쿼드마이너 랜섬웨어 대응방안

네트워크 보안

- 침입탐지시스템(IDS): 비정상적인 파일 암호화 시도를 감지하여 랜섬웨어 공격을 초기에 막을 수 있다.
- 프로토콜 분석도구: 비정상적인 외부 통신을 감지하고, 알려지지 않은 IP나 비정상적인 포트를 사용하는 통신을 식별하여 랜섬웨어의 존재를 파악하는 데에 도움을 준다. 또한 비정상적인 대량 트래픽이나 스캔 활동을 감지하여 랜섬웨어의 내부 확산을 미리 인지할 수 있도록 한다.

시스템 보안

- 패치관리시스템(PMS): 패치 여부를 확인하고 새로운 패치가 있다면 보안 패치를 진행하도록 유도하여 2차 피해를 막을 수 있도록 한다.

애플리케이션 보안

- 웹방화벽(WAF): 웹 기반의 공격(SQL 인젝션, XSS 등)으로부터 서버를 보호하여 웹 취약점을 통한 랜섬웨어 침투를 방지하고, 웹사이트를 통한 악성코드 유포를 막는 데 기여한다.
- 스팸메일차단솔루션: 랜섬웨어 감염의 주요 경로가 바로 스팸메일이기 때문에 추가 감염 방지, 재발 방지를 위해 필요하다.

통합 보안관리

- 보안구성관리(SCM): 시스템, 네트워크 장비, 애플리케이션 등이 안전한 보안 구성 표준에 따라 설정되고 유지되도록 관리하여 랜섬웨어의 침투 경로를 줄이고, 시스템 및 서비스의 취약점 노출을 최소화하며, 감염 시 확산을 어렵게 한다.

인증 및 접근통제

- 통합접근관리(EAM): 외부 사용자가 제한된 범위 내에서만 네트워크에 접근할 수 있도록 하며, 기밀 정보와 시스템에 대한 보안을 유지할 수 있다. 모니터링을 통해 침입 시도나 데이터 유출 등의 위험을 조기에 파악 가능하다.

PC 보안

- 개인용 PC 방화벽: 개별 PC에서 허용되지 않은 네트워크 통신을 차단하고, 악성코드가 외부와 통신하거나 다른 PC로 확산되는 것을 막아주면서 1차 방어선 역할을 수행할 수 있다.

기타 보안

- 무선랜 보안(Wireless): 인가된 사용자만 접근할 수 있도록 하며, 송수신된 자료들이 의도된 대상에 의해서만 처리되도록 한다.

보안 서비스

- 솔루션 유지보수: 도입된 모든 보안 솔루션이 최신 상태를 유지하고, 성능을 최적화하며, 새로운 위협에 대응할 수 있도록 지속적인 업데이트과 관리를 제공한다.