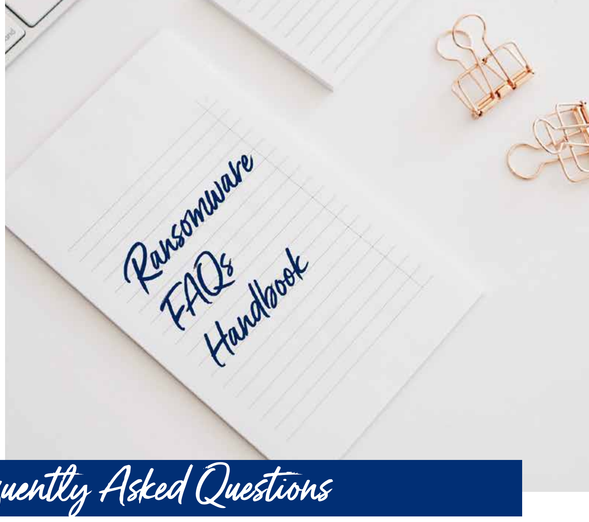
AhnLab

랜섬웨어 FAQs 핸드북



10 Frequently Asked Questions

Q. 최근 랜섬웨어 공격 동향은?

A. 랜섬웨어 공격 빈도는 줄어 들었으나 기법이 고도화 되면서 피해 규모는 커지고 있다. 공격 조직들은 무차별적인 랜섬웨어 유포로 몸값을 받아내는 고전적인 전략을 벗어나, 가치 있는 정보를 보유한 기업을 타깃해 주요 정보를 탈취하고 금전도 노리는 방식을 취하기 시작했다.

Q. 랜섬웨어 공격 시나리오 중 피해사례가 가장 많은 유형은?

A. 악성 이메일을 통한 정보탈취 악성코드가 여러 기업과 기관을 대상으로 유포되고 있다. 일정 규모 이상의 조직들에 대해서는 이미 내부 IT 인프라 분석과 공격 사전 작업이 상당히 진행되었을 가능성이 있다. 실제, 안랩이 진행한 주요 시스템 분석 과정에서 최종 랜섬웨어 공격 발생 전 단계까지 진행된 케이스가 보고된 경우도 있다.

Q. 효과적인 랜섬웨어 보안 전략 수립은 어떻게 해야 하나?

A. 현재의 고도화된 랜섬웨어 공격은 견고한 방어 체계를 통해 위협을 '최소화'한다는 관점으로 접근해야 한다. 이를 위해서는 준비(prepare), 예방(prevent), 탐지(detect), 완화(mitigate), 복구(recover), 5단계에 맞는 정책, 프로세스, 툴 등 대응 전략을 갖춰야 한다. 또, 네트워크, 이메일, 엔드포인트 각 구간별 운영 중인 솔루션 정책 최적화를 통해 위협을 최소화할 수 있다.

Q. 랜섬웨어를 100% 예방할 수 있는 방법은?

A. 견고한 보안 체계를 수립한다면 랜섬웨어 감염 가능성을 최소화할 수 있으나, 어떤 솔루션도 100% 랜섬웨어 예방을 보장할 수는 없다. 가장 효과적인 방법은 주요 자산부터 우선순위를 정해 최적화된 보안 정책, 솔루션, 인력 운영을 바탕으로 영역별 위험성을 최소화하고 취약한 부분을 지속적으로 점검해 업데이트 하는 것이다.

Q. 랜섬웨어 공격의 주요 타깃인 파일 서버 보안 방안은?

A. 파일 서버 보안은 크게 2가지를 검토해야 한다. 먼저, 파일 서버로 침투해 내부 데이터를 탈취하는 경우, 접근 통제와 권한 관리가 기본이며 추가로 지능형지속위협(APT) 솔루션의 취약점 스캔을 활용해 접근 시도를 탐지할 수 있다. 서버 저장 파일에 악성코드를 심어 감염 확산을 시도하는 경우, APT 솔루션의 미러링 방식을 통해 저장 및 다운로드 되는 파일을 실시간으로 검사하고 알람을 확인해 대응할 수 있다.

Q. 최근 성행하는 파일리스 랜섬웨어 대응 방안은?

A. 안랩의 경우, 안티 멀웨어 솔루션 V3와 APT 솔루션 AhnLab MDS를 통해 파일리스 랜섬웨어 탐지 및 차단 방안을 제공한다. 최근 발견되는 파일리스 랜섬웨어는 공격 경로를 확대해 나가는 모습을 보이고 있다. 일례로, 매그니베르 랜섬웨어는 기존 인터넷 익스플로러 뿐만 아니라 크롬과 엣지까지 공격에 활용하는 것으로 파악됐다. 효과적인 대응을 위해서는 솔루션의 최신 엔진 업데이트 및 행위분석 엔진 활성화가 필요하다.

Q. 망분리 환경은 랜섬웨어로부터 안전하다고 볼 수 있나?

A. 망분리 환경도 100% 안전하다고 보기는 어렵다. 망연계 솔루션 간 이동되는 파일을 통해 내부망 환경에서 랜섬웨어에 감염된 사례도 있다. 내부망 보안 강화를 위해 안랩이 제시하는 방안은 망연계 솔루션과 APT 솔루션 AhnLab MDS 연동을 통해 내부망으로 이동되는 파일을 전수검사하여 안전한 파일만 망간 이동되도록 하는 것이다. 또, MDS 에이전트를 내부망 PC에 설치해 사용자 PC에서 실행되는 의심 파일 및 문서를 가상환경에서 추가 분석 후 안전한 파일만 실행되도록 해야 한다.

Q. 재택근무 환경에서 랜섬웨어 예방을 위한 방안은?

A. 재택근무 시 사용하는 PC에 대해 기업 내부 PC와 유사한 수준의 보안성을 유지해야 한다. 기본적으로 백신을 설치해 업데이트를 최신 상태로 유지하고 VPN 인증 시 계정 및 패스워드 방식 외에 추가 인증 활용이 필요하다. 안랩의 경우, 엔드포인트 보안 플랫폼(EPP)와 VPN 솔루션을 연동하여 PC의 악성코드 감염여부 등 보안 상태를 실시간 체크하는 솔루션도 제공한다.

Q. 랜섬웨어 감염에 대비한 효과적인 백업 방법은?

A. 랜섬웨어 공격 시 치명적인 피해를 줄 수 있는 자산부터 우선순위를 정해 백업 정책을 운영해야 한다. 세부 정책 운영 방안은 컨설팅을 통해 확인하는 것이 효율적이다. 운영체제(OS)를 상이하게 하는 것도 랜섬웨어 피해를 줄이는데 도움이 된다. 다만 일반 PC는 윈도우, 백업 서버는 리눅스 환경이라 해도 상시연결(mount) 되는 상태라면, 랜섬웨어 동작 시 백업 서버 파일도 암호화된다. 따라서, 백업이 필요한 시점에만 시스템 간 접근이 이루어지도록 관리해야 한다.

Q. 랜섬웨어 대응 측면에서 안랩만의 장점은 무엇이 있나?

A. 안랩은 특정 영역에만 특화된 보안 기업들과는 달리 랜섬웨어 공격이 시도되는 모든 영역에서 정보를 수집하고 대응할 수 있는 인프라를 갖추고 있다. 이를 바탕으로 엔드포인트, 네트워크, 이메일까지, 넓은 영역에서 통합 보안 솔루션 체계를 제공한다. 또한, 전문 분석가가 진행하는 보안관제, 악성코드 분석 서비스 및 포렌식(forensic)에서 수집된 데이터를 기반으로 공격을 실시간 차단하는 클라우드 데이터베이스 인프라와 솔루션별 엔진을 배포한다.