"랜섬웨어" 특집호 발간에 즈음하여

오늘날 사이버 위협 환경은 그 규모와 정교함에서 과거와 비교할 수 없을 만큼 빠르게 진화하고 있다. 특히 랜섬웨어는 단일 악성코드를 넘어 조직화 된 범죄 생태계, 그리고 디지털 경제를 위협하는 구조적 공격 모델로 발전하고 있다. 2025년 들어 확인된 침해사고 추세에 따르면 랜섬웨어 피해 건수는 전년 동기 대비 크게 증가했으며, 피해 범위 역시 의료・공공・제조・교육・금융 등 사회 기반 전반으로 확산되고 있다. 이러한 현상은 기술 발전, 공격 자동화, 암호화폐 지급 구조, 조직화 된 협력 네트워크가 결합한 결과이며, 그 대응 역시 단일 기술 중심 접근이 아닌 종합적 보안 전략으로 확장되어야 함을 의미한다. 더욱 주목해야 할 변화는 생성형 인공지능과 대형언어모델(LLM)의 등장으로 랜섬웨어가 단순히 사람이 제작한 정적 악성코드를 넘어 AI 기반 자율형 공격 도구로 전환되고 있다는 점이다. 이러한 변화는 기존 탐지 체계, 정책 체계, 법적 대응 모델이 전제하던 구조를 근본적으로 흔들고 있다. 동시에 암호화폐 기반 거래, 사이버 범죄 서비스화 (Ransomware-as-a-Service), 오픈소스 기반 위협 요소의 재활용은 공격자 진입 장벽을 낮추며 랜섬웨어 생태계를 더욱 확산시키고 있다. 이는 단기 대응 중심 정책이나 단일 탐지 기술만으로 극복 가능한 문제가 아니며, 국가・산업・연구기관・법 집행체계가 연계된 지속적 순환형 대응 체계가 필요함을 보여준다.

이러한 배경 속에서 이번 랜섬웨어 특집호는 현재의 위협 현실을 정확히 진단하고, 기술적 대응뿐 아니라 정책, 탐지, 분류, 분석, 생태계 이해까지 아우르는 융합 연구 기반의 학술적 논의를 제시하고자 기획되었다. 생성형 AI 기반 자율형 랜섬웨어의 개념과 PrompLock 사례를 분석한 연구는 AI 활용이 공격 모델의 본질적 변화를 가져올 수 있음을 보여주었으며, 정적 분석 기반 탐지 결과의 설명 가능성을 확보하기 위한 연구는 기존 AI 탐지 모델의 신뢰성 한계를 넘어 실무 활용 가능성을 제시하고 있다. 또한 LLM 코드 생성 모델을 교란하는 SIMPLE, COVERT, TrojanPuzzle, CodeBreaker 등 주요 공격 기법과 최근의 AFRAIDOOR·Multi-target Backdoor의 특징을 종합 분석하였다. 새로운 변종으로 보고된 Cephalus 랜섬웨어에 대한 분석 연구는 실제 공격 사례 기반 암호화 구조와 동작 특성을 정리하였고, 해당 특성을 이용하여 복호화 방법까지 도출하였다. 랜섬웨어 현황을 종합적으로 분석한 동향 연구는 범죄 생태계, 갈취 구조, 지역별 확산 양상을 비교적 관점에서 정리하였다. 더불어 암호화폐 기반 랜섬머니 지급 흐름 연구는 자금 흐름과 포렌식 대응 방향을 제시하고 있으며, 오픈소스 기반 Yurei 랜섬웨어 분석 연구는 공격 도구의 공개화와 재활용이 새로운 확산 촉매가 되고 있음을 보여준다.

끝으로 바쁘신 중에도 소중한 시간을 내시어 원고를 집필해 주신 집필자분들과 편집에 수고해 주신 학회지 편집 위원회, 그리고 학회 사무국 관계자 여러분께 감사를 드립니다.

2025년 12월

한성대학교 융합보안학과 조교수 박 명 서