//1. 랜섬웨어 의 의미 2. 랜섬웨어의 역사 3. 랜섬웨어의 작동과 예방법

Ransomware

Ransomware란 무엇인가? // What is the Ransomware

몸값을 뜻하는 ransom과 software의 ware가 합쳐진 합성어로

사용자의 동의없이 컴퓨터에 불법으로 설치되어 사용자의 파일을 암호화시켜 인질로 잡아 금전을 요구하는 악성 프로그램을 말한다.

초창기의 랜섬웨어는 2005년 러시아에서 처음 확인되었고 2006년에 보고된 랜섬웨어가 특정 유형의 파일들을 압축하여 암호를 설정하여 300달러를 지불하면 파일을 복원시켜 주겠다는 메세지를 남기는 간단히 구현된 형태 였습니다.

하지만 비트코인과 크립토락커가 등장하면서 랜섬웨어는 널리 알려지게 됩니다.

비트코인은 쓰는 방법에 따라 거래내역은 추적이 되나 거래자의 정보를 알 수 없는 화폐로 이런 범죄에 사용되면 추적이 무척 어려워지는 특징이 있고

크립토락커는 2013년에 발생한 랜섬웨어의 일종으로 컴퓨터 내의 모든 파일 및 네트워크 드라이브의 파일을 RSA, AES키로 암호를 걸어 암호 해독키를 대가로 돈을 요구하는 현재 발생하는 랜섬웨어 형태의 시초이다.

이들이 등장하면서 해커들은 비교적 안전하면서 키 없이 거의 절대적으로 풀 수 없는 암호화로 손쉽게 돈을 벌 수 있게 되었다

널리 퍼짐에 따라 여러 발전된 변형들이 생겼는데 크립토락커.F, 토렌트락커, 크립토월, 워너크라이등 랜섬웨어는 더욱 강력하고 위험해졌다.

다음이 가장최근 2017년 5월에 발생한 워너크라이라는 랜섬웨어의 구동영상입니다.

랜섬웨어에 감염된 사이트나 감염된 메일을 확인하여 감염파일이 내 컴퓨터에 접근하게 되면 암호화가 시작되고 조금 있으면 파일의 확장자가 바뀌면서 금전을 요구하는 창이 뜨게됩니다. 파일들은 모두 암호화 되어 원래 텍스트 파일이었던 파일을 열어 보아도 암호화가 되어 글자가 전부 깨져 보이는것을 확인할 수 있습니다.

이러한 랜섬웨어를 예방하기 위한 방법은 무엇이 있는가?

없다. 단지 백업을 철저히 해놓는 것 만이 가장 좋은 해결책으로 제시 될 뿐 이 랜섬웨어를 원천 차단할 수 있는 방법은 없다. 그나마 항상 os의 업데이트를 최신으로 해놓아서 랜섬웨어들이 공격할 만한 취약점을 최소화 하는것이 가장 나은 방법일 것이다.