# nuri Anti-Ransom For PC 메뉴얼



2017년 7월 초판 발행


홈페이지: **http://www.nurilab.com**

# ▶ 목 차

# ▶ nuri Anti-Ransom For PC 소개

## 1. 주요 기능

새로운 형태의 신,변종 랜섬웨어로 인해 기존 패턴기반의 컴퓨터 백신, 방화벽, 침입차단 솔루션 등을 우회하여 많은 감염 피해를 입고 있습니다. NAR(nuri Anti-Ransom For PC)은 메일, 취약한 웹, 소프트웨어 취약점 등을 통해 유입되는 랜섬웨어에 대해 사전방역을 강화하고, 감염 시 랜섬웨어 동작을 인지하여 실시간 대응할 수 있는 새로운 형태의 솔루션입니다.

### 행위엔진 및 사전방역

랜섬웨어 악성코드의 동작 행위를 인지하여 랜섬웨어 행위를 차단하고, 한번 차단된 랜섬웨어는 행위 분석없이 차단합니다.

### 클라우드 엔진

랜섬웨어의 화이트리스트와 블랙리스트 제어기능을 통해 행위엔진을 보완하고 랜섬웨어를 차단, 치료합니다

### 자동백업 및 복원

랜섬웨어에 PC 데이터 감염 전 실시간 백업 및 자동복원 합니다

### MBR 보호

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

### 제품 보호

랜섬웨어 악성코드 공격으로부터 nuri Anti-Ransom For PC의 파일 및 프로세스 보호기능을 제공합니다.

### 자동 업데이트

프로그램 변경 시 사용자의 개입 없이 자동으로 업데이트 합니다.

### 검역소

nuri Anti-Ransom For PC로 치료 혹은 삭제된 파일을 검역소에 보관 및 복원합니다.

## 2. 시스템 요구사항

nuri Anti-Ransom For PC를 운영하기 위해 필요한 하드웨어, 소프트웨어 사양은 다음과 같습니다.

### [nuri Anti-Ransom For PC]

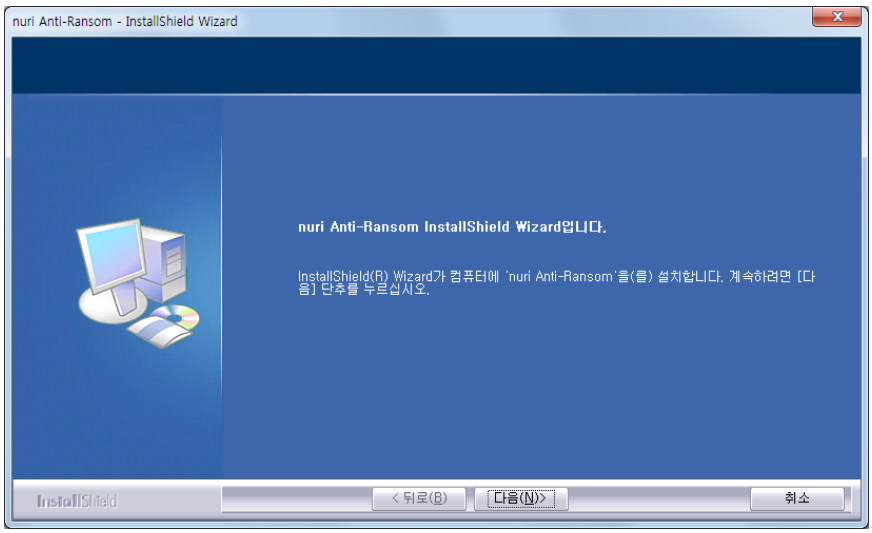
| | | |
|---|---|---|
| 하드웨어 | 최소사양 | - CPU : Intel Core 1.5GHz<br>- RAM : 2GB<br>- HDD : 5GB 여유공간 |
| | 권장사양 | - CPU : Intel Core i3 2.9GHz<br>- RAM : 4GB<br>- HDD : 10GB 여유공간 |
| 운영체제 | 윈도우 XP, Vista, 7, 8(8.1), 10 [32/64] 지원 | |

# 1. 설치/삭제/정품인증 하기

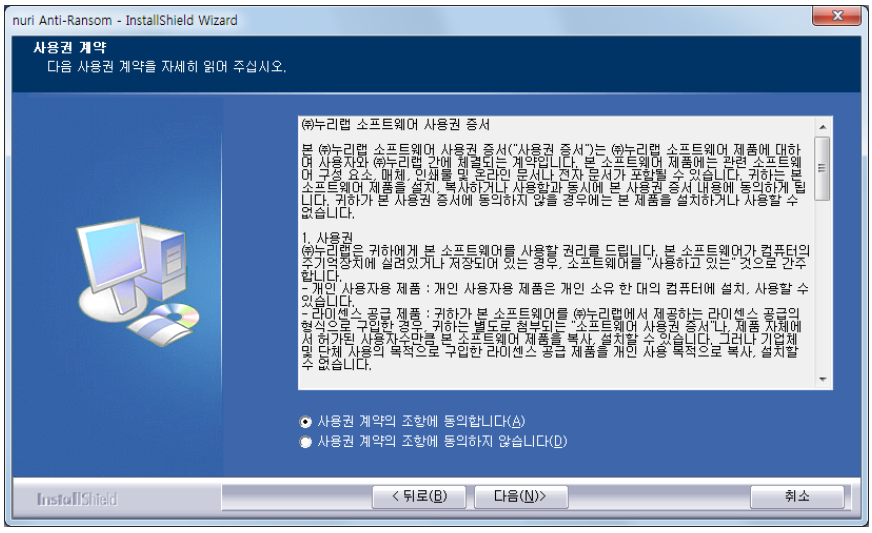
## 1.1. nuri Anti-Ransom For PC 설치하기

구매하신 다운로드 페이지에서 nuri Anti-Ransom For PC 설치파일을 다운로드 하여 실행합니다.

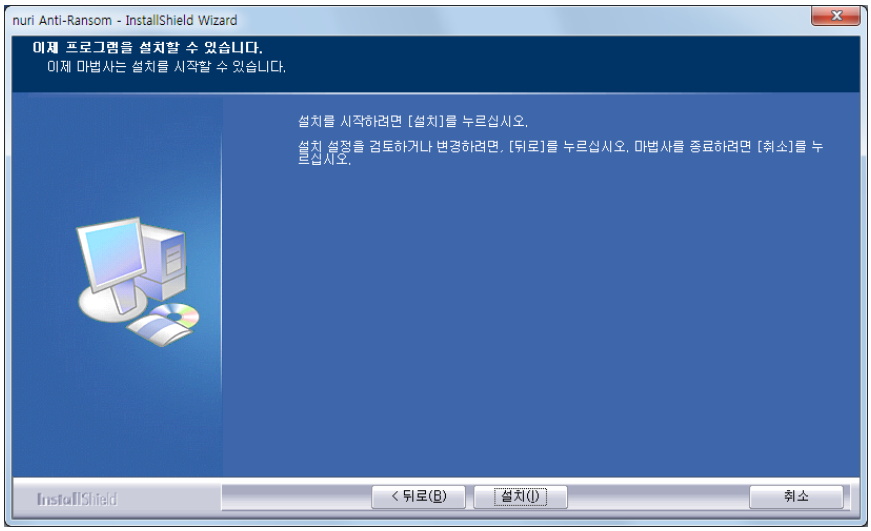
1) **[다음(N)]**을 클릭하면 설치가 진행됩니다.



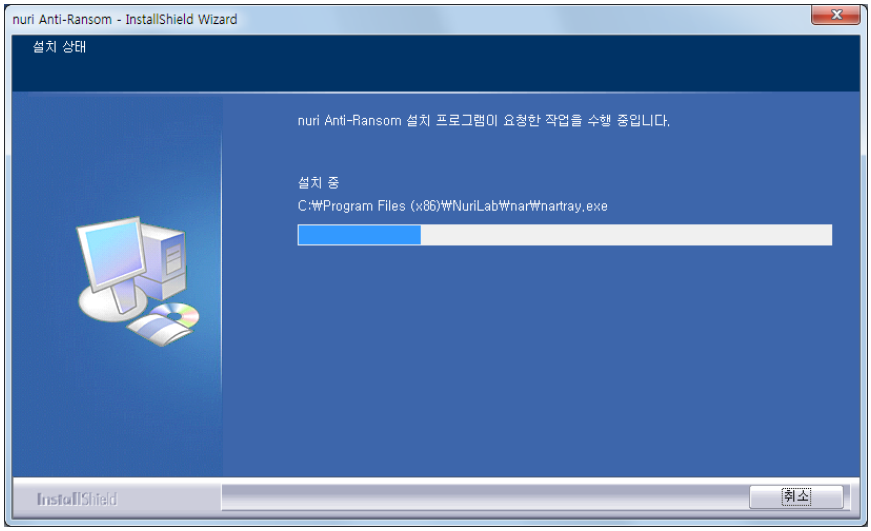

2) 다음 단계에서 사용자 약관을 읽고 '사용권 계약의 조항에 동의합니다(A)'를 선택하고 **[다음(N)]**을 클릭하면 다음 단계로 진행됩니다.



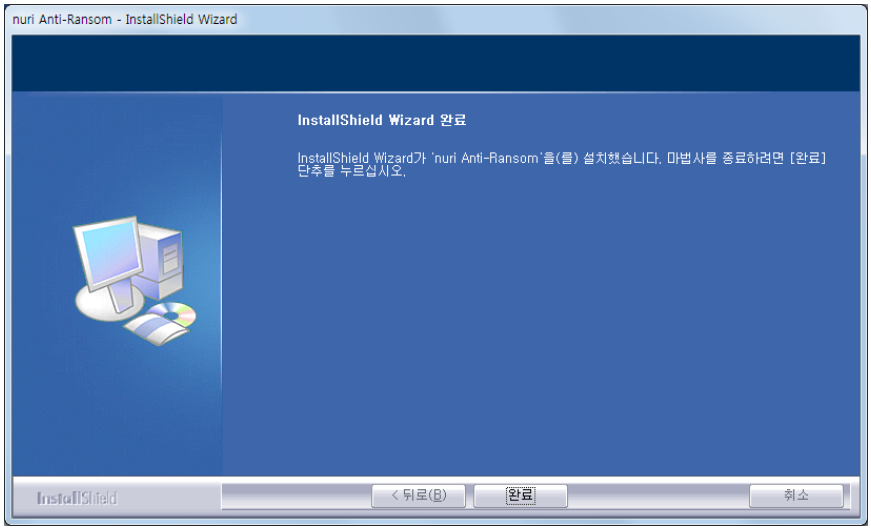
3) 다음 단계에서 **[설치(I)]**를 클릭하면 설치를 시작합니다.



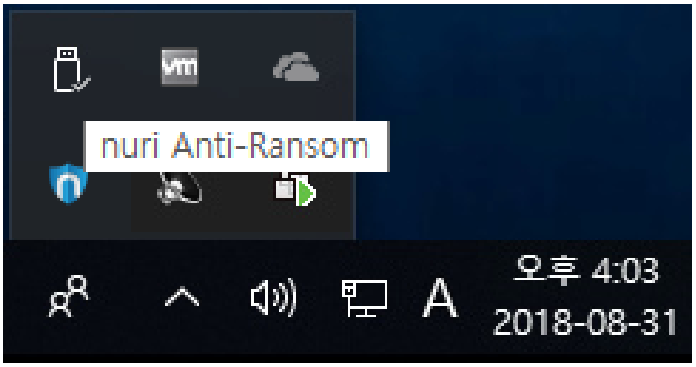

4) 설치 과정이 진행되는 동안 **[취소]**를 클릭하면 설치를 중단하고 설치 프로그램은 종료됩니다.



5) 설치 과정이 모두 끝난 후 **[완료]**를 클릭하면 설치 프로그램이 종료됩니다.

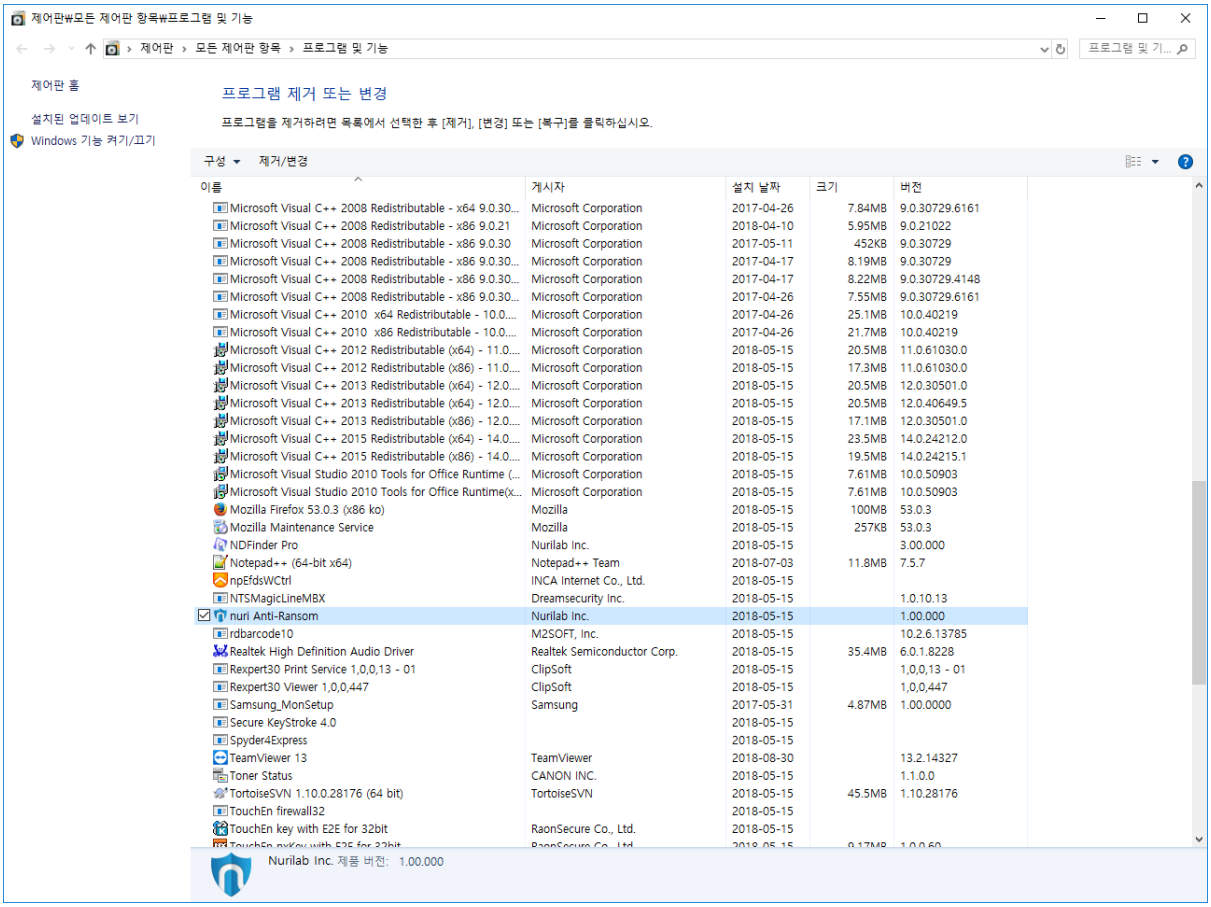



6) 정상적으로 설치가 완료되면 nuri Anti-Ransom이 실행되고 바탕화면 바로가기 아이콘과 및 트레이 아이콘이 생성됩니다.

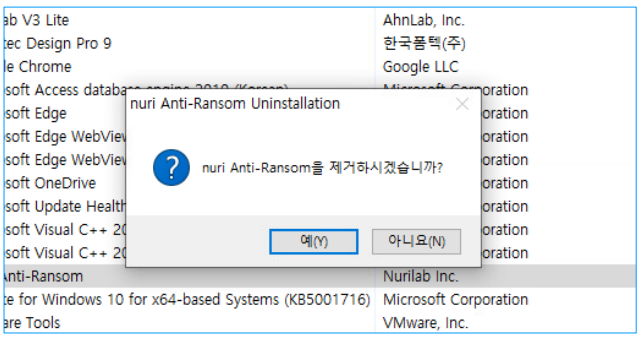



## 1.2. nuri Anti-Ransom For PC 삭제하기

1) 윈도우 '제어판' → '프로그램 및 기능'에서 **'nuri Anti-Ransom'**을 선택하여 제거합니다.



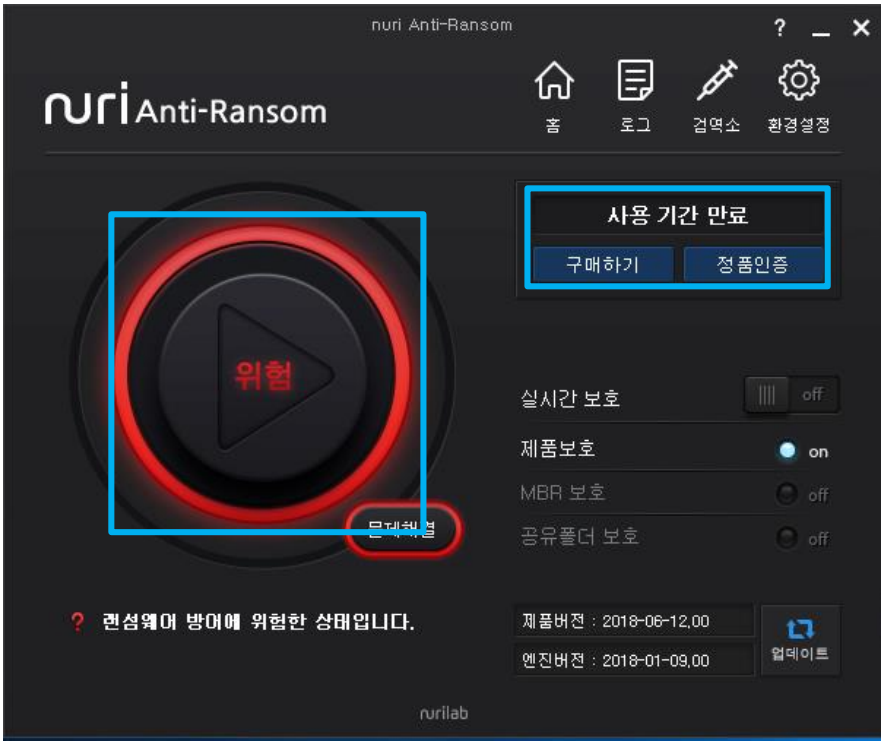

2) **[예(Y)]** 버튼을 클릭하여 프로그램 삭제를 진행합니다.



## 1.3. nuri Anti-Ransom For PC 정품인증하기

체험판 고객은 30 일 동안 사용할 수 있고, 유료 구매를 하지 않고 기간만료 후에는, 주요기능을 사용할 수 없습니다. 유료 구매 고객은 구매 및 설치하고 정품인증 완료 후 1PC 기준 1 년 동안 사용할 수 있습니다.

1) 제품사용기간 만료
체험판 30일, 유료구매제품 1년 사용 후, 제품메인화면(홈)에 '사용 기간 만료' 문구 및 '위험'이 표시됩니다.



2) 구매 및 정품인증

- 구매

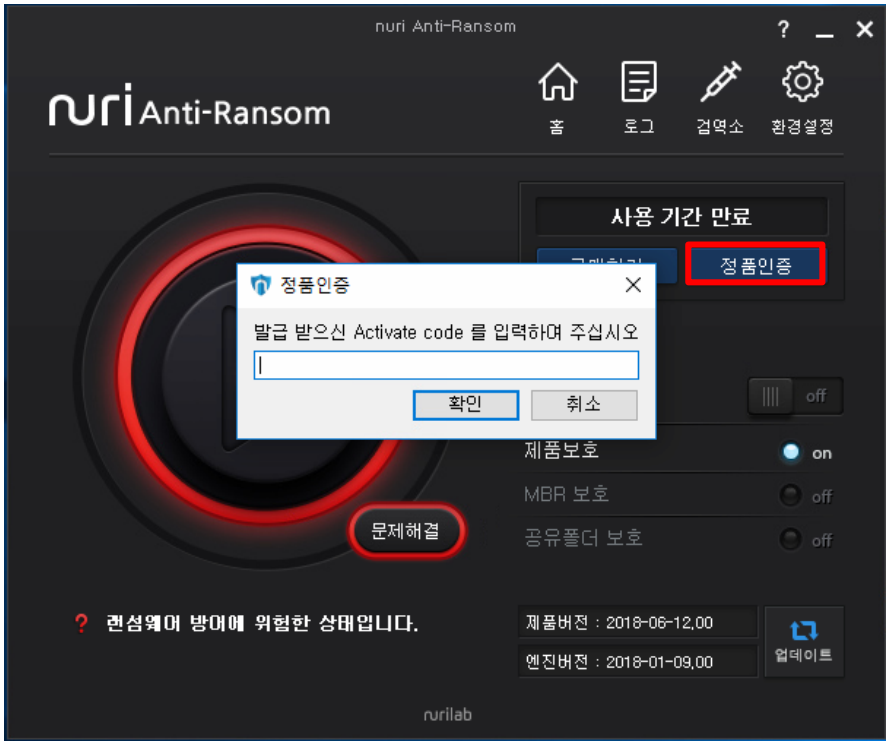
**'구매하기'** 및 **'문제해결'**을 클릭하여 '정품정보' 메시지 창을 이용하여
누리랩숍(http://www.nurilabshop.com)에 접속하여 **nuri Anti-Ransom For PC** 제품을 구매합니다.

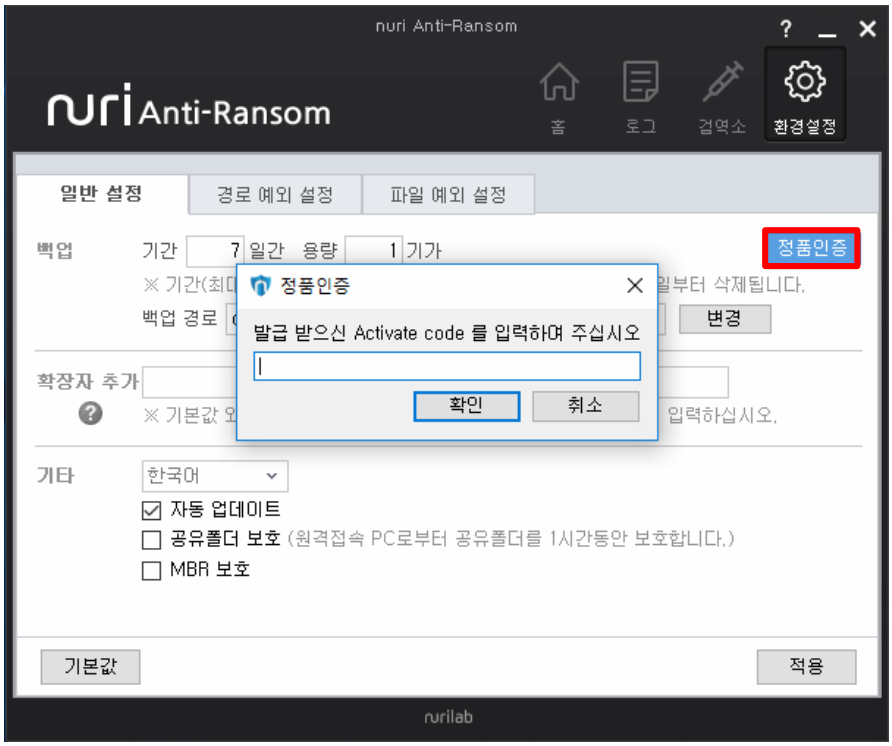
# ▶ nuri Anti-Ransom For PC 사용

- 정품인증

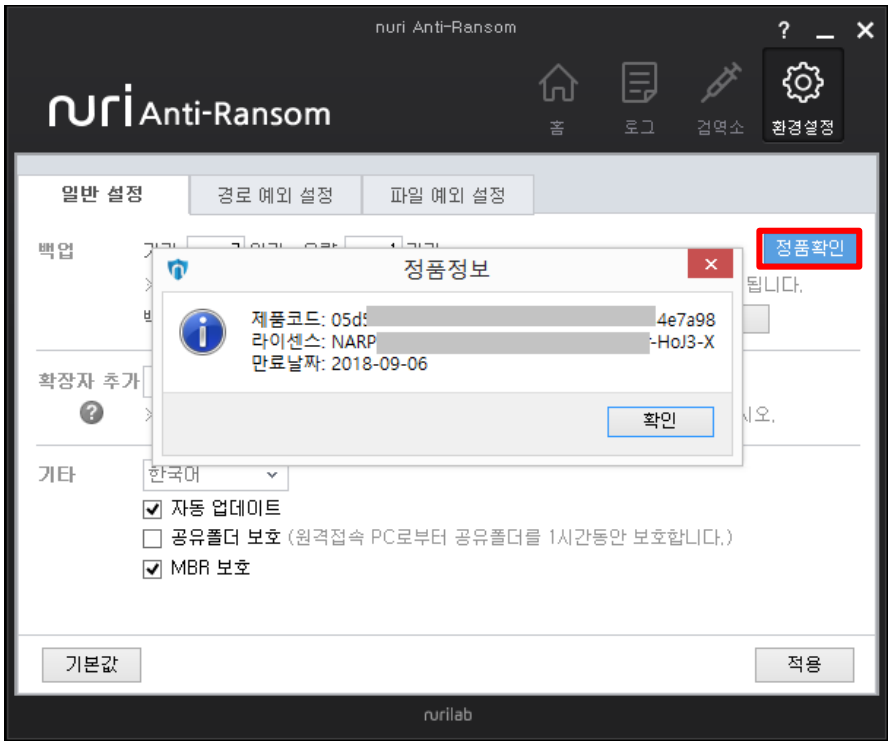
메인화면의 **'정품인증'** 메뉴 및 [환경설정] → [일반설정]의 **'정품확인'** 메뉴를 클릭하면 활성화 코드(activate code)를 입력할 수 있는 팝업 창이 나타납니다.
구매 시 발급 받은 **활성화코드(activate code)**를 입력하고 [OK]버튼을 클릭합니다.

※ 온라인 구매자의 경우. 구매 시 메일로 받은 활성화 코드(activate code)를 **'복사 & 붙여넣기'**로 입력합니다.



3) 정품인증 후 '정품인증' 버튼을 다시 클릭하여 정품 등록 정보를 확인합니다.

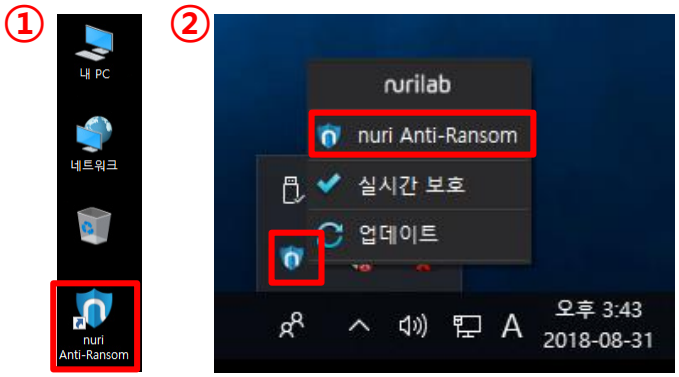


# 2. 실행하기

## 2.1. nuri Anti-Ransom For PC 실행하기

① 바탕화면의 **'nuri Anti-Ransom' 아이콘으로 실행**

② 윈도우 오른쪽 하단 트레이 아이콘을 '더블 클릭'하거나, 마우스 오른쪽메뉴에서 **'nuri Anti-Ransom'**을 선택




## 2.2. nuri Anti-Ransom For PC 화면 구성

### 2.2.1. 메인화면(홈)

메인화면 구성은 다음과 같습니다.


① 메뉴
- 홈 : 메인화면으로 이동합니다.
- 로그 : 프로그램 동작 정보가 시간대 별로 기록됩니다.
- 검역소 : 검역소로 이동합니다.
- 환경설정 : 환경설정으로 이동합니다.

② 사용기간
체험판을 제외하고 기본적으로 표기되지 않습니다.
정식버전의 경우, 사용기간이 7일 이하로 남았을 경우에 잔여일수가 표기됩니다.

③ 검사 버튼
사용자 디스크에 존재하는 랜섬웨어를 수동으로 검사하고 치료합니다.

④ 기능설정

- 실시간 보호 : 랜섬웨어 실시간 보호기능을 'ON' / 'OFF' 합니다.
- 제품보호 : 악의적인 공격으로부터 제품을 보호하는 기능으로 'ON'이 기본값이고, 'OFF' 할 수 없습니다.
- MBR보호 : 윈도우 MBR(Master Boot Record) 보호기능으로 'ON'이 기본값이고, [환경설정] → [일반설정]에서 'OFF' 할 수 있습니다.
- 공유폴더보호 : 윈도우 공유폴더를 보호하는 기능으로 'OFF' 가 기본값이고, 환경설정에서 'ON' 할 수 있습니다.

⑤ NAR 상태

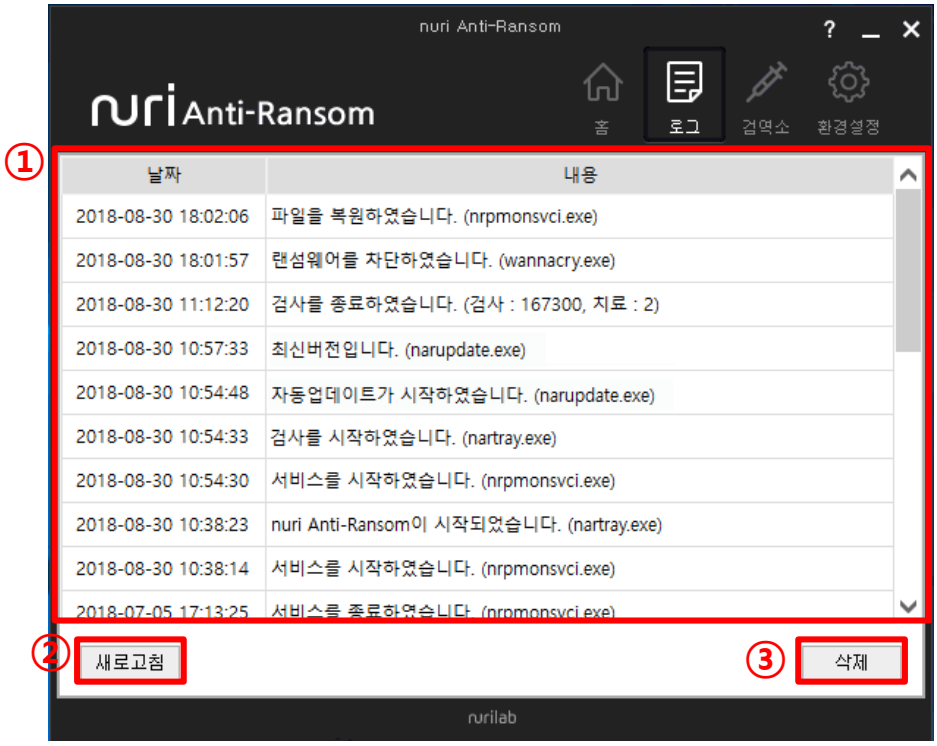
- 상태 : 기본은 **'V 현재 정상 상태입니다'**로 NAR 정상동작을 나타내고, NAR의 기능이 Off 상태이거나 비정상일 경우, **'? 랜섬웨어 방어에 위험한 상태입니다'**로 표시됩니다.
- 최근 업데이트 : 최근 업데이트 날짜가 표시됩니다.
- 최근 검사 : 최근 디스크 검사 날짜가 표시 됩니다. 디스크 검사를 수행하지 않을 경우 '정보없음'으로 표기됩니다.

⑥ NAR 버전 정보

- 제품버전 : nuri Anti-Ransom For PC 제품 버전 정보를 확인합니다.
- 엔진버전 : 검사 엔진 버전 정보를 확인합니다.
- 업데이트 버튼 : 제품 및 검사 엔진 업데이트를 수동으로 진행합니다.

## 2.2.2. 로그

nuri Anti-Ransom For PC 행위 정보가 기록됩니다.



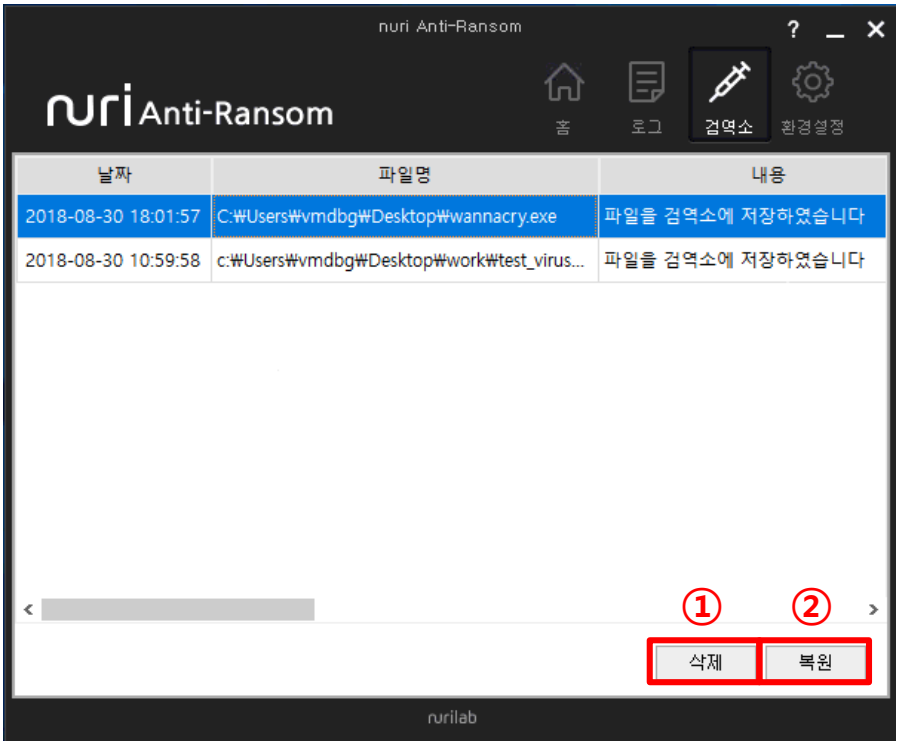

① 프로그램 시작정보, 서비스 동작, 업데이트 내역, 랜섬웨어 차단 및 복원, 수동검사 내역 등이 시간대 별로 기록됩니다.

② '새로고침' 은 마지막 갱신된 로그를 확인합니다.

③ '삭제'는 화면에 기록된 모든 로그를 삭제합니다.

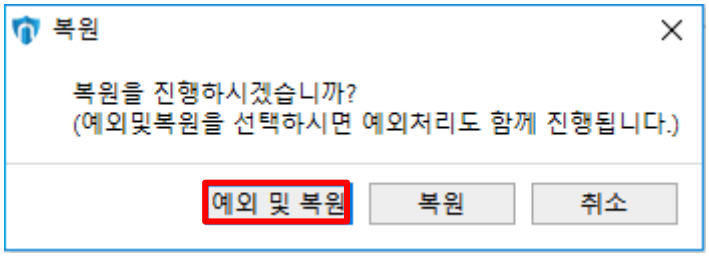
## 2.2.3. 검역소

랜섬웨어 차단 및 치료 후, 랜섬웨어 파일을 격리 보관합니다.




① 지정된 항목을 선택 후 '삭제'를 클릭하면 PC에서 파일을 삭제합니다.

② 지정된 항목을 선택 후 '복원'을 클릭하면 아래와 같은 메시지가 나타납니다
선택 항목이 정상 파일일 경우, **'예외 및 복원'**을 선택하면 파일명에 기록된 위치로 복원됩니다.



## 2.2.4. 환경설정

nuri Anti-Ransom For PC 설정을 확인하고 변경합니다.

- 값 변경 후, 오른쪽 하단 '적용' 버튼을 클릭하여 변경사항을 반영합니다.
- '기본값' 클릭 시, 제품설치 상태로 초기화 됩니다.

※ 사용 중 백업경로를 다른 경로로 변경했을 경우에 백업경로도 초기화 되어 백업데이터가 초기화(삭제) 되므로 주의하시기 바랍니다.


1) 일반설정

① 백업

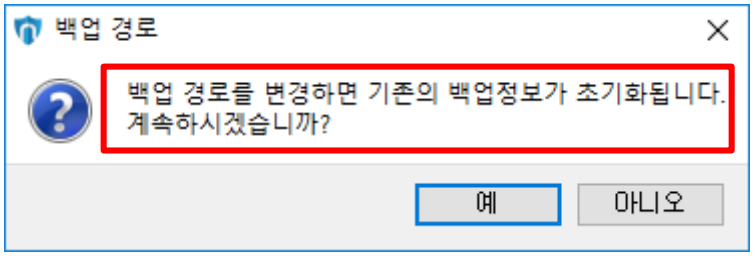
- 기간 및 용량

백업된 데이터는 설정된 기간 동안 보관되고, 설정된 용량 초과 시 오래된 파일부터 삭제됩니다.
기간 및 용량은 변경 가능합니다.
(백업용량은 최초 설치 시 설치 대상 볼륨 **여유 공간의 10%**로 자동 적용됩니다.)

- 경로

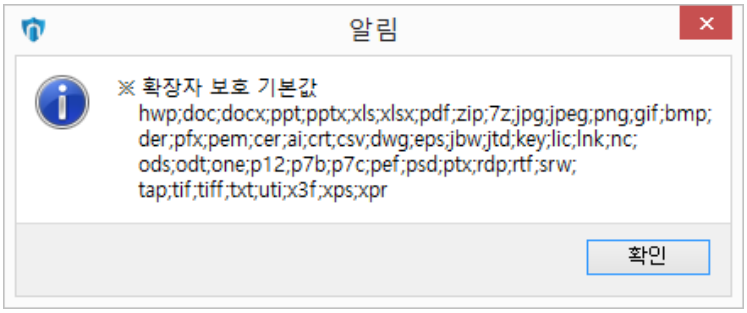
경로를 변경하려면, '변경'버튼을 선택하여 원하는 위치로 변경할 수 있습니다.

※ 백업 경로 변경 시, 백업된 데이터는 모두 초기화(삭제)되므로 주의하시기 바랍니다.



② 확장자 추가 : 랜섬웨어의 공격으로부터 보호대상이 되는 기본 파일 확장자 외에 확장자를 입력하면 추가로 보호됩니다. 추가 시, 세미콜론(;)으로 구분하여 입력하는데, 예는 아래 확장자 보호 기본값 화면을 참고합니다.

※ 확장자 추가 밑에 ⑦를 클릭하면 보호되는 기본 확장자 정보를 확인할 수 있습니다.




③ 기타

- 한국어 : 한글 윈도우에 설치되면 한국어로 설정되고, 영문 윈도우에 설치하면 영문으로 자동 적용됩니다. 사용자가 변경할 수 없습니다.
- 자동 업데이트 : 체크 시 사용자 개입 없이 자동으로 업데이트 됩니다.
- 공유폴더보호 : 체크 시, 윈도우 공유폴더 내의 데이터 파일을 보호합니다.
  ※ 참고 : 공유된 원격접속 PC가 랜섬웨어에 감염 될 경우, 1시간 동안 공유폴더 접속이 해제됩니다.
- MBR 보호 : 체크 시, 랜섬웨어로부터 MBR(Master Boot Record) 영역을 보호합니다.

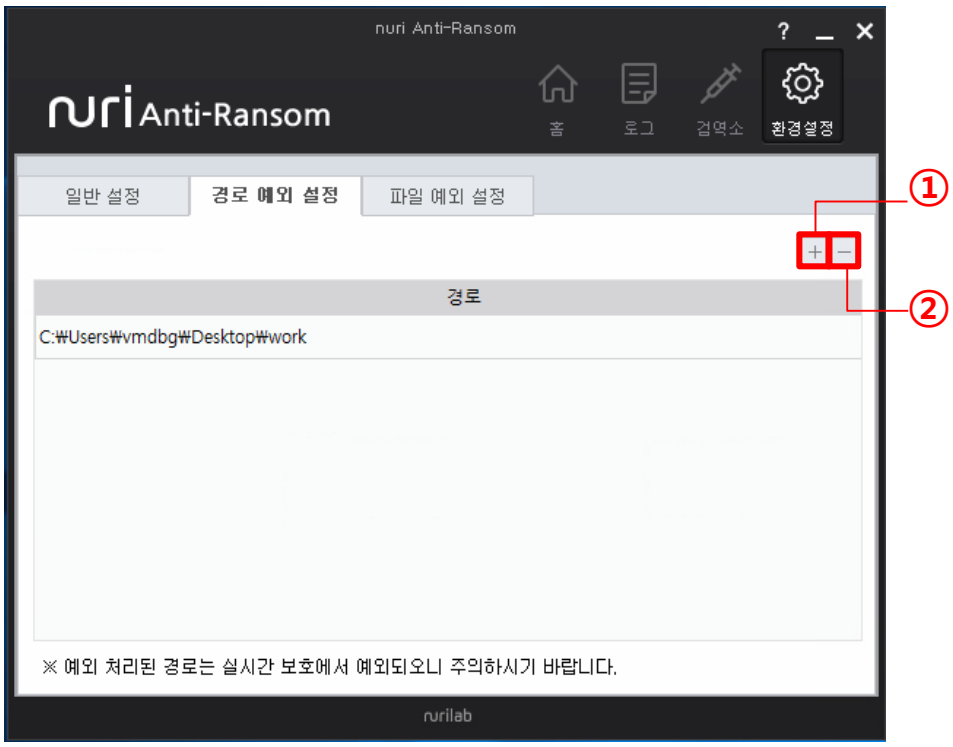
④ 정품확인

앞의 내용 중 **[1장. 설치/삭제/정품인증 하기] → [1.3. nuri Anti-Ransom For PC 정품인증 하기]** 를 참고합니다.

2) 경로 예외 설정

랜섬웨어 검사에서 폴더를 제외합니다.

경로 예외 설정 적용 시, 랜섬웨어에 감염되어도 검사 및 치료하지 않습니다.



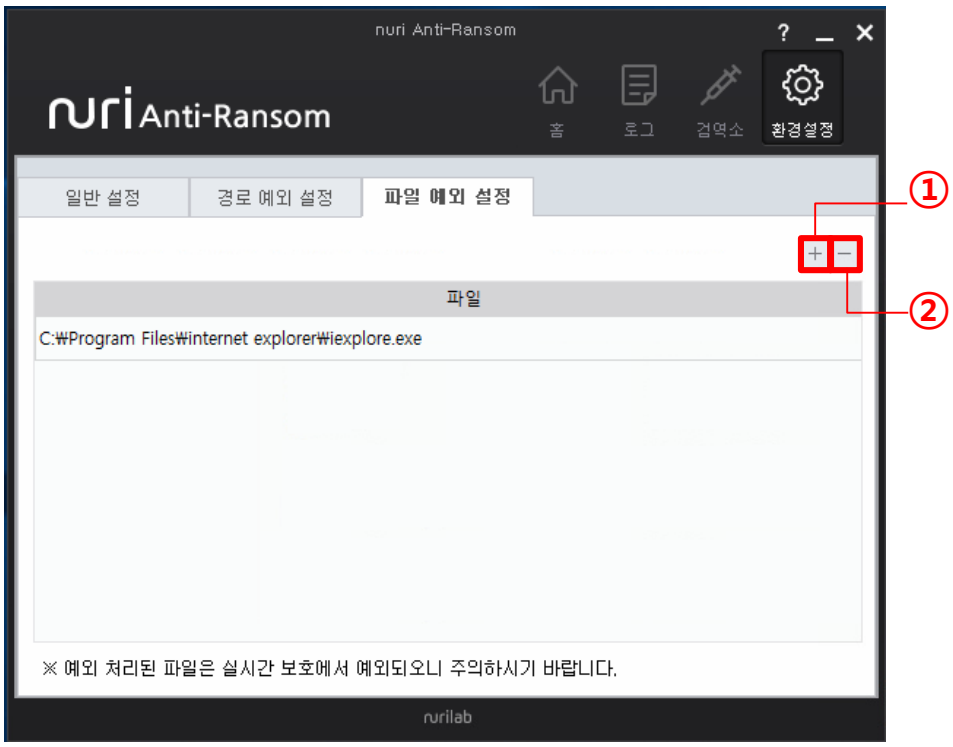

① '플러스버튼(+)' 클릭 후, 원하는 폴더를 지정하면 경로 예외 설정에 적용됩니다.

② 경로 예외 설정 목록에서 항목 선택 후, '마이너스버튼(-)'을 클릭하면 경로 예외 설정에서 삭제됩니다.

3) 파일 예외 설정

랜섬웨어 검사에서 파일을 제외합니다.

파일 예외 설정 적용 시, 랜섬웨어에 감염되어도 검사 및 치료하지 않습니다.




① 플러스버튼(+) 클릭 후, 원하는 파일을 지정하면 파일 예외 설정에 적용됩니다.

② 파일 예외 설정 목록에서 항목 선택 후, 마이너스버튼(-) 클릭하면 파일 예외 설정에서 삭제됩니다.

# 3. 활용하기

## 3.1. 실시간 보호

nuri Anti-Ransom For PC메인화면(홈)의 **'실시간 보호'**는 항상 **'ON'** 상태를 유지해야 랜섬웨어로 부터 실시간으로 보호할 수 있습니다.

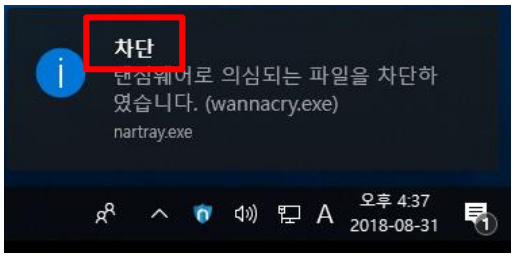
1) 실시간 보호 'ON'

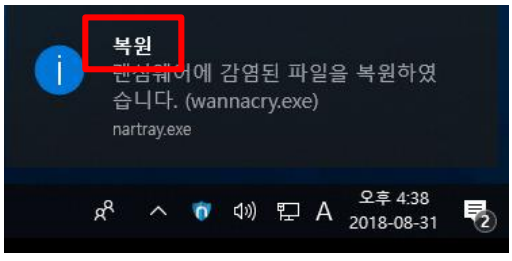
실시간 보호 'ON' 상태에서 랜섬웨어 감염 시도 시, 아래 2가지로 처리됩니다.


- 자동치료

사용자 개입 없이 랜섬웨어를 자동으로 치료 및 복원하고,

오른쪽 하단 트레이에서 랜섬웨어 차단 및 복원 알림 메시지가 나타납니다.



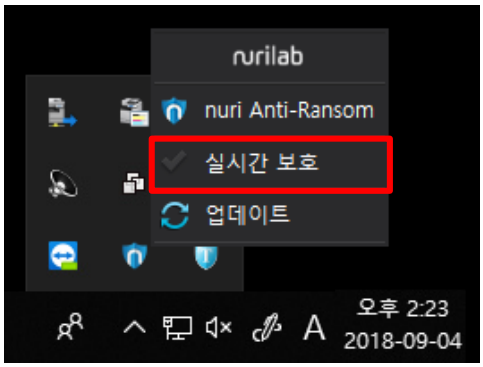



2) 실시간 보호 'OFF'

- 실시간 보호 'OFF' 방법

파란색 화살표 부분의 실시간 보호 **'ON' 글씨를 클릭**하거나 트레이 아이콘 메뉴에서 **'실시간 보호' 체크 해제** 시 'OFF' 됩니다.

결과는 25페이지의 그림 화면과 같습니다.

# ▶ nuri Anti-Ransom For PC 사용

- 실시간 보호 'OFF' 화면
  랜섬웨어 공격 시, 치료할 수 없는 상태입니다.
  ※ 정상 파일을 오진할 경우에만, 선조치로 '실시간 보호'를 'OFF' 합니다.

3) 실시간 보호 'ON' 방법

실기간 보호 'OFF' 상태에서 "ON' 으로 하는 방법은

① 메인화면 실시간 보호 **'OFF' 글씨를 클릭**합니다.

② '문제해결 ' 버튼을 클릭하고 문제해결 메시지 창에서 **'예'**를 선택하면 'ON'됩니다.

③ 윈도우 오른쪽 하단 트레이 메뉴에서 '실시간 보호' 항목에 체크합니다.

## 3.2. 랜섬웨어 검사

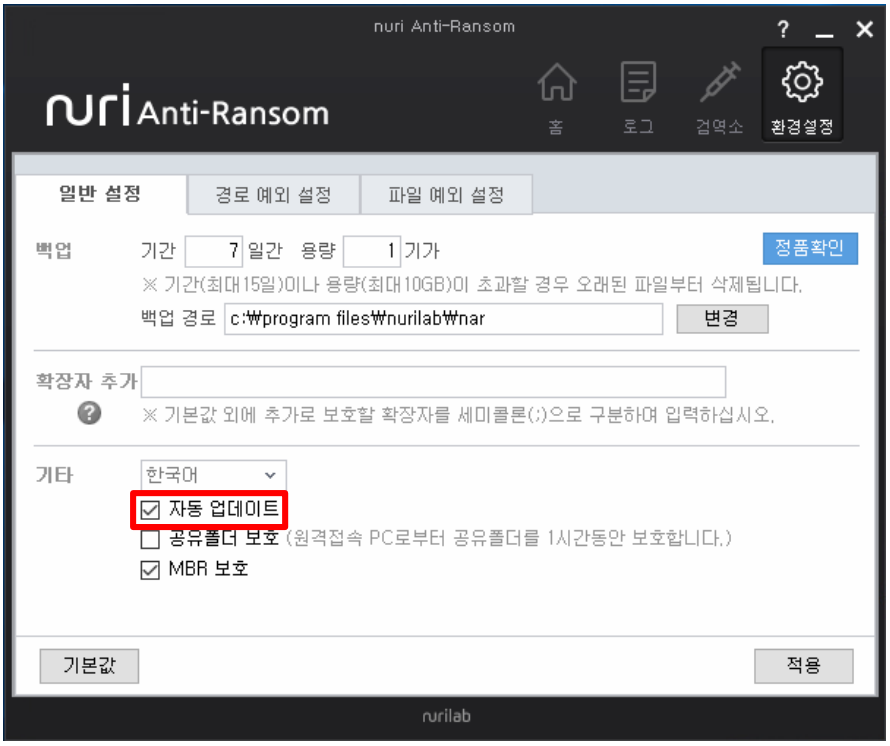
사용자가 직접 디스크에 있는 램섬웨어 파일을 검사합니다.
메인 UI에서 **'검사'** 버튼을 클릭하면 검사가 진행되고, 다시 클릭하면 검사가 중지됩니다.


## 3.3. 업데이트

자동업데이트와 수동업데이트 2가지 방식으로 업데이트를 수행합니다.

1) 자동업데이트

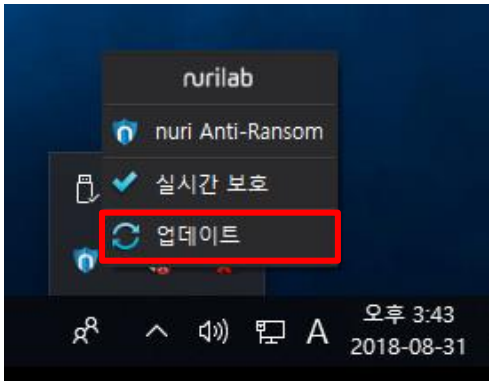
기본적으로 환경설정에 자동업데이트에 체크되어 있을 경우, 사용자의 개입 없이 자동으로 업데이트 됩니다.



2) 수동데이트

사용자가 원하는 시점에 수동으로 업데이트 합니다.

- 윈도우 오른쪽 하단 트레이 아이콘 오른쪽 메뉴의 '업데이트' 클릭




- 메인화면의 '업데이트 버튼' 클릭