Ransome DMZ PRO

랜섬디엠지 프로

비트라커 및 해킹형 랜섬웨어 대응 어플라이언스

ANTI RANSOMEWARE / DATA SECURITY SOLUTION

(주) 씨엠테스 기술사 사무소

INDEX

01 제안 배경

02 랜섬디엠지 프로 소개

03 주요 레퍼런스

04 회사 소개

제안 배경

- ☐ 랜섬웨어 위험성
- ☐ 랜섬웨어 최신 트랜드
- ☐ 랜섬디엠지 프로 솔루션 필요성

1. 제안배경

랜섬웨어 위험성

랜섬웨어는 데이터를 암호화한 후 돈을 요구하는 악성 프로그램 입니다
기업 및 기관에서 데이터가 핵심 자산인 만큼 랜섬웨어 감염은 금전 손실은 물론 업무중단 같은 비즈니스 연속성 문제,
기업 신뢰도 추락 및 개인정보 유출 같은 심각한 위험성을 추가로 내포하고 있어 대비가 반드시 필요합니다

경제적 손실

중요 데이터 복구비용이 발생,
막대한 금전적 손실을 입음

중요 정보의 유출과 2차 피해

기업 데이터 및 개인정보가 유출되
어 직접적 금전손실외에 2차 피해
발생이 유력

기업의 업무 연속성 중단

기업내 데이터 손실 뿐만 아니라
업무 중단으로 비즈니스 연속성
이슈 발생

기업 대외 신인도 추락

기업의 대외 이미지 및
운영 안정성에 대한 신뢰도가
하락하여 경영 안정성 하락

기업내 정보보호 체계의 붕괴

기업내 운영중인 시스템의
정보관리, 보호체계에 대한
불신으로 정보운영의 한계도출

1. 제안배경

랜섬웨어 최신 트랜드 (1)

초기 랜섬웨어는 시스템에 단순 바이러스를 유포, 설치해 데이터를 암호화하고 금전을 요구하는 방식이었으나
현재는 APT기반 해킹 공격을 통해 시스템 관리자 권한을 획득 한 뒤 백신을 무력화하고
백업 데이터 영역을 포맷하거나 비트라커로 잠그는 등 점점 지능화, 고도화 되고 있습니다

비트라커 출현과 성행

윈도우 자체 기능인Bit Locker를
활용하여 볼륨을 암호화하고 금품요구

백업 데이터의 삭제와 디스크 포맷

NAS서버 등의 스토리지에 저장된 데이터를
삭제하고 볼륨을 포맷하는 방식으로 진화

해킹기반 기업내 전체 시스템 공격

기업내 시스템을 해킹해 관리자 권한을
얻은 후 서버, 스토리지, PC를 동시 공격

백신 및 탐지 기반 보안 솔루션의 무력화

백신같은 보안솔루션을 탐지해 기능을
중지 또는 삭제한 후 랜섬웨어 공격

네트워크 동시 감염과 정보 유출

기업내 전체 시스템을 공격하며 개인정보
또는 기밀정보를 유출할 가능성 상승

1. 제안배경 랜섬웨어 최신 트랜드 (2)

✔서비스형 랜섬웨어(RaaS)
LockBit 4.0, Akira, Clop 등의 RaaS 모델 확산
데이터 탈취 및 다중 갈취 공격 지원, 비전문가도 쉽게 유포 가능

✔ 백업 서버 무력화
백업 소프트웨어 취약점 악용 및 데이터 변조
백업 파일 암호화, 스냅샷 삭제

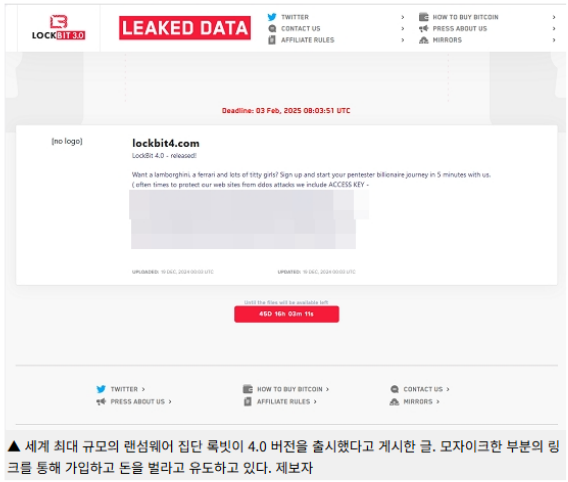
✔ 비트라커를 이용한 암호화
윈도우 내장 기능인 BitLocker 를 이용하여 드라이브 암호화함
백신으로 대응 불가

'록빗 4.0' 출시… 신인도 회복 나섰나

올해 2월 검거된 록빗… 다시 사이트 열었지만 신인도 추락
"4.0 버전 출시해 신인도 반등 노렸을 듯… 공격 기능 고도화"
록빗 4.0, 맞춤형 랜섬웨어·흔적 삭제·탐지 방해 등 탑재 예상

김기찬 기자 기자페이지 +

입력 2024-12-23 14:14:06



▲ 세계 최대 규모의 랜섬웨어 집단 록빗이 4.0 버전을 출시했다고 게시한 글. 모자이크한 부분의 링크를 통해 가입하고 돈을 벌라고 유도하고 있다. 제보자

세계 최대의 랜섬웨어 공격 집단 '록빗'(Lockbit)이 기존 버전인 3.0에서 업그레이드 한 4.0을 출시하겠다고 예고한 가운데 출시 배경과 업데이트되는 내용에 관심이 주목되고 있다.

랜섬웨어 공격자들 사이의 새로운 유행, "백업을 노려라"

입력 : 2024-04-04 14:40

요약 : 보안 외신 핵리드에 의하면 최근 랜섬웨어 공격자들 사이에서 우려되는 트렌드가 나타나고 있다고 한다. 보안 업체 소포스(Sophos)가 조사한 것인데, 바로 백업 드라이브와 자료들을 표적으로 삼고 있다는 것이다. 소포스는 최근 랜섬웨어 피해를 겪은 3천 명 이상의 IT 전문가들을 조사해서 이와 같은 트렌드를 파악할 수 있었다고 하는데, 지역과 산업을 불문하고 '백업을 공략한다'는 흐름이 나타나고 있다고 경고했다.

윈도우 서버 운영체제 '비트로커' 기능 악용해 데이터베이스 암호화 사례 등장
정상적인 암호화 기능인 만큼 랜섬웨어 대응 솔루션도 우회 가능해

[보안뉴스 이상우 기자] 랜섬웨어(Ransomware)는 이름처럼 사용자나 기업의 '파일'을 인질로 잡고 '몸값(Ransom)'을 요구하는 악성 소프트웨어를 말한다. 사용자 PC의 모든 데이터를 암호화한 뒤 사용하지 못하게 하고, 이 파일을 다시 사용하고 싶으면 일정 비용을 공격자에게 지불하라고 협박하는 것이다.

국내에서는 대형 커뮤니티 플래시 광고 취약점을 통해 일반 사용자에게 랜섬웨어가 유포되며 알려졌고, 최근에는 메이즈(Maze)라는 이름의 해킹 조직이 핸섬웨어 공격 및 해킹으로 유출한 자료를 일반에 공개하겠다고 협박하며 유명세를 타기도 했다.

랜섬웨어의 감염 경로와 공격방식은 계속해서 다양해지며 점점 진화하고 있습니다

1. 제안배경 랜섬디엠지 프로 솔루션의 필요성

백신 제품
랜섬웨어 정보를 엔진에 탑재하여 차단하는 방식으로 신종 변종에 대응한계

방화벽 제품
네트워크 보안제품으로 데이터보안에 한계

해킹 대응 한계
데이터 보존용 솔루션 부재

백업 제품
최근 백업데이터를 삭제 및 포맷하는 랜섬웨어 증가로 한계

기존 보안제품은
예방과 탐지 중심의 대응으로
신종 변종 랜섬웨어와 해킹에 취약

해결 방법은 ?

- 소프트웨어 방식의 한계를 극복한 **펌웨어** 기반의 랜섬웨어 대응 솔루션
- 관리자 권한이 **해킹되어도 중요 데이터를 보존**할 수 있는 보안백업 솔루션

솔루션 소개

- ☐ 랜섬디엠지 프로 솔루션 소개
- ☐ 주요 기능 상세
- ☐ 시스템 구성도
- ☐ 타사 솔루션 비교

2. 솔루션 소개 랜섬디엠지 프로 솔루션

랜섬디엠지 프로 솔루션은 나스서버, DB서버를 비롯한
기업내 운영중인 **중요 데이터를 해커와 비트라커, 랜섬웨어로부터 완벽히 보호하는 안전솔루션** 입니다

자동 보안백업후 접근제어, 비트라커 공격차단, 해킹방지, 원격데스크탑 기반 데이터전송 불가,
스크립트 실행 차단, 시스템 관리 구성요소의 접근권한 관리, 관리자 계정 보호기능 등을 제공하여
완벽하게 **해킹과 신종 변종 랜섬웨어, 비트라커 공격에 대응**이 가능한 제품입니다

랜섬디엠지 프로

2. 솔루션 소개

랜섬디엠지 프로 주요 기능

신종 변종 랜섬웨어 대응

특허받은 펌웨어 기술을 적용
소프트웨어적 한계점 극복

보호볼륨 데이터 실행 불가

보호된 볼륨 내에서는
랜섬웨어뿐 아니라
응용프로그램실행 불가

비트라커 공격 예방

보안 어플라이언스내
비트라커 구동 불가 및
스크립트 차단

다양한 백업방식 제공

풀, 증분, 차등의 보안 백업과
자동 복구기능 제공

백업 데이터 유출 방지

전용 브라우저를
통해서만 액세스 가능
접근제어 및 유출 방지

포맷 및 삭제 방지

관리자 권한 탈취 후에도
볼륨 포맷 또는 삭제 불가능

시스템 봉쇄

키보드, 마우스 제어기능
원격 공격 무력화, 스크립트,
파일전송 차단 등

자동화 보안백업

중요 데이터를 자동으로
백업하고 필요에 따라
소산백업 구성 가능

2. 솔루션 소개 랜섬디엠지 프로 기능 상세 (1)

신종 변종 랜섬웨어 대응

✔ 특허받은 펌웨어 기술을 적용
소프트웨어적 한계점 극복

랜섬디엠지 프로는
펌웨어 기반의 저장기술을 접목한 제품으로
기존 소프트웨어 방식 솔루션들의 보안취약점을 극복해
보안백업과 암호화 방지, 해킹 방지 등을 제공함으로써
신종, 변종 랜섬웨어로부터 안전하게 데이터를 보호할 수 있습니다

기존의 소프트웨어기반 방식의 보안솔루션들은
관리자 권한 획득후 감시기능을 끄거나 프로그램을
제거하는 방식으로 무력화 또는 우회가 가능합니다
랜섬디엠지 프로는
특허받은 펌웨어기반 비가시성 볼륨기술을 접목하여
보다 안전한 데이터 세상을 제공합니다

특 허 증
CERTIFICATE OF PATENT

특 허 제 10-1008939 호
(PATENT NUMBER)

발명의명칭 (TITLE OF THE INVENTION)
펌웨어기반 데이터

특허권자 (PATENTEE)

발명자 (INVENTOR)

위의 발명은 「특허법」에
되었음을 증명합니다.
(THIS IS TO CERTIFY THAT THE PATENT IS I
INTELLECTUAL PROPERTY OFFICE.)

특허증
CERTIFICATE OF PATENT

특허 Patent Number 제 10-1713034 호
출원번호 Application Number 제 10-2016-0066264 호
출원일 Filing Date 2016년 05월 30일
등록일 Registration Date 2017년 02월 28일

발명의 명칭 Title of the Invention
비가시성 가상볼륨을 이용한 서버 이중화 시스템

특허권자 Patentee
주식회사 씨엠테스(110111-*******)

발명자 Inventor
주낙완
서울특별시 동작구 등용로

위의 발명은 「특허법」에 따라 특허등록원부에 등록되었음을 증명합니다.
This is to certify that, in accordance with the Patent Act, a patent for the invention has been registered at the Korean Intellectual Property Office.

2017년 02월 28일

특허청
Korean Intellectual Property Office

특허청장
COMMISSIONER,
KOREAN INTELLECTUAL PROPERTY OFFICE
최 동 규

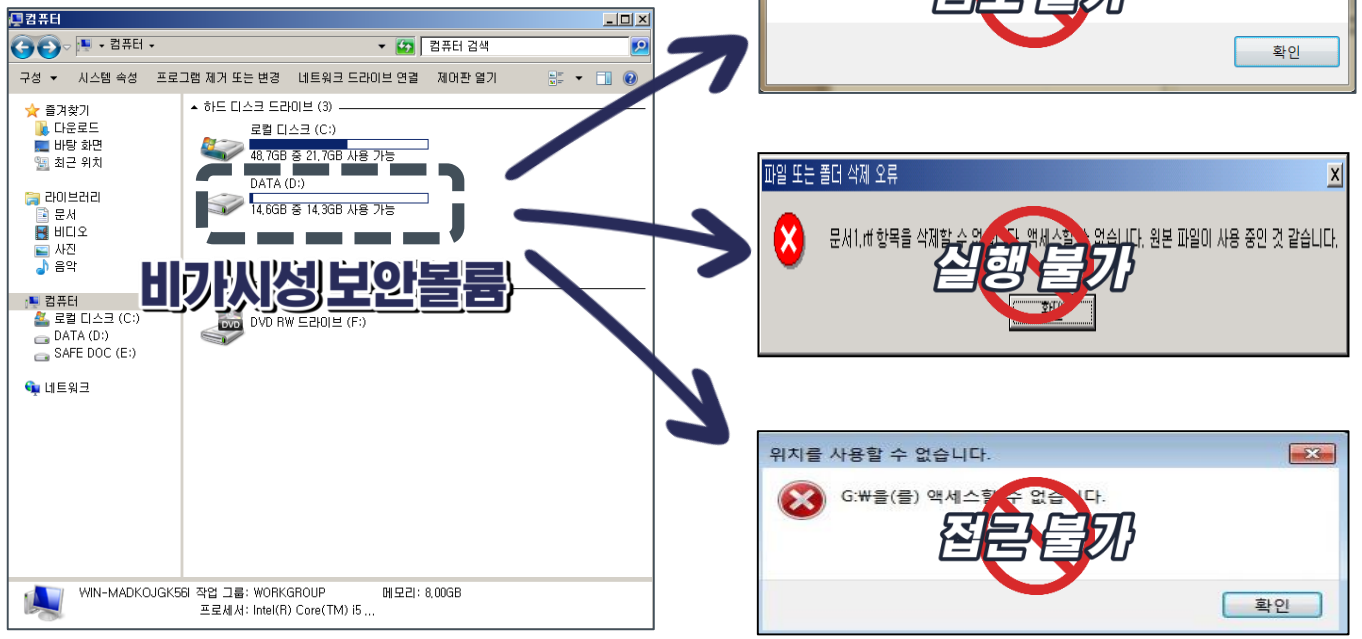
랜섬디엠지 프로 기능 상세 (2)

보호볼륨 데이터 실행 불가

✔ 보호된 볼륨 내에서는
랜섬웨어뿐 아니라 응용프로그램실행 불가

랜섬디엠지 프로는
특허기술인 데이터 실행 및
위변조 방지 기술과
스텔스 저장 기술을 접목하여
보호된 볼륨의 저장데이터는
디바이스 영역에서 접근이
불가하도록 설계되어 있습니다.

또한 보호된 영역에서는 실행 파일 및
스크립트의 실행도 불가능하게
고도화된 보안기술을 적용했습니다



2. 솔루션 소개 랜섬디엠지 프로 기능 상세 (3)

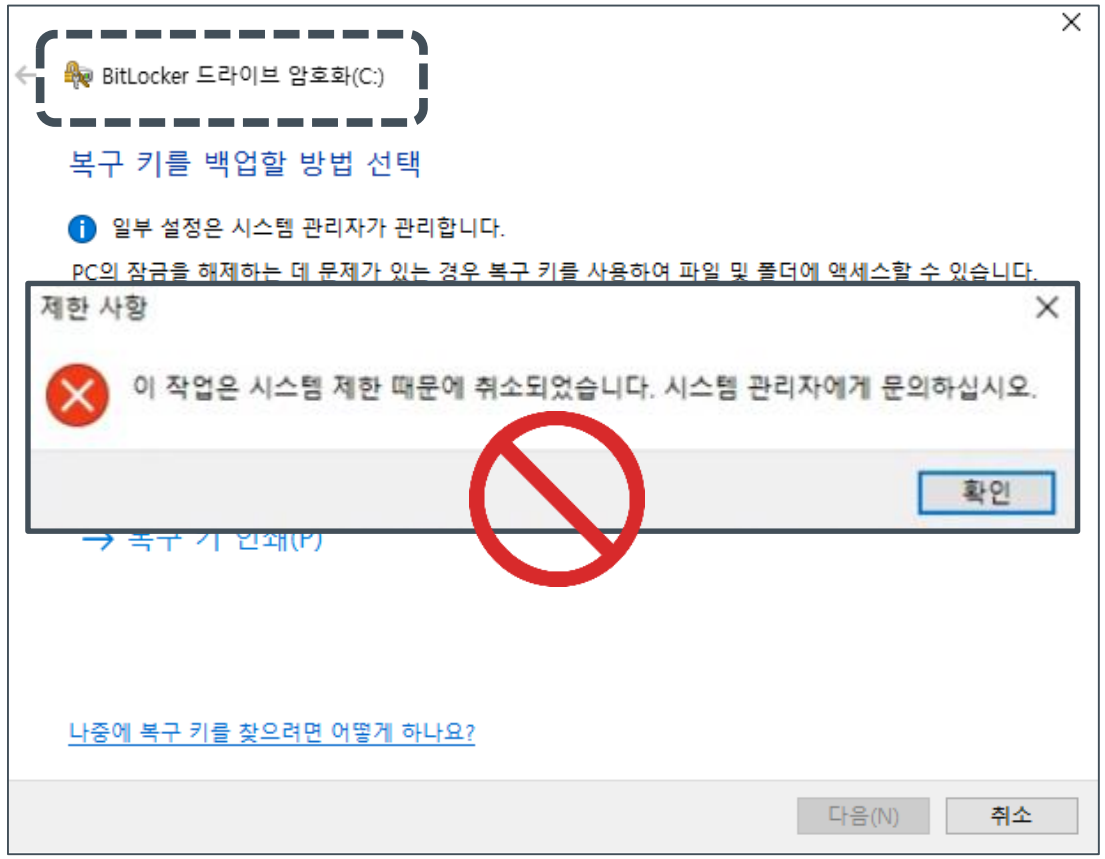
비트라커 공격 예방

✔ 보안 어플라이언스내
비트라커 구동 불가 및 스크립트 차단

랜섬디엠지 프로는
최근 급증하는 비트라커 공격을 방어할 수 있습니다

비트라커 공격은 해커가 관리자 권한을 얻은후
윈도우 내장 기능인 BitLocker를 이용하여
데이터가 저장된 드라이브를 암호화 하고
비트코인을 요구하는 기법으로 최근
중규모 이상의 기업에서 많은 피해를 입고 있습니다

랜섬디엠지 프로 솔루션에서는
비트라커 잠금을 차단하는 기능을 제공하고 있기 때문에
이를사전에 예방할 수 있습니다



랜섬디엠지 프로 기능 상세 (4)

다양한 백업방식 제공

✔ 풀, 증분, 차등의 보안 백업과
자동 복구기능 제공

랜섬디엠지 프로는 기업내 NAS서버,
웹서버, DB서버 등 중요 시스템의 데이터를
자동으로 백업하고 복구하는 기능을 제공합니다

파일백업, OS백업, 폴더백업 등
백업대상을 자유롭게 선택할 수 있고
풀, 증분, 차등으로 백업방식도 다양하게 지원합니다

필요에 따라 원격지 소산백업 구성도 가능합니다

랜섬디엠지 프로 기능 상세 (5)

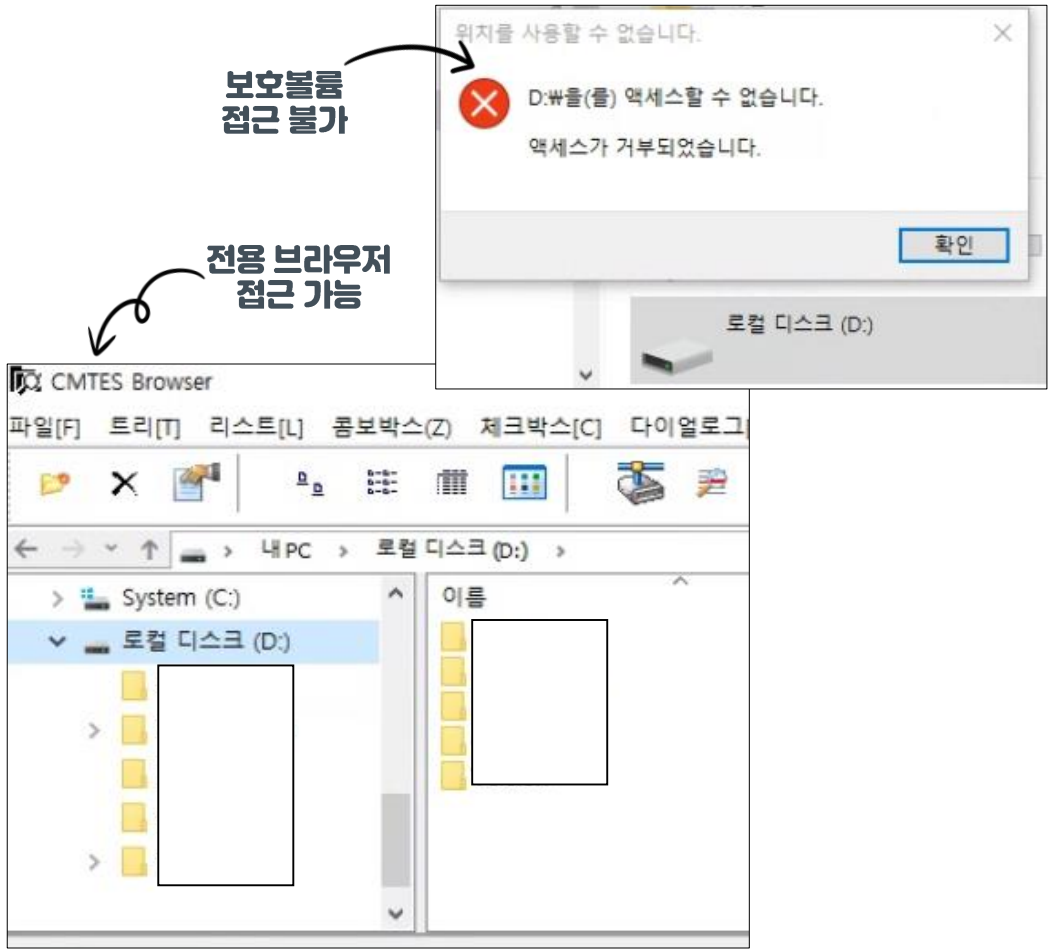
백업 데이터 유출 방지

✔ 전용 브라우저를 통해서만 액세스 가능
접근제어 및 유출 방지

랜섬디엠지 프로는 보호된 영역에 접근시 씨엠테스에서 제공하는 전용 브라우저를 통해서만 액세스 가능합니다

또한 별도의 관리자 권한이 있는 관계자 외에는
보호된 영역에 접근 할 수 없게 접근제어 기능과
이를 통한 유출 방지 기능을 제공하고 있습니다

이를 통해 보다 안전한 데이터 저장과
복구기능을 지원합니다.



랜섬디엠지 프로 기능 상세 (6)

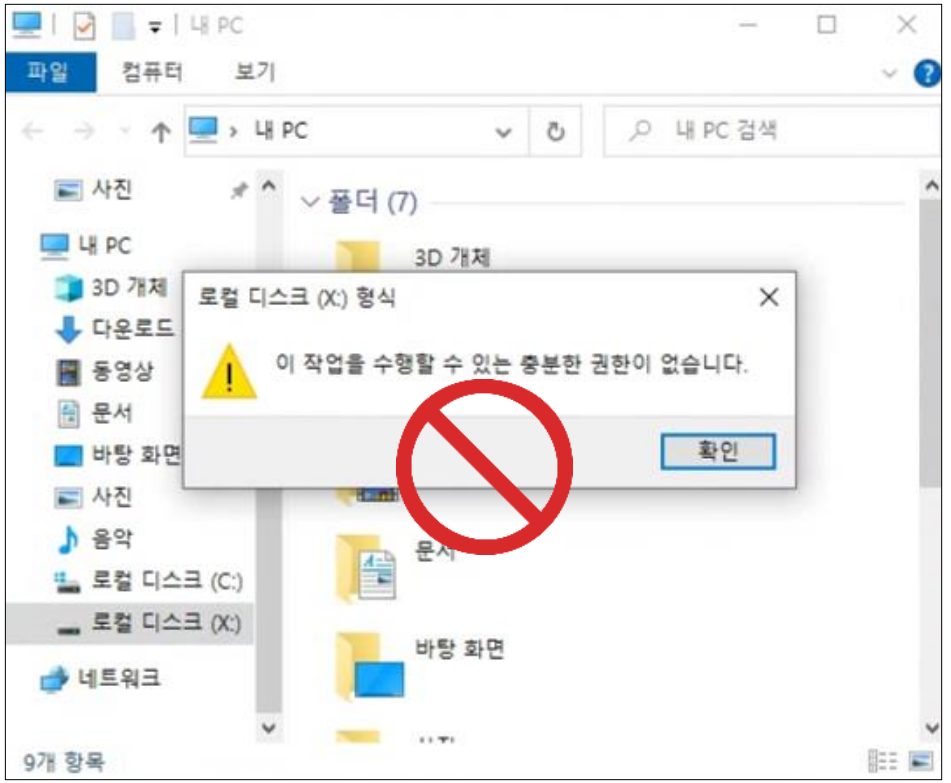
포맷 및 삭제 방지

✔ 관리자 권한 탈취후에도
볼륨 포맷 또는 삭제 불가능

랜섬디엠지 프로는 보호된 볼륨은 볼륨 전체를
포맷하거나 삭제 할 수 없도록 설계 되어
데이터는 금고 형태로 안전하게 보호 됩니다

해커에 의해서 발생하는 데이터 파괴형
사이버 공격인 포맷 공격에도 대응할 수 있습니다

뿐만아니라 볼륨을 삭제하거나
디스크 파티션, 레이드를 변경하지 못하도록
보호하는 기능까지도 탑재되어 있습니다.
심지어 관리자의 실수로 인한 포맷도 예방이 가능합니다



랜섬디엠지 프로 기능 상세 (7)

시스템 봉쇄

✔ 키보드, 마우스 제어기능.
원격 공격 무력화, 스크립트, 파일전송 차단 등

랜섬디엠지 프로는 시스템 계정이 탈취되더라도
시스템 봉쇄 기능으로 해킹을 차단하는 기능을 제공합니다

키보드, 마우스 제어권에서 부터 CMD 명령어 입력차단,
스크립트 및 프로그램 실행과 설치 차단,
파워쉘을 통한 해킹시도를 원찬 차단하여
악성코드 및 랜섬웨어의 실행을 방지합니다

이처럼 해킹 시도를 원천 차단하고
시스템 관리항목을 제어할수 없도록 제공해서
시스템 무결성을 보존할 수 있습니다

랜섬디엠지 프로 기능 상세 (8)

자동화 보안백업

✔ 중요 데이터를 자동으로 백업하고
필요에 따라 소산백업 구성 가능

랜섬디엠지 프로는
자동화된 보안백업 기능을 제공합니다

일별, 시간별, 주별, 월별로 필요에 따라
스케줄을 등록 하여 백업일정을 설정할수 있고
백업방식도 증분, 차등, 풀백업 등
원하는 방식으로 정해서 구성할 수 있습니다

또한 필요시에는 원격지 백업이 가능하도록
FTP, SFTP 를 지원하며
소산 백업 구성도 설정이 가능합니다

2. 솔루션 소개

랜섬디엠지 프로 시스템 구성

기업내 IT인프라 구성에 따라 적절한 방식으로 시스템 구성 가능

운영시스템 직접 연결형

운영중인 서버시스템
(ERP, GW, MES, PLM, PDM 등)에
직접 연결하여 보안 백업과 복구를
지원하는 시스템

랜섬디엠지 프로 시스템과
운영서버간 다이렉트 연결 구성
(SMB, SFTP, FTP 등 지원)

스케줄 (시간, 일, 주, 월, 이벤트)
단위로 백업 데이터 관리

NAS서버 연계형

PC, NAS서버, 랜섬디엠지 프로를
연계한 시스템 구성

기업내 PC 및 서버 데이터의 1차
NAS서버 백업 진행
(실시간, 스케줄 백업의 선택적 구성)

NAS서버와 랜섬디엠지 프로
시스템간 내부네트워크 기반
2차 보안 백업과 복원 구성

세이프리커버리 연계형

데이터베이스 서버의 운영 DB를
실시간 보호하는 세이프리커버리
솔루션과 랜섬디엠지 프로를
연계한 시스템 구성

운영중인 DB 저장폴더를
실딩처리하여 DB 접근제어와
1차적 랜섬웨어 및 바이러스 예방

세이프리커버리 보호 데이터의
2차 보안 백업과 복원 구성

재해복구 기반 소산백업

화재 등 재해상황에 대비한
중요데이터의 원격지 백업지원
랜섬디엠지 프로 시스템과
원격지 서버간 데이터 연동

로컬에 운영서버, NAS서버 등과
연계된 랜섬디엠지 프로
시스템을 구축하고
2차로 원격지 저장공간 구성

원격지 백업과 장애복구를 지원하는
재해복구시스템 구성

랜섬디엠지 프로 구성도 상세 (1)

직접연결형 시스템 구성

기업내 중요 서버의 데이터를 로컬네트워크 기반으로 직접 연결, 자동으로 백업 복구하는 시스템 구성
나스서버, DB서버를 비롯한 기업내 운영중인 중요 서버 데이터를 외부네트워크와는 분리한 내부 네트워크만을
이용하여 다이렉트로 연결한 후 자동으로 보안백업 해 안전하게 보존하고 필요시 복구하는 방식으로 활용

파일서버, DB서버, NAS서버 등

로컬백업

스케줄 백업

랜섬디엠지 프로

데이터 보존기술로 암호화 및
실행, 삭제 방지 기능 동작

데이터, 데이터베이스의 자동 백업과 데이터 보호

랜섬디엠지 프로 구성도 상세 (2)

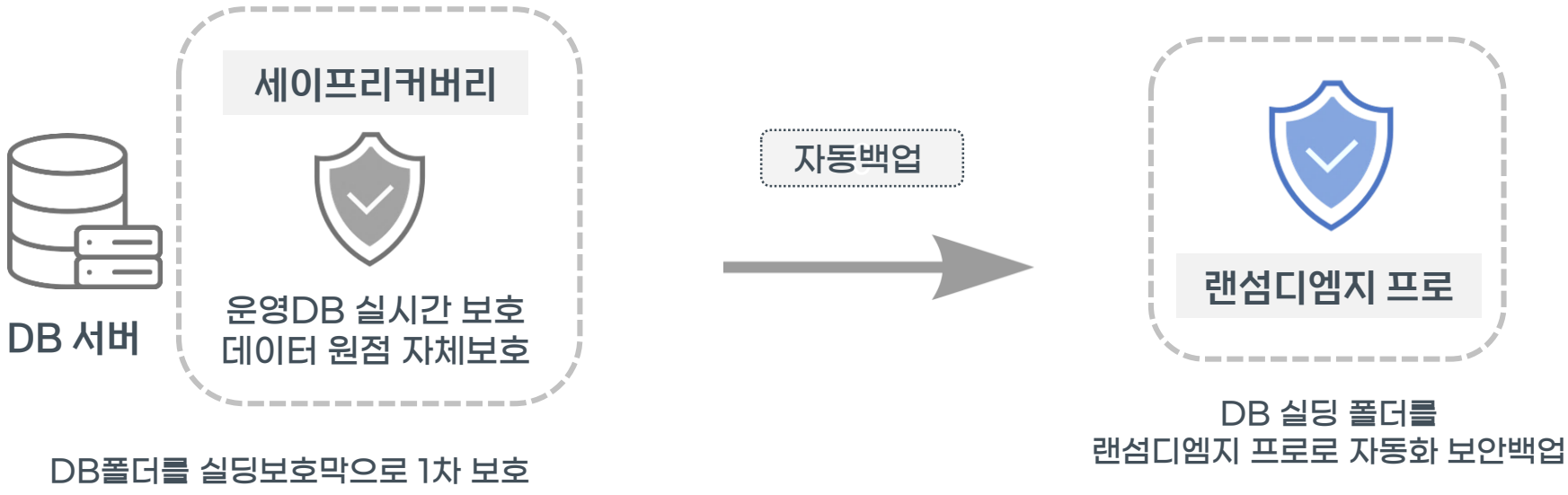
NAS서버 연계형 시스템 구성

1차 NAS서버 백업을 진행하고 2차 보안백업과 복구를 진행하는 방식 (NAS사용 기업에 적용)
PC 및 운영서버의 데이터를 1차 NAS서버로 저장하고 2차로 랜섬디엠지 프로 시스템과 연동하는 구성
사용자와 내 외부 연결을 지원하는 NAS공유 기능을 이용하면서 내부네트워크로는 랜섬디엠지 프로서버와 연결,
자동으로 보안백업하고 안전하게 관리하는 방식

랜섬디엠지 프로 구성도 상세 (3)

세이프리커버리 연계형 시스템 구성

데이터베이스 서버의 운영 DB를 실시간 보호하는 세이프리커버리 솔루션과 랜섬디엠지 프로를 연계한 시스템 구성
데이터베이스 서버를 운영하는 기업에서 DB폴더를 실딩보호막으로 1차로 보호하고 2차로 랜섬디엠지 프로 시스템을 연동
스마트팩토리에서 사용하는 ERP, PLM, PDM 서버에 사용하기 적당한 구성으로
운영DB의 백업없는 보호와 보안백업을 통한 2차 관리 방식



랜섬디엠지 프로 구성도 상세 (4)

재해복구 기반 소산백업 구성

화재 등 재해상황에 대비하여 원격지 NAS 또는 서버와 연동하여 재해복구 시스템을 구성하는 방식
Tier2 기반의 재해복구로 서버별 운영체제, 데이터 및 데이터베이스파일을 원격지 스토리지에 소산 백업하고
장애시 복구를 지원하도록 구성이 가능. 로컬에 랜섬디엠지 프로 시스템을 구축하고 2차로 원격지 저장공간 구성

- 자동 보안백업, 복구지원
- 데이터 보호 구성 지원
- 서버 마이그레이션 지원

재해복구시스템
- 소산 백업, 복구 지원
- 원격지 마이그레이션

2. 솔루션 소개 랜섬디엠지 프로와 타사 솔루션 비교

	랜섬디엠지 프로	타사 솔루션 (백신 & 백업방식)
랜섬웨어 대응 방식	특허받은 펌웨어 기반 저장기술로 랜섬웨어로부터 데이터를 안전하게 보호하고 데이터 위변조, 암호화를 방지함	특허받은 펌웨어 기반 저장기술로 랜섬웨어로부터 데이터를 안전하게 보호하고 데이터 위변조, 암호화를 방지함
데이터 정합성 및 무결성 보장	데이터 보호 영역에 저장된 데이터는 신, 변종 랜섬웨어를 포함한 악성코드에 감염된 데이터가 유입되더라도 보호영역의 데이터들이 위변조, 삭제되지 않고 정합성과 무결성을 보장	랜섬웨어 감염시에는 백업된 데이터 자체가 암호화 되기 때문에 백업 데이터의 무결성과 정합성이 보장되지 않음
랜섬웨어에 따른 업무 연속성 보장	신, 변종 랜섬웨어가 침투 하더라도 보호영역에 저장된 데이터는 암호화 되지 않기 때문에 업무연속성 보장 가능	랜섬웨어에 감염된 순간, 백업데이터도 암호화 되기 때문에 복구 전까지 업무 전체가 중단 될 가능성 높음. 또한 해커에게 비용을 지불하더라도 시간이 소요되며 복구된다는 보장이없음
소프트웨어 해킹 가능성	어셈블리어 기반 금고형 저장 기술은 물리적인 디바이스 술을 응용해 동작하기 때문에 해킹에 의해서 프로세스 무력화 및 우회공격이루어 지지 않음	소프트웨어 프로세스가 노출되면 실시간 감시를 끄거나 프로 그램을 제거하는 등 보안프로그램을 무력화시키거나 우회할 수 있는 가능성이 존재
비트라커 공격	윈도우 기본 기능인 비트라커 잠금을 차단하는 기능을 제공하고 있기 때문에 이를 사전에 예방할 수 있음	윈도우 자체기능인 비트라커로 볼륨을 암호화하면 백신은 탐지가 불가능하고 백업 데이터도 모두 비밀번호로 잠김
포맷 공격	포맷, 파티션 삭제의 원천 차단 기술로 해커가 악의적으로 포맷하거나, 관리자가 실수로 포맷 하는 것도 예방함	해커가 관리자 권한 획득후 악의적으로 포맷이 가능하며 또한 백신을 무력화 하거나 백업된 데이터를 삭제할수 있음
시스템 봉쇄	시스템 봉쇄 기능으로 키보드, 마우스 제어를 차단하며 악성코드 가 포함된 스크립트 실행을 원천차단하여 랜섬웨어로부터 데이터를 안전하게 보호함	ATP공격을 통해 관리자 권한 획득시 백업서버 원격 접속을 통해 공격이 가능

주요 레퍼런스

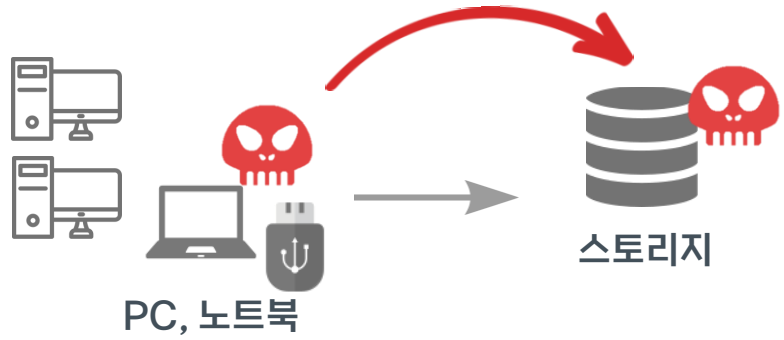
3. 주요 레퍼런스 고객 사례 (1)

희성촉매주식회사
soulbrain
대구해바라기센터
HKC (주)한국기능공사
BOSCH
GDay
KARI 한국항공우주연구원 Korea Aerospace Research Institute
LG화학
한국회계기준원 Korea Accounting Institute KAI
Woojung
삼보E&C주식회사
Aimsak
대원정밀
SAMHWA Air Conditioning Engineering
S.M METAL
충청소방학교 CHUNG CHEONG FIRE SERVICE ACADEMY
국기원
광명시
KT
KBS 교향악단 KBS Symphony Orchestra
족보닷컴 ZOCBO.COM
삼광의료재단
UNEX
SEAH HIGHTECH
가천대 길병원 Gachon University Gil Medical Center
중앙심리부검센터
대현회계법인
ACT
한국수력원자력
KAIST 한국과학기술원
한국천문연구원
HIAB
안산대학교 ANSAN UNIVERSITY
주식회사 유신당
AUSTEM

3. 주요 레퍼런스

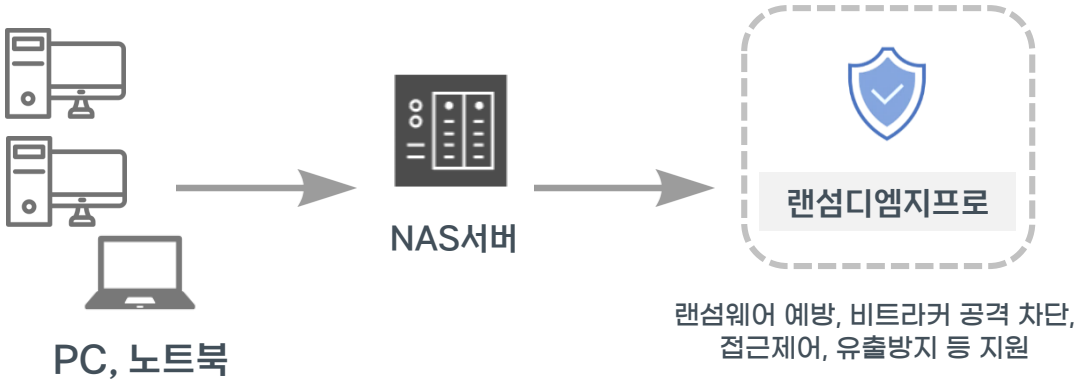
고객 상세 사례 (2)

업종	공구 생산 업체
사용환경	스토리지를 통해 기업의 내부, 외부 사용자가 데이터를 공유하는 방식으로 사용
랜섬웨어 공격유형	영업사원들의 노트북이 네트워크에 연결된 상태에서 **USB 이용시** 신종 변종 랜섬웨어 공격
피해 사례	백신이 신종 변종 랜섬웨어 탐지하지 못해 네트워크 스토리지의 데이터 까지 감염
구축 방식	NAS연계형 랜섬디엠지 프로 구축, 월 구독형 계약 진행



↑ 랜섬디엠지 프로 구축 전

↓ NAS 연계형 랜섬디엠지 프로 구축 후

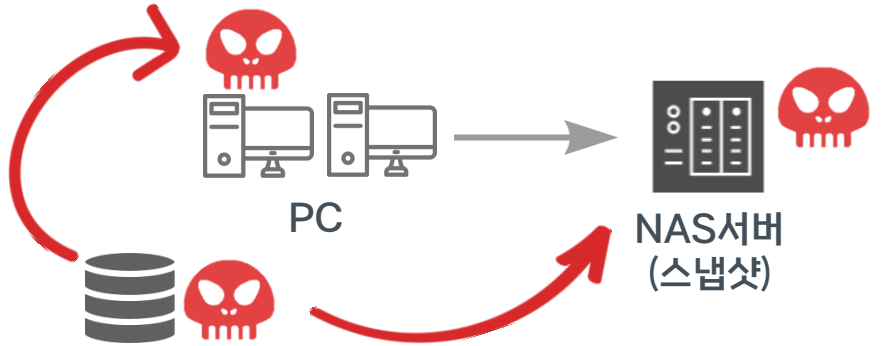


랜섬웨어 예방, 비트라커 공격 차단,
접근제어, 유출방지 등 지원

3. 주요 레퍼런스

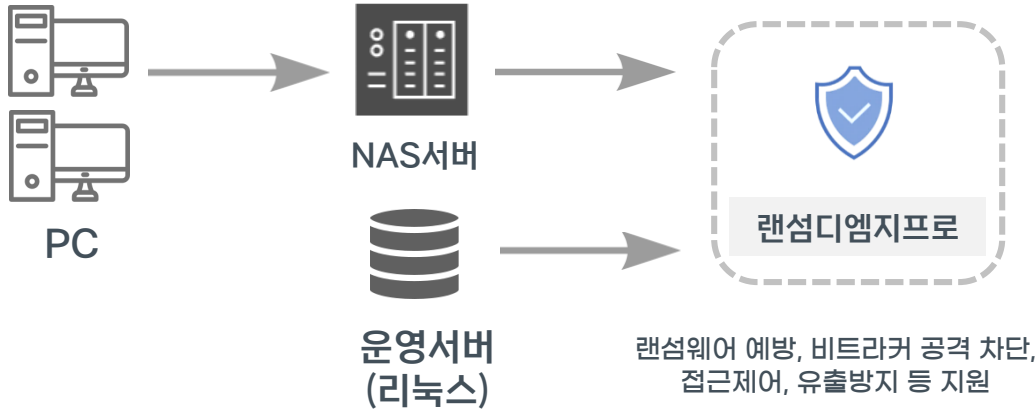
고객 상세 사례 (3)

업종	자동차 범퍼 제조업체
사용환경	자동차 범퍼 설계 도면을 NAS서버에 저장 및 공유하여 사용 NAS서버 스냅샷 기능을 활용하여 자체적인 백업 구성 적용
랜섬웨어 공격유형	일반 데이터 및 리눅스 기반 서버 OS를 공격하는 신종 변종 **리눅스 랜섬웨어 공격**
피해 사례	PC 데이터 및 NAS서버 파일 암호화 및 시스템 손상
구축 방식	직접연결형과 NAS연계형 랜섬디엠지 프로 구축 구축형 계약



↑ 랜섬디엠지 프로 구축 전

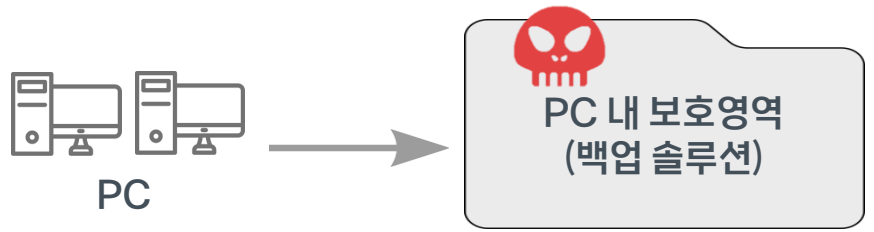
↓ 직접연결형, NAS 연계형 랜섬디엠지 프로 구축 후



랜섬웨어 예방, 비트라커 공격 차단,
접근제어, 유출방지 등 지원

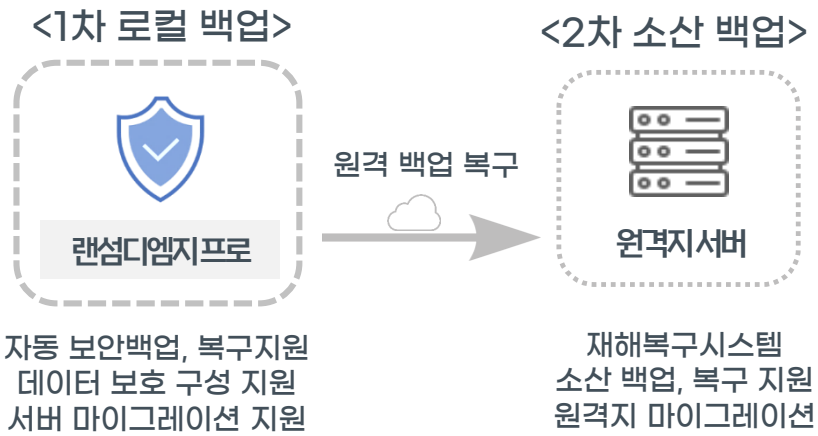
3. 주요 레퍼런스 고객 상세 사례 (4)

업종	대형 B2C 쇼핑몰 기업
사용환경	디스크 드라이브 영역의 일부를 보호영역으로 지정하여 암호를 설정하여 사용 (**백업 솔루션**)
랜섬웨어 공격유형	보호영역내에 랜섬웨어 감염된 파일을 모르고 저장, 추후 데이터 열람 실행시 램섬웨어 공격 수행. **보호영역내 랜섬웨어 감염 데이터의 유포** 중심
피해 사례	보호영역에 저장되어 있던 PC데이터 암호화
구축 방식	소산백업형과 직접연결형 랜섬디엠지 프로 구축, 구축형 계약



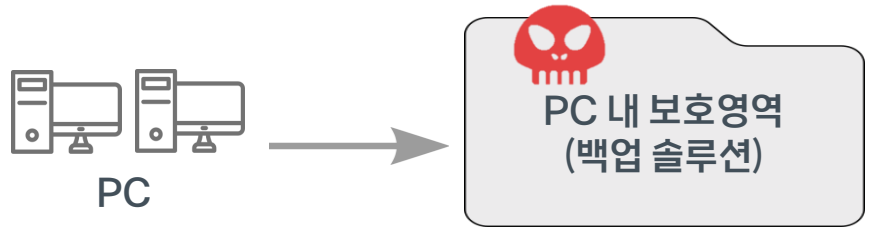
↑ 랜섬디엠지 프로 구축 전

↓ 소산백업형, 직접연결형 랜섬디엠지 프로 구축 후



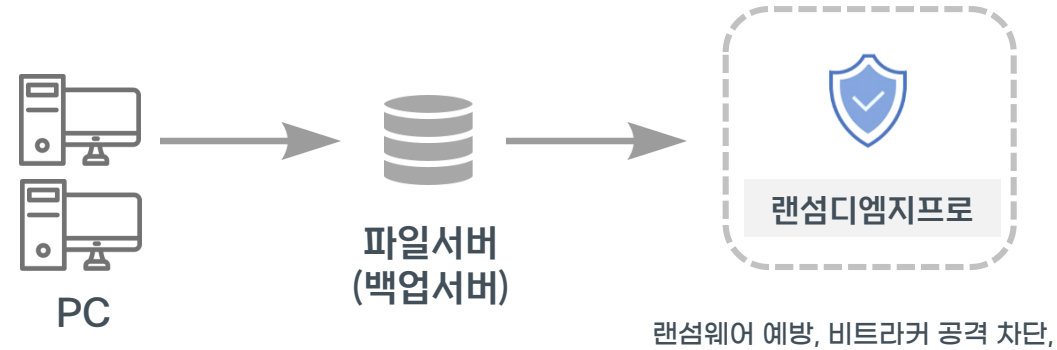
3. 주요 레퍼런스 고객 상세 사례 (5)

업종	대학교 행정지원과
사용환경	디스크 드라이브 영역의 일부를 보호영역으로 지정하여 암호를 설정하여 사용 (**백업솔루션**)
랜섬웨어 공격유형	보호영역내에 랜섬웨어 감염된 파일을 모르고 저장, 추후 데이터 열람 실행시 램섬웨어 공격 수행. **보호영역내 랜섬웨어 감염 데이터의 유포** 중심
피해 사례	보호영역에 저장되어 있던 PC데이터 암호화
구축 방식	직접연결형 랜섬디엠지 프로 구축, 월 구독 서비스 계약



↑ 랜섬디엠지 프로 구축 전

↓ 소산백업형, 직접연결형 랜섬디엠지 프로 구축 후



랜섬웨어 예방, 비트라커 공격 차단,
접근제어, 유출방지 등 지원

회사 소개

4. 회사 소개 씨엠테스 기술사사무소

◆ **회사 개요**

- ✓ 회사명 : 주식회사씨엠테스
- ✓ 등록번호 : 206-86-66036
- ✓ 종 목 : SW개발공급, 컴퓨터시스템 구축 및 자문
- ✓ 설립년도 : 2012년 6월 1일
- ✓ 홈페이지 : http://cmtes.co.kr

◆ **주요 사업**

- ✓ 랜섬웨어대응솔루션, 랜섬디엠지 프로 개발 및 공급
- ✓ 이중화솔루션, 트라이HA 개발 및 공급
- ✓ DB실딩, 팩토리리커버리 솔루션 개발 및 공급
- ✓ 스토리지 구축 및 자문 / 문서보안, 네트워크 보안 솔루션 구축
  (시놀로지, 큐냅, 넷기어, QSAN, 소포스 공인 파트너)

THANK YOU


02-2236-9329


webmaster@cmtes.co.kr


서울시 영등포구 여의도동 61-4 콤비빌딩 823호