AI기반 신·변종 악성코드 및 랜섬웨어 대응 솔루션 전문기업

랜섬웨어도 이제는 ZERO 시대

당신의 데이터를 지키는 완벽한 방패, RansomZERO로 랜섬웨어 걱정 없는 세상

RANSOMZERO

NDCore
New Paradigm Core

Contents

1

랜섬웨어 특화 솔루션의 필요성 및 도입효과

1. 랜섬웨어 특화 솔루션의 필요성 및 도입효과

랜섬웨어 특화 솔루션의 필요성

급증하는 랜섬웨어 공격:
랜섬웨어 공격은 최근 몇 년 동안 급격히 증가하고 이러한 공격들은 기업과 개인의 데이터를 암호화하여 몸값을 요구하며, 그 피해 규모는 늘고 있음

도입효과
기업은 각종 랜섬웨어 공격으로부터 보다 안전하게 보호받을 수 있으며, 데이터 손실 및 비즈니스 중단의 위험을 줄일 수 있어 꼭 필요한 제품임

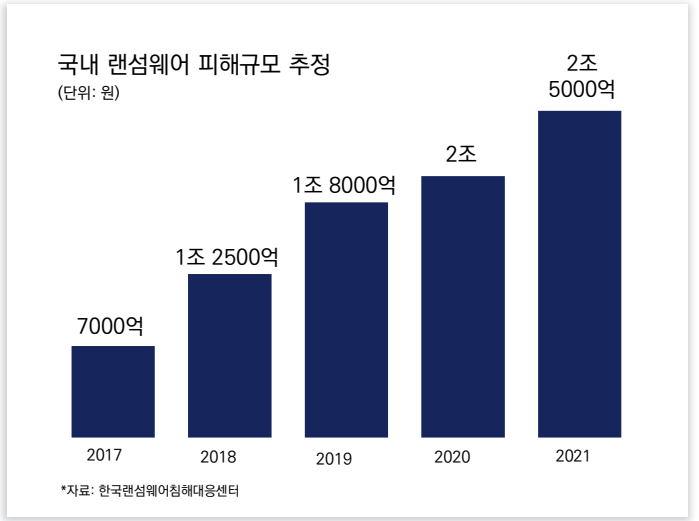
데이터 보호:
랜섬웨어에 특화된 제품은 중요한 데이터를 보호하는 데 중점을 두고 있으며 이러한 솔루션은 파일을 실시간으로 모니터링하고, 비정상적인 활동을 탐지하여 즉각 대응 가능

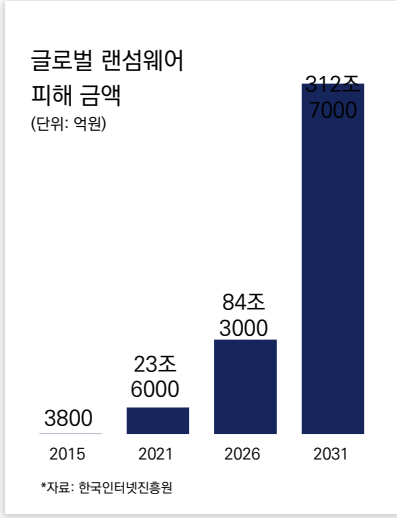
비즈니스 연속성:
랜섬웨어 공격으로 인해 비즈니스 운영이 중단되면 막대한 금전적 손실과 평판 손상이 발생할 수 있으며 랜섬웨어 특화 솔루션은 공격을 사전에 차단하고, 신속한 복구를 지원하여 비즈니스 연속성을 유지

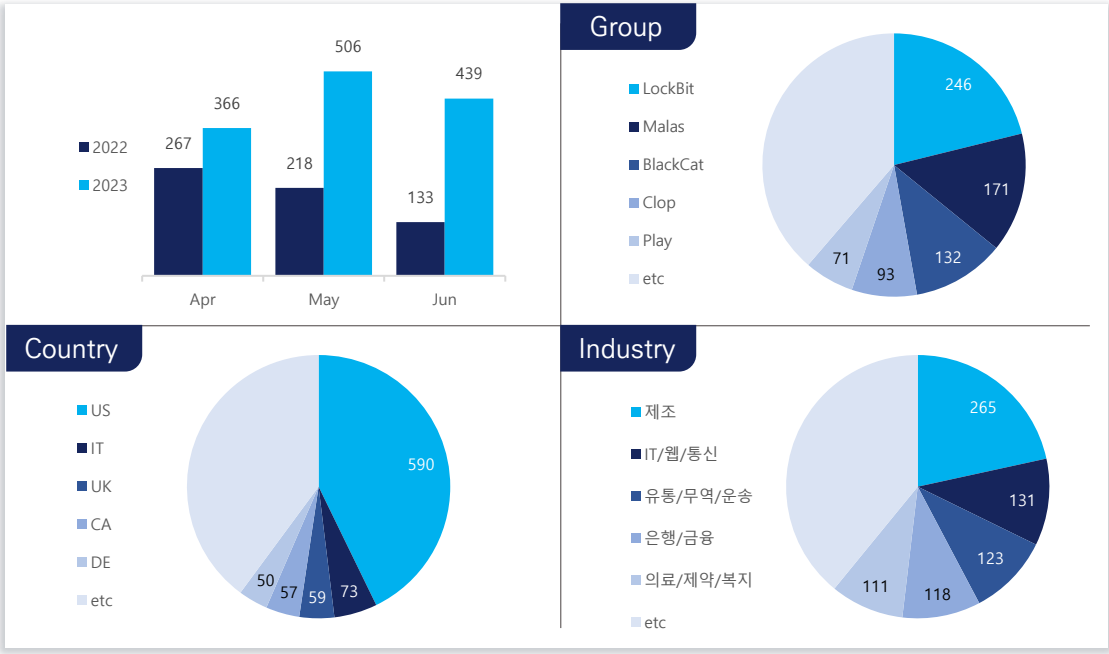
고도화된 탐지 및 대응:
랜섬웨어는 점점 더 정교해지고 있어, 일반적인 보안 솔루션만으로는 충분히 대응하기 어려움. 랜섬웨어에 특화된 솔루션은 최신 위협 정보를 바탕으로 한 고도화된 탐지 및 대응 기능을 제공

복구 능력 강화:
랜섬웨어 공격을 완전히 방어하는 것은 어렵기 때문에, 공격 후 데이터를 복구하는 능력도 중요한 포인트. 랜섬웨어 특화 솔루션은 백업 및 복구 기능을 제공하여, 데이터 손실을 최소화하고 빠르게 시스템 정상화 가능

규제 준수:
많은 산업에서 데이터 보호와 관련된 규제가 강화되고 있음. 랜섬웨어 방지 솔루션을 도입함으로써, 기업은 이러한 규제를 준수하고, 법적 리스크를 줄일 수 있음







〈SK Shieldus 랜섬웨어 동향 보고서 2023. 7〉

2

RansomZERO 구성 및 주요기능

2-1. 엔피코어 제품군 구성도

네트워크부터 엔드포인트까지!

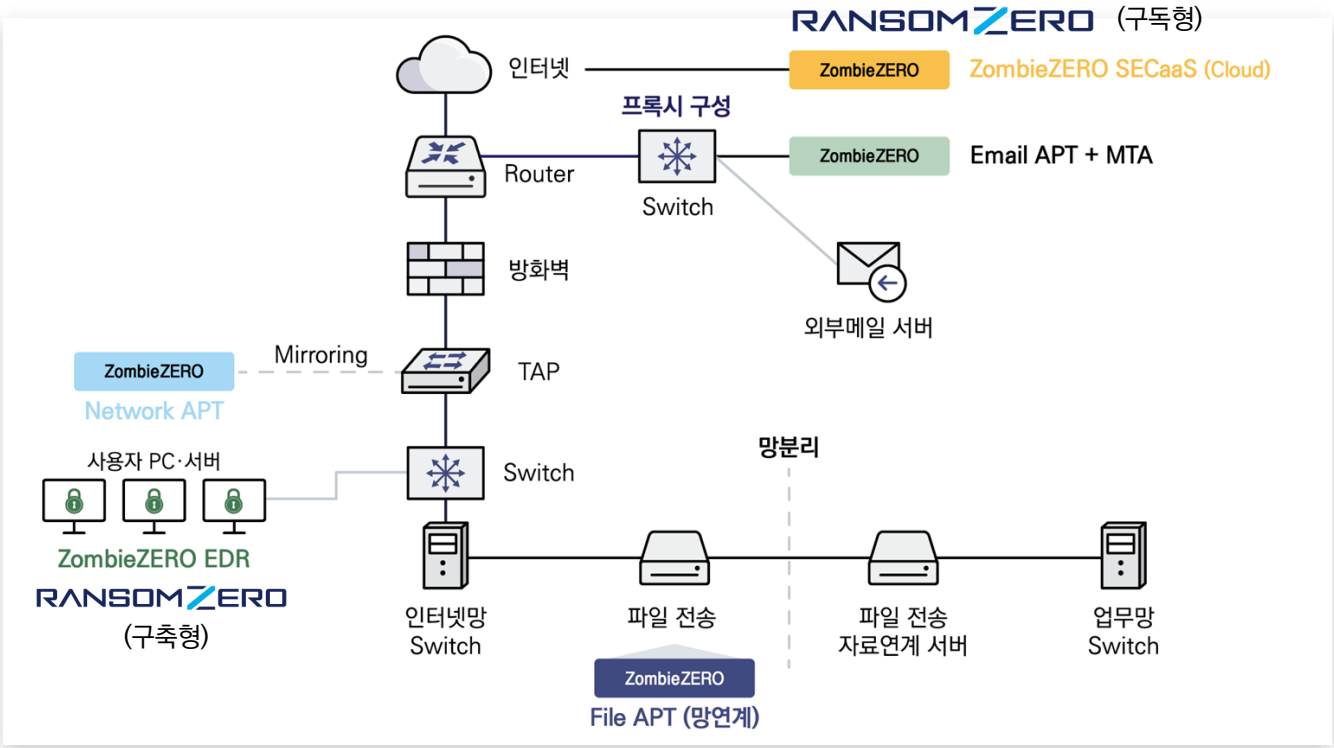
악성코드가 유입될 수 있는 다양한 경로에 솔루션 구축이 가능합니다.

APT Security

- Network APT
- Email APT
- File APT
- 통합관리 솔루션

EDR Security

- EDR
- RANSOMZERO
- SECaaS



2-1. RansomZERO 주요기능

데이터를 지키는 완벽한 방패

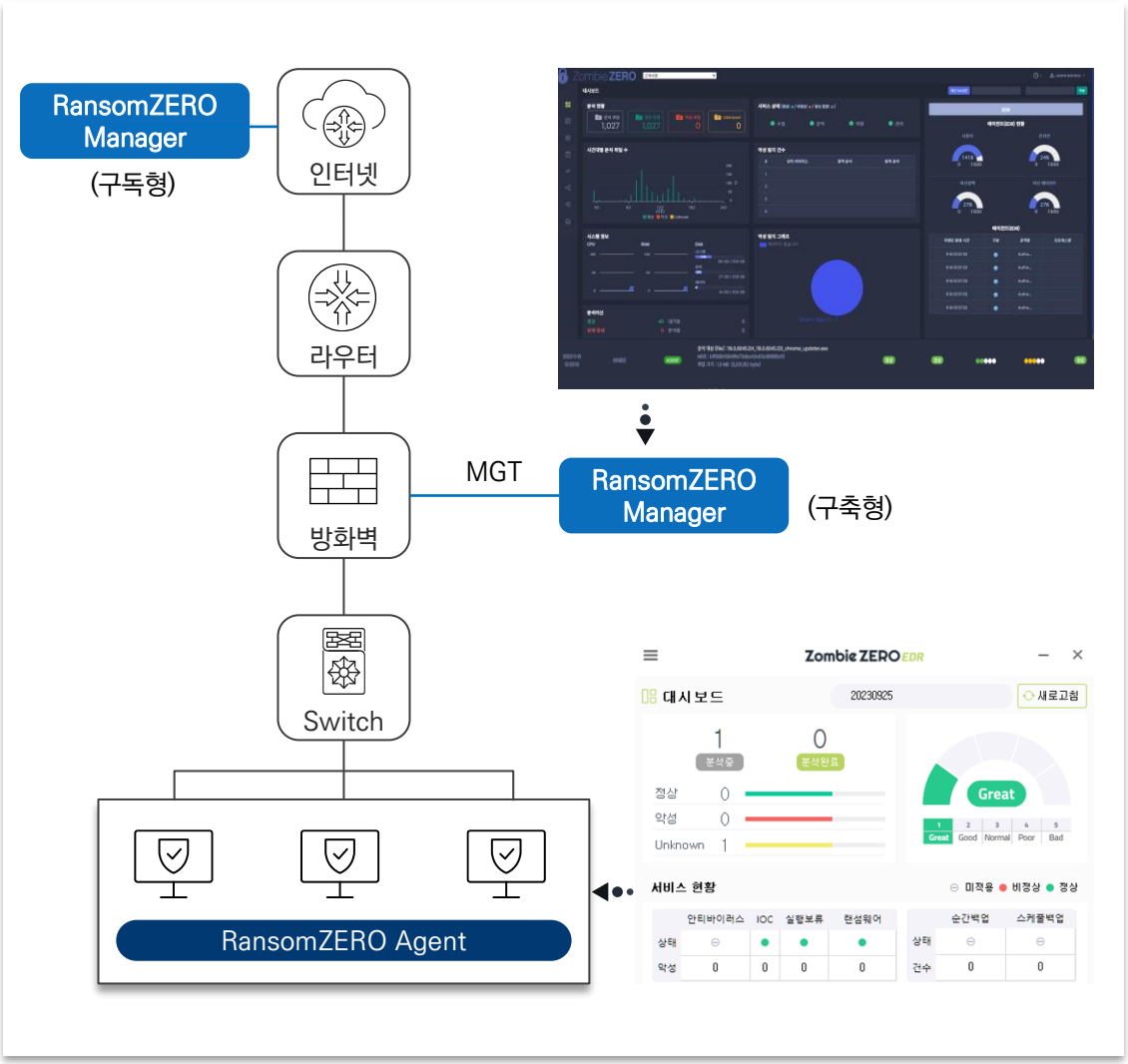
- 실행보류 (제로트러스트)
- File AI 분석
- 목록기반 블랙리스트
- AV (Bitdefender) 분석
- Yara룰 기반 정적분석

- 임계치 기반 탐지
- 더미(함정) 파일 변조 탐지
- MBR 부트영역 손상 시 탐지

- 차단, 격리, 제거
- 실시간 순간백업 (복원)
- 스케줄 백업 (복원)

- 사용자 이벤트 정보 수집
- 악성 도메인 차단
- 그레이리스트 (추적/감시)

2-2. RansomZERO 구성도



RansomZERO 분석 프로세스

랜섬웨어 사전 탐지 프로세스

- 사용자 PC에 신규 파일 유입 및 실행
- 분석 서버 (RansomZERO Manager)로 파일 업로드
- 다단계 파일 분석 (FileAI→Blacklist→AV→Yara)
- 분석 결과 정책 배포
- **정상 파일 경우 파일 실행**
  악성 파일 경우 차단 / 격리

RanzomZERO 위협대응 기능

위협(랜섬웨어 행위) 탐지

- 임계치 기반의 탐지
- MBR 부트영역 손상 탐지
- 더미 (함정) 파일 손상 탐지

실시간 모니터링

- 사용자 이벤트 정보 수집
- 악성 도메인 접속 차단 기능

위협(랜섬웨어) 대응

- 실시간 순간 백업 기능
- 스케줄 백업 기능

2-2. RansomZERO 감지 영역 및 탐지 시 대응

랜섬웨어 감지 영역

보호대상	감시영역	보호범위
문서, 중요 시스템, 이미지	로컬 디스크	로컬 디스크 드라이브(C. D 등)
	네트워크 드라이브	다른 PC에서 공유된 폴더
	이동식 디스크	연결된 외부 저장 장치(USB)
	공유 폴더	내 PC에서 제공한 공유 폴더
	MBR 부트 영역	MBR 부트 영역

랜섬웨어 탐지 시 대응

랜섬웨어 행위		대응기능
파일명 변경		파일명 변경 (파일이 격리되기 이전 경로)
파일 확장자 변경	.avi .bat .bmp .dat .doc .exe .html .hwp .iso .jpg .mid .mp3	확장자 변경 (해당파일을 실행할 수 없도록)
격리 폴더 접근		접근 통제 (격리된 파일에 접근하지 못하도록)

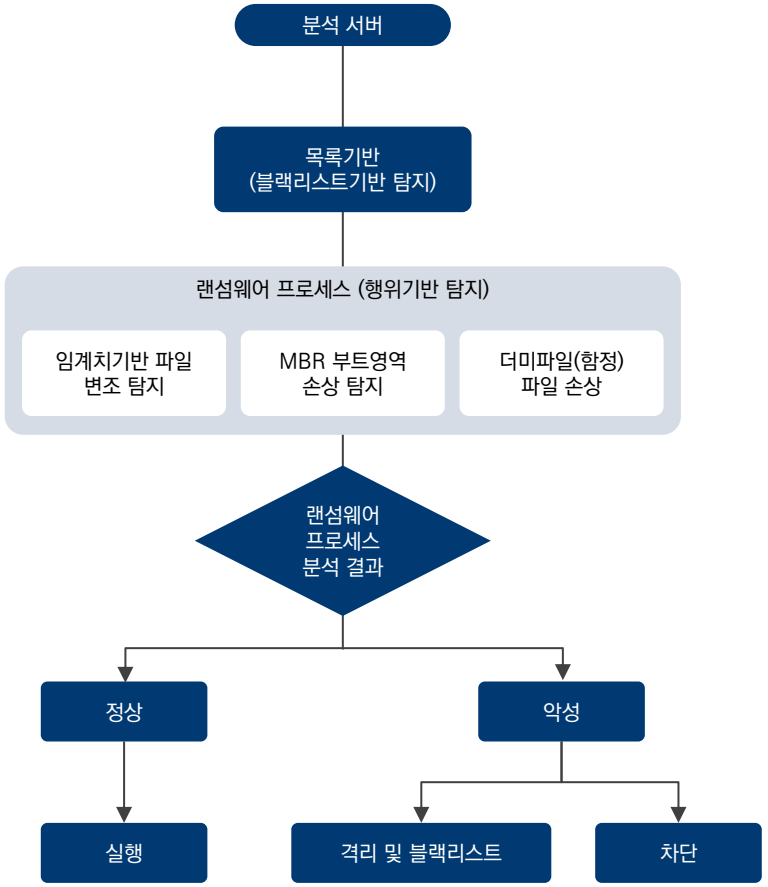
3

RamsomZERO
랜섬웨어 탐지 특화기능

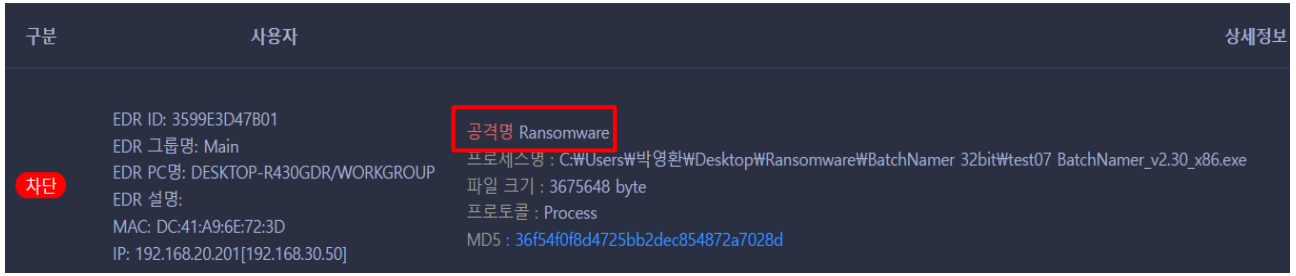
3-1. 랜섬웨어 탐지 프로세스

랜섬웨어 행위 탐지 / 차단 기술은 사용자 PC에서
실시간으로 랜섬웨어 행위를 탐지하며 차단, 파일 암호화 및 위변조에 대응하는 기술

랜섬웨어 탐지 프로세스



랜섬웨어 행위가 탐지된 에이전트 이벤트 로그



RansomZERO

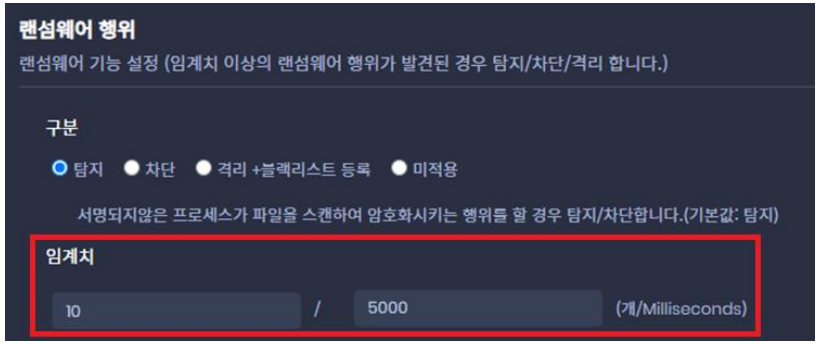
3-2. 임계치 및 더미(함정) 파일 손상 기반 랜섬웨어 행위 탐지

사용자 PC를 모니터링하여 임계치 기반으로 파일 변조/더미(함정)파일 손상 행위를 탐지하는 기술로 파일 정보의 변조 행위 발생 시 해당 프로세스를 종료하여 파일을 변조행위를 차단

사용자 PC를 모니터링하여 임계치 기반으로 파일 변조 행위를 탐지하는 기술로 파일 정보의 변조 행위 발생 시 해당 프로세스를 종료하여 파일을 변조행위를 차단

더미 파일에 대한 접근 통제 기술은 랜섬웨어에 감염되기 쉬운 파일을 시스템 여러 폴더에 저장하여 사용자가 아닌 임의의 프로세스가 접근하여 파일을 암호화하려는 순간 접근하는 프로세스를 차단

랜섬웨어 행위 탐지 임계치 설정



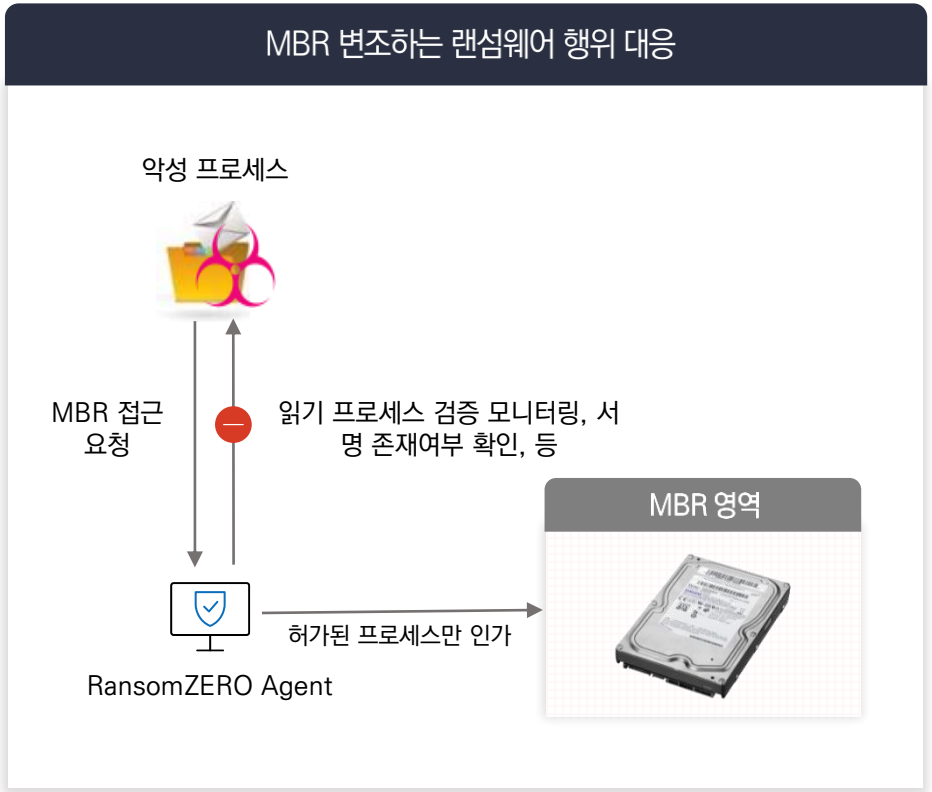
랜섬웨어 행위 탐지를 위한 더미파일

이름	수정한 날짜	유형	크기
Kjs8l8haof9v.bmp	2021-03-25 오후 2:26	BMP 파일	1KB
Kjs8l8haof9v.cell	2021-03-25 오후 2:23	CELL 파일	27KB
Kjs8l8haof9v.doc	2021-03-25 오후 2:15	Microsoft Word 9...	27KB
Kjs8l8haof9v.docm	2021-03-25 오후 2:15	Microsoft Word ...	13KB
Kjs8l8haof9v.docx	2021-03-25 오후 2:14	Microsoft Word ...	13KB
Kjs8l8haof9v.dot	2021-03-25 오후 2:14	Microsoft Word 9...	26KB
Kjs8l8haof9v.dota	2021-03-25 오후 2:14	DOTA 파일	27KB
Kjs8l8haof9v.hwp	2021-03-25 오후 2:26	한컴오피스 NEO ...	9KB
Kjs8l8haof9v.ini	2021-03-25 오후 2:26	구성 설정	1KB
Kjs8l8haof9v.jpeg	2021-03-25 오후 2:26	JPEG 파일	1KB
Kjs8l8haof9v.jpg	2021-03-25 오후 2:26	JPG 파일	1KB
Kjs8l8haof9v.pdf	2021-03-25 오후 2:25	PDF 파일	25KB
Kjs8l8haof9v.png	2021-03-25 오후 2:26	PNG 파일	1KB
Kjs8l8haof9v.ppt	2021-03-25 오후 2:17	Microsoft PowerP...	90KB
Kjs8l8haof9v.pptm	2021-03-25 오후 2:17	Microsoft PowerP...	38KB
Kjs8l8haof9v.ppts	2021-03-25 오후 2:18	PPTS 파일	87KB
Kjs8l8haof9v.pptx	2021-03-25 오후 2:17	Microsoft PowerP...	38KB
Kjs8l8haof9v.txt	2021-03-25 오후 2:26	텍스트 문서	1KB
Kjs8l8haof9v.xls	2021-03-25 오후 2:22	Microsoft Excel 9...	27KB
Kjs8l8haof9v.xlsa	2021-03-25 오후 2:23	XLSA 파일	27KB
Kjs8l8haof9v.xlsm	2021-03-25 오후 2:22	Microsoft Excel ...	10KB
Kjs8l8haof9v.xlsx	2021-03-25 오후 2:21	Microsoft Excel ...	10KB

랜섬웨어 탐지 시 알람팝업

3-3. MBR 부트영역 손상 탐지 기능

부트 영역(MBR)에 대한 접근을 통제하여 시스템 부트 영역에 Windows 시스템 / 바이오스를 제외하고 임의로 수정하려는 순간 MBR 정보를 보호하고 변경하지 못하도록 보호하는 기능



- RansomZERO Agent의 필터 드라이버는 프로세스에서 발생할 수 있는 거의 모든 동작을 모니터링하며, MBR 관련 읽기 및 쓰기 동작을 모니터링
- 감지된 동작에 대해 필터 드라이버는 콜백 함수를 통해 RansomZERO Agent 에 알리며, RansomZERO Agent는 화이트리스트에 없는 경우 해당 프로세스를 차단

* 부팅 과정에서 중요한 역할을 하는 MBR (Master Boot Record) 영역의 무결성을 감시하고, 이 영역이 손상되었거나 변조되었을 때 이를 탐지하는 보안 기능으로 필터 드라이버를 사용하여 운영 체제의 파일 시스템 계층에 위치하여 MBR과 관련된 모든 읽기 및 쓰기 작업을 필터링 및 분석하고 화이트리스트를 통해 안전한 MBR 동작을 미리 정의하여, 그 외의 모든 활동을 잠재적 위협으로 간주함

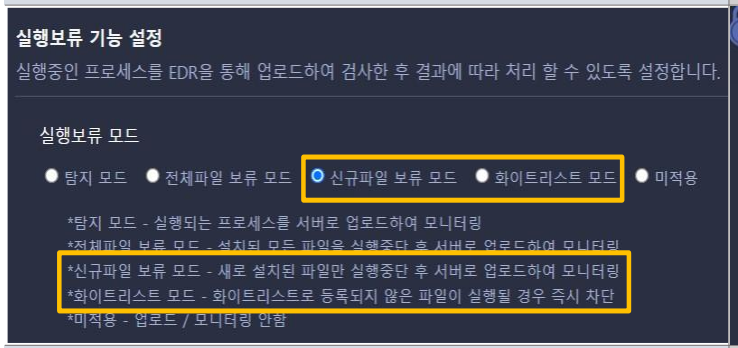
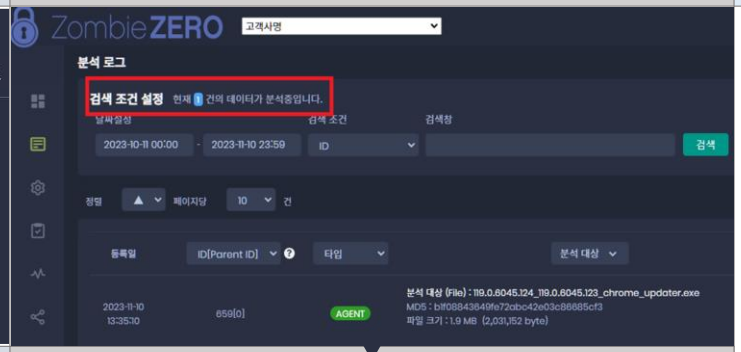
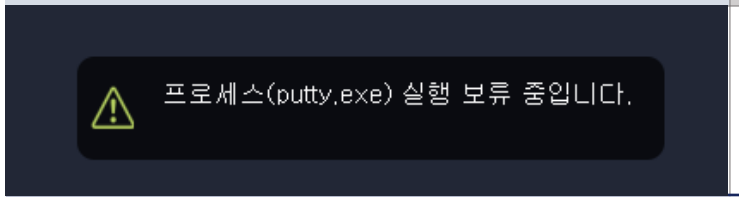
4

RamsomZERO 주요기능

4-1. ZERO Trust 기능 (실행보류)

ZERO Trust 기능은 엔드 포인트에서 파일의 실행을 잠시 보류하고,
분석 서버의 분석 결과에 따라서 실행 가능 여부를 판단

ZERO Trust 란 '절대 믿지 말고 항상 검증하라(Never Trust, Always Verify)'는 원칙을 기반으로, 모든 접속을 경계하고 체계적 확인 절차를 거치는 보안 모델

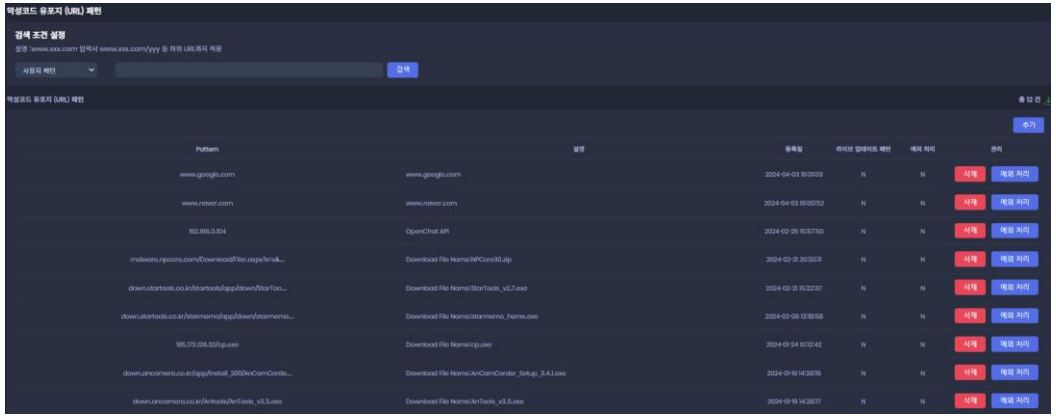
ZERO Trust(실행보류) 기술	실행보류 후 서버에서 분석 진행	보안 패러다임에 따른 ZERO Trust 정부 지원 예정
		**정부가 지원 나선 '제로트러스트' 보안… 기업들도 합종연횡** 美·日·英, 정부가 앞장서 '제로트러스트' 강조 IT 시스템 각각 영역 분리·보호 KOZETA 회원사 50곳 넘어
프로세스 ZERO Trust(실행보류) 기능	분석 결과	
	• 분석결과 정상 : 파일 실행 • 분석결과 악성 : 관리자 정책에 따라 차단, 격리, 삭제	

4-2. 악성 도메인 접속 차단 기능

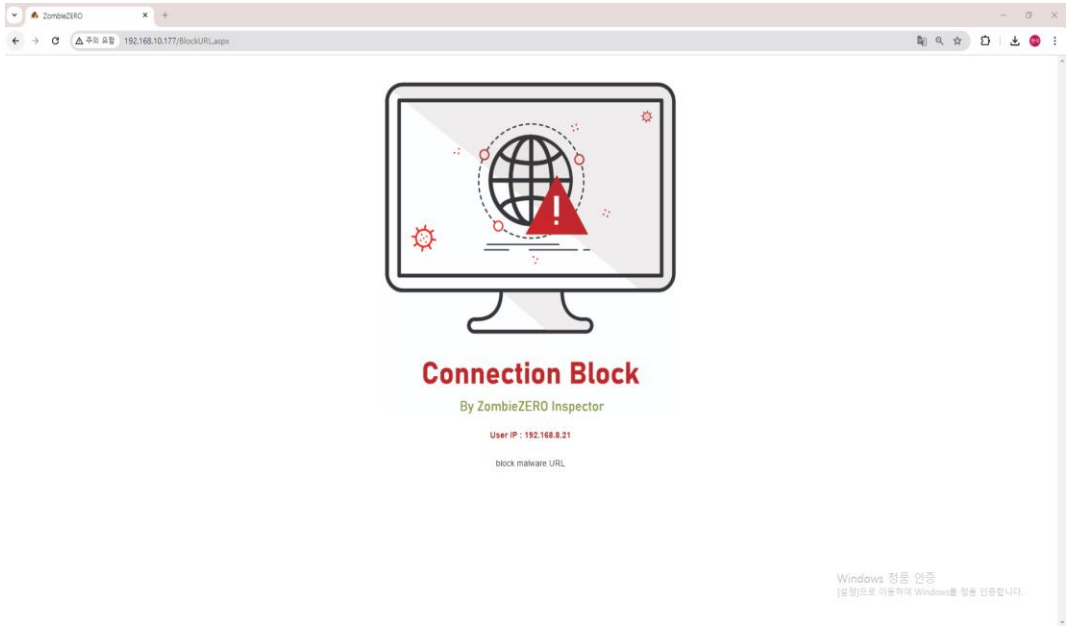
악성코드 유포지, C&C 등 유해 사이트에 접속하려고 하는 경우 연결된 네트워크 세션 정보를 강제로 해제하여 접속을 차단

C&C 처리 설정 기능

악성코드 유포지 패턴 추가 기능

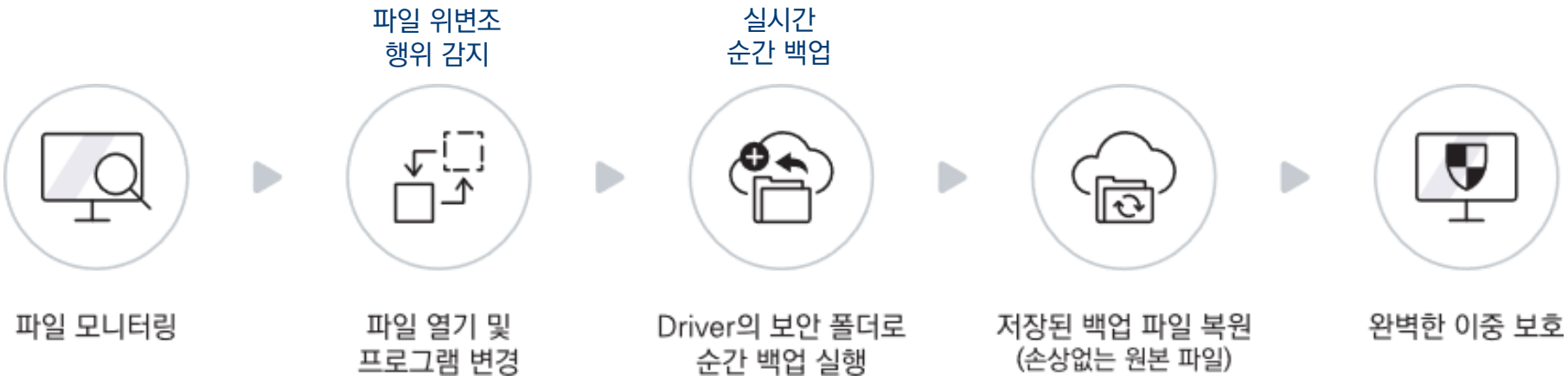


악성코드 유포지 URL/IP 접속 시 리다이렉트 URL으로 이동



4-3. 순간 백업 기능 1

실시간 순간 백업



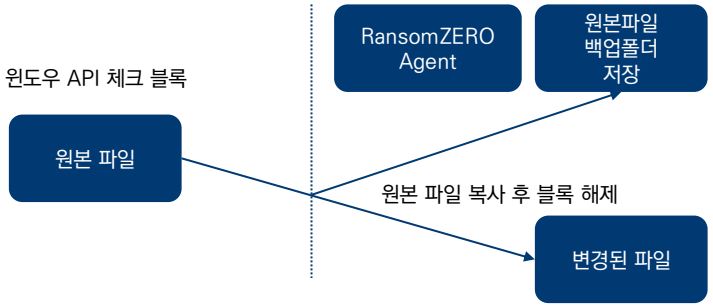
RansomZERO는 랜섬웨어 대응 보안솔루션 이지만,
순간 백업 기능을 통하여 더욱 완벽한 정보 보안을 제공함

4-3. 순간 백업 기능 2

엔드포인트 구간의 APT 공격 대응 기술

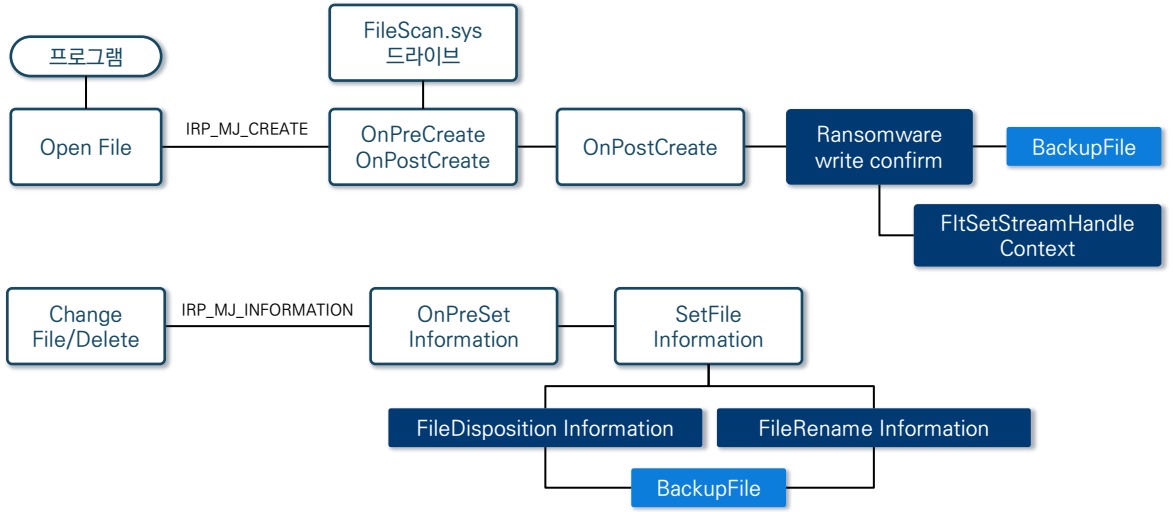
순간백업 기술

〉순간 백업 로직



이러한 과정이
순식간에 발생됨

파일이 새롭게 저장/변경 될 시 RansomZERO Agent가 커널단에서 윈도우 Write API를 체크해서 (커널반응은 어플리케이션보다 빠름) 변경되는 시점에 잠시 파일 변경되는 것을 블록 그 다음, 원본 파일을 Rans 백업 폴더에 저장 그 후 블록 된 Write API를 해제시켜 변경된 파일로 저장



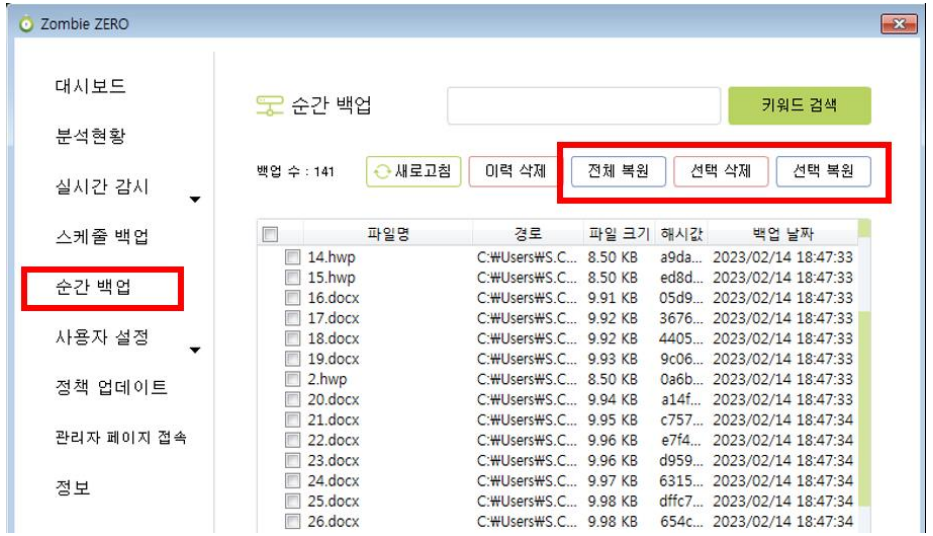
4-3. 순간 백업 기능 3

엔드포인트 구간의 APT 공격 대응 기술

제로트 러스트 보안 기술 + 랜섬웨어 대응 기술 + 순간백업 기술

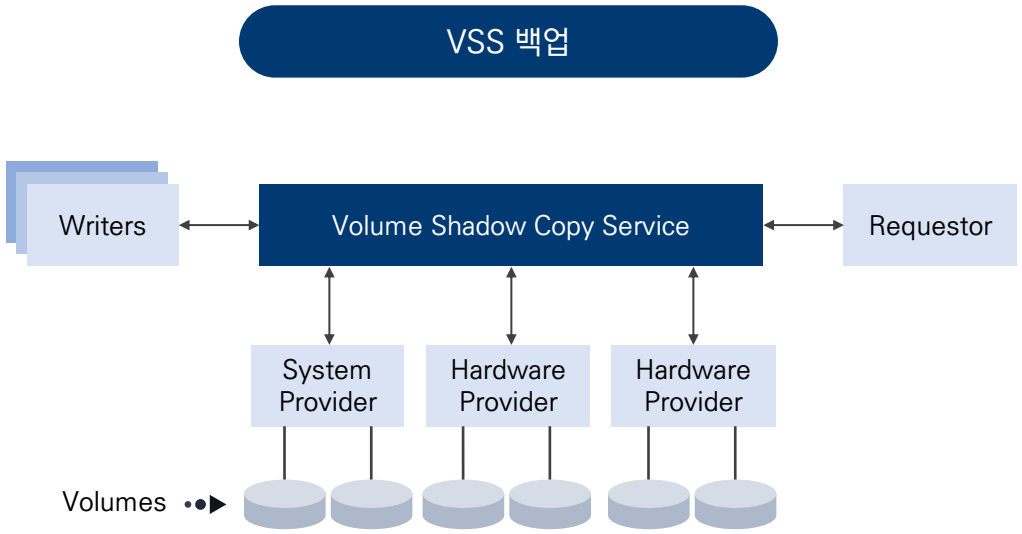
랜섬웨어 대응

순간백업



4-3. 순간 백업 기능 4

경쟁사의 경우 Snapshot Type of “VSS” 백업 기능 사용



VSS (Volume Shadow Copy Service) :
과거 특정 시점으로 복원 시켜주는 스냅샷 기술

경쟁기술 특징

- 특정 시점으로 시스템 전체를 복원
- 백업된 시점의 완벽한 복구가 가능
- 백업 주기가 존재 (시간, 일)

경쟁기술 단점

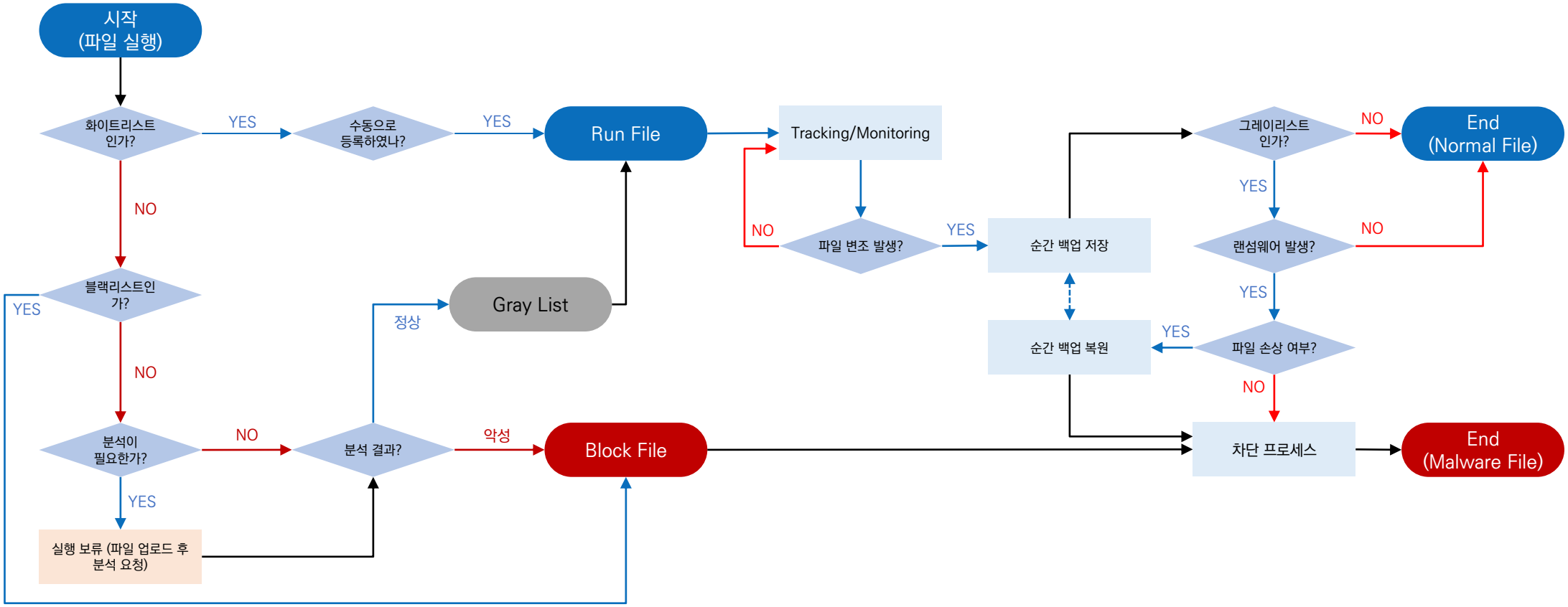
- 백업 이전의 파괴된 파일은 복구 불가능
- 백업 이미지 (스냅샷)에 대한 많은 용량 필요
- 백업 이미지에 대한 직접적인 공격으로 손상 발생시 복구 불가능

SentinelOne Symantec

19

4-4. 그레이리스트 기능

특정 조건에서만 동작하는 악성 코드와 발전하는 APT 공격에 대응하기 위해, 그레이리스트 기능으로 의심스러운 파일을 지속적인 행위 모니터링(추적•감시)하고 악성행위 발생 시 차단하며, 순간 백업 기능으로 시스템을 즉시 복구하는 완벽한 대응 솔루션을 구현



4-6. 실시간 모니터링 기능 (추가 기능)

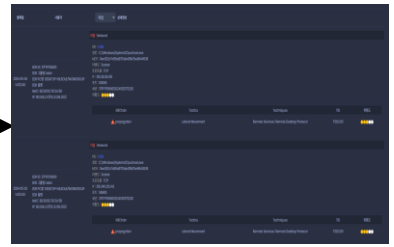
엔드포인트(PC, 서버 등)에서 발생하는 악성 활동을
실시간으로 탐지하고 분석하여 이에 대한 대응 조치를 취하는 하는 기능을 제공

실행 중 파일 / 프로세스

행위로그

랜섬웨어 유사 행위
프로세스

이벤트 로그



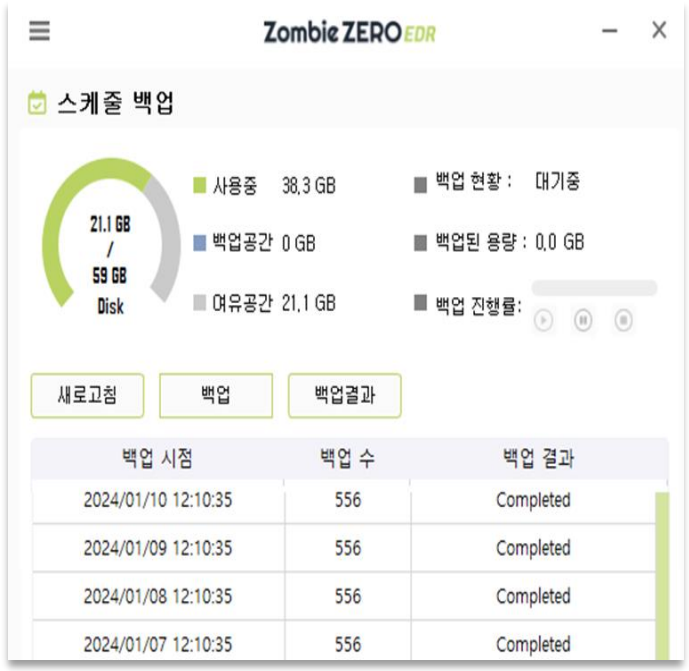
실시간 모니터링

대응 조치

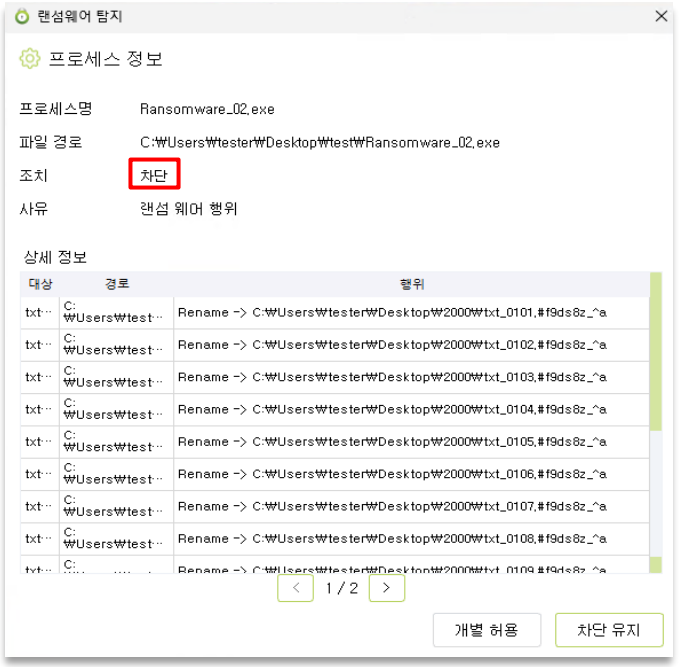
4-7. 랜섬웨어 대응 조치

엔드포인트에서 위협이 탐지가 되면 이에 대응하기 위해서 스케줄 백업 기능과 프로세스 차단 및 파일 격리를 통한 대응

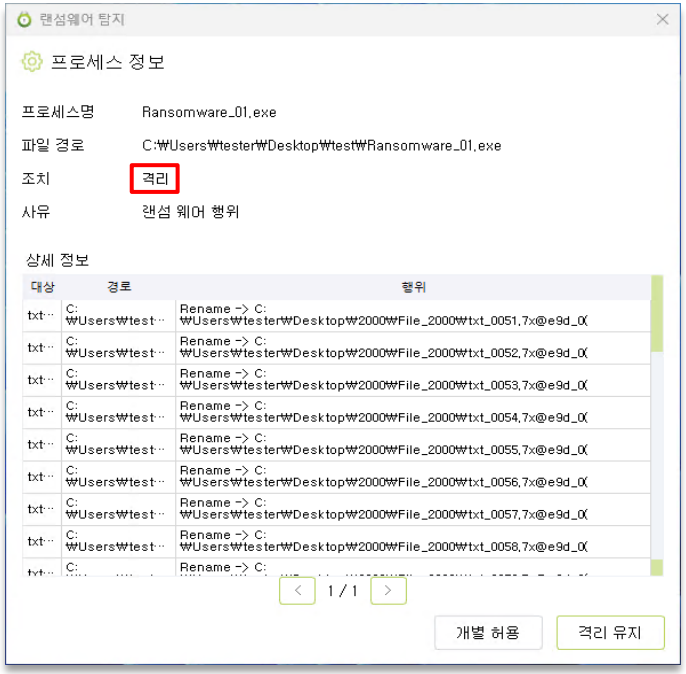
스케쥴 백업 기능



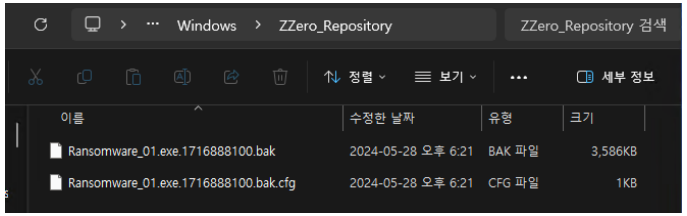
프로세스 차단



악성파일 격리



지정된 폴더로 실행 방지 처리 후 격리



5

RamsomZERO FILE AI 기능

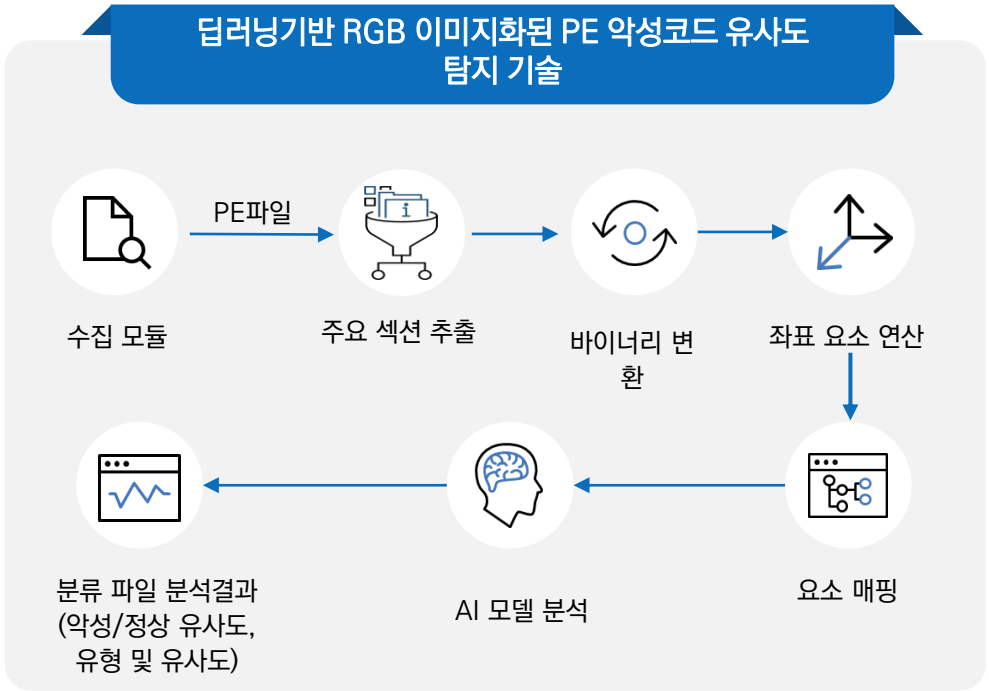
2-3-1. AI기술 적용범위 및 프로세스 – FILE AI(NET 선정기술)

FILE AI

악성코드 유사도를 기반으로 악성 또는 정상 판정 및 해당파일과 유사한 카테고리 정보 (%매칭) 제공하여 보다 진보된 악성코드 정보 제공

- 상세 내용
  - 딥러닝기반 RGB 이미지화된 PE 악성코드 유사도 탐지 기술은 네트워크와 엔드포인트에서 수집되는 정보를 RGB 이미지로 변환하여 신 변종 악성코드를 탐지하는 기술
  - 알려져 있는 Grayscale기법으로 파일을 이미지 변환하여 딥러닝을 활용하여 분석 시 크기 조절로 인해 데이터 손실이 있었으나 고정된 이미지 크기를 활용하는 신기술의 경우 딥러닝 분석 시 크기 조절을 하지 않아 데이터 손실이 없는 기술.

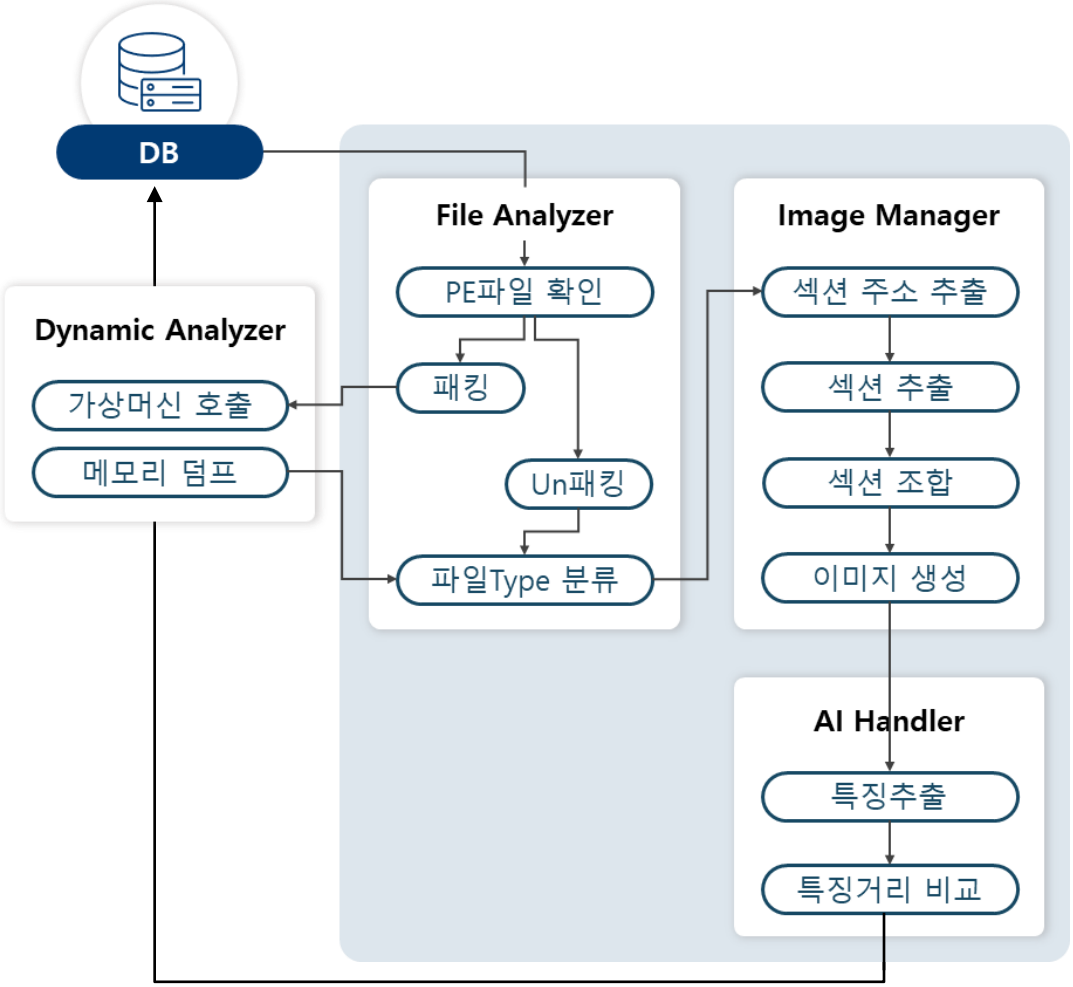
- 우수성
  - 이미지화된 데이터를 활용하여 알려진 악성코드와 동종 혹은 유사계열의 신 변종 악성코드 탐지 가능
  - 정보를 담을 수 있는 크기가 $\{0\sim2^{24}\}$로 데이터 유실이 최소화된 이미지 변환기술
  - 최소화된 자원으로 정확도 신속성을 겸비한 차세대 악성코드 분석기술
  - 98.8%이상의 정탐율 성능을 달성
  - 하나의 파일당 평균 0.06s 내의 분석시간에 따른 대량의 악성코드 분석기술



2-3-3. AI기술 적용범위 및 프로세스 – FILE AI

File AI 전체 구성도

단순 악성 유/무 뿐만 아니라 탐지한 악성코드에 대한 세부정보 제공
빠른 탐지 속도 및 정적분석 (Yara 등) 결과를 함께 제공하여 File AI만 의존하는 불안감 해소



악성코드 이미지 변환 결과 (악성유무)

악성코드 유사도 및 유형 분류 결과

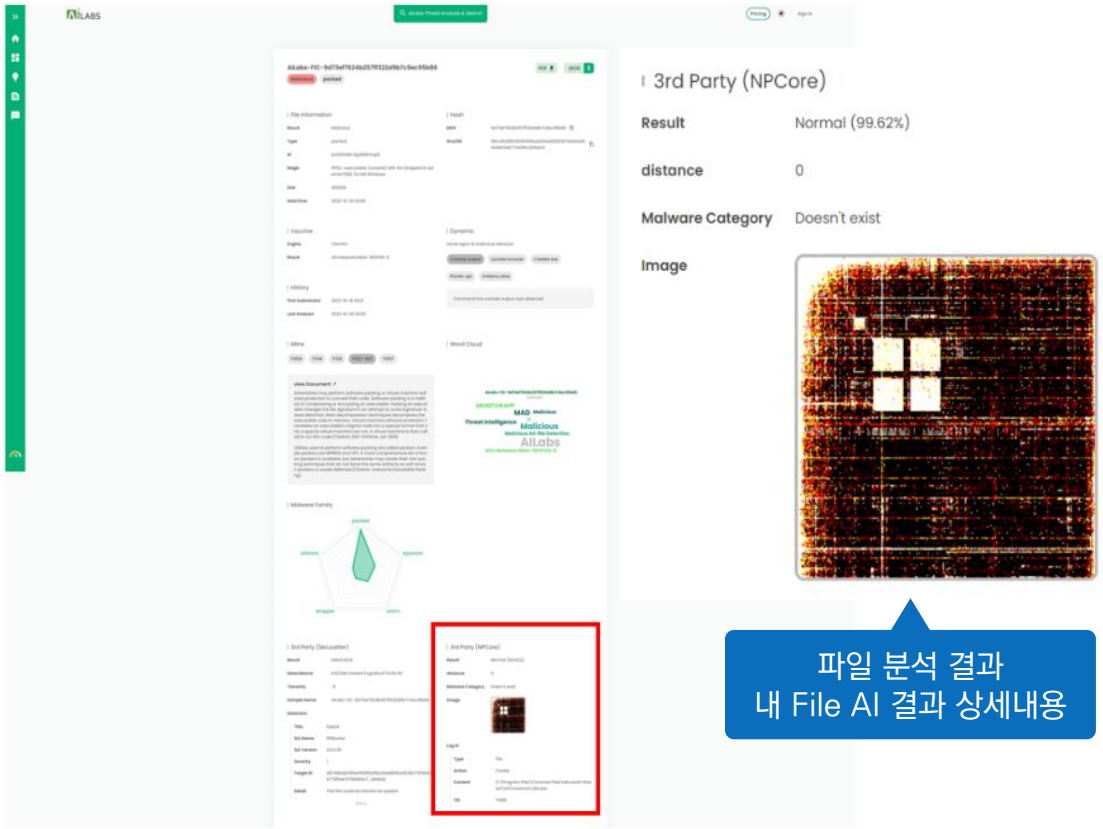
4-6. 활용된 AI기술의 차별성 및 우수성 – AI활용 악성코드 분석기술

AI를 활용한 악성코드 분석기술 차별성 및 우수성

구분	RGB채널이 포함된 이미지 변환 방식을 활용한 딥러닝 기반의 악성코드 분석기술	질감 표현 방식의 이미지를 활용한 딥러닝 기반 악성코드 탐지 기술	회색조 채널 이미지를 활용한 딥러닝 기반 악성코드 탐지 기술
적용 알고리즘	[Self Attention]계열 Vision Transformer	[CNN]계열 ResNet, VGG19 등	[CNN]계열 ResNet, VGG19 등
악성코드 분석시간	0.06초 이하	0.1초	0.1초
악성코드 유사도 탐지	97.2%	ResNet (82.03%) VGG19 (91.3%)	ResNet (82.03%) VGG19 (91.3%)
정상파일 오탐율	0.8%	ResNet (11.8%) VGG19 (11.0%)	ResNet (11.8%) VGG19 (11.0%)
F1-Score	99.002%	ResNet (90.09%), VGG19 (91.002%)	ResNet (90.09%), VGG19 (91.002%)
우회형 악성코드 탐지	가능	가능	가능
유사도기반 위협유형 탐지	95.3%	X	X
패킹된 악성파일 탐지 기술	가능 (메모리에 올라간 프로세스 덤프를 활용)	X	X
테스트 환경	동일한 학습 데이터 셋 활용 동일한 성능평가 테스트 셋 활용		

2-3-21. File AI와 CTIP와 연동 구축사례

File AI 연동



파일 분석 결과
내 File AI 결과 상세내용

타 보안제품과 File AI 연동

기존 CTIP 정적 분석과 동적기반 분석 모듈에 머신러닝 기반 AI모듈 적용하여 분석 결과 추가 연동

기존 머신러닝 알고리즘에 이미지 기반 분석기법을 적용을 통해 유사도 분석과 유사유형코드를 분석하고 분석 결과를 기반으로 유사성 근거 도출

File AI 분석 결과를 기존 CTIP 내 파일분석(MAD) 결과의 상세로그 화면에 API 기반 연동을 통해 구현(Third-party)

Thank YOU

A specialized in AI-based solutions for combating new and evolving Malware and Ransomware.

RANSOMZERO