"랜섬웨어" 특집호 발간에 즈음하여

랜섬웨어(Ransomware)는 악성 소프트웨어(악성코드)의 일종으로 몸값(Ransom)과 소프트웨어(Software)의 합성어이다. 랜섬웨어는 시스템을 잠그거나 데이터를 암호화해서 사용할 수 없도록 한 뒤 피해자에게 대가로 금전을 요구한다. 익명성, 추적 어려움의 특성을 가진 가상화폐의 등장 이후로 랜섬웨어는 더욱 빠르게 성장하였고, 최근에는 랜섬웨어 해킹 그룹 형태로 더욱 활발히 운영되고 있다. 랜섬웨어는 이미 전세계적으로 주요한 이슈로 랜섬웨어 해킹 그룹에 의한 피해 대응을 위해 랜섬머니 지불 금지 정책, 국제 공조를 통한 랜섬웨어 갱단 소탕, 랜섬웨어 복구 도구 배포 등 다수의 노력을 하고 있다. 이러한 노력에도 불구하고 2024년 상반기 동안 랜섬웨어 공격자들이 4억 5980만 달러의 수익을 올리면서 역대 최대 기록을 갱신하는 등 피해 규모는 꾸준히 증가하고 있다. 이러한 피해 규모 증가는 건당 높은 금액을 요구할 수 있는 대상을 위주로 공격하는 이른바 빅게임 헌팅에 기인하고 있다고 분석할 수 있다. 랜섬웨어 피해를 근본적으로 대응할 수 있는 수단은 감염된 파일을 복원하는 기술, 즉, 암호화된 파일을 복호화하는 기술을 개발하는 것이나, 대부분의 랜섬웨어는 안전하다고 알려진 암호 알고리즘을 사용하기 때문에 이러한 기술을 개발하는 것은 쉽지 않다. 하지만, 일부 랜섬웨어는 시스템적 취약요소, 자체 개발한 알고리즘 사용 등의 감염된 파일을 복원할 수 있는 요소를 포함하는 경우가 존재한다. 이러한 사실만으로도 랜섬웨어에 대한 분석 연구를 꾸준히 수행할 필요가 있다.

본 특집호에서는 최근 다수의 피해를 입힌 주요 랜섬웨어 LockBit, Cl0p, BlackCat, Black Basta, Rhysida의 동향 및 피해 사례를 살펴보았다. 주요 랜섬웨어의 피해 사례에서 살펴보았듯 랜섬웨어의 공격 대상은 개인이 아닌 기업, 의료, 교육 등 사회 기반 시설을 주요 타겟으로 삼아 큰 규모의 몸값을 요구하는 것을 알 수 있었다. 또한, 윈도우, 리눅스, 안드로이드와 같은 주요 운영체제에서 동작하는 최신 랜섬웨어를 분석하여 해당 랜섬웨어의 악성 행위 및 동작 과정을 살펴보았다. 데이터 암호화 또는 잠금이라는 주요 악성 행위는 동일하였으나, 각 운영체제가 갖는 고유 특성으로 인한 랜섬웨어 동작의 특징점을 파악할 수 있었다. 다음으로 LLM(Large Language Model)을 활용한 랜섬웨어 탐지를 위한 보안 프레임워크에 대한 연구에 대해 소개하였다. 본 연구는 기존 AI 기술을 접목한 랜섬웨어 탐지의 한계를 극복할 수 있는 대안으로 제시되었으며, 랜섬웨어 탐지 및 대응의 정확성을 크게 향상시킬 수 있을 것으로 기대한다. 마지막으로 패스워드 크래킹 암호들에 대한 양자 컴퓨팅 기반 해킹 동향에 대해 살펴보았다. 본 연구를 통해 기존 랜섬웨어에 적용된 암호 알고리즘 크래킹을 위한 양자 컴퓨팅 활용 가능성을 살펴볼 수 있다.

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

2024년 10월

한성대학교 융합보안학과 조교수 박 명 서