# 랜섬웨어로부터
# 어떻게 당신의 비즈니스를 보호할 수 있을까?

랜섬웨어로부터 회사 파일이 표적이 되지 않도록 사전 대책을  세우세요.


Malwarebytes | EMSISOFT

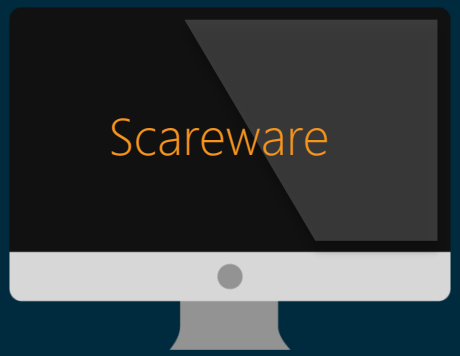
# 랜섬웨어 위험도별 3단계

**랜섬웨어 ( Ransomware )**

랜섬웨어는 요구한 돈이 지불될 때까지 시스템에 대한 액세스를 차단하도록 설계된 악성 소프트웨어 중 하나입니다.

## 낮 음

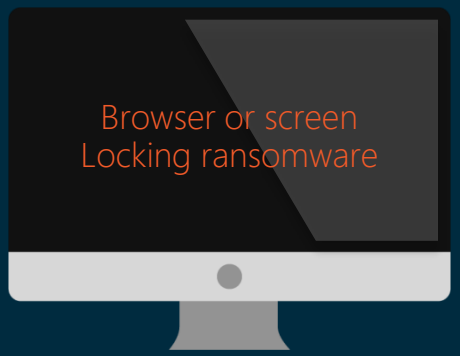
☆




거짓 안티 바이러스 도구로 멀웨어 문제를 탐지하고, 이를 해결하기 위해 지불을 요구합니다.

## 중 간

☆☆




가짜 FBI 또는 미국 법무부 메시지를 사용하여 컴퓨터에서 불법 활동을 감지했다며 벌금을 요구합니다.

## 가장 위험

☆☆☆


팝업 메시지로 귀하의 파일이 암호화되어 있고, 이를 해제하기 위해서는 기한까지 돈을 지불할 것을 요구합니다.

# 비즈니스에서 암호화된 랜섬웨어는 얼마나 위험할까요?

## 빈 도

해마다 크고 작은 회사에서 수백만 건의 랜섬 공격이 시도되고 있습니다.

NPR, All Things Considered, 2/22/16

## 데이터

랜섬웨어는 회계, 의료 데이터 또는 고객의 기밀 정보와 같은 회사 중요 파일을 암호화할 수 있습니다.
일단, 암호화되면 대가를 지불하지 않으면 파일을 다시 가져올 수 없습니다.

## 돈

2016년 2월 할리우드 장로교 병원은 해커로부터 환자 데이터를 검색하기 위해 17,000달러를 지불했습니다. 보고서에 따르면 1,000개의 레코드가 손실되면 기업은 37,000달러 이상의 손실을 입을 것으로 보고 있습니다. 위반 규모가 커지면 비용-비즈니스-가 기하 급수적이 됩니다.

## 평 판

일부 최신 형태의 랜섬웨어는 파일 암호화 뿐만 아니라 온라인에 해당 정보들을 누출하기도 합니다.

## 돈을 지불해야 할까요?

FBI 및 기타 법 관련 공무원은 개인 및 기업이 몸값을 지불하도록 권장할 수 있습니다.
이는 파일을 검색할 수 있는 가장 빠른 방법입니다.
그러나 사이버 보안 전문가는 이를 권장하지 않습니다.
몸값을 지불하면 파일에 다시 액세스할 수 있다는 보장이 없기 때문입니다.
또한 향후 멀웨어 감염의 타켓이 될 수 있습니다.

Malwarebytes | EMSISOFT

# 다음과 같이 컴퓨터가 취약하다면…

1. 기존 소프트웨어를 사용합니다.
2. 브라우저 및 OS가 패치되지 않고 오래 되었습니다.
3. 정기적인 백업 계획이 없습니다.
4. 포괄적 사이버 보안 전략이 부족합니다.

**- 최상의 보호는 사전 예방입니다 -**

Malwarebytes | EMSISOFT

# 사전 예방

"최상의 보호는 예방입니다."
랜섬웨어가 비즈니스에 해를 끼치지 않도록 하려면 다음 단계를 수행하십시오.

## 1. 시스템 패치

브라우저, OS 및 기타 소프트웨어 응용 프로그램을 최신 상태로 유지하십시오.

NPR, All Things Considered, 2/22/16

## 2. 사용자 교육

컴퓨터가 랜섬웨어에 감염되는 가장 일반적인 방법 중 하나는 사회 공학을 사용하는 것입니다.
피싱 캠페인, 의심스러운 웹 사이트 및 기타 사기를 탐지하는 방법에 대해 사용자를 교육합니다.

## 3. 파일 백업

정기적으로
데이터의 안전한 복사본을 만들고,
이를 오프 사이트에 저장하십시오.

- 백업 파일이 매핑된 드라이브에 저장되어 있지 않은지 확인하십시오. 랜섬웨어의 일부 변형은 매핑되지 않은 네트워크 공유를 통해 파일을 암호화할 수도 있습니다.
- USB 또는 외장 하드 드라이브에 백업하는 경우 장치가 컴퓨터에서 물리적으로 분리되어 있는지 확인하십시오.
- 고급 암호화 및 다중 요소 인증을 사용하는 보안 클라우드 서버의 스토리지를 권장합니다.

## 4. 계층화된 보안에 투자

사이버 보안 보호의 여러 계층을 설치하면 랜섬웨어 공격이 발생하기 전에 탐지하고 차단할 수 있습니다. 최상의 보호를 위해 다음과 같이 레이어를 사용하는 것이 좋습니다.

- 방화벽
- 안티-익스플로잇
- 액티브 모니터링을 갖춘 안티바이러스
- **안티-멀웨어**
- 안티-랜섬웨어

## 감염된 경우 어떻게 해야 하나요?

책임감있게 파일을 백업한 경우 모든 희망이 사라지는 것은 아닙니다.
백업되지 않은 다른 PC에서 멀웨어가 있는지 검사하십시오. 그런 다음 감염된 시스템에서 검사를 실행하여 랜섬웨어 또는 기타 멀웨어의 흔적을 치료하십시오. 백업이 깨끗한 경우 백업본을 컴퓨터에 복원할 수 있습니다.

Malwarebytes | EMSISOFT


랜섬웨어 사전 예방 조치의 첫 단계로
안티 - 멀웨어 제품을 사용해보세요
Malwarebytes
www.malwarebytes.co.kr
EMSISOFT
www.emsisoft.co.kr
SoftMail
Tel. 1661-9331 / E-mail : sales@softmail.co.kr