[카드뉴스] 무심코 연 파일에 랜섬웨어가? 랜섬웨어 예방법

시스템을 잠그거나 데이터를 암호화하여 사용할 수 없도록 한 뒤, 이를 인질로 삼아 금전을 요구하는 악성 프로그램 랜섬웨어. 랜섬웨어의 감염 경로와 예방수칙, 대처법을 알아본다.

랜섬웨어란?

Ransom(몸값)
+
Software(소프트웨어)

시스템을 잠그거나 데이터를 암호화하여
사용할 수 없도록 한 뒤, 이를 인질로 삼아
금전을 요구하는 악성 프로그램입니다.

koscom NEWSROOM

랜섬웨어의 감염경로

응용 프로그램이나 운영체제의 취약점을 공격해
악성코드를 감염시키는 **익스플로잇 킷**,
이메일을 통한 **URL** 또는 **첨부파일**,
광고 서비스의 **멀버타이징** 등이 있습니다.
이 외에도 다양한 경로를 통해 감염될 수 있으며
수법이 날로 진화하고 있습니다

서버를 공격하는 랜섬웨어

중소기업, 병원 등 기관을 대상으로 서버 및
데이터베이스를 공격하는 **서버 타깃형**도 있습니다.
랜섬웨어를 공격받아 암호화가 시작되면
파일의 확장자가 변화하게 되어 실행이 불가능해집니다.
랜섬웨어의 종류 별로 패턴이 각각 다르거나 매번 랜덤한
암호를 만들어내는 **매그니베르**와 같은 타입도 있습니다.

한국에서만 작동하며 이외 국가 사용자일 경우에는 암호화를 진행하지 않고
자기자신을 삭제하게끔 설계되어 있다.주로 윈도우, IE의 보안 취약점을 통하여 유포된다.

예방이 중요한 이유

개발자가 체포되어 암호 키를 압수하거나,
랜섬웨어 자체적인 결함으로 인해 복구될 수 있는
경우가 간혹 있지만 일반적으로 **이미 감염된**
PC를 복구하는 것은 매우 어렵기 때문에
무엇보다 **미리 예방**하는 것이 **가장 중요**합니다.

랜섬웨어 예방수칙

1

중요한 자료는 반드시 별도 매체에
정기적으로 백업합니다.

문서 사진 ▶ 별도 매체 백업

2

출처가 불분명한 이메일과 메시지 등의
URL 링크는 실행하지 않습니다.

스팸메일 첨부파일 URL 링크 ▶ 실행 주의

출처 : 과학기술정보통신부

랜섬웨어 예방수칙

3

신뢰할 수 없는 사이트 등에서
파일 다운로드를 하지 않습니다.

파일공유 사이트 신뢰할 수 없는 사이트 ▶ 실행주의

4

모든 소프트웨어는 최신 버전으로
업데이트하여 사용합니다.

운영체재 OS 응용프로그램 SW ▶ 최신 업데이트

출처 : 과학기술정보통신부

랜섬웨어 예방수칙

5

최신 버전의 백신을 설치하고
실시간 감시를 실행합니다.

백신 안티 익스플로잇 도구 ▶ 설치, 최신 업데이트

출처 : 과학기술정보통신부