

랜섬웨어 감염 대응을 위한 보안권고

<‘26.09.21(월), 의료정보보호센터>

□ 개요

- 최근 추석 연휴를 앞두고 의료기관의 주요 의료정보시스템(EMR, PACS, 검진서버, 전자동의서 등)을 대상으로 랜섬웨어 공격이 증가함에 따라 해킹사고가 발생하고 있습니다.
- 의료기관에서는 피해 예방을 위해 진료기록, 영상정보 등 민감 정보를 보유하고 있기에 각별한 주의 필요하며 아래와 같이 점검 및 보안관리 강화 조치하여 주시기 바랍니다.

□ 조치 방안

확인 사항	조치 방법
① 원격 프로그램(Teamviewer, Anydesk)이 확인 될 경우	즉시 프로그램 삭제
② 랜섬웨어 파일 확인 될 경우 (C:/사용자/사용자명/문서/locker/locker.exe)	즉시 locker.exe 파일 삭제
③ 파일 암호화 및 확장자명 .nspire가 확인 될 경우	locker.exe 실행 종료 네트워크 케이블 탈거
②번 또는 ③번 사항이 확인 될 경우	의료정보보호센터 신고 (www.hisc.or.kr)

□ 기타 사항

- 기타 문의사항 의료정보보호센터로 연락하여 주시기 바랍니다.
- (연락처) 의료정보보호센터
 - email: cert@hisac.or.kr
 - Tel: 02-6360-6280