nuri Anti-Ransom Reference Manual

Nurilab Incorporated July, 2017

2017년 7월 초판 발행

홈페이지: **http://www.withuspc.com**

Contents

I. nuri Anti-Ransom 소개

1장. 주요 기능

새로운 형태의 랜섬웨어로 인한 피해가 지속적으로 발생하고 있고 기존 패턴기반의 컴퓨터 백신, 방화벽, 침입차단 솔루션 등을 우회하여 많은 감염 피해를 입고 있는 상황에서 메일이나 취약한 웹, 메신저등의 소프트웨어 취약점을 통해 유입되는 랜섬웨어에 대해 사전 차단을 강화 하고, 감염 시 랜섬웨어 동작을 인식하여 실시간 대응할 수 있는 형태의 솔루션이 필요합니다

인공지능(AI) Anti-Ransomware Enigne
클라우드 엔진을 통해 다양한 랜섬웨어 악성코드 파일에 대한 분석 및 진단. 치료, 차단할 수 있는 기능을 제공합니다.

행위기반 및 사전 방역
랜섬웨어 악성코드의 행위를 분석하여 랜섬웨어 동작을 인지함으로 유사한 행위에 대한 차단, 기 검진 및 차단된 랜섬웨어 악성코드는 행위 분석없이 차단합니다.

자동백업 및 복원
랜섬웨어의 감염 대상에 대하여 사전 백업, 관리하고 랜섬웨어 감염 시 이를 확인하여 복원 합니다.

MBR 보호
랜섬웨어를 포함한 악성코드가 MBR(Master Boot Record)를 변조하여 윈도우 시스템 부팅 시 문제를 일으키는 것을 보호합니다.

제품 보호
랜섬웨어 악성코드 공격으로부터 nuri Anti-Ransom의 구성 파일 삭제 및 프로세스 종료가 되지 않도록 보호합니다.

자동 업데이트
프로그램 변경 시 사용자의 수동 조작 없이 자동으로 업데이트 적용합니다.

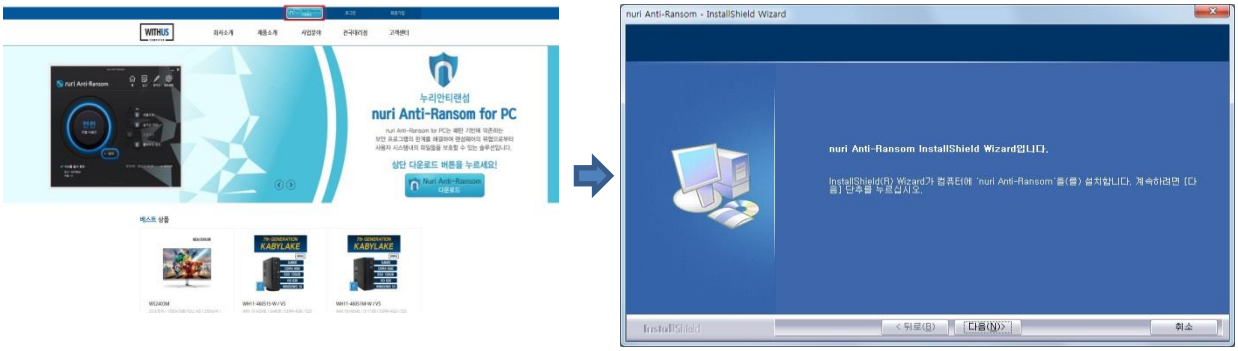
검역소
nuri Anti-Ransom로 치료 혹은 삭제된 파일을 검역소에 보관하여 복원합니다.

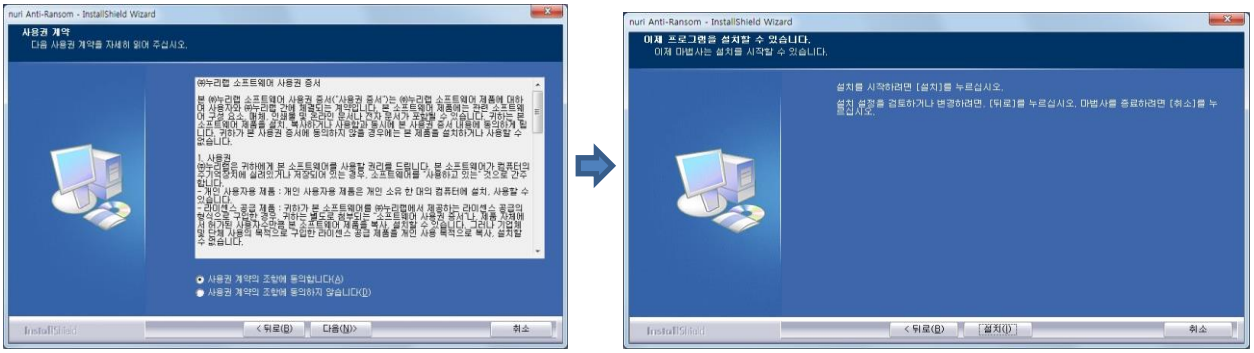
II. nuri Anti-Ransom 사용

1장. 설치/삭제/정품인증 하기

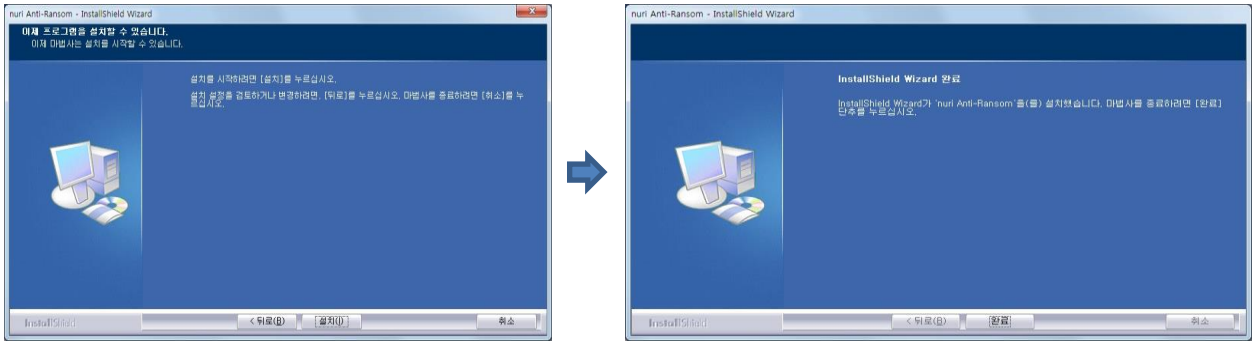
1.1. PC 다운로드 및 설치하기

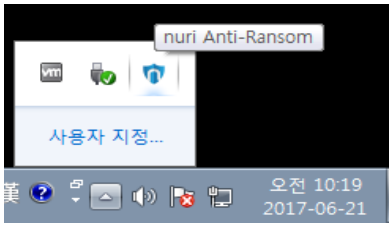
nuri Anti-Ransom의 설치 방법은 빠르고 간편합니다.
위더스컴퓨터 홈페이지에서 상단 nuri Anti-Ransom 설치파일을 다운로드하여 실행합니다.





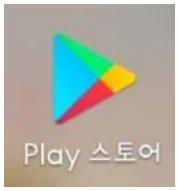
2) 동의하시고 설치 진행을 해주시면 됩니다.

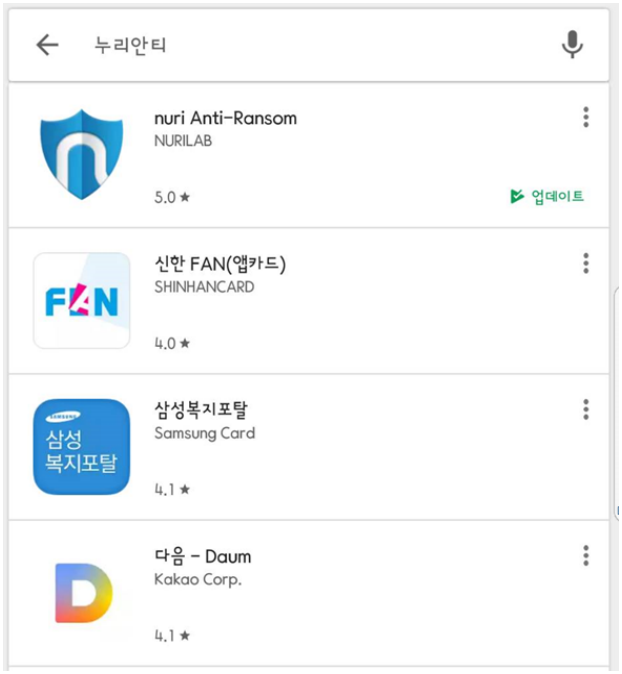




1.1-1 스마트폰 다운로드 및 설치하기

1) 구글 Play 스토어에서 '누리안티' 검색 후 다운로드 및 설치



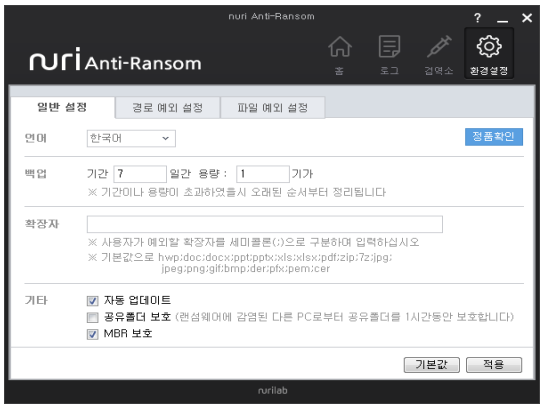


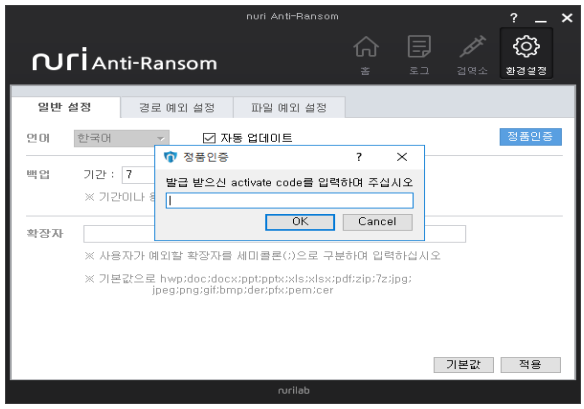
2) 아이콘 및 실행화면

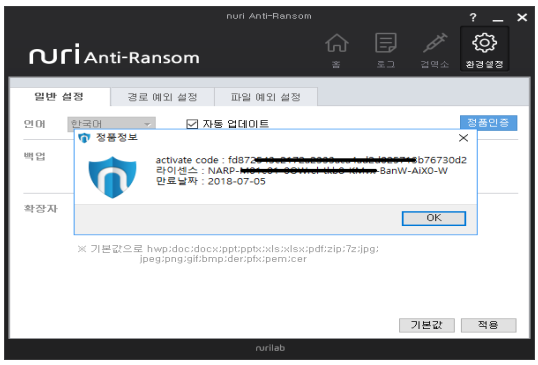
1.3. PC 정품인증 및 인증확인

유료 구매 고객의 경우 정식 제품으로 인증을 받아야 계약한 기간동안 사용이 가능합니다. 정품인증을 하지 않을 경우 30일 평가판 형태로 사용하게 되며 30일 이후에는 주요기능을 사용할 수 없게 됩니다.

1) 정품인증을 받기 위해서 nuri Anti-Ransom을 실행하고 "환경설정"에서 정품인증 버튼 을 클릭합니다.







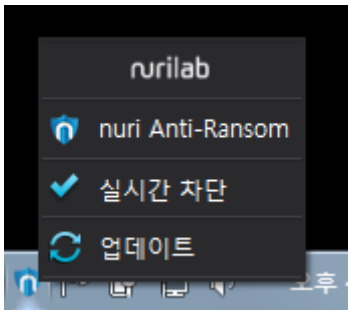
2) "**정품인증**" 버튼을 클릭하면 활성화 코드(activate code)를 입력할 수 있는 팝업 창이 나타납니다.

구매 시 발급 받은 활성화 코드(activate code)를 입력하고 "**OK**" 버튼을 클릭합니다.
정품인증 후 '정품인증' 버튼을 다시 클릭하면 정품 등록 정보를 확인할 수 있습니다.

2장. PC 실행하기

2.1. 실행화면

nuri Anti-Ransom의 Main UI는 다음과 같은 방법으로 실행할 수 있습니다. nuri Anti-Ransom 트레이아이콘에서 오른쪽 마우스를 클릭합니다.



여기에서 **'nuri Anti-Ransom'**을 클릭하여 Main UI를 실행합니다.

2.2. 화면구성

nuri Anti-Ransom의 화면 구성은 다음과 같습니다..

① 메뉴

홈 : 어떤 메뉴에서든 nuri Anti-Ransom 메인 UI로.

로그 : 사용 시 설정변경, 랜섬웨어 차단 및 격리, 수동검사 등의 실행 내역을 시간별로 보여줍니다.

검역소 : 랜섬웨어 차단 후 백업 및 격리된 파일의 목록을 보여줍니다.

환경설정 : 최적화된 사용을 위해 사용자 시스템의 환경에 맞게 설정

② 기능설정 상태

실시간 차단 : 랜섬웨어를 실시간 차단할지 여부를 설정할 수 있습니다.

제 품 보 호 : 프로그램을 외부의 공격으로부터 보호하는 기능

MBR 보호 : 사용자 시스템의 Master Boot Record 보호 기능의 적용 상태를 확인할 수 있습니다. 환경설정에서 사용하도록 'On'으로 설정한 상태일때는 'On'으로 파란, 'Off' 상태일 경우 빨간으로 보여집니다.

공유폴더 보호 : NAR이 설치된 시스템에 있는 공유폴더내의 파일을 보호합니다. 환경설정에서 사용하도록 'On'으로 설정한 상태일때는 파란, 'Off' 상태일 경우 빨간

③ NAR 상태

상태 : 프로그램 정상 동작중인지 여부를 확인 할 수 있습니다. 보통은 파란색 '√' 표시와 함께 '현재 정상 상태입니다'로 표시되며, NAR이 정상 동작 중임을 나타냅니다.NAR의 기능이 Off 상태이거나 프로세스가 정상 동작 하지 않을 경우 빨간색 '?' 표시와 함께 '랜섬웨어 방어에 위험한 상태입니다'로 표시됩니다.

최근 업데이트 : 마지막으로 업데이트 한 날짜가 표시됩니다.

최근 검사 : nuri Anti-Ransom으로 사용자 디스크의 랜섬웨어 감염 여부를 검사한 마지막 날짜가 표시 됩니다.

④ NAR 버전 정보

제품버전 : nuri Anti-Ransom의 UI 및 기능 버전 정보를 확인할 수 있습니다.

엔진버전 : 랜섬웨어를 탐지하고 치료하는 nuri Anti-Ransom 검사 엔진의 최신버전 정보를 확인할 수 있습니다.

업데이트 버튼 : 제품 및 검사 엔진을 최신 버전으로 유지할 수 있도록 사용자가 수동업데이트 실행버튼입니다.

⑤ 검사 버튼

사용자 디스크에 랜섬웨어가 존재하는지 여부를 검사할 수 있습니다.

"검사" 버튼을 클릭하면 수동 검사를 수행하고 수행하는 도중에 검사 버튼을 다시 클릭 하면 검사를 중지합니다.

3장. PC 사용하기

3.1. 실시간 차단 화면

nuri Anti-Ransom은 설치와 동시에 랜섬웨어를 실시간으로 차단하도록 기본 설정되어 있습니다.

실시간 차단이 설정되어 있는 상태는 메인 프레임을 실행하여 '실시간 검사'가 **'On'** 설정 되어 있거나 트레이아이콘이 파란색 아이콘일 경우 정상 설정되어 있음을 확인할 수 있습 니다.

랜섬웨어가 실행되면 시스템을 잠그거나 데이터를 암호화하여 사용할 수 없도록 합니다. 이러한 활동을 하는 도중에 문서파일의 확장자를 변경하고 Anti-Virus 나 Anti-Ransom 프로그램을 무력화 시키기도 합니다.

nuri Anti-Ransom은 기본적으로 랜섬웨어가 공격을 시작하면 랜섬웨어 동작으로 인해 암호화되어 변형되는 파일을 백업하고 랜섬웨어 행위를 인지한 시점에 해당 랜섬웨어 행위 을 차단, 삭제하고 암호화되어 변형된 파일을 원본으로 복원합니다.

3.2. 랜섬웨어 검사

nuri Anti-Ransom은 랜섬웨어의 행위를 실시간으로 차단할 수 있지만, 사용자가 직접 디스크에 있는 파일을 대상으로 랜섬웨어 감염 여부를 검사할 수 있습니다.

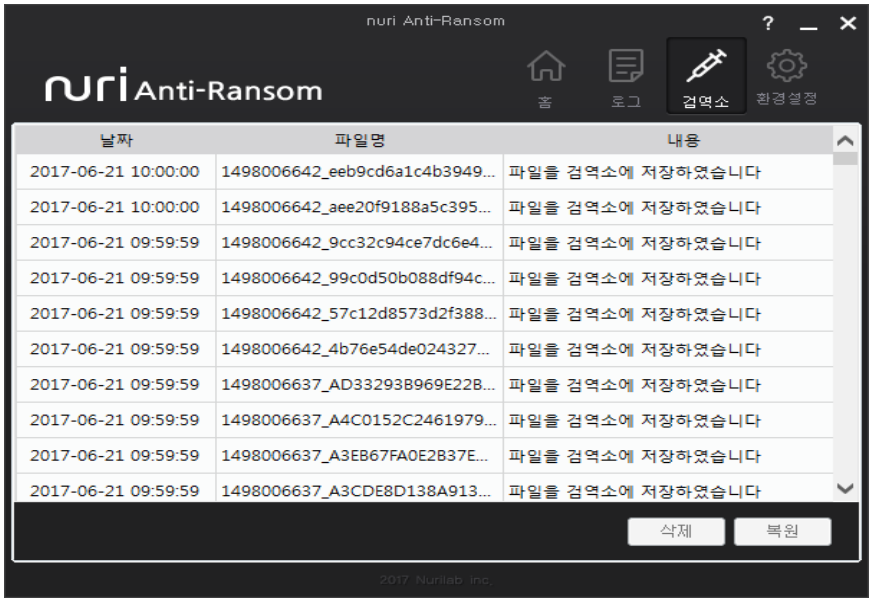
1) 사용자는 메인 UI에서 **'검사'** 버튼을 클릭합니다.

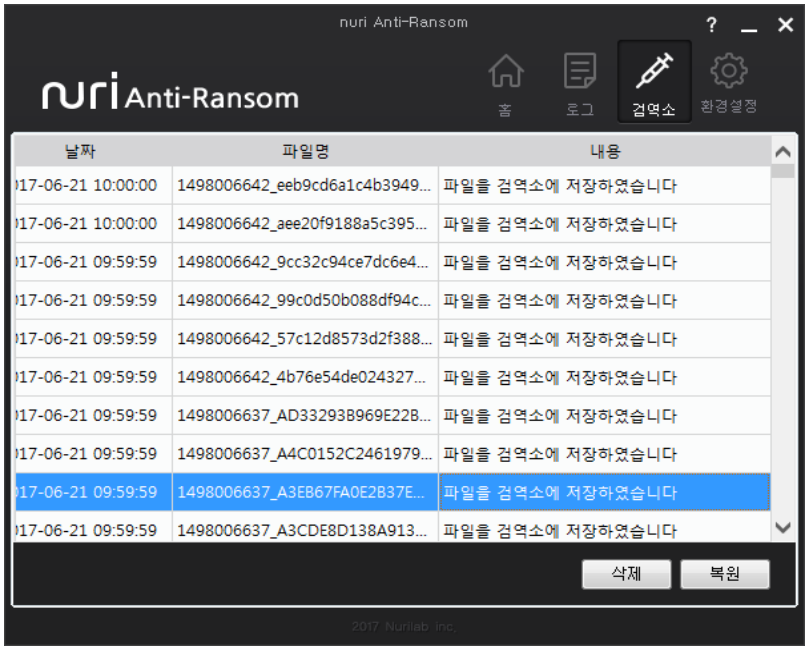
2) 검사가 진행되는 중간에는 검사 버튼이 초록색으로 변경되며 버튼 내부에서는 검사 시간이 카운트 됩니다. 아래의 NAR 상태창에서는 '검사 중입니다' 라는 메시지와 함께 검사한 파일의 갯수와 랜섬웨어로 진단된 파일의 갯수가 카운트 됩니다.
검사가 끝나면 진단된 랜섬웨어를 제거하고 시스템의 상태가 **'정상'**으로 변경됩니다.
최근 검사 날짜도 표시됩니다. 검사 결과는 로그에서 확인할 수 있습니다.

3.4. 검역소

nuri Anti-Ransom은 랜섬웨어 행위를 인지하면 차단, 치료하고 원본 파일은 검역소에 격리 합니다. 필요에 따라 격리된 원본 파일은 복원이 필요할 때 사용합니다.

1) **"검역소"** 버튼을 클릭합니다. // '복원' 혹은 '삭제' 하려는 파일을 선택합니다





3.5. PC 환경설정

nuri Anti-Ransom의 최적화된 사용을 위해 사용자 시스템의 환경에 맞게 설정을 변경합니다. ‘

환경설정’ 버튼을 클릭합니다.

3.5.1 일반 설정

nuri Anti-Ransom을 사용하기 위한 기본 설정을 확인할 수 있습니다.

언어 : nuri Anti-Ransom에서 사용할 언어를 선택할 수 있습니다.
(현재는 한국어만 지원되며 추후 다른 언어도 확장 지원 예정입니다.)

백업 : 랜섬웨어 또는 랜섬웨어로 의심되는 프로세스에 의해 문서의 변형이나 암호화 될때 자동 백업을 수행합니다.
백업된 파일은 nuri Anti-Ransom이 설치된 폴더 내에 백업되며 설정한 기간과 용량만큼 자동 백업됩니다. 설정된 기간과 용량이 초과되면 오래 저장된 순서부터 정리됩니다.

확장자 : 보호하는 기본 확장자 외에 추가 문서를 백업하고 복원 하려면 사용자가 원하는 확장자를 등록하여 보호할 수 있습니다. 확장자의 구분은 ‘;’ 으로 구분합니다.
예) txt, cad를 추가할 경우의 입력방법 : txt;cad

자동 업데이트 : 자동 업데이트를 체크하면 사용자 시스템 부팅 시 서비스가 재시작 될때 업데이트를 수행합니다.
자동 업데이트가 체크되어있지 않을 경우 사용자가 업데이트 버튼을 수동으로 클릭해야만 업데이트가 수행 됩니다.

공유 폴더보호 : 공유 폴더보호를 체크하면 nuri Anti-Ransom이 설치된 시스템에 설정된 공유 폴더를 보호합니다. 랜섬웨어로부터 위협을 차단한 이후 1시 간동안 네트워크를 차단하게 되며 다른 PC로부터 지속적인 공격이 오기 전에 추가 조치(네트워크 내 다른 PC 검사)를 취해야 합니다. 설정을 할 경우 NAR 메인창에 공유폴더 보호가 ‘On’으로 표시됩니다.

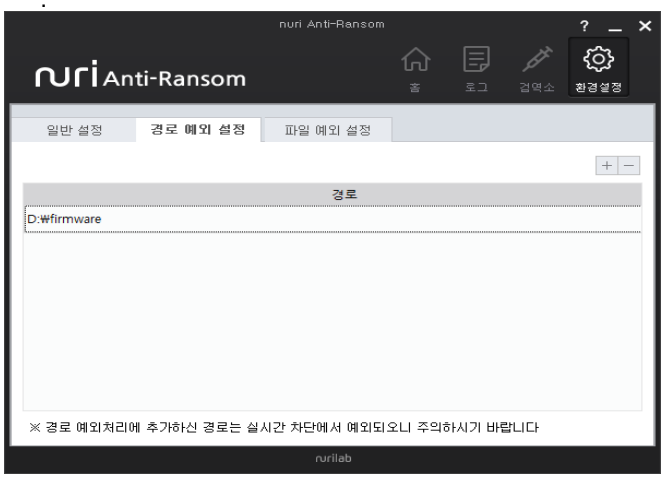
MBR 보호 : MBR 보호를 체크하면 사용자 시스템의 MBR(Master Boot Record)를 보호 합니다. 자동 업데이트가 체크 설정을 할 경우 NAR 메인창에 MBR 보호가 ‘On’으로 표시됩니다.

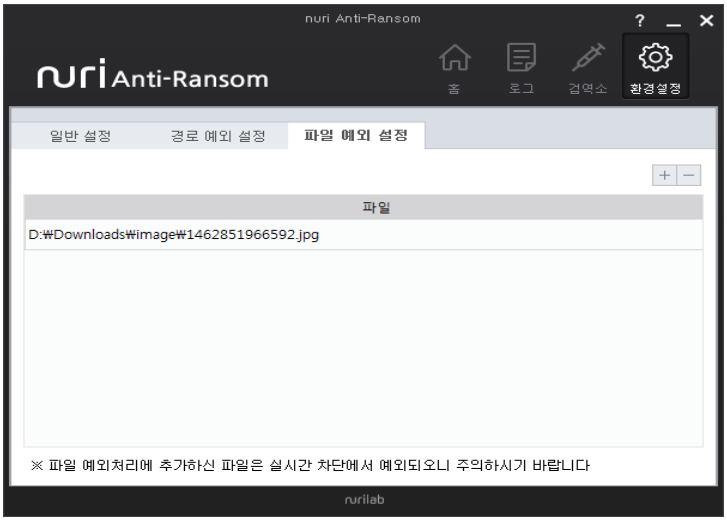
기본값 : 기본값 버튼을 클릭할 경우 모든 설정이 초기화 됩니다.

3.5.2 경로 예외 설정

nuri Anti-Ransom에 의해 랜섬웨어의 의심 행위를 차단하지 않도록 특정 폴더를 설정할 경우 해당 폴더내에 존재하는 파일은 의심되는 행위가 발생하여도 차단하지 않습니다. (보통 사용자가 다른 프로그램에 영향을 받지 않고 무조건 실행해야 하는 프로그램을 위해 해당 경로를 등록합니다.)

1) '+' 을 클릭한 후에 제외하고 싶은 경로를 선택하고 '폴더선택' 버튼을 클릭하여 등록 합니다
.





2) 이미 등록되어 있는 경로를 삭제하려면 해당 리스트에서 경로를 선택한 후에 '–' 버튼 을 클릭하여 삭제합니다.

3.5.3 파일 예외 설정

nuri Anti-Ransom에 의해 랜섬웨어의 의심 행위를 차단되지 않도록 특정 파일을 설정할 수 있습니다.

1) '+' 을 클릭한 후에 제외하고 싶은 파일을 선택하고 '열기' 버튼을 클릭하여 등록합니다.

2) 이미 등록되어 있는 파일을 삭제하려면 해당 리스트에서 파일을 선택한 후에 '–' 버튼 을 클릭하여 삭제합니다.

3.6. 부가기능

[제품 보호]

랜섬웨어 악성코드를 비롯하여 다른 프로세스에 의해 nuri Anti-Ransom이 종료됨으로 사용자의 시스템이 위협받지 않도록 제품을 보호하는 기능입니다. 해당 기능에 이상이 생길 경우 'Off'로 변경되며 붉은색으로 나타납니다.
또한, nuri Anti-Ransom의 상태가 '랜섬웨어 방어에 위험한 상태입니다'로 표시됩니다.

[MBR 보호]

랜섬웨어를 포함한 악성코드가 사용자 시스템의 MBR(Master Boot Record)를 변조하여 윈도우 시스템 부팅 시 문제를 일으키는 증상을 보호합니다.
해당 기능에 이상이 생길 경우 'Off'로 변경되며 붉은색으로 나타납니다.
또한, nuri Anti-Ransom의 상태가 '랜섬웨어 방어에 위험한 상태입니다'로 표시됩니다.

[공유폴더 보호]

nuri Anti-Ransom이 설치된 시스템에 설정된 공유 폴더를 보호합니다. 랜섬웨어로부터 위 협을 차단한 이후 1시간동안 네트워크를 차단하게 되며 다른 PC로부터 지속적인 공격이 오기 전에 추가 조치(네트워크 내 다른 PC 검사)를 취해야 합니다.

(주의)
100MB이상의 파일이 공유폴더에 있는 경우는 정상적으로 백업이 되지 않을 수 있습니다.
이런 파일은 별도의 백업을 해야 합니다.

해당 기능에 이상이 생길 경우 'Off'로 변경되며 붉은색으로 나타납니다.
또한, nuri Anti-Ransom의 상태가 '랜섬웨어 방어에 위험한 상태입니다'로 표시됩니다