[S2W LAB] Kaseya supply chain attack delivers mass ransomware.pdf

Archived: 2026-04-05 19:36:21 UTC

Sida 2 av 11

2

• VSA 웹 패널에서 인증을 우회한 이후, VSA 어플라이언스에서 SQL 명령을

실행하고 연결 된 모든 클라이언트에 랜섬웨어 배포

• 취약한 이전 버전의 Microsoft Defender 앱을 사용하여 바이러스 백신

솔루션을 무력화하는 “VSA 에이전트 핫픽스” 패키지를 배포

2021 년 7 월 3 일 오후 21:00 (EDT), Kaseya 는 공지사항으로 침해여부를 탐지할 수 있는

Detection Tool 을 이메일로 요청 시 보내준다고 게시

- 이후 공식 다운로드 링크 제공

• https://kaseya.app.box.com/s/0ysvgss7w48nxh8k1xt7fqhbcjxhas40

REvil 은 최근 사고에 대한 협상 채팅에서, 기존 방식과는 다르게 1 개의 파일 확장자 별로

복호화 비용을 요구하고 있음

- 1 개 확장자 당 복호화 비용 : $40,000 ~ $45,000

- 전체 파일 복호화 비용 : $500,000

공격자는 피해 기업과의 협상 채팅을 통해서 파일만 암호화했을 뿐이며, 피해 기업의

데이터를 훔치지 않았다고 언급

현재까지 알려진 피해 기업 목록

- MSP : Visma EssCom, Synnex, Avtex

- MSP 에 의해 영향 받은 기업 : Swedish Coop 수퍼마켓 체인, 스웨덴 약국 체인, SJ

대중 교통 시스템 등 1,000 개 이상의 기업이 공격에 영향을 받은 것으로 추정됨

피해 기업 동향

- 출처 : ESET 공식 트위터

Source: https://drive.google.com/file/d/1ph1E0onZ7TiNyG87k4WjofCKNuCafMLk/view