Truecut Security News Letter
23년 9월 간추린 보안 이슈
Truecut Security, LAB

이달의 보안 동향 및 대응

- 7월 랜섬웨어 피해 11%↑…"암호화·비주류언어로 탐지 우회"
- 구글 "사이버 공격 31% 아태지역서…탐지 늦고 인재 부족"
- 증권사·대부중계 플랫폼 등 9개 업체 해킹… 개인정보 유출 일당 검거
- 中 해커, 미 국무부 이메일 6만건 탈취

보안뉴스 요약

ZDNET 23.09.12
"어디든 취약"…랜섬웨어 피해액 더 늘었다

연합뉴스 23.09.12
기아 美공장 협력사·한화큐셀 中공장, 랜섬웨어 공격 받아

보안뉴스 23.09.14
새롭게 등장했지만 평범한 랜섬웨어, 진짜 문제는 '복수 랜섬웨어'

NEWSIS 23.09.18
FBI가 쫓던 그 랜섬웨어 그룹, 국내 IT기업도 당했다

이달의 랜섬웨어 NoEscape

< 공격에 성공한 화면 >

< trueEP의 차단 화면 >

침투

MS-SQL DB운영 시스템 침투

- 취약점(Exploit)에 의한 감염

» 침투단계에서 trueEP의 대응

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

공격준비

DNS서버와 통신 및 추가 페이로드 다운

- 사용자 계정 컨드롤(UAC)비활성화
- 시스템 백업 및 섀도우 복사본 삭제
- 이벤트 로그 삭제
- 랜섬웨어 복제본 스케줄러 등록

» 공격준비단계에서 trueEP의 대응

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

공격

유포된 악성코드 실행

- 〈9~10자리 A~J Random 확장명〉 패턴으로 데이터 암호화
- "HOW_TO_RECOVER_FILES.txt" 랜섬노트 생성

» 공격단계에서 trueEP의 대응

- 사용자입력 없는 암호화 행위 차단
- 행위 차단 시 프로세스 킬

랜섬웨어 상세 분석

NoEscape

단계	사용된 기법	trueEP의 대응
침투(유포)	1) Vmware ESXI 서버를 표적으로 삼는 서비스형(RaaS)랜섬웨어로, MS-SQL DB운영 시스템에 침투	**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) 사용자 계정 컨트롤(UAC)알림 기능을 비활성화하여 재실행 시 알림 메시지를 띄우지 않고 동작 2) 시스템 복원 무력화WMIC(Windows Management Instrumentation 명령줄)를 사용하여 모든 VSS(볼륨 섀도 복사본), 백업 카탈로그 및 섀도 복사본을 삭제, 이벤트로그 삭제 3) "C:₩Users₩%UserName%₩AppData₩Roaming₩<Random>.exe" 파일을 생성하여 작업 스케줄러 등록값에 추가된 SystemUpdate 값을 통해 10분마다 자동 재실행	**trueEP는 계정을 탈취하고, 권한을 상승 등 일련의 진행 과정에서 trueEP 행위기반 알고리즘에 위배될 경우, 이를 탐지하여 차단함** • 사용자입력 없는 정보탈취 행위 차단 • 기타 준비 단계에서의 행위가 trueEP 행위기반 알고리즘에 위배될 경우 차단 • MS백업 무력화 공격 차단 (옵션)
공격	1) 공격 대상 폴더 및 파일 목록 식별 2) <9~10자리 A~J Random 확장명> 패턴으로 데이터 암호화 3) "HOW_TO_RECOVER_FILES.txt" 랜섬노트 생성	**trueEP는 사용자 입력이 없는 파일 암호화 행위를 탐지 시 해당 프로세스를 중단시켜 악성행위를 차단** • 공격대상 폴더 및 파일 목록 식별 행위 차단 • 사용자입력 없는 암호화 행위 차단 • 행위 차단 시 프로세스 킬

BlackBit

단계	사용된 기법	trueEP의 대응
침투(유포)	1) 원격 제어(RDP) 접근 방식으로 시스템에 침투하여 랜섬웨어를 실행	**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) 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** • 시스템 레지스트리 접근 시 차단 • MS방화벽, MS백업 무력화 공격 차단 (옵션) • 폴더 및 파일 목록 식별 행위 차단
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	**trueEP 사용자 입력이 없는 파일 암호화 행위를 탐지하는 순간에 프로세스를 중단시켜 악성행위를 차단** • 공격대상 폴더 및 파일 목록 식별 행위 차단 • 사용자입력 없는 파일 암호화 행위 차단