

랜섬웨어 킬체인 차단

측면 이동을 차단하는 5단계

하나의 머신 또는 디바이스가 감염되었다고 랜섬웨어가 확산되지는 않습니다. 사이버 범죄자들은 이러한 멀웨어 변종을 이용해 최대한 많은 네트워크 정보를 암호화함으로써 피해자에게 랜섬을 갈취합니다.



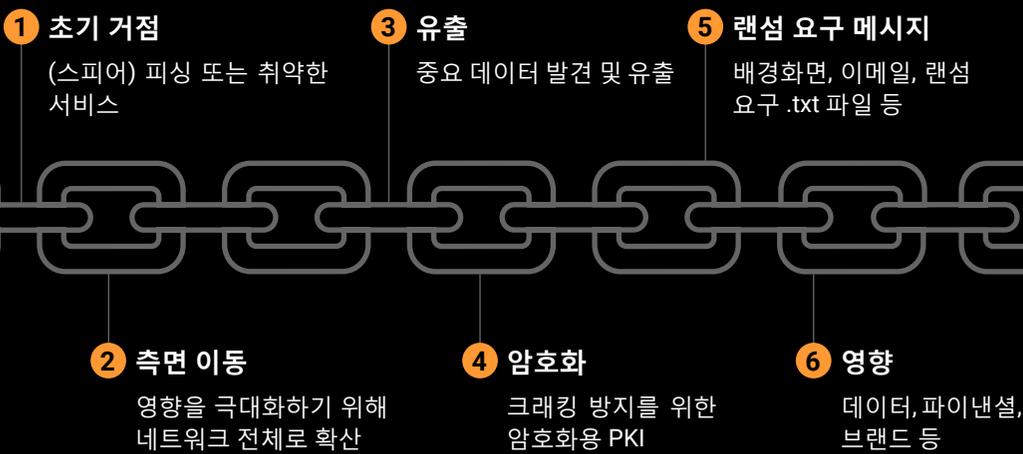
2031년까지 랜섬웨어가 2초마다 기업, 소비자, 디바이스를 공격할 것으로 예상됩니다.

[사이버 보안 벤처 랜섬웨어 시장 보고서\(Cybersecurity Ventures Ransomware Market Report\)](#)

기존의 네트워크 보안을 확신하고 계신가요?

세그멘테이션을 위해 레거시 방화벽을 계속 사용하고 있다면 랜섬웨어가 네트워크 전체에 확산되어 중요한 애플리케이션과 인프라가 락다운되는 상황을 막을 수 없습니다.

랜섬웨어 킬체인



유출은 불가피합니다

동서 데이터 센터 트래픽의 위협을 탐지하고 측면 이동을 차단하는 보안 솔루션이 필요합니다.

체인 차단



준비 - IT 환경에서 실행되는 모든 애플리케이션과 자산 파악



방지 - 일반적인 랜섬웨어 전파 기법을 차단하는 룰 생성



탐지 - 세그멘테이션된 애플리케이션 및 백업에 대한 접속 권한을 얻으려는 모든 시도에 대한 알림 수신



조치 - 공격 탐지 시 스레드 억제 및 격리 조치 시작



복구 - 단계별 복구 전략을 지원하는 시각화 기능 활용

2022년의 랜섬웨어 공격은 지난 5년의 공격을 합친 것보다 약 13% 증가했습니다.

[Verizon 2022 Data Breach Investigations Report](#)

빈번한 공격과 비용이 많이 드는 랜섬 요구로부터 아직 방어할 준비를 갖추지 못했다면, 이제 방어 전략에 세그멘테이션과 가시성을 통합할 때입니다.

[자세히 알아보기](#)