**설 연휴 대비 랜섬웨어 피해주의 권고**

**출처 : 인터넷침해대응센터**
**작성일 : 2020.01.15**

□ 개요
o 최근 공정거래위원회로 위장하는 등 정부기관, 국내 업체, 입사지원서 등을 사칭한 피싱 메일을 통해 랜섬웨어 유포가 지속되고 있어 국내 감염피해 주의
o Nemty, Sodinokibi, Clop, Revil 등 랜섬웨어는 컴퓨터 파일을 암호화 한 뒤 해독키를 제공하는 대가로 금전을 요구

□ 주요내용
o 랜섬웨어 공격자는 지난 해 클롭(CLOP), 갠드크랩(GandCrab), 소디노키비 등 유포 시 해킹메일, AD서비스 및 취약점 등을 악용
- (해킹메일) 갠드크랩, 소디노키비 등 랜섬웨어가 첨부된 이메일을 정상 발송자로 위장하여 첨부파일을 열어보도록 유도
- (AD서비스) 윈도우 AD서버를 공격하여 기업 내부망으로 랜섬웨어를 유포시키는 형태로 지난 해 클롭 랜섬웨어 등이 해당
- (취약점) VPN 제품에서 발견된 오류를 악용하여 유포하는 형태로 최근 해외에서는 레빌(소디노키비 변종) 랜섬웨어 발생
o 설 연휴, 연말정산 기간 등 사회적 이슈를 틈타 개인 및 기업 대상으로 감행되는 랜섬웨어 공격 피해 최소화를 위한 주의 필요

□ 대응방안
o 출처가 불분명한 이메일 열람 금지
o 윈도우 등 OS 및 사용 중인 프로그램의 최신 보안업데이트 적용
o 신뢰할 수 있는 백신 최신버전 설치 및 정기적으로 검사 진행
o 불필요한 공유폴더 연결 해제
o 파일 공유사이트 등에서의 파일 다운로드 및 실행 주의
o 중요 자료는 네트워크에서 분리된 저장장치에 별도 저장하여 관리
o 이상 징후 및 침해사고 발생시, KISA 인터넷침해대응센터(KISC)로 즉시 신고 등
※ 보호나라 홈페이지 - 상담 및 신고 - 해킹사고

▣ 참고자료 (보호나라 홈페이지 → 자료실 → )
(1) 랜섬웨어 대응 가이드을 위한 안내 및 백업 가이드
- 보호나라 홈페이지 → 자료실 → 가이드 및 매뉴얼 내 34번 게시물
(2) 랜섬웨어 대응을 위한 안전한 정보시스템 백업 가이드
- 보호나라 홈페이지 → 자료실 → 가이드 및 매뉴얼 내 35번 게시물
(3) AD(Active Directory) 관리자가 피해야 할 6가지 AD운영 사례
- 보호나라 홈페이지 → 자료실 → 보고서 내 213번 게시물
(4) AD서버 악용 내부망 랜섬웨어 유포 사례 분석
- 보호나라 홈페이지 → 자료실 → 보고서 내 215번 게시물

Eyeon Security
Information security company
주소 : 서울특별시 서초구 서초대로 255 고덕빌딩 2층 [06595]
전화 : 02-2105-4400 (영업문의 1, 보안관제문의 2, 기술문의 3)
팩스 : 02-2105-4456
영업문의 : sales@eosec.co.kr, 보안관제 및 기술문의 : tech@eosec.co.kr