새벽에 온 암호화 손님 Endpoint(Midnight) 랜섬웨어 분석

ATCP

June 2, 2026

RANSOMWARE
YOUR FILES
ARE ENCRYPTED
00:59:59
PAY NOW TO UNLOCK
RANSOMWARE
PAY ransom
TO UNLOCK FILES
PAY NOW
RANSOMWARE
RANSOMWARE
RANSOMWARE

요약

EndPoint는 이전에 Midnight으로 알려졌던 랜섬웨어 변종으로, Babuk 랜섬웨어 프레임워크를 기반으로 개발된 것으로 알려져 있다. Windows 환경뿐 아니라 ESXi와 NAS 환경도 겨냥하며, 파일 암호화와 데이터 유출 협박을 함께 수행하는 Double Extortion 방식을 사용한다.

개요

Babuk 소스코드 유출 이후 여러 파생 랜섬웨어가 등장했으며, EndPoint도 그중 하나로 확인된다. 감염 파일에는 `.endpoint` 확장자가 부여되며, 랜섬노트에는 피해자와 연락하기 위한 uTox ID가 포함된다. 과거 랜섬노트의 `schipkealfred@gmail.com` 계정은 동아시아연구소 소장을 사칭한 계정으로, 2024년 이후 북한 연계 공격자가 사용한 것으로 식별된 바 있다.

분석 내용

파일 암호화

EndPoint는 실행 인자를 통해 암호화 범위를 조정한다. `-paths=`는 특정 경로만, `/n`은 네트워크 공유 폴더만 암호화하며, `/e`는 `.endpoint` 확장자 변경을 비활성화한다. 실행 경로에는 `debug.endpoint` 파일을 생성해 `FindFirstFileW`와 `MoveFileExW` 실패 로그를 기록한다.

암호화 전에는 데이터베이스, 오피스, 메일 클라이언트 등 여러 프로세스를 종료하고, `vssadmin.exe delete shadows /all /quiet` 명령어로 볼륨 섀도우 복사본을 삭제한다. 또한 `vss`, `sql`, `Veeam`, `Sophos`, `Acronis` 등 백업·보안 관련 서비스를 강제로 중단한다.

암호화 대상에서는 `Windows`, `Program Files`, `AppData` 등 일부 디렉터리와 `bootmgr`, `ntuser.dat` 같은 파일, `.exe`, `.dll`, `.msi`, `.endpoint` 확장자를 제외한다. CPU 코어 수 기준으로 스레드를 생성하며, 중복 실행 방지를 위해 `Mutexisfunnylocal` 뮤텍스를 사용한다.

암호화에는 ChaCha20(대칭키 암호)을 사용하고, 생성된 세션 키는 자체 구현된 RSA 공개키 연산으로 보호된다. 파일 크기에 따라 전체가 아니라 일부 구간만 암호화하는 부분 암호화를 사용해 처리 속도와 영향 범위를 조절한다. 암호화 후에는 Footer에 세션 키와 SHA-256 해시값이 저장된다.

랜섬노트

바탕화면은 변경하지 않으며, 랜섬노트는 `How To Restore Your Files.txt` 이름으로 모든 암호화 경로에 생성된다. 랜섬노트에는 데이터 탈취와 암호화 사실, 금전 지급 후 복구 지원 주장, `Session` 메신저 기반 연락 방법, 무료 복호화 3개 파일 제공, 지연 시 금액 증가 경고가 포함된다.

안랩 대응 현황

안랩 제품군에서는 `Trojan/Win.Generic.C5765109`, `Ransom/MDP.Delete.M2117`, `Ransom/MDP.Command.M2255`, `Ransom/MDP.Decoy.M1171`, `Ransom/MDP.Event.M1946`, `Ransom/MDP.Event.M1875`, `SystemManipulation/EDR.Event.M2486`, `Ransom/EDR.Decoy.M2470`로 진단된다.

결론

EndPoint는 파일 크기에 따라 암호화 범위를 조절하는 부분 암호화 기법, `ChaCha20` 기반 암호화, 자체 RSA 공개키 연산, Footer 기반 정보 저장, 뮤텍스 사용 등 체계적인 구조를 가진다. 효율성과 은폐성을 함께 고려해 빠른 피해 확산과 복구 방해를 노리는 위협으로 평가된다.

대응 가이드

중요 데이터는 서비스망과 분리된 오프사이트에 백업하고, 백업 저장소 접근 통제와 정기 복구 훈련을 수행해야 한다. 또한 운영체제와 소프트웨어의 최신 보안 업데이트 적용, 보안 소프트웨어 최신 유지, 오프라인 또는 별도 네트워크 백업 보관, 신뢰할 수 없는 링크와 첨부 파일 주의, 추측하기 어려운 패스워드와 2FA 인증 사용이 필요하다.

MD5
34be5e70f1260da87096b80dc7b026ac
b77ad606ba04d2d0077130679a257c96
c00cc937e064946ee42776cfe80754d7
e82bcf417f51acc6b2d8a94ceabd5e36