Truecut Security News Letter
23년 1월 간추린 보안 이슈
Truecut Security, LAB

이 달의 보안 동향 및 대응

- 공공기관 해킹시도 118만건…사이버 공격에 멍들어
- 전문화 되어 가는 랜섬웨어의 과거, 현재, 미래
- '랜섬웨어' 춘추전국시대, 2023년 생태계 살펴보기
- 국가정보원이 예측한 2023년 주요 사이버안보 위협 5가지
- 공격 사례로 살펴본 서비스형 랜섬웨어 'RaaS', 거대 생태계 구축하다

보안뉴스 요약

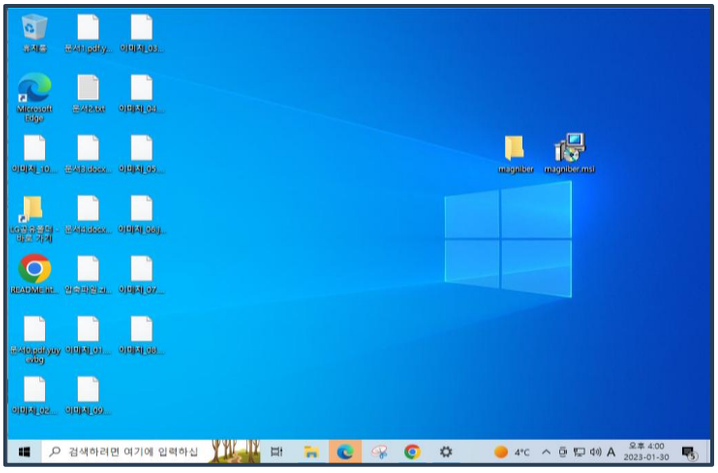
디지털데일리 23.01.03
LG유플러스 데이터 또 유출됐나… "사용자 데이터 2000만건 판매"

디지털데일리 23.01.24
"한국 인터넷 침입을 선포하다"… 中 해커에 뚫린 대한민국 보안

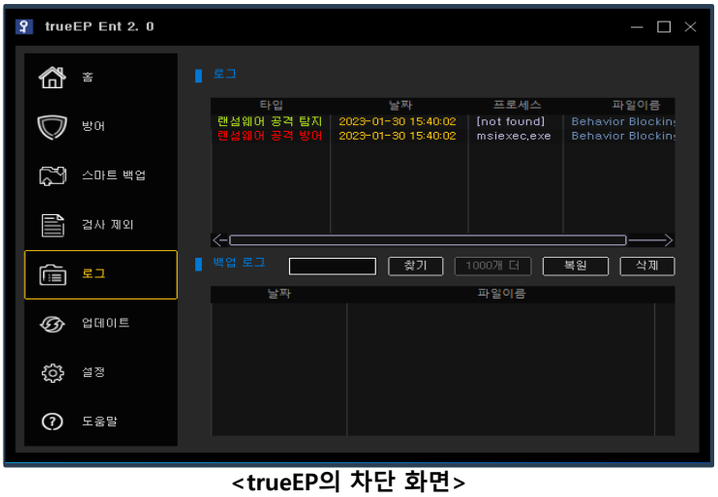
보안뉴스 23.01.31
매그니베르 랜섬웨어, 윈도 인스톨러로 위장해 재유포

한국경제 23.01.31
올 최대 위협은 '클라우드 보안'

이 달의 랜섬웨어 magniber



< 공격에 성공한 화면 >



<trueEP의 차단 화면>

침투

윈도우 긴급 업데이트 설치 패키지로 위장

- 불법 다운로드, 광고 사이트로 위장한 악성코드 유포사이트를 통해 배포
- 윈도우 긴급 업데이트 설치 패키지로 위장
- 도메인 오탈자를 악용한 타이포스쿼팅(Typosquatting) 방식으로 유포

» 침투단계에서 trueEP의 대응

- trueEP는 순수 행위기반 방어 원리로 프로세스가 실제 공격행위를 하기 이전인 침투 단계에서는 대응하지 않음
- trueEP는 악성코드가 프로세스로 실행되어 실공격 행위를 하는 단계에서 탐지하고 차단하는 원리임

공격준비

코드 인젝션 수행

- 긴급 업데이트 파일로 위장한 랜섬웨어 악성코드는 피해자들에 의해 직접 실행
- 정상 윈도우 프로세스에 코드 인젝션 수행

» 공격준비단계에서 trueEP의 대응

- 윈도우 logoff 행위 탐지 시 방어(옵션)

공격

정상 프로세스에 인젝션하여 공격 실행

- 정상 윈도우 프로세스에 인젝션된 랜섬웨어 코드에 의해 랜섬웨어 암호화 공격 실행

» 공격단계에서 trueEP의 대응

- 사용자 입력 없이 실행되는 랜섬웨어 암호화 행위 탐지 시 차단 후 해당 프로세스 킬

랜섬웨어 상세 분석

magniber

단계	사용된 기법	trueEP의 대응
침투(유포)	1) 불법 다운로드, 광고 사이트로 위장한 악성코드 유포사이트를 통해 배포 2) 윈도우 긴급 업데이트 설치 패키지로 위장 3) 도메인 오탈자를 악용한 타이포스쿼팅(Typosquatting) 방식으로 유포	**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) 긴급 업데이트 파일로 위장한 랜섬웨어 악성코드는 피해자들에 의해 직접 실행 2) 정상 윈도우 프로세스에 코드 인젝션 수행 3) 윈도우 log off를 통해 보안 솔루션들을 비활성화 시킴	trueEP는 사용자 행위 없는 윈도우 log off 행위를 탐지하는 순간에 이 행위를 차단시킴 ☞ 윈도우 logoff 공격 방어기능을 옵션으로 제공함.
공격	정상 윈도우 프로세스에 인젝션되어 랜섬웨어의 암호화 공격 행위를 수행함	trueEP 사용자 입력이 없는 파일 암호화 행위를 탐지하는 순간에 이 행위를 차단시키고 해당 프로세스 킬함

vicesociety

단계	사용된 기법	trueEP의 대응
침투(유포)	1) 인터넷 연결 애플리케이션을 악용하여 손상된 자격 증명을 통해 초기 네트워크 악세스 권한 취득 2) PowerShell Empire, SytemBC 및 Cobalt Strike등 사용하여 피해자의 네트워크를 탐색	**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) 피해자의 환경을 열거하고 적절한 Active Directory 구성에 대한 추가 정보 취득 2) 보안 로그 내용 삭제 시도 3) 복구 방지를 위한 PC환경 백업 솔루션에 액세스하려고 시도 4) 원격 비활성화를 위한 Windows 레지스트리 수정 시도	**trueEP는 아래의 행위를 탐지할 경우 차단함** • 행위 차단 시 프로세스 킬 1) AD접근 차단(옵션) 2) 백신 무력화 행위 차단(옵션) 3) 시스템 레지스트리 접근 시 차단
공격	1) 공격 대상 폴더 및 파일 목록 식별 2) 특정 경로와 확장자를 제외한 모든 파일을 대상으로 암호화한 후 '*.v1cesO0ciety' 파일명으로 변경	**trueEP는 아래의 각 행위를 탐지할 경우 차단함** • 행위 차단 시 프로세스 킬 1) 공격대상 폴더 및 파일 목록 식별행위 차단 2) 사용자입력 없는 자료유출 행위 차단 3) 사용자입력 없는 파일 암호화 행위 차단