24. "당신의 컴퓨터가 암호화되었습니다, 풀려면 돈을 지불하세요"

작년에만 4400건, 랜섬 웨어 극성… 이메일·광고창 클릭 통해 감염병원·기업·학교 등이 주 타깃…최근엔 일반인 피해도 늘어나

어느 날 갑자기 컴퓨터 화면에 "당신의 컴퓨터가 암호화되었습니다"는 표시가 뜬다. 그러고 작업 중이던 파일과 저장된 자료가 열리지 않는다. 당황하는 당신에게 이어지는 메시지. "암호를 풀려면 암호 해제 프로그램을 사야 합니다. 2비트코인(bitcoin·가상 화폐)을 지불하세요."

사이버 범죄의 일종인 '랜섬 웨어(ransom ware)'가 한국에도 상륙해 기승을 부리고 있다. 컴퓨터의 중요 데이터를 암호화해 쓰지 못하게 하고, 이를 풀어 주는 대가로 돈을 요구한다. '랜섬(ransom·몸값)'이라는 말뜻대로 컴퓨터의 데이터를 인질로 삼아 몸값을 요구하는 것이다. 학교와 병원, 기업에서 피해 사례가 속출한 데 이어, 최근엔 인터넷 커뮤니티 사이트를 통해 대중을 상대로 랜섬 웨어가 퍼지면서 문제가 심각해지고 있다.

◇컴퓨터 데이터를 인질로 몸값 요구

랜섬 웨어는 컴퓨터 바이러스 같은 '악성코드(malware)'의 일종이다. 이메일이나 인터넷 사이트, 불법 복제 소프트웨어 등을 통해 주로 전파되며, 운영체제나 웹브라우저의 보안 취약점을 이용해 PC 내로 침투해 활동한다. 출처가 불분명한 이메일의 첨부 파일을 열어 보거나 인터넷 커뮤니티 사이트에 올라온 동영상 등을 열어 보는 것으로 감염될 수 있다. 심지어 인터넷 사이트에 접속했을 때 뜬 광고창을 통해 감염된 사례도 있다.

랜섬 웨어는 단순히 파일을 삭제하거나, PC의 정상적인 작동을 방해하고, 다른 PC를 감염시켜 특정 목적에 이용하는 것에 그치지 않는다. 이 악성코드는 메모리상에서 계속 실행 상태로 있으면서 컴퓨터 내의 다양한 파일들을 계속 암호화한다. 업무용으로 많이 쓰는 오피스 파일(xls·doc·ppt)과 한글 파일(hwp), 사진 파일(jpg·png), PDF 파일(pdf), 그림 파일(psd) 등이 대상이다.

랜섬 웨어에 감염되면 PC가 갑자기 바빠진다. 하드 드라이브(HDD)에 있는 파일들을 계속 읽어들여 암호화하기 때문이다. 이런 식으로 암호화된 파일들은 일반적인 방법으로 열리지 않는다. 암호를 풀어주는 '복호화 프로그램'이 있어야 한다. 랜섬 웨어를 유포한 해커들은 이러한 복호화 프로그램을 주겠다며 돈을 요구한다. 본격적인 범죄의 단계로 접어드는 것이다.

계좌로 돈을 주고받으면 바로 추적을 당하므로 보통 가상 화폐인 비트코인을 요구한다. 경찰청 사이버수사팀 관계자는 " 0.5~2비트코인 정도를 부르는데, 최근 시세로 따지면 280~1100달러(약 127만원)인 셈"이라며 "하지만 이 돈을 준다고 해서 해커가 진짜로 암호를 풀어주는 경우는 매우 드물다"고 했다.

◇지난해만 4400여 건 발생, 백업 자주 해야

지난 2005년부터 해외에서 주로 등장했던 랜섬 웨어는 지난해부터 우리나라에도 등장하기 시작했다. 보안 업체 시만텍에 따르면 지난해 국내에서 발생한 랜섬 웨어만 4400건에 달했다. 특히 중요한 데이터를 많이 갖고 있는 기업이나 학교, 병원 등을 타깃으로 한 랜섬 웨어 범죄가 빈발하고 있다.

보안 업계 관계자는 "서울의 한 대학교, 부산의 대형 병원, 경기도의 중견 기업 등에서 이런 랜섬 웨어 피해 사례가 보고됐다"면서 "랜섬 웨어를 덫처럼 설치해놓고 걸려들기를 기다리는 수법"이라고 했다. 최근에는 국내 한 커뮤니티 사이트를 통해 랜섬 웨어가 확산한 것으로 알려졌다. 이 커뮤니티 사이트에서 보인 광고 배너 중 일부에 랜섬 웨어가 심어져 있었던 것이다.

랜섬 웨어에 일단 감염되면 이를 돌이키기 매우 어렵다. 결국 감염되지 않는 것이 상책(上策)이다. 보안 업체 하우리 관계자는 "랜섬 웨어 공격자들이 한국을 하나의 시장으로 인식하면서 한글 버전 랜섬 웨어도 등장하고 있다"면서 "의심스러운 이메일이나 웹페이지의 첨부 파일은 열어 보지 말아야 한다"고 했다. 또 불확실한 내용의 광고창이나 링크 역시 함부로 클릭해서는 안 된다.

무엇보다 중요한 업무용 파일을 자주 백업하는 것이 좋다. 보안 업계 관계자는 "별도 외장 하드나 클라우드(인터넷 저장소)를 이용해 중요 파일은 주기적으로 자동 백업되도록 설정하면 랜섬 웨어에 감염됐을 때 피해를 최소화할 수 있다"고 조언했다.