2026.03.23.

KIRI 리포트

보험회사 랜섬웨어 리스크의 확대와 대응 과제

| 글로벌 이슈 |

강윤지(姜允池) 연구원

요 약

기업을 대상으로 한 조직화된 공격으로 진화하고 있는 랜섬웨어는 정보 가치가 높고, 복구가 어려우며, 지급 능력이 있는 표적을 선호하는 경향이 있음. 보험회사는 공격 대상이 되기 쉬운 것으로 평가되는데, 최근에는 랜섬웨어 공격으로 인한 손실이 누적돼 경영 파탄으로 이어진 피해 사례도 발생함. 이에 따라 보안 대책뿐 아니라 피해 후 회복력을 강화하는 등 다층적 대비의 필요성이 높아짐

○ 랜섬웨어는 개인을 대상으로 한 금전 요구를 넘어 기업의 업무 지속성을 흔드는 조직화된 공격으로 진화하고 있으며, 피해 규모와 침해 비중 지표에서도 위협이 지속적으로 확대되고 있음

- 랜섬웨어 지불액은 2023년 12억 5,000만 달러로 사상 최고치를 기록했고, 2024년에는 8억 1,355만 달러로 전년 대비 35% 감소했으나, 공격 시도 자체는 하반기에 오히려 증가함[1)]
- 랜섬웨어는 시스템 침투형 피해의 핵심 구성요소로, 2025년 기준 전체 침해 사고의 44%를 차지하며 대규모 사고의 주된 원인이라는 분석이 제기됨[2)]
  - 랜섬웨어의 공격 빈도는 전년 대비 37% 늘었고, 취약점을 이용한 침입도 34% 증가했다는 분석이 있어 원격 접속 장비나 VPN[3)] 같은 경계 구간이 공격의 주요 출발점이 되고 있음을 시사함

○ 랜섬웨어 공격자는 정보 가치가 높고, 복구가 어려우며, 지급 능력이 있는 표적을 선호하는 경향이 있어 보험회사도 표적이 될 수 있고, 보험금 지급과 고객 안내가 지연될 경우 고객 영향이 즉시 발생해 위험이 빠르게 확대될 수 있음

- 전형적인 랜섬웨어 공격은 이메일 사칭이나 취약한 VPN 등을 통해 침입한 뒤 내부에서 정보를 탐색하고, 민감 데이터를 빼내거나 시스템을 사용하지 못하도록 암호화해 업무를 멈추게 하며, 이후 탈취한 데이터의 외부 공개를 하지 않겠다는 조건이나 암호키 제공을 대가로 금전을 요구하는 단계로 진행됨(〈표 1〉 참조)
- 보험회사는 고객정보가 많아 위협받기 쉽고, 시스템 의존도가 높아 업무 정지에 따른 손해가 크며, 고객 대응 및 지급 처리 지연으로 평판·소송 리스크가 발생할 수 있어 경영의사결정에 대한 압박이 커질 수 있다는 점에서 표적이 되기 쉬움
  - 랜섬웨어 공격자가 보험계약의 보상 수준이나 보험회사의 지급 여력을 가늠해 요구 금액을 조정할 가능성도 있음

1) CyberSecurityDIVE(2025. 2. 5.), "Ransomware payments fell 35% in 2024"
2) Verizon(2025), "Verizon Data Breach Investigations Report"
3) Virtual Private Network의 약자로, PC와 회사 네트워크 사이를 암호화된 터널로 연결해 회사 내부망에 있는 시스템을 밖에서도 사용할 수 있도록 함

〈표 1〉 보험회사 표적 시 랜섬웨어 공격 단계별 영향

단계	공격자의 핵심 활동	징후 및 영향
1단계: 초기 침투	• 피싱과 계정 탈취 • 취약한 원격 접속 악용 • 제3자 접점 경유 침투	• 비정상 로그인 • 다중인증 우회 시도 • 계정 잠금 증가
2단계: 권한 장악 및 내부 이동	• AD(Active Directory)[4] 및 주요 계정 장악 • 내부망 탐색	• 권한 변경 흔적 • 관리자 계정 생성 • 내부 트래픽 급증
3단계: 데이터 탈취	• 고객정보, 청구 서류 등 민감 데이터 수집 후 외부로 반출	• 대량 다운로드 • 외부 전송 트래픽 증가
4단계: 암호화 및 운영 마비	• 서버와 단말 암호화 • 백업·보안도구 무력화 • 서비스 중단 유발	• 시스템 접속 불가 • 보험금 지급 지연 • 고객 문의 증가
5단계: 협상 및 갈취	• 탈취 데이터의 외부 공개를 하지 않겠다는 조건 또는 암호화 해제키 제공을 대가로 금전 요구	• 유출 사이트 게시 위협 • 협상 압박

자료: Vectra(2025), "Ransomware explained: The complete 2025 defense guide"; Verizon(2025), "Verizon Data Breach Investigations Report"

○ 최근에는 랜섬웨어 공격으로 인한 손실이 누적돼 단기적인 업무 정지에 그치지 않고 경영 파탄으로 이어진 피해 사례도 생겨남에 따라, 보안 대책뿐 아니라 피해 후 회복력 강화 필요성이 커지고 있음

- 독일의 모바일 단말 보험회사 Einhaus는 2023년 랜섬웨어 공격으로 핵심 시스템이 암호화되어 장기간 업무 정지를 겪었고, 이로 인한 여파로 손실이 누적되면서 2025년 7월 파산 절차에 들어감[5]
  - 이 회사는 중요 데이터에 대한 접근 권한을 되찾기 위해 20만 유로 상당의 비트코인을 지급한 것으로 알려짐
- 이 외에도, 2024년 인도의 건강 보험회사 Star Health는 고객 데이터와 의료 기록 유출과 관련해 68,000달러를 요구받았고, 2025년 12월 독일의 생명보험회사 IDEAL은 랜섬웨어로 네트워크가 마비돼 업무가 전면 중단되는 등 관련 피해가 이어지고 있음[6]

○ 보험회사는 랜섬웨어 공격에 대비하여 침투 차단과 복구 역량을 확보하고 보험금 지급 연속성과 운영 복원력 중심의 체계를 갖춰 대응할 필요가 있음

- 관련 지침은 운영 마비가 협상 압박으로 이어질 수 있다는 점을 고려해 고객 접점과 지급 기능을 우선 복구 대상으로 지정하고, 지급 업무 장기 마비를 가정한 지급 우회 절차를 정기 훈련에 포함할 것을 권고함[7]
- 백업 시스템 분리, 대체 업무 및 수작업 처리 훈련과 절차 정비 등을 통해 채널 복원력을 강화할 수 있음[8]

4) 회사 내부에서 쓰는 사용자 계정, 비밀번호, 로그인 권한, 컴퓨터·서버 정보를 중앙에서 관리하는 시스템을 의미함
5) Techradar(2025. 8. 5.), "A single ransomware attack has pushed this business into insolvency"
6) Reuters(2024. 10. 12.), "India's Star Health says it received $68,000 ransom demand after data leak"; InsuranceERM(2025. 12. 15.), "German life insurer hit by ransomware attack"
7) CISA(2020. 9.), "RANSOMWARE GUIDE"
8) EIOPA(2023. 7.), "METHODOLOGICAL PRINCIPLESOF INSURANCE STRESS TESTING"