이달의 보안 동향 및 대응

- 세종텔레콤, 보안 취약 중소기업 위한 '트로이컷 클라우드형' 출시
- 이니텍 'INISAFE CrossWeb EX V3' 보안 업데이트 필수
- "정부기관 털리고 핵 기밀까지" 북 해킹에 속수무책
- '지닥 해킹'의 재구성…'타임라인'으로 보는 논란 4가지
- 4월의 패치 튜즈데이, MS는 97개 취약점 해결해

보안뉴스 요약

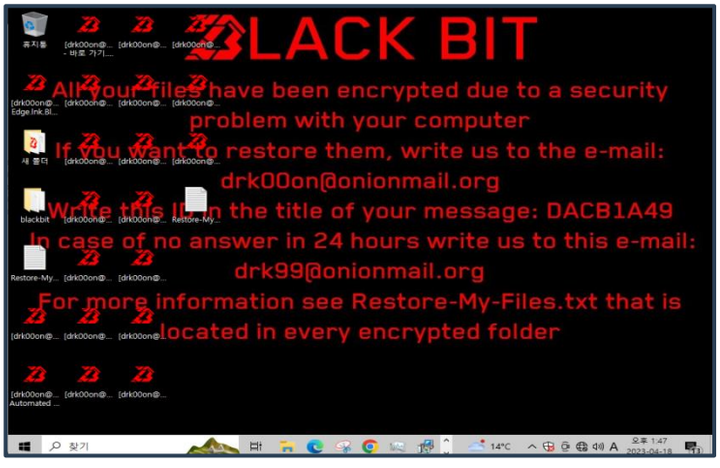
보안뉴스 23.04.05
수수께끼와 같은 랜섬웨어 로르샤흐, 암호화 속도는 추종불허

보안뉴스 23.04.11
KFC와 피자헛 소유한 얌! 브랜즈, 랜섬웨어 공격에 당해

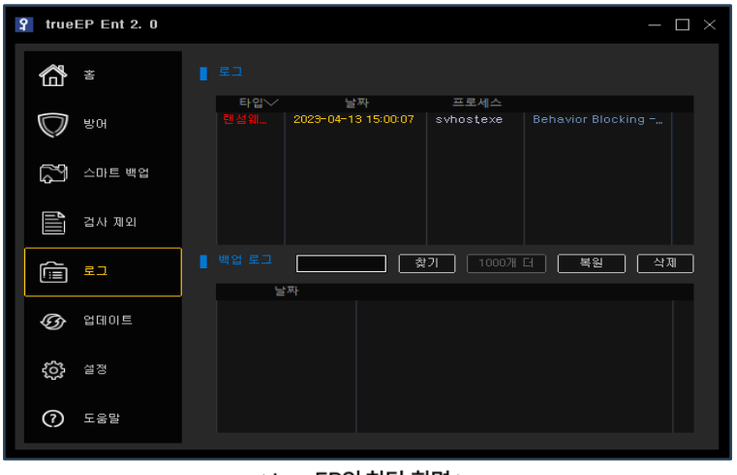
보안뉴스 23.04.12
트리고나 랜섬웨어, 부적절하게 관리되는 MS-SQL 서버 통해 유포

보안뉴스 23.04.18
블랙빗 랜섬웨어, 정보 유출과 탐지 방해 기능 무장한 채 국내 유포

이달의 랜섬웨어 BlackBit



< 공격에 성공한 화면 >



< trueEP의 차단 화면 >

침투

원격제어(RDP) 접근 방식 침투

- 공격자가 직접 침투하여 악성코드 설치 및 악의적인 명령 실행

» 침투단계에서 trueEP의 대응

- trueEP는 순수 행위기반 방어 원리로 프로세스가 행위를 하기 이전인 침투 단계에서는 대응하지 않음

공격준비

BAT레지스트리 등록 및 보안 해제

- 작업관리자 비활성화 레지스트리 등록
- Windows방화벽 및 디펜더 기능 해제

» 공격준비단계에서 trueEP의 대응

- 시스템 레지스트리 접근 차단
- MS방화벽 무력화 행위 차단(옵션)
- MS백업 무력화 행위 차단(옵션)

공격

유포된 악성코드 실행

- 공격 대상 폴더 및 파일 목록 식별
- '*.BLACKBIT' 파일명으로 변경

» 공격단계에서 trueEP의 대응

- 공격대상 폴더 및 파일 목록 식별행위 차단
- 해당 프로세스를 중단시켜 악성행위 차단

랜섬웨어 상세 분석

BlackBit

단계	사용된 기법	trueEP의 대응
침투(유포)	1) 원격 제어(RDP) 접근 방식으로 시스템에 침투하여 랜섬웨어를 실행	**trueEP는 인바운드 영역에는 개입하지 않음** • 시그니처기반 제품들의 방어 영역 • 악성코드가 파일형태로 존재하는 실공격 이전의 단계 trueEP는 악성코드가 프로세스로 실행되어 실공격 행위를 하는 단계에서 탐지하고 차단하는 원리임.
공격준비	1) 작업관리자를 통한 프로세스 종료를 방해하기 위해 BAT파일을 활용하여 레지스트리 등록 2) Windows방화벽, 디펜더 기능 해제 3) Recycle.bin에 존재하는 파일 및 볼륨쉐도우 삭제	**trueEP는 사용자 행위 없는 레지스트리 접근 행위를 탐지 시 해당 프로세스를 중단시켜 악성행위 차단** 1) 시스템 레지스트리 접근 시 차단 2) MS방화벽 무력화 행위 차단(옵션) 3) MS백업 무력화 행위 차단(옵션)
공격	1) 공격 대상 폴더 및 파일 목록 식별 2) VM환경에 대한 검사 및 암호화 대상의 범위 탐색을 위한 특정 프로세스 종료 시도 3) '*.BLACKBIT' 파일명으로 변경 4) 각 감염 경로 폴더에 Restore-My-Files.txt를 생성	**trueEP는 사용자 입력이 없는 파일 암호화 행위를 탐지 시 해당 프로세스를 중단시켜 악성행위를 차단** 1) 공격대상 폴더 및 파일 목록 식별 행위 차단 2) 사용자입력 없는 파일 암호화 행위 차단

Trigona

단계	사용된 기법	trueEP의 대응
침투(유포)	1) 보안에 취약한 환경에 공격자가 직접 침투하여 악성코드 설치 및 악의적인 명령 실행 2) CLR Shell 악성코드를 먼저 설치하는 것으로 추정되며, 권한 상승 취약점을 악용하여 서비스로 동작하는 Trigona랜섬웨어의 악성 행위 수행을 도움	**trueEP는 인바운드 영역에는 개입하지 않음** • 시그니처기반 제품들의 방어 영역 • 악성코드가 파일형태로 존재하는 실공격 이전의 단계 trueEP는 악성코드가 프로세스로 실행되어 실공격 행위를 하는 단계에서 탐지하고 차단하는 원리임.
공격준비	1) 권한 상승 취약점(MS16-032)을 악용하여 악성 행위 수행 2) Trigona 바이너리를 Run키에 등록하여 재부팅 이후에도 실행될 수 있도록 함 3) 볼륨 쉐도우 삭제 및 시스템 복원 기능 비활성화 4) 백그라운드에서 악성행위 동작 (공격 대상 폴더 및 파일 목록 식별)	**trueEP는 사용자 행위 없는 레지스트리 접근 행위를 탐지 시 해당 프로세스를 중단시켜 악성행위 차단** 1) 공격대상 폴더 및 파일 목록 식별행위 차단 2) MS백업 무력화 행위 차단(옵션)
공격	1) 델파이로 개발된 랜섬웨어로서 파일 암호화 시 확장자를 구분하지 않고 암호화 2) '*._locked' 파일명으로 변경 3) 각 폴더에 "how_decrypt.hta" 랜섬노트 생성	**trueEP 사용자 입력이 없는 파일 암호화 행위를 탐지하는 순간에 프로세스를 중단시켜 악성행위를 차단** 1) 해당 프로세스를 중단시켜 악성행위 차단