LWS기반의 휴리스틱 랜섬웨어 탐지 기술

LWS기반의 휴리스틱 탐지기술은 일반 시그니처 보안으로
탐지하기 어려운 신·변종 랜섬웨어도 탐지 및 차단합니다.

Lite Pro Server

초경량 행위기반 사용성 안정성

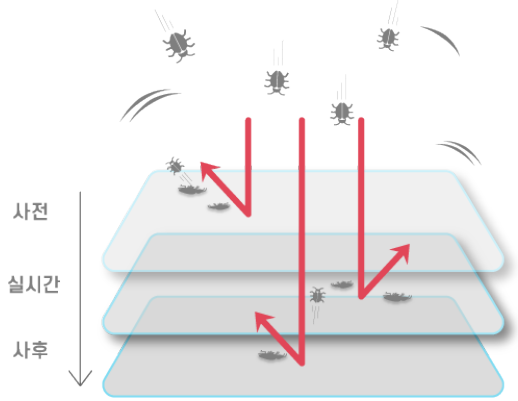
GS인증 1등급 제품 [인증번호 / 19-0272]

제품개요

현재의 랜섬웨어는 APT 및 각종 지능형 공격과 결합되어 다양한 형태의 변종 공격이 지속적으로 발생하고 있습니다.
기존 시그니처 차단 방식으로는 최근의 랜섬웨어를 방어하기에 분명한 한계가 있습니다.
행위기반 탐지 엔진을 탑재한 랜섬스톱은 신종 및 변종 랜섬웨어까지 탐지하여 사용자 데이터를 보호하는 강력한 안티랜섬웨어 솔루션 입니다

다중 계층 보안

RansomStop은 랜섬웨어 탐지를 위한 LSW 진단, 공격자 프로파일링을 통한 휴리스틱 진단, 커널 접근 및 메모리 I/O 분석을 통한 행위분석 진단 등 다중계층 탐지엔진을 통하여 더 높은 수준의 랜섬웨어 보안을 제공합니다.



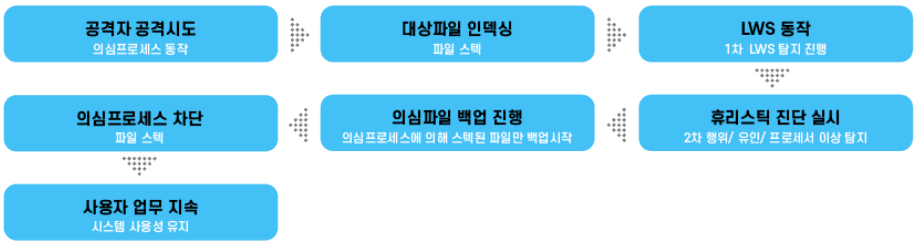
LWS 진단
Signature DB | Windows Process | Program

휴리스틱 진단
Code Signing | Header Anomaly Detection

행위분석 진단
Process Analysis | File Encryption Analysis |
Entropy Analysis | I/O Analysis | Back-Up

탐지차단 프로세스

사용자의 PC가 랜섬웨어로부터 노출되면 다음과 같은 순서로 공격을 차단합니다.



주요 기능

사용자 행위 기반의 탐지 엔진을 탑재한 RansomStop은 기존의 안티 랜섬웨어와는 비교할 수 없는 높은 탐지율과 차단 성능을 자랑합니다.

사전 방어 및 파괴행위 차단	• 랜섬스톱 엔진을 통한 다양한 랜섬웨어 행위 실시간 차단 및 행위 롤백
랜섬웨어 대피소	• 파일 훼손 시 원본 파일을 백업 폴더로 실시간 백업 및 폴더 보호
랜섬웨어 자율보호	• 자체 프로세스 및 파일 보호
자동백업	• 랜섬 행위 및 악성코드 탐지 시 차단과 동시에 자동 백업
SMB 서버 보호	• 랜섬웨어에 감염된 원격지 PC가 공유된 폴더 내 파일을 변조 시 보호
중요 데이터 자동백업	• 지정한 폴더를 파일 히스토리 방식으로 주기적 자동 백업 및 폴더 보호

사용 환경

구분	상세 버전
평가판/ 프로	Windows 7 / 8(8.1) / 10 (32bit/ 64bit) *.NET Framework 4.5이상 필요
서버	Windows Server 2003 SP1(R2 포함) Windows Server 2008 / 2012(공통 사항: R2 포함) Windows Server 2016 / 2019 * 상기 OS의 64bit 호환 모드 지원

knowwhere soft
서울특별시 성동구 성수이로 66 서울숲드림타워 #304 (04784)
홈페이지: www.knowwheresoft.com
대표전화: 070-722-8000 팩스: 031-722-8901