www.avastkorea.com

Avast 랜섬웨어 예방 가이드

2015년부터 국내에서 간간히 출현하던 랜섬웨어는 올해 수 십 억에 이르는 피해를 가져올 정도로 대중화되고 있다. 게다가, 공격자들은 이메일 뿐만 아니라 웹사이트를 통해서도 공격을 시도하는 등 기법도 날로 교묘해지고 있다.

랜섬웨어는 기존의 악성코드와는 전혀 다른 전략을 쓰고 있다. 먼저, 기존의 악성코드들은 스팸을 발송하거나 컴퓨터를 잘 쓰지 못하게 방해하는 형태였다면, 랜섬웨어는 감염자 PC에 저장된 문서, 사진, 음악과 같이, 개인의 고유한 정보를 사용하지 못하게 하고, 특히, 돈을 달라고 하는 아주 나쁜 형태로 진화해 오고 있다. 또, 기존에는 대량 감염이 대세였다면, 랜섬웨어는 대량으로 뿌리는 것은 유사하지만, 감염자가 적더라도 충분한 이득을 가져올 정도로 간이 배 밖에 나온 도둑놈이라고 볼 수 있다. 따라서, 악성코드도 기존에는 유명한 몇 개 보안 제품에서 탐지가 되지 않는다면, 그냥 배포하는 형태를 띠었지만 랜섬웨어는 거의 따끈따끈한 새로운 악성코드를 배포하는 형태를 보이고 있다.

다시 말하면, 새로운 악성코드를 이용하여 공격하기 때문에 안티바이러스 고유의 기능만을 보안 제품으로는 일부 한계가 있는 것이 사실이다 이러한 한계를 넘어서기 위해 국내외 보안 회사들은 행동기반의 엔진을 보유한 형태의 제품, 특정 폴더를 감시하여 감염되었을 때 개인의 파일이 변조되는 피해를 차단하는 형태의 방식, 일부 유틸리티에서는 백업 및 복원 기능을 강화한 형태 등 랜섬웨어 대응 솔루션도 다양화되고 있는 상황이다.

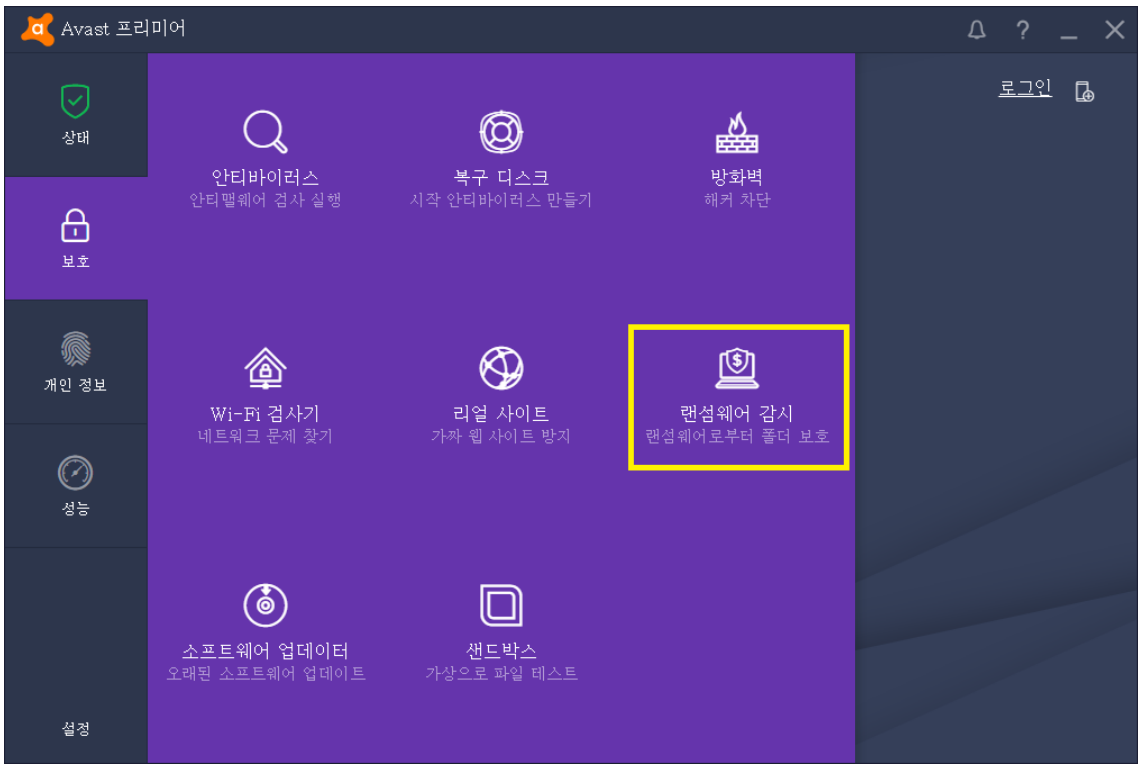
어베스트에서는 랜섬웨어에 대응하기 위해 기존의 파일 방어, 메일 방어, 웹 방어와 함께 랜섬웨어를 예방할 수 있는 기능인 **랜섬웨어 감시** 모듈을 탑재하고 있다. 참고로, **어베스트 인터넷 시큐리티**와 **프리미어** 제품(이하 특별히 언급하지 않는 경우 2 제품을 통칭하여 **어베스트**라고 부른다)에서 제공하고 있으며, 무료 제품인 프리 안티바이러스와 프로 안티바이러스 제품에서는 지원하지 않는다. 어베스트 제품별 주요 기능은 다음 표를 참고하기 바란다.

www.avastkorea.com

개인용 라이선스 제품 기능별 비교

	Avast 프리미어 [명품]	Avast 인터넷시큐리티 [고급]	Avast 프리 [필수]
바이러스 및 악성코드 차단 바이러스 랜섬웨어, 기타 위협을 실시간으로 차단	●	●	●
WIFI 보안 취약점 검사 WiFi 네트워크에 존재할 수도 있는 보안 취약점 및 공격자 적발	●	●	●
안전한 비밀번호 관리 웹사이트에 로그온할 때 이용하는 비밀번호를 안전하고 저장하고, 원클릭만으로 손쉽게 이용 가능	●	●	●
가짜 쇼핑몰 사이트 차단 고객의 비밀번호 또는 금융정보를 훔쳐갈 수 있는 사이버 금융 범죄 예방	●	●	
샌드박스 위험할 가능성이 있는 프로그램을 안전한 공간에서 실행함으로써 PC에 미치는 피해 예방	●	●	
고급 방화벽 해커가 직접 공격하거나, 네트워크를 통해 침입하는 공격을 차단	●	●	
안티 스팸 스팸 및 피싱 메일 차단	●	●	
랜섬웨어 예방 PC에 저장되어 있는 사진, 파일 등에 대한 자물쇠 기능을 제공하여 랜섬웨어가 무단 변경할 수 없도록 차단	●	●	
기밀 데이터 삭제 제3자가 복구할 수 없도록 PC에 저장된 파일을 안전하게 영구 삭제	●		
소프트웨어 자동 업데이트 취약점이 자주 발견되는 위험한 앱을 최신 버전으로 업데이트함으로써 보안 위험 감소	●		

랜섬웨어 감시 모듈은 어베스트를 설치할 때 기본 옵션을 선택되어 있다. 만약, 아래 화면과 같이 어베스트의 방어 모듈 가운데 **랜섬웨어 감시**가 보이지 않는 경우에는 제어판 -> 프로그램 제거 -> 어베스트 제품 선택 -> 변경 버튼을 클릭하여, **랜섬웨어 감시** 모듈을 설치한다.



이제 **랜섬웨어 감시** 모듈에 대해 좀더 자세히 소개한다.

어베스트가 제공하는 **랜섬웨어 감시** 모듈은 사용자가 지정한 폴더(및 파일)에 대해서 랜섬웨어 같은 악성코드가 제멋대로 파일을 액세스하는 것을 차단한다. 좀더 자세한 설정을 지원하기 위해 해당 폴더에 접근할 수 있는 앱(프로그램)과 접근할 수 없도록 차단하는 앱도 지정할 수 있다. 또한, 동영상이나 설치 파일과 같이 파일이 변조되더라도 사용자가 쉽게 복구하거나 구할 수 있는 파일은 랜섬웨어 감시 모듈이 보호하지 않고, 한글, 사진, 오피스 파일과 같이 개인에게 중요한 파일들만 선별하여 보호하는 확장자 관리 기능을 제공한다.

아래 화면과 같이, "랜섬웨어 감시" 모듈은 전체적으로 5가지의 항목과 옵션을 가지고 있으며, 복잡해 보이지만, 지원하는 기능에 대해서 이해만 한다면, 3분 내에 랜섬웨어를 만족스러울 정도로 차단할 수 있는 자신의 모습에 놀랄지도 모른다.

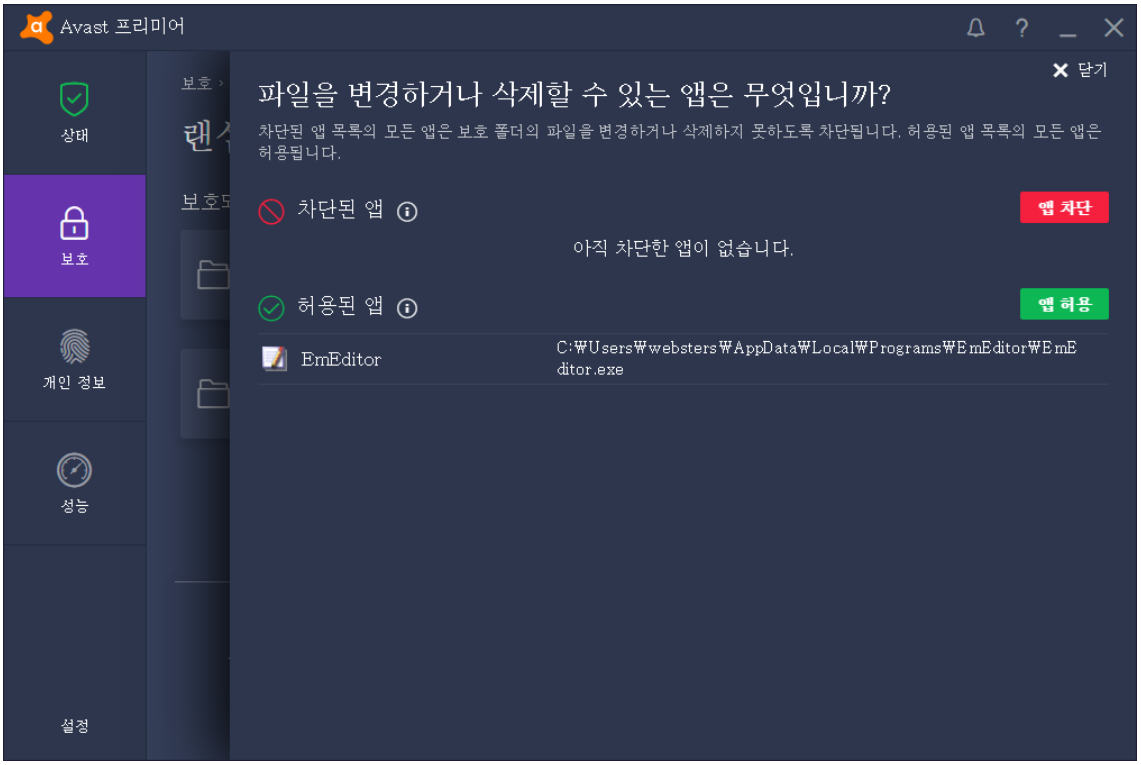
1. **켜기 / 끄기** : 랜섬웨어 감시 모듈의 기능을 켜거나 끈다. 당연히 초록색 바탕으로 표시된 **켜기**를 선택한다. 만약, PC를 사용하는 중에 어떤 이유로 인해서 자꾸 랜섬웨어 감시 모듈을 끄고 켜고 하는 창을 보게 될 경우에는, 무언가 랜섬웨어 감시 모듈의 설정을 제대로 잡아 주지 않았다고 볼 수 있으며, 그런 경우에는 다시 한번 본 설명서를 읽어보고, 적절한 설정 값을 정한다.

2. **보호되고 있는 폴더, 폴더 추가** : 어베스트가 설치될 때에는 자동으로 사용자가 문서와 같은 파일을 저장하는 경로를 찾아 자동으로 보호되고 있는 폴더에 추가한다. 보통, ₩USERS₩사용자ID 폴더 아래에 있는 문서(Documents)와 사진(Pictures) 폴더가 추가되면, 컴퓨터를 여러 명이 사용하는 경우에는 각 사용자ID(프로파일)별로도 추가한다. 따라서, 사용자가 어베스트를 잘 설정해 놓는다면, 이 컴퓨터를 쓰는 다른 사용자도 랜섬웨어의 피해를 예방하는데 도움이 된다. 사용자가 다른 드라이브에 사진이나 노래(MP3) 파일들

을 저장해 놓는다면, 그 폴더를 "폴더 추가" 버튼을 클릭하여 추가한다.

다만, 랜섬웨어 감시 모듈은 개인이 사용하는 환경을 기준으로 하기 때문에, 네트워크 공유 드라이브(및 폴더)와 이동형 매체(예. USB 메모리스틱)는 지원하지 않는다. 또한, C:₩Windows와 같이 윈도우 운영체제가 이용하는 폴더도 선택할 수 없도록 제한되어 있다. 다시 말하면, 개인이 보관하고 있는 폴더만을 보호한다.

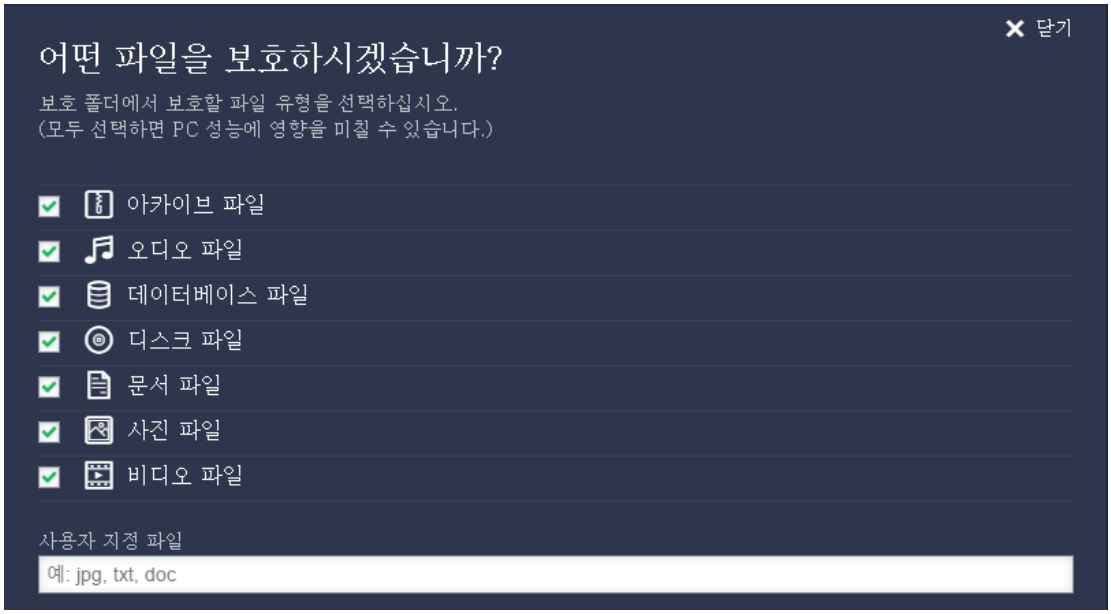
3. **차단된 / 허용된 앱** : 사용자가 보호하고자 하는 폴더에는 수많은 프로그램들이 읽고 쓸 수 밖에 없다. 예를 들어, .HWP 확장자를 가진 문서 파일은 한글 프로그램이나 뷰어로 이용한다. 한글 프로그램으로는 다른 폴더는 접근할 기회가 별로 없다. 이런 방식으로, 사용자가 문서 폴더에 저장하는 파일의 특성에 맞게 앱을 선택하여 지정하면 해당 앱 이외에는 차단되어 더욱 안전하다. 다만, 앱을 차단하거나 허용하는 정책은 폴더 단위가 아닌 전체적으로 적용되는 정책이다.



4. **보호되는 파일 유형 변경** : 랜섬웨어 감시 모듈은 특정한 확장자를 기준으로 보호 여부를 결정할 수 있으며, 사용자가 확장자를 추가할 수도 있다. 기본적으로 아카이브(7z, rar, zip), 오디오(m3u, m4a, mp3, wma, ogg, wav), 데이터베이스(sqlite, sqlite3), 디스크(iso, img, nrg, tc), 문서(doc, docx, odt, rtf, wpd, wps, csv, key, pdf, pps, ppt, pptm, pptx, ps, psd, vcf, xlr, xls,

5. xlsx, xlsm, ods, odp, indd, dwg, dxf, kml, kmz, gpx, cad, wmf), 사진(3fr, ari, arw, bay, bmp, cr2, crw, cxi, dcr, dng, eip, erf, fff, gif, iiq, j6i, k25, kdc, mef, mfw, mos, mrw, nef, nrw, orf, pef, png, raf, raw, rw2, rwl, rwz, sr2, srf, srw, x3f, jpg, jpeg, tga, tiff, tif, ai), 비디오(3g2, 3gf, asf, avi, flv, m4v, mkv, mov, mp3, mpg, rm, swf, vob, wmv)를 선택하여 보호할 수 있다.

   하지만, 한글(hwp)이나 알집(egg)과 같은 확장자가 기본적으로 설정되어 있지 않기 때문에 사용자 지정 파일 부분에 확장자를 추가해야 한다.



6. **스마트 모드, 엄격 모드**: 이 기능은 랜섬웨어 감시 모듈을 적용하는 정책을 지정한다. 스마트 모드는 기본적으로 선택된 모드이며, 대부분의 경우 이 모드만으로도 충분하다.

   A. **스마트 모드**: 어베스트는 컴퓨터 사용자의 사용 습성을 충분히 고려하여 보편적인 정책을 자동으로 제공한다. 먼저, 자주 이용하는 프로그램들은 어베스트가 인식하여 불필요하게 차단하는 문제가 발생하지 않게 미연에 방지한다. 게다가, 사용자가 (자주 쓰이지는 않는) 어떤 앱을 이용하여 폴더에 접근하고자 할 경우에는 그 사실을 알려 주고, 사용자가 선택하는 지능성 모드다.

   B. **엄격 모드**: 앱에서 폴더에 접근할 때마다 어베스트가 해당 사실을 알려 주고, 사용자가 지속적으로 선택하는 엄격한 정책이 적용되는 모드로, **차단된/허용한 앱** 이외의 모든 행동에 대해 사용자가 일일이 답을 줘야 하기 때문에 사용자가 귀찮아 할 수도 있고, 특히, 경고 창이 자주 나오다 보니 다른 경고 창과 헷갈려서 실수로 허용하는

등 문제의 발생 소지도 있을 수 있다. 따라서, 특정한 프로그램이나 확장자만을 쓰는, 특별한 상황인 경우를 제외하고는 이용하지 않는 것을 추천한다.

지금까지 소개한 내용을 통해 어베스트의 랜섬웨어 감시 기능을 100% 활용하여, 개인의 소중한 파일을 보호할 수 있다. 마지막으로, 랜섬웨어 감시 모듈을 사용하는데 나오는 질문과 답변을 소개한다.

1. 내 PC에 설치된 어베스트에는 랜섬웨어 감시 메뉴가 안보여요!

   답: 설치된 어베스트 제품이 어베스트 인터넷 시큐리티, 프리미어 인지 확인한다. 무료인 프리 안티바이러스, 유료 제품인 프로 안티바이러스에서는 지원되지 않는다. 해당 제품 구매를 원하시는 경우에는 아래 링크를 참고한다.

   ※ 어베스트 개인용 제품 구매 : http://shop.avastkorea.com/hlicense.asp

2. 어베스트 인터넷 시큐리티 또는 프리미어 버전인데도 랜섬웨어 감시 메뉴가 안보여요!

   답: 해당 모듈이 설치되지 않았다. 제어판 -> 프로그램 제거 -> 어베스트 제품 선택 -> 변경 에서 랜섬웨어 감시 모듈을 선택하여 추가로 설치한다.

3. 랜섬웨어 경고창이 너무 자주 뜹니다. 짜증나 죽겠어요!

   답: 엄격 모드로 설정되어 있다. 스마트 모드로 변경한다. 또는, 허용한 앱에 사용자가 자주 이용하는 앱을 등록하는 것도 좋은 방법이다.

4. 앱에서 저장 기능을 쓰려고 하니 오류가 납니다!

   답: 앱이 차단된 앱 목록에 포함되어 있는지 확인한다. 가급적이면, 사용하는 앱을 허용한 앱에 등록한다.