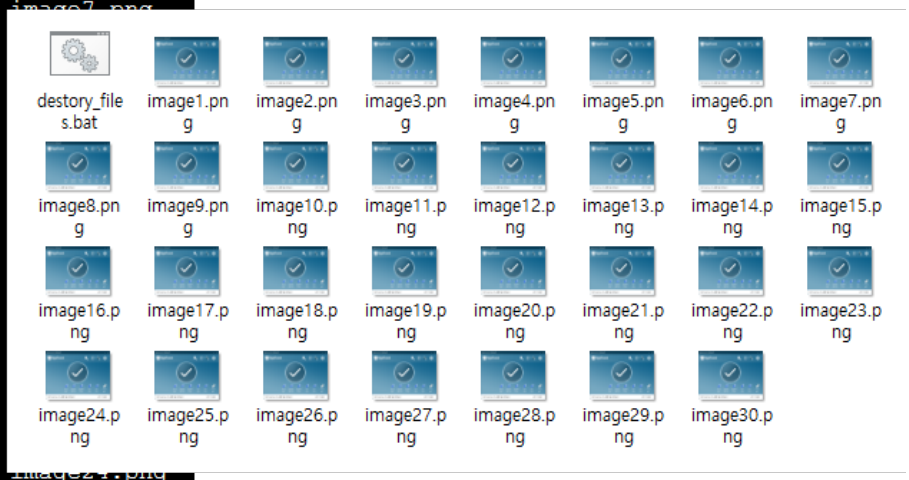
1. AppCheck 안티랜섬웨어 설치 파일을 다운로드하여 설치를 진행하시기 바랍니다.

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



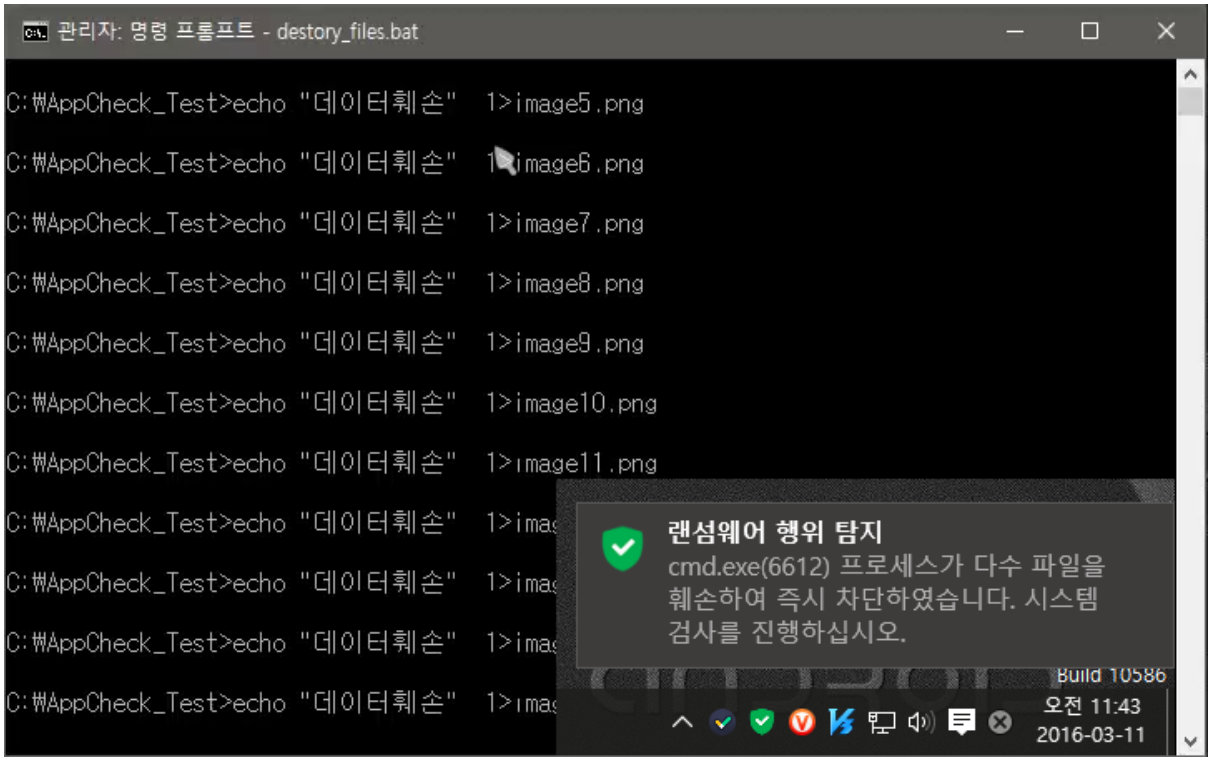
3. 압축 해제된 폴더에는 30장의 PNG 그림 파일과 destory_files.bat 파일이 존재하며, destory_files.bat 파일은 echo의 redirect 명령을 통해 PNG 그림 파일을 훼손할 목적으로 제작되었습니다.

```
echo "데이터훼손" > image1.png
echo "데이터훼손" > image2.png
echo "데이터훼손" > image3.png
echo "데이터훼손" > image4.png
echo "데이터훼손" > image5.png
echo "데이터훼손" > image6.png
echo "데이터훼손" > image7.png
echo "데이터훼손" > image8.png
echo "데이터훼손" > image9.png
echo "데이터훼손" > image10.png
echo "데이터훼손" > image11.png
echo "데이터훼손" > image12.png
echo "데이터훼손" > image13.png
echo "데이터훼손" > image14.png
echo "데이터훼손" > image15.png
echo "데이터훼손" > image16.png
echo "데이터훼손" > image17.png
echo "데이터훼손" > image18.png
echo "데이터훼손" > image19.png
echo "데이터훼손" > image20.png
echo "데이터훼손" > image21.png
echo "데이터훼손" > image22.png
echo "데이터훼손" > image23.png
echo "데이터훼손" > image24.png
echo "데이터훼손" > image25.png
echo "데이터훼손" > image26.png
echo "데이터훼손" > image27.png
echo "데이터훼손" > image28.png
echo "데이터훼손" > image29.png
echo "데이터훼손" > image30.png
```



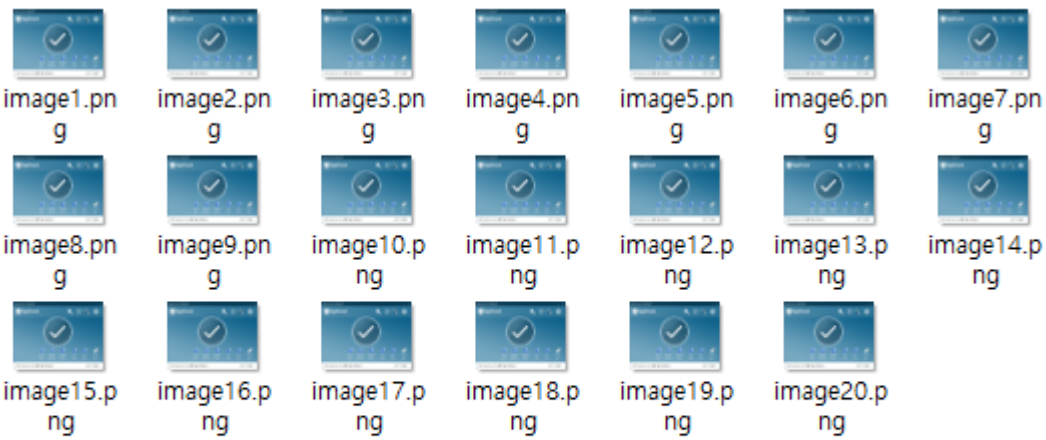
4. destory_files.bat 파일을 실행하시면 자동으로 30장의 PNG 그림 파일에 대한 데이터 훼손 행위가 진행되며, 이 과정에서 AppCheck 안티랜섬웨어는 **"랜섬웨어 행위 탐지"** 알림창을 생성하여 파일 훼손 행위를 차단합니다.

만약 **"랜섬웨어 사전 방어 사용(랜섬웨어 행위 차단)"** 옵션이 OFF인 경우에는 실시간 랜섬웨어 행위 탐지를 통한 차단이 이루어지지 않습니다.



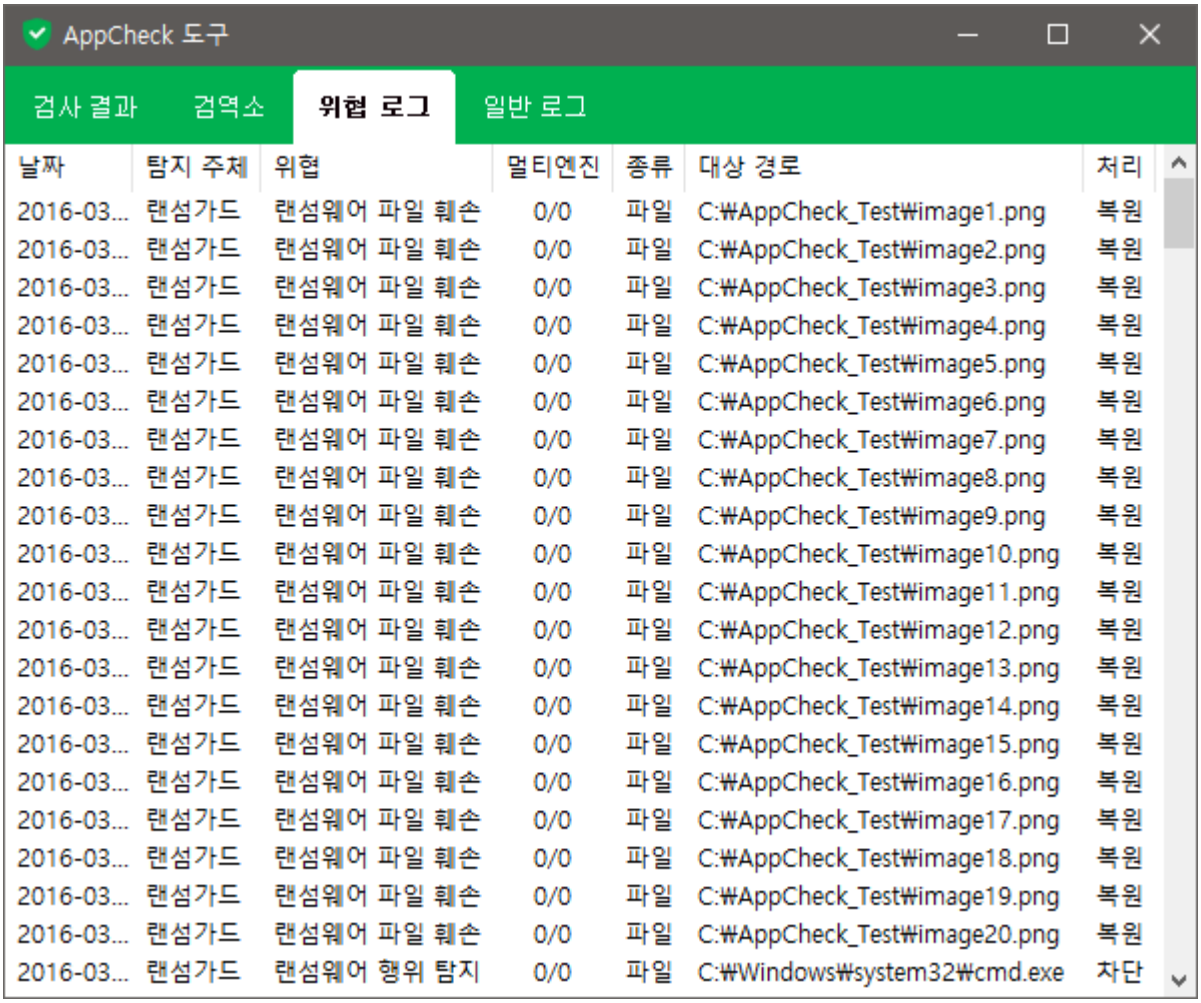
일부 훼손된 PNG 그림 파일의 원본 파일은 랜섬웨어 대피소 폴더<C:₩Backup(AppCheck)>에 백업되며, 일부 훼손된 파일은 랜섬웨어 대피소 폴더<C:₩Backup(AppCheck)>에 백업된 원본 파일을 이용해 자동 복원됩니다.

만약 **"랜섬웨어 대피소 사용"** 옵션이 OFF인 경우에는 랜섬웨어 행위 탐지를 통한 실시간 차단은 이루어지지만 훼손된 일부 파일은 자동 복구되지 않습니다.



랜섬웨어 대피소 폴더
<Backup(AppCheck)>

5. AppCheck 도구의 **"위협 도구"** 항목을 통해 랜섬웨어 행위 탐지를 통해 차단된 프로세스(파일) 및 일부 훼손된 파일이 자동 복원(랜섬웨어 행위 롤백)된 상세한 정보를 확인할 수 있습니다.



날짜	탐지 주체	위협	멀티엔진	종류	대상 경로	처리
2016-03...	랜섬가드	랜섬웨어 파일 훼손	0/0	파일	C:₩AppCheck_Test₩image1.png	복원
2016-03...	랜섬가드	랜섬웨어 파일 훼손	0/0	파일	C:₩AppCheck_Test₩image2.png	복원
2016-03...	랜섬가드	랜섬웨어 파일 훼손	0/0	파일	C:₩AppCheck_Test₩image3.png	복원
2016-03...	랜섬가드	랜섬웨어 파일 훼손	0/0	파일	C:₩AppCheck_Test₩image4.png	복원
2016-03...	랜섬가드	랜섬웨어 파일 훼손	0/0	파일	C:₩AppCheck_Test₩image5.png	복원
2016-03...	랜섬가드	랜섬웨어 파일 훼손	0/0	파일	C:₩AppCheck_Test₩image6.png	복원
2016-03...	랜섬가드	랜섬웨어 파일 훼손	0/0	파일	C:₩AppCheck_Test₩image7.png	복원
2016-03...	랜섬가드	랜섬웨어 파일 훼손	0/0	파일	C:₩AppCheck_Test₩image8.png	복원
2016-03...	랜섬가드	랜섬웨어 파일 훼손	0/0	파일	C:₩AppCheck_Test₩image9.png	복원
2016-03...	랜섬가드	랜섬웨어 파일 훼손	0/0	파일	C:₩AppCheck_Test₩image10.png	복원
2016-03...	랜섬가드	랜섬웨어 파일 훼손	0/0	파일	C:₩AppCheck_Test₩image11.png	복원
2016-03...	랜섬가드	랜섬웨어 파일 훼손	0/0	파일	C:₩AppCheck_Test₩image12.png	복원
2016-03...	랜섬가드	랜섬웨어 파일 훼손	0/0	파일	C:₩AppCheck_Test₩image13.png	복원
2016-03...	랜섬가드	랜섬웨어 파일 훼손	0/0	파일	C:₩AppCheck_Test₩image14.png	복원
2016-03...	랜섬가드	랜섬웨어 파일 훼손	0/0	파일	C:₩AppCheck_Test₩image15.png	복원
2016-03...	랜섬가드	랜섬웨어 파일 훼손	0/0	파일	C:₩AppCheck_Test₩image16.png	복원
2016-03...	랜섬가드	랜섬웨어 파일 훼손	0/0	파일	C:₩AppCheck_Test₩image17.png	복원
2016-03...	랜섬가드	랜섬웨어 파일 훼손	0/0	파일	C:₩AppCheck_Test₩image18.png	복원
2016-03...	랜섬가드	랜섬웨어 파일 훼손	0/0	파일	C:₩AppCheck_Test₩image19.png	복원
2016-03...	랜섬가드	랜섬웨어 파일 훼손	0/0	파일	C:₩AppCheck_Test₩image20.png	복원
2016-03...	랜섬가드	랜섬웨어 행위 탐지	0/0	파일	C:₩Windows₩system32₩cmd.exe	차단