디코이 진단 고객 안내 가이드

고객 가이드

2016. 06. 20

AhnLab

목차

1. PC 에 이상한 폴더가 생겼어요, 악성코드에 감염 된 건가요? 3

2. 디코이(Decoy)가 뭔가요? 3

3. 폴더는 왜 생성하는 건가요? 3

4. 폴더 생성이 안되게 하고 싶은데 방법이 없나요? 3

5. 성능상의 문제는 없나요? 3

6. 이런 내용을 왜 미리 공지하지 않았나요? 3

7. 해당 기능을 계속 사용 했을 때 장점은 무엇인가요? 3

8. 디코이 기능이 동작하고 있는지 어떻게 확인하나요? 4

9. 디코이 기능을 사용하려면 어떻게 해야 하나요? 5

10. 디코이 기능 Test 는 어떻게 해야 하나요? 6

1. PC에 이상한 폴더가 생겼어요, 악성코드에 감염 된 건가요?

V3 9.0 제품군(IS/ES/Net)은 랜섬웨어 탐지를 위해 디코이라는 진단 방법을 사용하고 있습니다.
폴더명 앞에 특수기호(@, $, % 등)가 있다면 V3가 생성한 폴더이니 악성코드에 감염 된 것은 아닙니다.
V3에서 랜섬웨어 탐지를 하기 위한 정상적인 동작 입니다.

2. 디코이(Decoy)가 뭔가요?

디코이는 사전적으로 유인한다는 의미를 가지고 있습니다. V3가 랜섬웨어를 유인하기 위해 생성한 파일에 랜섬웨어가 암호화 하려고 접근 하면 탐지하고 차단 합니다.

3. 폴더는 왜 생성하는 건가요?

랜섬웨어는 일반적으로 저장 된 데이터(그림, 문서 파일 등)들을 암호화 합니다.
랜섬웨어는 최대한 빠르게 모든 파일을 암호화 하기 위해 사용자 PC의 최상위 경로부터 암호화를 진행합니다.
V3는 이러한 랜섬웨어의 행위를 탐지하는데, V3가 생성한 폴더를 랜섬웨어가 접근하게 되면 즉시 탐지하고 차단하여 피해를 예방 할 수 있습니다.

4. 폴더 생성이 안되게 하고 싶은데 방법이 없나요?

V3의 환경설정에서 '행위 기반 진단 사용' 옵션을 OFF 하면 됩니다.
다만, 랜섬웨어를 가장 빨리 진단할 수 있는 진단 방법은 행위기반 진단이므로 해당 옵션을 OFF 할 경우 더 많은 악성코드에 노출 될 수 있기에 유지하는 것을 추천합니다.

5. 성능상의 문제는 없나요?

랜섬웨어 탐지를 위해 폴더를 생성하지만, 해당 폴더가 어떠한 동작을 하지는 않습니다.

6. 이런 내용을 왜 미리 공지하지 않았나요?

디코이 진단법은 이미 2015년부터 V3에서 제공하고 있습니다.
새로운 기능이 추가 된 것은 아니며, 폴더를 생성하는 방법이 일부 개선 된 것이기에 공지하지 않았습니다.

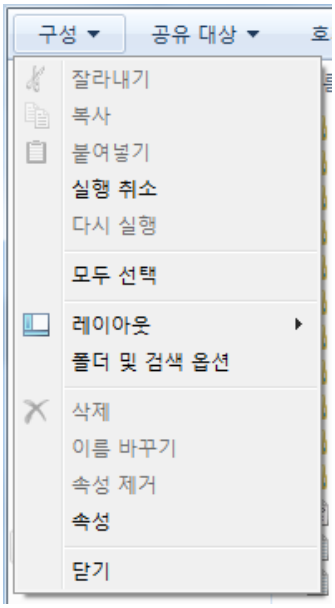
7. 해당 기능을 계속 사용 했을 때 장점은 무엇인가요?

최근 랜섬웨어가 급증하고 있으며, 그 만큼 다양한 방법으로 사용자 PC를 노리고 있습니다.
V3 역시 다양한 행위 진단법을 통해 탐지하고 대응하고 있습니다.
디코이 진단은 랜섬웨어라면 빠짐없이 하는 행위 중 하나인 암호화를 탐지하는 것으로 효과적으로 대응하기 위한 진단법 중 하나 입니다.

8. 디코이 기능이 동작하고 있는지 어떻게 확인하나요?

디코이는 PC의 모든 드라이브에 임의 폴더를 생성합니다. 모든 드라이브에서 아래 절차로 확인이 가능합니다.

1) C드라이브 – 상단 메뉴의 '구성' Click

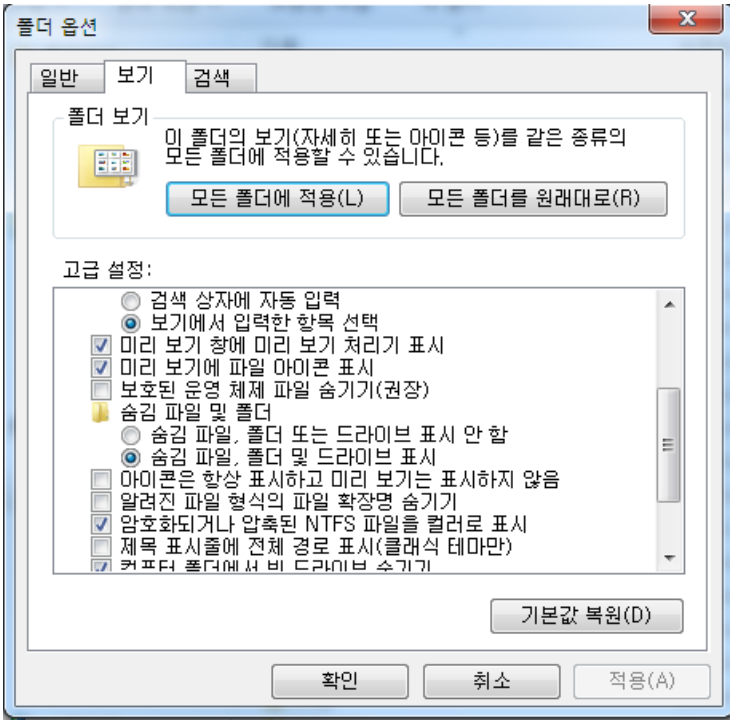


2) 폴더 및 검색 옵션 Click – 보기

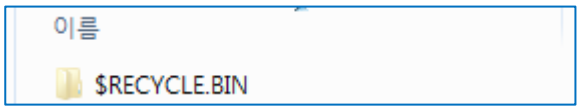
a. 보호된 운영체제 파일 숨기기(권장)체크 해제

b. 숨김 파일, 폴더 및 드라이브 표시 체크

c. 우측 하단의 '적용' Click



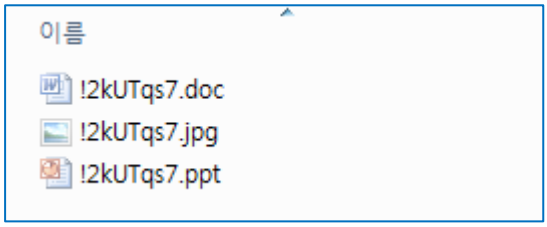
d. 랜덤한 폴더명 확인(폴더명 맨 앞에 특수문자 적용(랜덤))



3) 내 컴퓨터 – Windows(C:) – 사용자(Users) – 내 컴퓨터 이름 – 내 문서(Documents)

a. 폴더 명 앞의 특수문자(랜덤)가 포함 된 디코이 폴더 확인

b. 폴더 내 생성 된 V3가 생성한 파일 확인 가능(파일명 랜덤)



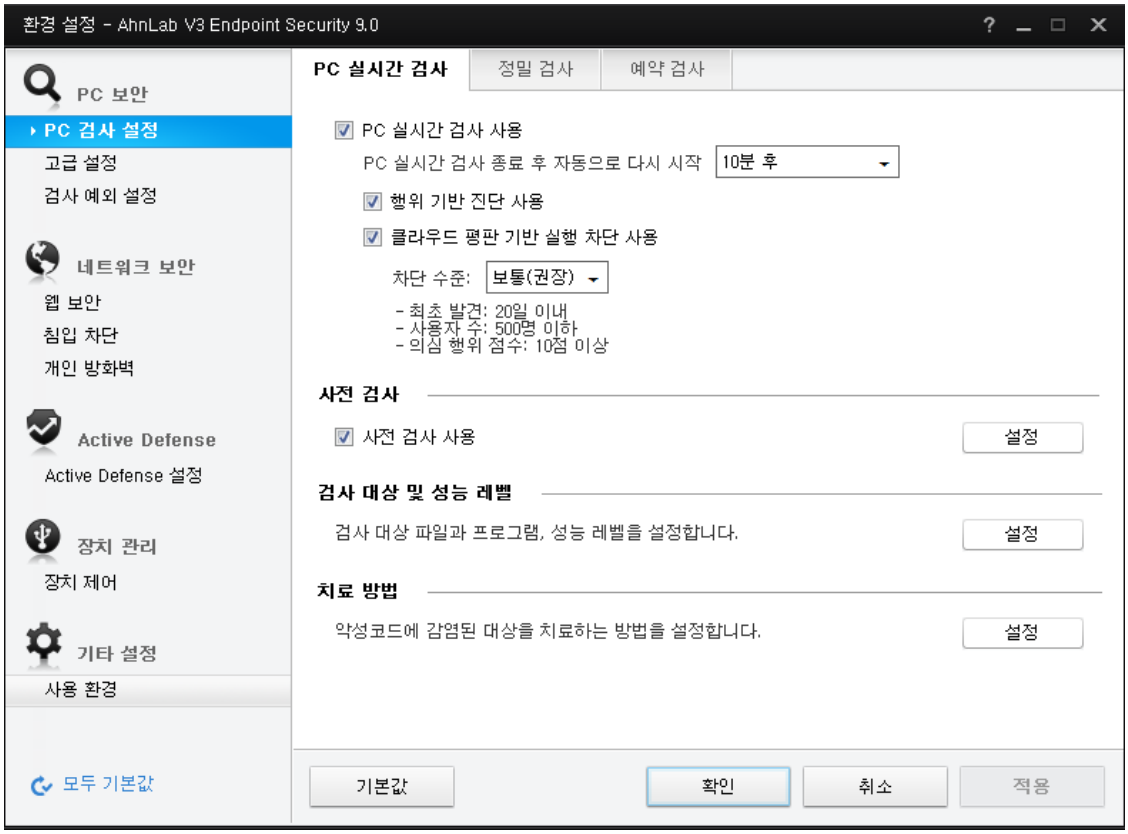
c. .doc 파일 클릭 시 **'This is Ahnlab Decoy File.'** 문구 확인

4) PC내 C드라이브 외 다른 드라이브도 같은 방법으로 확인

9. 디코이 기능을 사용하려면 어떻게 해야 하나요?

V3의 환경설정 – 행위 기반 진단 사용 체크

- V3 9.0 제품군(IS/ES/Net)은 디코이 진단 뿐만 아니라 랜섬웨어의 모든 대응을 행위 기반으로 합니다.



10. 디코이 기능 Test는 어떻게 해야 하나요?

1) 랜섬웨어 탐지

a. 유저 문서 경로 / C 경로 등에 문서 파일 준비

b. Test 할 랜섬웨어 악성코드 실행

c. 랜섬웨어 탐지를 통한 파일 암호화 방어 → 차단 팝업 창 확인

[End of Document]

AhnLab

경기도 성남시 분당구 판교역로 220 (우)463-400

홈페이지: http://www.ahnlab.com

대표전화: 031-722-8000 / 팩스: 031-722-8901