PC에 랜섬웨어 바이러스에 대한 경고

곽 수 동
경상대학교 명예교수

우리나라는 사이버안전국가를 만드는 것이 국가의 주요 목표의 하나로 되어있으나 근래에 랜섬웨어 바이러스의 침투로 많은 기업이나 일반인의 PC에 피해가 일어나고 있다.

랜섬웨어 바이러스(Ramsomware virus)란 ?

컴퓨터에 잠입하여 내부문서, 그림파일, 스프레트시트(spreadsheet)[1] 등을 암호화해서 이상한 이름으로 확장자를 바꾸게 하여 열지 못하도록 만든 후 돈을 보내 주면 해독용 열쇠프로그램을 전송해 준다며 금품을 요구하는 악성프로그램으로 컴퓨터사용자의 문서를 인질로 잡고 돈은 요구한다고 해서 ransom(인질의 몸값)과 ware(제품, 프로그람) 두 단어를 결합해 붙여졌다고 한다.

피해가 계속 늘어나고 있다.

19세기에 미국에서 돈을 벌기 위해 금광지역에 사람이 모이듯이 해커들이 돈을 벌 수 있다는 인식이 퍼지고 있어 급속히 확대 전파되고 있다고 한다.

우리나라에서 2016년 상반기에만 피해 건수는 2,000 여 건이라 하며 심각한 문제로 부상하고 있으나 랜섬웨어 대부분이 세계적이고 The Onion Router 라는 익명화된 네트워크 우회방식툴의 웹페이지(webpage)를 이용하기 때문에 각국의 수사당국에서도 추적이 어렵다고 한다.

근래 우리주위 PC에 이 바이러스 침입으로 오래 동안 저장해 모아둔 모든 자료가 갑자기 열리지 않아 낭패를 당하는 사람이 많이 있고 또 누구나 이러한 위험성에 직면하고 있는 것이 현실이다.

이러한 문제는 과거에는 없던 현상이고, 외부 침입 바이러스는 알약(ALYac)이나 V3 · 고클린(GoClean) 등의 바이러스 침입방제 프로그램이 막아 준다고 믿어 왔다.

그러나 이러한 믿음은 우리가 모르는 사이에 2013년 CryptoLocker 랜섬웨어 바이러스 등의 침입자가 처음 나타나면서부터 믿음은 공상으로 변하고 말았다고 하며, 이후 이 바이러스는 2016년까지 계속해서 변종 바이러스가 나와 현재까지 파악된 랜섬바이러스와 그 변종은 20여개 이상이 되고 그 피해대상인 확장자도 xls, xlsx, doc, docx, pdf, txt, jpg, psd, wav, mp4, mpg, avi, wmv 등에서 그 범위가 증가되고 복원방법도 더 복잡하게 되어 해커(hacker)[2]에게 또는 복원회사에 비용을 지불하고 복원하는 수밖에 없게 되었다고 하며 외국의 한 보고에 의하면 수백 종의 이러한 악성바이러스가 전파되었다는 보고가 있다.

1) 데이터 처리를 할 수 있게 되어 있는 컴퓨터 응용 프로그램
2) 해커 : 다른 사람의 컴퓨터 시스템에 침입하여 데이터를 열람 · 변조 · 파괴하는 사람

필자도 피해를 입은 한사람이다.

필자도 2016년 5월 램섬웨어 바이러스 침입으로 인해 컴퓨터에 저장해둔 모든 자료를 잃었고, IT 클럽회원들에 수소문 해보니 나 같이 피해를 입은 회원이 몇 명 있는 것을 확인 하였고 앞으로 피해자가 계속 있을 것으로 생각된다.

랜섬웨어 바이러스로 인해 국내에서는 새로운 복원업체가 많이 생겼다는 것은 놀라운 현실이다. 인터넷에 떠도는 복원업체를 찾아보니 많은 복원사업체가 있고 심지어 각 도시에, 경남에도 창원시, 진주시에 그 복원지점까지 둔 회사도 있었다.

이들 업체들은 저마다 95%이상 복원이 가능하며 믿을 수 있는 사업체이며 저렴한 가격으로 복원해 준다며 요구하는 가격이 100만원 또는 용량에 따라 200만원이 된다고 하여 의뢰를 포기하고 일반 IT 서비스 업체에 문의하니 복원작업은 불가능하고 감염된 바이러스로 인해 앞으로도 피해가 더 진행된다며 모든 프로그램을 지우고 새로 깔아야 한다고 하였다. 아마 피해를 입은 대부분의 분들은 모든 운영체제와 자료를 지우고 다시 깔았을 것으로 생각된다.

그러나 이 바이러스가 운영체제에는 손상을 주지 않고 저장된 자료를 암호화하여 열지 못하게 한다는 것을 생각하고 본 필자는 저장되어 확장자가 바뀐 중요하지 않은 자료는 모두 지우고 꼭 중요하다고 생각되는 자료는 훗날 복원할 기회가 있을 까 다른 USB에 그대로 옮겨두고 오늘까지 약 5개월 이상 그냥 PC를 사용하고 있어도 불편이 없는 실정이다.

나 자신이 복원할 수 있었던 것은 과거에 포스팅(posting)하였던 것은 그 사이트에 자료를 찾아 복사해 복원하기도 하고 다행히도 Zip으로 압축해둔 폴더는 손상이 없어서 그대로 복원할 수 있었다.

필자가 큰 낭패를 본 또 한 가지는 확장자가 바뀐 폴더를 클릭하면 자동으로 인쇄에 기억 저장되어 인쇄를 클릭하면 수많은 바뀐 확장자의 암호자료(?)인 듯 한 자료가 인쇄되어 나오게 되어 당황하게 되었다는 것을 전하고자 한다.

침투 경로는 어떤가

발신지가 명확하지 않은 이메일 첨부파일을 실행 하거나 웹사이트(website) 방문, Web ActiveX 설치, YouTube 등에서 자료나 동영상 등을 다운받아 실행할 때 감염된 자료로부터 침투한다고 한다.

메일에서 첨부된 파일 패턴은 zip, exe, scr, cab, pdf 등의 형식의 파일이라고 하며 이에 대한 PC의 방화벽 장비는 무용지물이 된다고 한다.

피해 범위는 어떤 파일인가

침입하는 파일은 문서, 엑셀, 이미지 파일등의 개인파일들로의 확장자는 xls, xlsx, doc, docx, pdf, txt, jpg, psd, wav, mp4, mpg, avi, wmv 등이라고 하며 모든 한글문서도 여기에 포함된다.

방제하는 방법이 쉽지 않다

랜섬웨어 바이러스에 대처하는 방법은 ① PC상태를 최신버전으로 업데이트 하고 ② PC 및 서버의 모든 데이터(data)는 백업해 두고 ③ 웹페이지(webpage) 접속시 사이트 및 파일 안전 확인 등 몇 가지를 제시하고 있으며, 회사나 단체에서 공유 폴더는 권한이 있는 사용자만 접근하게 해당 공유폴더를 "숨김 공유 설정"하도록 권장하고 있으나 전문가가 아닌 일반사용자는 이들 사항들을 준수하기는 어려울 것 같아 감염에 무방비 상태인 것 같다.

복원방법은 복원업체에 돈을 주고 의뢰하는 수밖에 없다

외국에서는 백신업체들에서 복구프로그램들을 무료로 배포한다고 하나 계속 변종이 전파되어 이들 파일을 복구하는데 한계가 있기 때문에 백업만이 랜섬웨어의 피해를 최소화 할 수 있는 방법이라고 한다.

원본 파일 자료를 미리 복사본을 만드는 것을 백업(backup)이라 하는데 일반사용자는 미리 USB에 별도로 폴더를 백업해서 보관해 두는 것을 생활화 할 것을 권장하고 있다.

필자의 경우 알집으로 압축해둔 폴더는 손상이 없어 복원하는데 이용했다는 것을 처음 알리고자 하며 아마 이 방법도 활용해도 도움이 될 것 같다. 만약 피해를 입으면 우리나라에서는 복원업체에 돈을 주고 복원하는 방법밖에 없는 것 같고 누구에게 하소연 할 때도 없는 것 같다.