2021.05.16

우리 삶에 깊숙이 내재된 악성 프로그램, 랜섬웨어

랜섬웨어에 대한 모든 것 파헤치기

Ransomware

= Ransome(몸값) + Ware(제품)

최근 들어, 랜섬웨어로 피해를 보는 대상의 스펙트럼이 개인에서 기업으로까지 넓어지고 있다. 그러면, 우리가 사전에 랜섬웨어를 어떻게 예방할 수 있을까?

지금부터 랜섬웨어가 무엇인지, 더 나아가 화제가 되고 있는 랜섬웨어의 종류와 예방 방법에 대해 알아보자.

Q. 랜섬웨어란..?

컴퓨터 시스템을 감염시킴으로써 접근을 제한하고, 이를 불모로 금전을 요구하는 악성 소프트웨어이다.

2005년 러시아에서부터 발생하기 시작한 랜섬웨어는 사람들이 흔히 사용하는 확장자명의 파일을 중심으로 암호화하기 시작했다.

하지만, 2011년에 들어서서는 특정 번호로 연락을 하여 결제를 유도하게 하는 방식으로 까지 나아가게 되었다.

랜섬웨어 중 가장 유명한 '크립토락커'(CryptoLocker)는 마이크로소프트 윈도우 운영체제를 사용하는 x86컴퓨터 대상으로 시작한 랜섬웨어이다.

이외에도, 다양한 종류의 랜섬웨어들이 등장하기 시작했으며 정보유출 뿐만 아니라 파일 암호화를 동시에 진행하는 '타깃형 랜섬웨어' 공격도 나타나고 있다.

최신 랜섬웨어 종류 알아보기

1. Snake 랜섬웨어

주로 기업을 노리는 랜섬웨어로, 산업용 제어 시스템(ICS)과 관련된 프로세스 일부를 종료시키며 감염된 시스템의 파일을 암호화시킨다.

2. Ravack 랜섬웨어

불법 소프트웨어를 운영하는 유튜버가 유포한 랜섬웨어로, 영상을 통해 불법 소프트웨어 자료를 다운받도록 유도하고 이 과정에서 악성코드가 실행되도록 한다.

3. Mailto 랜섬웨어

NetWalker라고도 불리는데, 주로 피싱메일 방법을 이용하여 유포하고 있다.

랜섬웨어를 예방하는 방법은 무엇일까?

일반인들이 랜섬웨어를 직접 치료하기는 어렵지만, 발생하지 않도록 예방하는 방법은 여러가지가 존재한다.
아래의 3가지 방법을 이용하여 랜섬웨어를 예방하도록 하는 것이 가장 바람직하고 쉽다.

1. 파일 확장자명 나타내기

평소 파일들을 쉽게 다운받고 여는 경우가 많은데, 먼저 확장자명의 여부를 판단하고 만약 없다면 폴더 옵션으로부터 수정할 수 있도록 해줘야 한다.

2. 사이트 방문 주의하기

가장 기본적인 것이 그만큼 중요하다고 볼 수 있다. 평소에 사이트를 방문할 때 접근을 허용해달라는 팝업창이나 컴퓨터 시스템 자체에서 연결을 거부하는 사이트라면 더더욱 조심해야 한다.

3. 소프트웨어 주기적 업데이트 & 백신 설치

소프트웨어가 최신 버전이 아니라면 이와 관련한 취약점 공격이 이루어질 수 있다. 하지만, 일반 사용자들이 소프트웨어를 전문적으로 관리하기는 어렵다. 따라서, 국내에서 제공하는 다양한 백신 서비스를 활용하면 더욱 손쉽게 컴퓨터를 예방할 수 있다.

[랜섬웨어 한눈에 요약해보기]

랜섬웨어는 최근 발생하고 있는 컴퓨터 악성 프로그램 중 일부로, 2005년 러시아에서 시작해 지금은 전 세계적으로 퍼져나가고 있다. 가장 대표적인 랜섬웨어, '크립토락커'를 시작해 현재 코로나 19바이러스를 악용한 랜섬웨어들이 대거 등장하고 있다. 랜섬웨어의 방식은 다양하다. 주로, 특정 사이트로 접속을 유도하거나 파일을 다운받도록 한다.

그러면 랜섬웨어를 사전에 예방할 수 있는 방법이 없는가? 당연히 있다. 예를 들면, 파일 확장자명 나타내기, 사이트 방문 시 주의하기, 소프트웨어 업데이트하기 등이 존재한다.

하지만, 일반인들이 직접적으로 랜섬웨어를 치료하기 어려우므로 전문가의 도움을 얻어 예방할 수 있도록 하는 것이 가장 바람직하다.