

- 캅(CARB)엔진 동작 확인 방법 -



AppCheck 안티랜섬웨어의 캅(CARB)엔진을 통해 파일 훼손 행위 차단 여부를 사용자가 직접 확 인할 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) : <u>https://www.checkmal.com/download/appcheck_test.zip</u>
- 1. AppCheck 안티랜섬웨어 설치 파일을 다운로드하여 설치를 진행하시기 바랍니다.
- 2. 테스트 파일(appcheck_test.zip)을 임의의 폴더에 다운로드 후 압축 해제하시기 바랍니다.

appcheck_test.zi p	X 0 0 0 0	
	配 열기	Enter
	₩ 연결 프로그램	>
	🐻 압축 풀기	
	🛅 ZIP 파일로 압축	
	💷 경로로 복사	
	🖻 속성	Alt+Enter

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.

1 echo "데이터훼손" > image1.png 2 echo "데이터훼손" > image2.png	이름	날짜	유형	크기	1
3 echo "데이터훼손" > image3.png	destory_files.bat	2016-02-18 오후 3:22	Windows 배치 표	1KB	
4 echo "데이터훼손" > image4.png	image1.png	2016-02-18 오후 3:26	PNG 파일	298KB	
5 echo "데이터훼손" > image5.png	image2.png	2016-02-18 오후 3:26	PNG 파일	298KB	
6 echo "데이터웨손" > 1mage6.png	image3.png	2016-02-18 오후 3:26	PNG 파일	298KB	
8 echo "데이터훼손" > image7.prig	image4.png	2016-02-18 오후 3:26	PNG 파일	298KB	
9 echo "데이터훼손" > image9.png	image5.png	2016-02-18 오후 3:26	PNG 파일	298KB	
10 echo "데이터훼손" > image10.png	image6.png	2016-02-18 오후 3:26	PNG 파일	298KB	
11 echo "데이터훼손" > image11.png	image7 ppg	2016-02-18 오호 3-26	PNG파악	298KB	
12 echo "데이터훼손" > image12.png	image8 png	2016-02-18 오프 3:26	PNG 파일	298KB	
14 echo "데이터웨는 기mage15.phg		2016-02-18 9 = 3.26	DNIG THE	208KB	
15 echo "데이터훼손" > image15.png	image10 ppg	2016-02-18 9 = 2.26	DNG TRO	20888	
16 echo "데이터훼손" > image16.png	Thingero.prig	2010-02-10	FRO HE	23010	
17 echo "데이터훼 손 " > image17.png	사진 - image1.png	✓ 전체	화면 -	- 🗆 X	
18 echo "데이터훼손" > image18.png	AppCheck Pro	영종 버진		_ X	
19 echo 데이터웨쓴 > image19.png			-		
21 echo "데이터훼☆" > image20.phg	🕑 Api	Check	🔍 🗆 🐴	· 🗢	
22 echo "데이터훼손" > image22.png					
23 echo "데이터훼손" > image23.png					
24 echo "데이터훼손" > image24.png					
25 echo "데이터훼 손 " > image25.png					
26 echo "데이터훼 솓 " > image26.png					
27 echo "데이터훼손" > image27.png					
28 echo "데이터훼손" > image28.png					
29 echo "데이터훼손" > image29.png		-		100	
30 echo "데이터훼손" > image30.png		0 0 1	\mathcal{O}	1	
		44.0 Base Ba		U.S.E.	
		RE 38995 No	14 42 98	18 <u>11</u>	
	[密지] AppCt	eck Pro 제품이 출시되었습니다.	ы	2: 1,5,0,1	

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

AppCheck 알림 (1)				
전 랜섬웨어 행위가 탐지되어 차단하였습니다.				
프로그램 이름 : cmd.exe (자세히) 프로그램 설명 : Windows 명령 처리기 프로그램 게시자 : Microsoft Corporation				
<u>신뢰 파일 등록</u> <u>파일 격리하기</u>	확인			

파일 훼손 행위가 발생하는 파일(.png 그림 파일)의 복사본은 실시간으로 랜섬웨어 대피소 폴더 (기본값 : C:\ProgramData\CheckMAL\AppCheck\RansomShelter)에 임시 백업되며, 랜섬웨어 행 위 탐지를 통해 차단이 이루어질 경우 랜섬웨어 대피소 폴더에 임시 백업된 파일을 이용하여 자 동 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.

S Ap	opCheckPro					_	
Ø	일반 로그	위협 로그				검색	
ÿ⊟	위협 로그	기간 설정 파일 위치 일	볼기				
	검역소	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
រលូវ		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_	TestWimage3.png	복원
\bigcirc		2022-04 랜섬 가드	랜섬웨어 파일 생성	파일	D:#CheckMAL#appcheck_test#AppCheck_	_TestWimage4.png	복원
\bigcirc		2022-04 랜섬 가드	랜섬웨어 파일 생성	파일	D:#CheckMAL#appcheck_test#AppCheck_	_TestWimage5.png	복원
		2022-04 랜섬 가드	랜섬웨어 파일 생성	파일	D:#CheckMAL#appcheck_test#AppCheck_	TestWimage6.png	복원
		2022-04 랜섬 가드	랜섬웨어 파일 생성	파일	D:#CheckMAL#appcheck_test#AppCheck_	_TestWimage7.png	복원
		2022-04 랜섬 가드	랜섬웨어 파일 생성	파일	D:#CheckMAL#appcheck_test#AppCheck_	_TestWimage8.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	1 소식] Microsoft .NET 파일(N	ISBuild.exe)을 이용하는 T	argetCompany 랜섬	웨어(.b	ozon)	田;	천: 3.1.17.1