[정보보호] 몸값, 요구하는 대로 주시겠습니까?

얼마 전, 전 세계적으로 많은 사람들이 인질 사건에 휘말리는 일을 겪었다. 사실 인질 사건은 아니지만 사람을 대상으로 한 것이 아니라는 것뿐이지 기존의 인질 사건과 동일한 형태의 범죄 행위가 여기저기서 목격된 것이다. 그래서인지 그러한 유사 사건에 사용되는 불법 프로그램의 이름을 랜섬웨어(ransomware)라 명명하고 있다. 랜섬이란 말 그대로 인질의 몸값을 말하며 랜섬웨어는 일반 사용자의 PC, 스마트폰 등 기타 여러 종류의 매체에 침입하여 사용자의 파일을 암호화하여 사용하지 못하게 만들고, 이러한 암호를 풀기 위해서는 자신들에게 일정한 금액의 돈을 지불하라는 형태로 몸값을 요구하여 실제로 그 피해가 상당했다고 한다. 스마트 세상, 정보화 세상의 역기능에 대해 많은 이야기들이 있었고 아직도 진행형이지만 거기에 또 다른 형태의 새로운 역기능이 하나 추가되는 상황인 것이다. 그동안 해킹이나 개인 정보의 침해로 많은 고통을 겪어왔던 사용자들이 이번에는 새로운 형태의 몸값 요구에 떨며 컴퓨터를 맘대로 켜지도 못하고 실제로 많은 정보나 돈을 잃게 되는 상황까지 이르게 되었다.

그렇다면 이러한 랜섬웨어는 정확히 무엇이고 우리는 이에 대해 어떻게 대처해야 할까? 세계적으로 피해가 많이 발생하고 있는 랜섬웨어는 파일을 인질로 삼아 금전을 요구하며 이러한 이유로 몸값을 뜻하는 랜섬(ransom)과 컴퓨터의 소프트웨어(software)를 합성하여 만든 신조어이다. 이러한 랜섬웨어는 주로 신뢰할 수 없는 사이트, 스팸 메일, 파일 공유 사이트, 네트워크망(인터넷) 등을 통해 유포된다. 랜섬웨어에 감염되면 기기 부팅 시 암호를 요구하거나 문서, 그림 등의 파일을 암호화해서 정상적으로 사용하지 못하게 만든 뒤, 이를 복구할 수 있는 키값을 알려준다는 조건으로 금품을 요구하게 된다. 이 때, 요즈음 논란이 되고 있는 비트 코인과 같은 추적이 어려운 전자 화폐(물론 현금을 요구할 수도 있다)를 요구한다. 랜섬웨어의 최대 목적은 결국 피해자로부터 금전적인 이득을 취하는 것이므로 금전적 손해를 보지 않기 위해서는 랜섬웨어에 감염되지 않도록 예방 활동을 철저히 하는 것이 가장 중요하다.

본고에서는 이러한 랜섬웨어에 의한 피해를 예방하기 위한 개인 및 기업이나 기관 차원의 가이드라인을 제시하고자 한다. 랜섬웨어 피해를 줄이기 위해 가장 좋은 방법은 랜섬웨어에 감염되지 않도록 하는 것이다. 이러한 점은 일반적인 악성코드에 대한 대처 방법과 대체적으로 동일하다. 다만, 일반 악성코드 대응 방법에서는 크게 강조되지 않았던 백업이 랜섬웨어 대응책으로는 매우 강조된다는 차별점이 존재한다. 이를 위한 몇 가지 예방법을 정리하면 다음과 같다.

- 운영 체제 및 응용 프로그램은 최신 버전으로 업데이트하여 사용
- 백신 프로그램은 최신 버전으로 유지

- 안티-랜섬웨어 프로그램 사용
- 스팸 메일의 첨부 파일 실행 금지
- 신뢰할 수 없는 사이트 혹은 파일 공유 사이트 등에서의 파일 다운로드나 실행에는 매우 높은 수준의 주의 필요
- 중요한 자료 백업하기 필수: 정기적 백업 필요

또한 기업이나 기관 차원의 대응으로는 비용 등의 부담 때문에 개인 차원에서 실행하기 어려운 전략을 수립하여 실행할 수 있다. 몇 가지 예방법을 정리하면 다음과 같다.

- 다단계 방어 전략 수립 및 시행
- 정기적이고 일관된 백업 체계 구축과 운영
- OS 및 응용 프로그램에 대한 패치관리 보안 솔루션 구축과 운영
- 스팸 메일 대응과 같은 보안 솔루션 구축과 운영
- 주기적인 보안 교육 실시
- 기타:
  - 각종 프로그램에 대한 화이트 리스트 작성 관리
  - 주요 IT 보안 담당자들에게 보안 심화 교육을 정기적으로 실시
  - 기업에 심각한 영향을 주는 사이버 보안 위반자에 대한 인사상 불이익 제도 운영 등

이러한 내용을 담은 기고문이 2017년 8월에 태국 방콕에서 열린 제29차 ASTAP 포럼에서 가이드라인 형태로 기고되었고, 회의에서는 이를 반영하여 기존에 정보보호 전문가 그룹에서 승인된 가이드라인인 'Guidelines for secure use of IT devices and services – Security: Protect your data –'에 추가적으로 반영하거나 새로운 가이드라인을 만들어 나가기로 결정하였다. 이 가이드라인은 3년여에 걸쳐 개발되어 다양한 상황에서의 사용자를 위한 정보를 제공하고 있는데 올해 세계적으로 문제가 된 랜섬웨어 관련 내용이 추가되어 보급된다면 이를 통해 사용자들이 좀 더 마음 놓고 IT 관련 기기나 서비스를 사용할 수 있을 것이다.

류희수 (경인교육대학교 수학교육과 교수, hsryu@ginue.ac.kr)