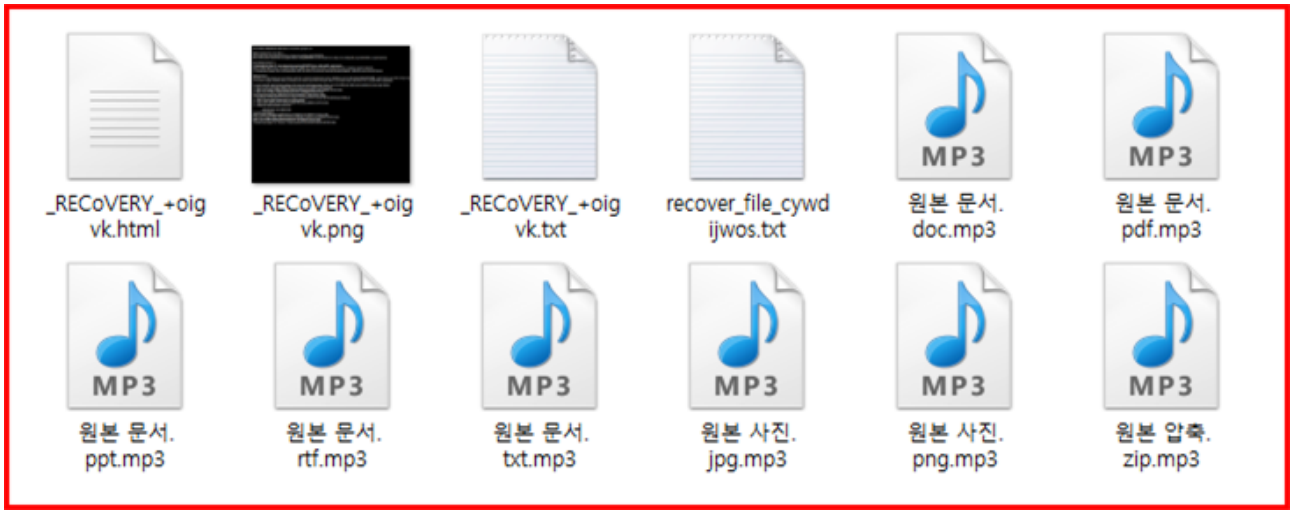
AppCheck Pro 제품 소개서

CHECKMAL

■ 기업 보안을 위협하는 랜섬웨어(Ransomware)

2015년 상반기 경부터 국내에서도 랜섬웨어(Ransomware) 유포가 활발하게 이루어지기 시작하였으며, 보편적인 유포 방식은 메일 첨부 파일 또는 SW 취약점을 악용하여 웹사이트 접속 시 자동 감염되고 있습니다.

특히 개인 인터넷 사용자를 넘어 병원, 교육 기관, 경찰서를 비롯한 관공서, 기업 내부, 웹사이트(웹 서버) 등 다양한 공격 대상으로 확대되어 가고 있는 추세이며, 알려진 국내외 피해 사례에서도 랜섬웨어 감염으로 인하여 익명의 범죄자들에게 상당액의 금전을 지불하였다는 소식을 접할 수 있습니다.



.mp3 확장명으로 암호화하는 TeslaCrypt 랜섬웨어 감염 모습

랜섬웨어 악성코드에 감염된 경우 문서, 사진, 도면, 인증서, 압축, 음악, 동영상, 소스 파일 등 다양한 파일에 대한 암호화를 통해 정해진 기간 안에 금전을 지불하도록 요구하며 심지어 유출된 정보를 공개하겠다는 허위 협박까지 이루어지고 있는 사이버 범죄 산업으로 발전하였습니다.

매일매일 새롭게 제작되는 랜섬웨어(Ransomware) 변종은 기존의 안티 바이러스, 방화벽, 침입 방지 시스템(IPS), 가상화 기반의 APT 대응 솔루션(Sandbox)도 탐지 우회할 수 있도록 제작되어 유포되므로 단 한 번의 감염으로도 공유 네트워크를 타고 빠른 시간 내에 다수의 PC를 감염시켜 상당한 피해를 유발할 수 있다는 점에서 그 어느 때보다도 랜섬웨어 전문 백신이 필요합니다.

■ 현재와 미래의 랜섬웨어에 대응하는 AppCheck Pro

AppCheck Pro 랜섬웨어 백신은 **"상황 인식 기반 랜섬웨어 행위 탐지(Context-awareness based ransomware behavior detection)"** 기술이 적용된 캅(CARB) 엔진으로 현재까지 발견된 패턴 뿐 아니라 차후 출현 가능한 랜섬웨어까지도 탐지하여 기존 백신의 탐지 및 대응 방식으로는 빠르게 대응할 수 없는 랜섬웨어 위협으로부터 가장 확실하고 안전하게 방어할 수 있습니다.

다양한 상황에서 탐지 여부	시그니처 기반	행위 기반	상황 인식 행위 기반
시그니처 우회 변종 파일	✗	○	○
미끼 파일 포함한 파일 암호화	✗	△	○
미끼 파일 우회한 파일 암호화	✗	✗	○
확장명 우회 후 암호화 (파일 변경 추적)	✗	✗	○
복호화 결제 안내 파일 삭제 (파일 생성 롤백)	✗	✗	○
탐지 전 암호화된 파일 복구 (파일 훼손 롤백)	✗	✗	○
비암호화 파일 훼손 인식	✗	✗	○
정상적인 파일 수정 행위 인식 (변화 분석)	✗	✗	○
생성/변경/덮어쓰기/삭제 상황별 연계 분석	✗	✗	○
프로세스별 행위 연계 추적	✗	✗	○

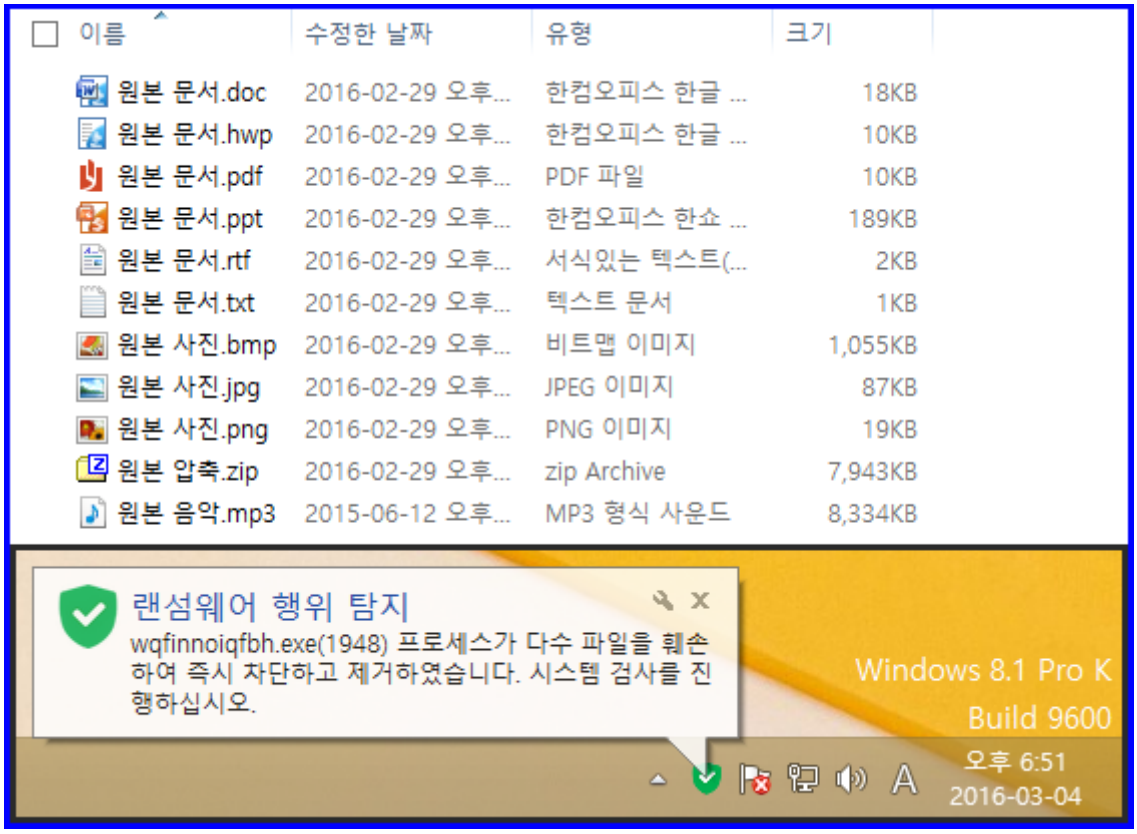
캅(CARB)엔진 탐지 방식

캅(CARB)엔진은 랜섬웨어 악성 파일이 시스템에 침투한 후 원본 파일이 변조되는 시점의 상황부터 단계별로 행위를 추적하여 파일 암호화를 수행하는 악성 파일 차단 및 치료(삭제) 뿐 아니라 파일 암호화로 일부 훼손된 원본 파일 백업 및 파일 복구, 생성된 협박 메시지 삭제, 변경된 파일명 복원과 같은 일련의 절차를 자동화하여 피해 복구에 소요되는 시간을 최소화합니다.

특히 방어에 실패하는 최악의 상황까지 대비하여 파일 암호화(훼손) 행위 시 원본 파일은 안전한 랜섬웨어 대피소 백업 폴더에 보호하여 고객의 데이터를 끝까지 책임집니다.

■ AppCheck Pro 랜섬웨어 백신 : 랜섬가드 기능

AppCheck Pro 랜섬웨어 백신에서 제공하는 랜섬가드 기능은 ① 랜섬웨어 사전 방어 및 자동 치료 ② 랜섬웨어 대피소 ③ 파괴 행위 탐지 ④ 보호 대상 파일 추가 ⑤ 랜섬웨어 대피소 백업 폴더<Backup(AppCheck)> 용량 관리 ⑥ 랜섬웨어 대피소 백업 폴더 보호 기능이 포함되어 있습니다.

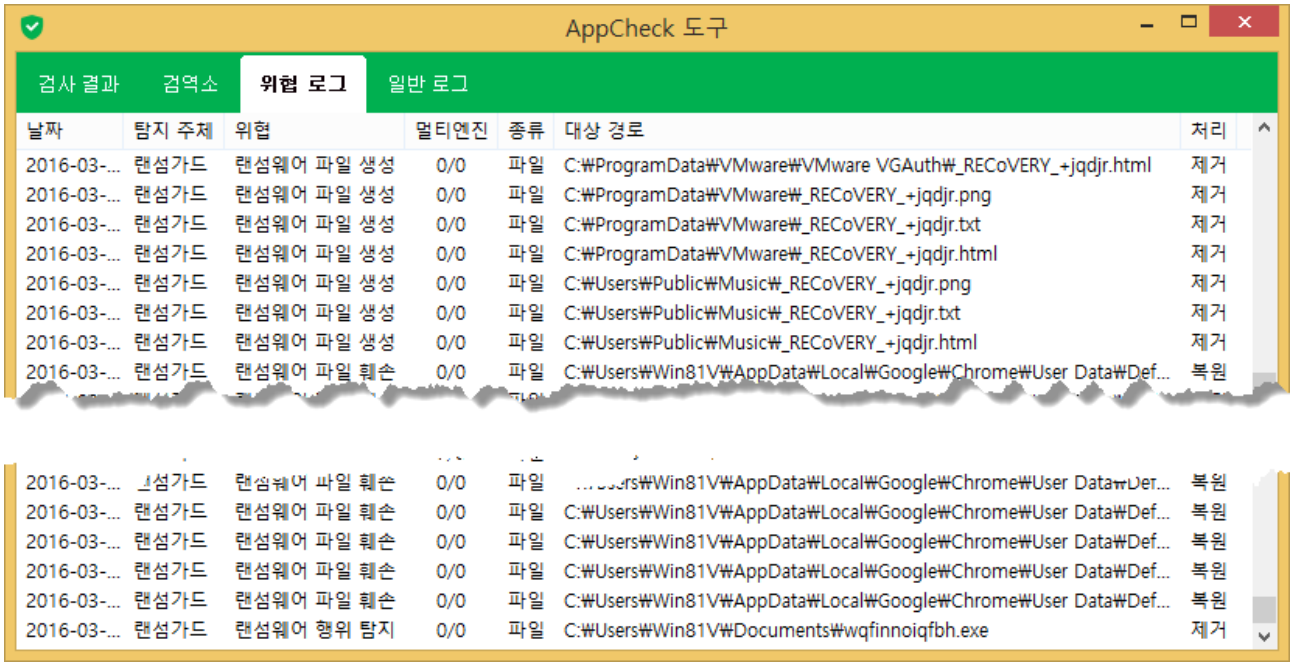


랜섬웨어 사전 방어 및 자동 치료로 원본 파일 보호

랜섬웨어(Ransomware) 감염으로 파일 암호화 행위가 발생한 후 **"랜섬웨어 행위 탐지"**를 통한 악성 프로세스 차단/제거, 랜섬웨어 대피소를 활용한 일부 훼손된 파일에 대한 자동 복원을 통해 고객이 지정한 보호 파일을 감염 이전 상태로 완벽하게 복구시켜 드립니다.

특히 국내외 랜섬웨어 대응 솔루션의 경우 랜섬웨어에 의한 파일 암호화 행위를 탐지하여 차단이 이루어지더라도 일부 훼손된 파일에 대한 복구 기능이 없어서 중요

데이터 일부를 잃어버릴 수 있다는 점에서 랜섬웨어 대피소 기능은 2중 안전장치를 제공합니다.



날짜	탐지 주체	위협	멀티엔진	종류	대상 경로	처리
2016-03-...	랜섬가드	랜섬웨어 파일 생성	0/0	파일	C:₩ProgramData₩VMware₩VMware VGAuth₩_RECoVERY_+jqdjr.html	제거
2016-03-...	랜섬가드	랜섬웨어 파일 생성	0/0	파일	C:₩ProgramData₩VMware₩_RECoVERY_+jqdjr.png	제거
2016-03-...	랜섬가드	랜섬웨어 파일 생성	0/0	파일	C:₩ProgramData₩VMware₩_RECoVERY_+jqdjr.txt	제거
2016-03-...	랜섬가드	랜섬웨어 파일 생성	0/0	파일	C:₩ProgramData₩VMware₩_RECoVERY_+jqdjr.html	제거
2016-03-...	랜섬가드	랜섬웨어 파일 생성	0/0	파일	C:₩Users₩Public₩Music₩_RECoVERY_+jqdjr.png	제거
2016-03-...	랜섬가드	랜섬웨어 파일 생성	0/0	파일	C:₩Users₩Public₩Music₩_RECoVERY_+jqdjr.txt	제거
2016-03-...	랜섬가드	랜섬웨어 파일 생성	0/0	파일	C:₩Users₩Public₩Music₩_RECoVERY_+jqdjr.html	제거
2016-03-...	랜섬가드	랜섬웨어 파일 훼손	0/0	파일	C:₩Users₩Win81V₩AppData₩Local₩Google₩Chrome₩User Data₩Def...	복원
2016-03-...	섬가드	랜섬웨어 파일 훼손	0/0	파일	rs₩Win81V₩AppData₩Local₩Google₩Chrome₩User Data	복원
2016-03-...	랜섬가드	랜섬웨어 파일 훼손	0/0	파일	C:₩Users₩Win81V₩AppData₩Local₩Google₩Chrome₩User Data₩Def...	복원
2016-03-...	랜섬가드	랜섬웨어 파일 훼손	0/0	파일	C:₩Users₩Win81V₩AppData₩Local₩Google₩Chrome₩User Data₩Def...	복원
2016-03-...	랜섬가드	랜섬웨어 파일 훼손	0/0	파일	C:₩Users₩Win81V₩AppData₩Local₩Google₩Chrome₩User Data₩Def...	복원
2016-03-...	랜섬가드	랜섬웨어 파일 훼손	0/0	파일	C:₩Users₩Win81V₩AppData₩Local₩Google₩Chrome₩User Data₩Def...	복원
2016-03-...	랜섬가드	랜섬웨어 행위 탐지	0/0	파일	C:₩Users₩Win81V₩Documents₩wqfinnoiqfbh.exe	제거

위협 로그에 기록된 랜섬가드 자동 치료 및 행위 롤백

또한 AppCheck 도구에서 제공하는 **“위협 로그”**에서는 랜섬웨어 행위 탐지를 통해 치료(제거)된 악성 파일 정보, 일부 훼손된 파일에 대한 자동 복원 정보, 랜섬웨어 악성 파일이 생성한 협박 메시지 자동 제거 등의 정보를 통해 피해 상황을 파악하는 데 도움을 받을 수 있습니다.

■ AppCheck Pro 랜섬웨어 백신 : 자동 백업 기능

AppCheck Pro 랜섬웨어 백신은 랜섬웨어(Ransomware) 출현에 따라 백업(Backup)에 대한 중요성이 강조됨에 따라 추가적인 백업 솔루션 도입 없이 제품에 통합된 자동 백업 기능으로 자동 백업 폴더<AutoBackup(AppCheck)>에 고객이 지정한 데이터를 지속적이고 안전하게 백업하도록 지원합니다.

자동 백업 기능은 ① 주기적인 자동 백업 수행 ② 백업할 폴더 지정 ③ 제외 폴더 지정 ④ 백업 시 제외 파일 확장명 지정 ⑤ 백업 폴더 위치 지정 ⑥ 자동 백업 폴더 보호 ⑦ 파일 히스토리(File History) 방식의 백업 기능이 포함되어 있습니다.

파일 히스토리(File History)를 지원하는 자동 백업

파일 히스토리(File History) 방식의 누적 백업은 기존 원본 파일과 비교하여 변경된 부분이 확인될 경우 .history 파일 확장명으로 이전 원본 파일을 지속적으로 백업하는 방식입니다.

자동 백업 기능 역시 랜섬가드 기능을 통한 랜섬웨어(Ransomware) 감염을 차단할 수 없는 최악의 상황에서도 자동 백업 폴더<AutoBackup(AppCheck)>에 저장된 데이터는 파일 암호화 행위로부터 안전하게 보호받을 수 있습니다.

■ AppCheck Pro 랜섬웨어 백신 : 멀티 엔진 기능

AppCheck Pro 랜섬웨어 백신은 멀웨어즈닷컴(malwares.com) 또는 메타스캔 온라인(Metascan Online) 서비스에서 제공하는 50여종의 국내외 백신 엔진을 기반으로 실행되는 파일 및 실행 중인 프로세스에 대한 실시간 검사와 시스템 검사를 통해 악성 파일 실행을 차단/삭제할 수 있습니다.

멀티 엔진 기능은 ① 실행 중인 프로세스에 대한 시스템 검사 ② 실행되는 파일에 대한 검사 ③ 기존 검사 결과가 없는 파일인 경우 자동 전송 검사 ④ 기존 검사 결과가 없는 파일에 대한 실행 차단(기본값 체크 해제) ⑤ 3단계 진단 수준 설정 ⑥ 업체명, 진단명 기준의 진단 제외 설정 기능이 포함되어 있습니다.

멀티 엔진의 특성상 정상 파일에 대한 오탐(오진) 발생 가능성을 고려하여 사용자가 설정한 진단 수준(높음<3개 이상 엔진 진단 시 차단/삭제>, 약간 높음<8개 이상 엔진 진단 시 차단/삭제>, 보통<15개 이상 엔진 진단 시 차단/삭제>)에 따라 악성 파일 실행을 차단할 수 있습니다.

■ AppCheck Pro 랜섬웨어 백신 : 도입 효과

AppCheck Pro 랜섬웨어 백신은 파일 암호화 기술을 악용한 랜섬웨어 (Ransomware) 보안 위협으로부터 고객의 디지털 자산을 3중(랜섬가드, 자동 백업, 멀티 엔진) 안전장치로 보호할 수 있는 최상의 랜섬웨어 대응 솔루션을 제시하며 이를 통해 다음과 같은 도입 효과를 누릴 수 있습니다.

1. 현존 백신 솔루션의 끊임없는 시그니처 업데이트 방식이 아닌 상황 인식 기반 랜섬웨어 행위 탐지를 통해 지속적으로 변화하는 랜섬웨어 보안 위협으로부터 능동적인 대응이 가능합니다.

2. 제품 설치 파일(2MB), 설치 후 생성 파일(3.4MB), 10MB 수준의 메모리 점유률로 동작하는 AppCheck Pro 랜섬웨어 백신은 기업 내 대규모 배포 · 설치 · 적용에 부담이 없습니다.

3. 기존에 사용하는 안티 바이러스, 방화벽, APT 보안 솔루션 등과 충돌 없이 상호 보완적으로 운영이 가능합니다.

4. 기본 로컬 드라이브 뿐 아니라 외장 하드, USB, 공유 네트워크 폴더까지 랜섬가드로 보호하여 공용 네트워크 환경에서도 안전하게 보호해줍니다.

5. 시스템 리소스에 부담을 주지 않는 조건에서 진행되는 자동 백업 기능으로 저사양 하드웨어 환경에서도 안정적으로 운영이 가능합니다.

6. AppCheck Pro 랜섬웨어 백신에서 제공하는 “멀티 엔진 - 랜섬가드 - 자동 백업”으로 통합된 보호 기능은 어떠한 랜섬웨어 보안 위협으로부터 고객이 원하는 데이터를 안전하게 보호해 줍니다.

7. 랜섬웨어 행위 탐지를 통해 차단된 악성 파일 및 관련 생성 파일, 훼손된 파일에 대한 원본 파일 복원 일체를 자동 처리하여 피해 복구를 위한 업무 중단을 최소화합니다.

CHECKMAL

■ AppCheck Pro 랜섬웨어 백신 : 사용 환경

구분	최소 사양	권장 사양
운영체제	Microsoft Windows 7 SP1 / 8 / 8.1 / 10 (32/64bit)	
CPU	Intel Core 1.6 GHz 이상	Intel Core I 2.66 GHz 이상
메모리(Memory)	1GB 이상	2GB 이상
디스크 여유 공간	2GB 이상	10GB 이상
웹 브라우저	Internet Explorer 8	Internet Explorer 11 / Chrome / Firefox

체크멀(CheckMAL) 경기도 수원시 영통구 센트럴타운로 85 메트로큐브 201동 1004호
www.checkmal.com T 031.212.0766 / F 031.212.0766 / M b2b@checkmal.com