무상 진단 보고서 Ransomware Database Forensic Diagnosis

랜섬웨어 감염 SQL Server 데이터베이스 진단 보고서

LockBit 계열 감염 · SQL Server 2008 R2 ERP 데이터베이스 · 복구 착수 전 진단

문서 번호	DIAG-SAMPLE-02
발행일	2026-11-21 (판 1.0)
보고서 단계	무상 진단 (복구 착수 전)
진단 대상	ERP 용 SQL Server 데이터베이스 3 개 + 임시 DB (데이터 파일 4 · 로그 파일 4 · 백업 파일 5)
의뢰 기관	***** (비식별)
작성 기관	(주)베일리테크 DB 복구팀

공개 샘플

이 문서는 실제 진단 사례를 바탕으로 고객사·데이터베이스·파일·서버 이름과 해시를 모두 가린 홈페이지용 샘플입니다. 수치는 실제 측정값입니다. 실제 고객 보고서에는 받은 파일 목록과 SHA-256 이 부록에 함께 실립니다.

문서 관리

구분	성명	소속	일자	서명
작성		(주)베일리테크 DB 복구팀	2026-11-21	
검토		(주)베일리테크 DB 복구팀		
승인		(주)베일리테크 DB 복구팀		

판	일자	변경 내용
1.0	2026-11-21	무상 진단 결과 발행

목차

1. 진단 결과 요약 3

2. 받은 자료와 증거 보존 4

3. 대상 데이터베이스 4

4. 감염 분석 5

5. 손상 범위 5

6. 복구 가능성 판정 6

7. 복구를 진행하면 6

8. 추가로 필요한 자료 7

9. 즉시 조치 권고 7

10. 진단의 한계 8

부록. 용어 8

1. 진단 결과 요약

복구 가능성 등급	데이터 파일 페이지 보존	암호화된 바이트	감염 전 정상 백업
A 복구 가능	**99.995%**	**0.0017%**	**3 개**
데이터 보존 99% 이상 + 카탈로그 생존 + 정상 백업 (6 장 기준표)	799,259 / 799,296 페이지 (DB 3 개) [계산]	808,960 / 47,166,117,840 B [계산]	DB 3 개 모두, 감염 약 10 일 전 [측정]

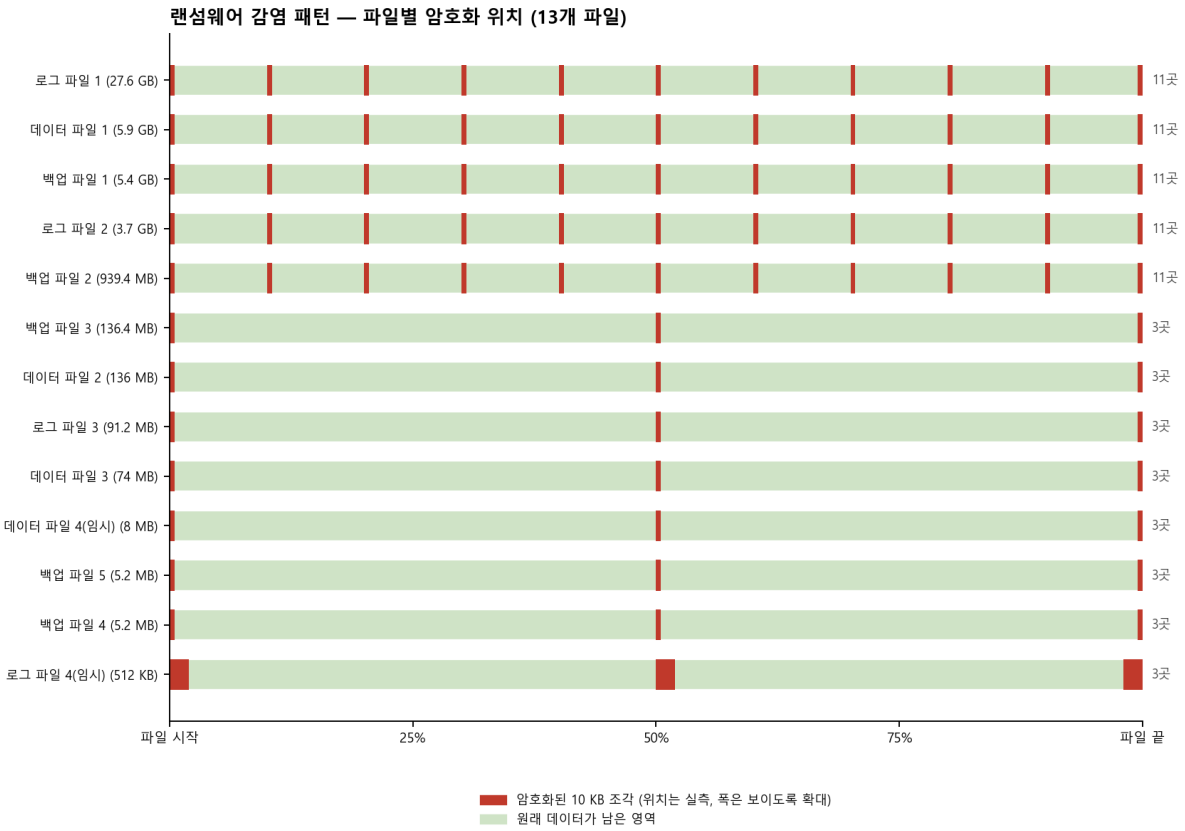


그림 1. 파일별 암호화 위치 — 13 개 파일 모두 같은 규칙(작은 파일 3 곳: 시작·가운데·끝 / 큰 파일 11 곳: 시작·10% 간격·끝)

빨간 조각만 암호화되고 나머지(초록)는 원래 데이터가 그대로 남아 있습니다. 조각 하나는 10 KB 로, 5.9 GB 본 ERP 데이터 파일에서도 11 곳 110 KB 만 암호화됐습니다 [측정]. 데이터 파일·로그 파일·백업 파일이 모두 같은 방식으로 일부만 암호화됐습니다.

1. LockBit 계열 랜섬웨어가 파일마다 10 KB 조각 3 곳 또는 11 곳만 암호화했습니다. 세 데이터베이스의 데이터 파일 페이지 99.995%가 원래 상태 그대로입니다 [측정].

2. 각 파일의 첫 페이지(파일 헤더)가 암호화돼 SQL Server 에 바로 연결할 수는 없지만, 같은 데이터베이스의 감염 약 10 일 전 정상 백업이 3 개 모두 있어 손상된 구조 영역을 보완할 수 있습니다 [측정].

3. SQL Server 가 원래 카탈로그로 데이터베이스를 다시 열 수 있는 상태로 복구할 수 있을 것으로 예측합니다. 이 경우 표·인덱스·제약·프로시저 정의는 원본 그대로이며, 행 손실은 암호화 조각이 걸친 소수 페이지로 한정됩니다 [예측].

고객이 결정할 일 ① 복구 의뢰 여부 ② 감염 시점 데이터(현재 시점)와 백업 시점 데이터를 모두 받을지 ③ 운영 SQL Server 버전 확인 — 복구 DB 를 같은 버전 이상에서 연결하기 위해.

2. 받은 자료와 증거 보존

항목	내용
받은 파일	13 개 (데이터 파일 4 · 로그 파일 4 · 백업 파일 5), 총 약 47.2 GB
증거 보존	원본은 읽기 전용으로만 열고, 진단은 작업 사본에서 했습니다. 작업 전후 SHA-256 이 13 / 13 일치합니다 [측정].
파일 특징	모든 파일 이름 뒤에 .lockbit 가 붙었고, 파일 크기는 원래 크기 + 272 B 입니다(13 / 13) [측정].

3. 대상 데이터베이스

항목	값	근거
제품·버전	Microsoft SQL Server 2008 R2	부트 페이지·인스턴스 정보 [측정]
DB 구성	본 ERP DB · 연동 DB · 복제 배포 DB (3 개) + 임시 DB	데이터 파일·로그 파일 짝 [측정]
규모	본 ERP DB 사용자 표 2,570 개 · 772,416 페이지	카탈로그 [측정]
백업	DB 3 개 각각 정기 백업 1 개(감염 약 10 일 전) + 오래된 영구 백업 2 개	백업 머리 [측정]

4. 감염 분석

항목	결과	근거
랜섬웨어 계열	LockBit 계열	확장자 .lockbit · 파일 끝 272 B 추가 · 간헐 암호화 [예측] — 악성 실행 파일 미확보
암호화 방식	파일 전체가 아니라 10,240 B 조각 3 개(작은 파일) 또는 11 개(큰 파일)만 암호화	13 개 파일 모두 같은 위치 공식에 맞음 [측정]
복호 가능성	복호 키 없음	키 없이 암호화되지 않은 페이지와 백업으로 복구

파일별 암호화 위치는 1 장 그림 1 과 같습니다.

5. 손상 범위

항목	값	분자 / 분모
암호화된 바이트 (전체 파일)	0.0017%	808,960 / 47,166,117,840 [계산]
본 ERP DB 데이터 파일 — 조각이 걸친 페이지	0.0032%	25 / 772,416 [측정]
연동 DB 데이터 파일 — 조각이 걸친 페이지	0.034%	6 / 17,408 [측정]
복제 배포 DB 데이터 파일 — 조각이 걸친 페이지	0.063%	6 / 9,472 [측정]
파일 헤더(첫 페이지)	모든 데이터 파일에서 암호화	바로 연결 불가 [측정]
정상 백업	DB 3 개 모두 있음(백업 파일도 같은 방식으로 일부만 암호화)	손상 구조 영역 보완 가능 [측정]

※ 그림 1 의 공식 위치 밖에도 원래부터 압축·이진 형태인 데이터 구간이 일부 있으며, 이는 암호화로 세지 않았습니다.

6. 복구 가능성 판정

영역	판정	근거
업무 데이터(행)	복구 가능	페이지 보존 99.995% [계산] · 조각이 걸친 소수 페이지만 손실 예상, 그중 백업에 사본이 있는 페이지는 보충 [예측]
표 구조(표·열·자료형)	복구 가능	카탈로그 생존, 손상 부분은 정상 백업으로 보완 [예측]
인덱스·제약·프로시저	복구 가능	SQL Server 가 원래 정의로 직접 여는 방식 [예측]
현재 시점과 백업 시점	둘 다 제공 가능	감염 시점 DB 와 백업 시점 DB 를 따로 만들어 차이 비교표 제공 [예측]
원래 행 수 대비 복구율	복구 후 확정	원래 행 수 기준 자료 필요 [확인 필요]

※ 판정 등급 A(복구 가능): 데이터 보존 99% 이상 + 구조 정보 생존 + 정상 백업. 예상 범위는 진단 시점의 판단이며 보증이 아닙니다.

복구 가능성 등급 기준 (모든 고객 공통)

등급	이름	기준
A	복구 가능	데이터 영역 보존 99% 이상, 구조 정보(데이터 사전·카탈로그) 생존 또는 같은 DB 정상 백업 있음
B	조건부 복구	데이터 영역 보존 90% 이상, 구조 정보 일부 손실 — 추가 자료에 따라 범위가 달라짐
C	부분 복구	데이터 영역 보존 90% 미만 또는 구조 정보 대부분 손실 — 남은 데이터 조회용 추출
D	복호 키 필요	파일 전체 암호화 — 키 없이는 복구 불가

7. 복구를 진행하면

항목	내용
복구 방식	감염 파일에서 손상되지 않은 영역을 최대한 살리고, 데이터베이스를 여는 데 필요한 구조 영역만 같은 데이터베이스의 정상 백업으로 보완해 SQL Server 가 원래 카탈로그로 데이터베이스를 직접 열게 합니다.

받게 되는 결과물	① 복구된 데이터베이스 파일(현재 시점 · 백업 시점, 데이터 파일·로그 파일) ② 표마다 앞 100 행 미리보기 엑셀 ③ 현재·백업 시점 비교표와 연결 순서를 담은 복원 안내서 ④ 축별 복구 결과 최종 보고서
납품 전 검증	SQL Server 무결성 검사(DBCC CHECKDB) · 빈 인스턴스 연결 시험 · 응용 사용 가능성 시험
진행 단계	의뢰 → 정밀 분석 → 구조 보완·데이터베이스 재구성 → 무결성 검사·연결 시험 → 납품
예상 기간	12 시간 [예측] — 받은 자료 약 47.2 GB(50 GB 미만) 기준

※ 예상 기간 기준(받은 자료 전체 크기): 50 GB 미만 12 시간 · 100 GB 미만 24 시간 · 300 GB 미만 36 시간 · 300 GB 이상은 별도 안내. 의뢰·자료 수령 후부터 계산합니다.

8. 추가로 필요한 자료

자료	있으면 좋아지는 것
더 최근의 백업(차등·로그 백업)	백업 시점 이후 바뀐 데이터 보충
운영 SQL Server 버전	복구 DB 를 운영 환경에 맞게 납품
업무 기준 행 수·합계(전표·원장 등)	원래 행 수 대비 복구율 확정
감염 발견 시각·서버 정보	감염 범위 확정

9. 즉시 조치 권고

1. 감염 파일을 지우거나 덮어쓰지 마십시오. 이름 변경·복사도 원본은 그대로 두고 사본으로 하십시오.
2. 감염 서버는 네트워크에서 분리한 상태를 유지하십시오.
3. 복호 협상 전에 진단 결과를 먼저 확인하십시오. 이 사례처럼 간헐 암호화이고 정상 백업이 있다면 키 없이도 대부분 복구됩니다.
4. 재발 방지: 백업을 운영 저장소와 분리된 쓰기 금지 저장소 또는 오프라인 매체에 보관하고, 가상화 관리 계정에 다중 인증을 적용하며, 분기마다 복원 시험을 하십시오.

10. 진단의 한계

- 무상 진단은 파일을 읽기만 한 결과입니다. 행 단위 복구 수치는 복구 작업 후 최종 보고서에서 확정합니다.
- [예측] 표시는 진단 시점의 판단이며 결과를 보증하지 않습니다.
- 랜섬웨어 계열은 파일 특징에 근거한 판단이며, 악성 실행 파일 분석은 진단 범위에 들지 않습니다.

부록. 용어

용어	뜻
페이지	SQL Server 가 데이터를 저장하는 8 KB 단위
카탈로그	표·열·인덱스 등 데이터베이스 구조 정보를 담은 시스템 표
간헐 암호화	파일 전체가 아니라 일부 구간만 암호화하는 방식 — 나머지는 원래 데이터가 남음
DBCC CHECKDB	SQL Server 가 데이터베이스 구조·할당·인덱스 일관성을 검사하는 기능
SHA-256	파일 내용이 바뀌지 않았음을 확인하는 지문 값