이달의 보안 동향 및 대응

- 키오스크·POS 보안 솔루션 '키오스크필터' 출시
- 23만명 개인정보 유출한 '워크넷', 해킹 방지에 106억원이나 썼다고?
- 제로트러스트 개념·보안원리·핵심원칙 설명하는 가이드라인 나왔다
- 지금으로부터 14년 전 '7.7 디도스 대란', 그 현장 속으로

보안뉴스 요약

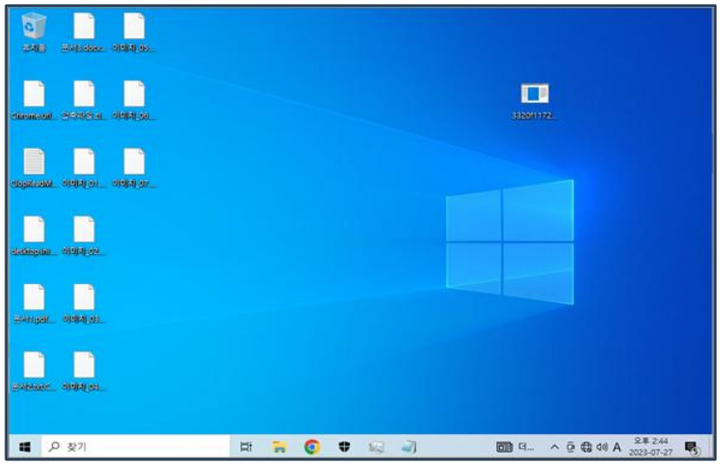
보안뉴스 23.07.06
해외에서 난리난 무브잇 사태, 랜섬웨어 산업에 새 바람 일으킬까

조선일보 23.07.03
"923억원 내놔라" 랜섬웨어 해킹에 TSMC도 당했다

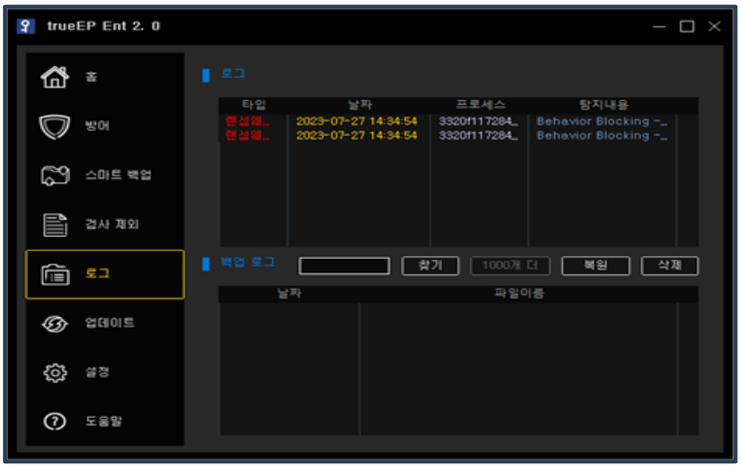
보안뉴스 23.07.17
2023년 상반기 역대급 피해 써내려가는 랜섬웨어, 얼마나 당했나

보안뉴스 23.07.24
클롭 랜섬웨어, 드디어 무브잇 사태 피해자들 공개 시작

이달의 랜섬웨어 CLOP



< 공격에 성공한 화면 >



< trueEP의 차단 화면 >

침투

· 지속적으로 진화하고 있는 랜섬웨어.
· 최근에는 무브잇 파일전송 프로그램의 제로데이 취약점을 익스플로잇

침투단계에서 trueEP의 대응

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

공격준비

AD도메인 구성 정보 접근

- 취약점을 이용한 실행 권한 상승
- 각 도메인 컨트롤러 서버에 연결하여 연결된 시스템 장악
- 사용자 정보 파일 탈취
- 공격대상 폴더 및 파일 목록 식별

공격준비단계에서 trueEP의 대응

- AD접근 행위 차단(옵션)
- 기타 준비 단계에서의 행위가 trueEP 행위기반 알고리즘에 위배될 경우 차단
- 공격대상 폴더 및 파일 목록 식별 행위 차단
- 사용자입력 없는 정보탈취 행위 차단

공격

유포된 악성코드 실행

- 작업 스케줄러 또는 원격 명령 이용하여 유포된 CLOP랜섬웨어를 실행
- 공격대상 파일 암호화 실행
- ClopReadMe.txt랜섬노트 생성

공격단계에서 trueEP의 대응

- 사용자입력 없는 암호화 행위 차단
- 행위 차단 시 프로세스 킬

랜섬웨어 상세 분석

CLOP

단계	사용된 기법	trueEP의 대응
침투(유포)	1) 침투 방법이 지속적으로 진화되고 있는 랜섬웨어로 최근에는 무브잇 파일전송 프로그램의 제로데이 취약점을 익스플로잇	**trueEP는 인바운드 영역에는 개입하지 않음** • 시그니처 기반 제품들의 방어 영역 • 악성코드가 파일 상태로만 존재하며 행위는 없는 단계 **trueEP는 악성코드가 프로세스로 실행되어 실공격 행위를 하는 단계에서 탐지하고 차단하는 원리임.**
공격준비	1) AD도메인 구성 정보 확인 및 취약점을 이용한 실행 권한 상승 2) AD도메인 관리자 계정이 성공적으로 획득되면 도메인 컨트롤러 서버에 연결하여 각 연결된 시스템 장악 3) 사용자 정보 파일 탈취 4) 공격 대상 폴더 및 파일 목록 식별	**trueEP는 계정을 탈취하고, 권한을 상승 등 일련의 진행 과정에서 trueEP 행위기반 알고리즘에 위배될 경우, 이를 탐지하여 차단함** 1) 사용자 정보 탈취 행위 차단 2) 폴더 및 파일 목록 식별 행위 차단
공격	1) AD도메인에 연결된 시스템에 작업 스케줄러 또는 원격 명령을 이용, CLOP Ransomware를 실행 2) 공격대상 파일 암호화 실행 - '<File Name>.CLOP' 파일명으로 변경 3) 각 감염 경로 폴더에 ClopReadMe.txt 랜섬노트 생성	**trueEP는 사용자 입력이 없는 파일 암호화 행위를 탐지 시 해당 프로세스를 중단시켜 악성행위를 차단** 1) 사용자입력 없는 파일 암호화 행위 차단

monti

단계	사용된 기법	trueEP의 대응
침투(유포)	1) " Log4Shell " 취약점(일명 CVE-2021-44228)을 악용하여 침입한 것으로 추측	**trueEP는 인바운드 영역에는 개입하지 않음** • 시그니처 기반 제품들의 방어 영역 • 악성코드가 파일 상태로만 존재하며 행위는 없는 단계 **trueEP는 악성코드가 프로세스로 실행되어 실공격 행위를 하는 단계에서 탐지하고 차단하는 원리임.**
공격준비	1) 자격 증명 덤프 및 네트워크 스캔 후 원격 데스크톱 프로토콜(RDP)를 사용하여 다른 서버에 연결 2) DropMeFiles 파일 공유 웹사이트에 덤프파일 유출시도 3) 네트워크 공유에 있는 데이터 파일 액세스 후 MONTI 랜섬웨어 배포 4) 공격 대상 폴더 및 파일 목록 식별	**trueEP는 사용자 행위 없는 레지스트리 접근 행위를 탐지 시 해당 프로세스를 중단시켜 악성행위 차단** 1) 사용자입력 없는 자료유출 행위 차단 2) %programdata% 디렉토리 선감시 3) 폴더 및 파일 목록 식별 행위 차단
공격	1) 공격대상 파일 암호화 실행 - '<File Name>.PUUUK' 파일명으로 변경	**trueEP 사용자 입력이 없는 파일 암호화 행위를 탐지하는 순간에 프로세스를 중단시켜 악성행위를 차단** 1) 사용자입력 없는 파일 암호화 행위 차단