이달의 보안 동향 및 대응

- 북한발 해킹 주의보… 국정원 “네이버 베껴 개인정보 탈취 시도”
- 말할 수 없는 '아픔'도 턴다…기업화 되는 '랜섬웨어 해킹'
- SK쉴더스 "급증하는 랜섬웨어 배후는 IAB"
- 미국 정보분석업체 “북한, 지난 14년간 최소 29개국에서 사이버 공격”

보안뉴스 요약

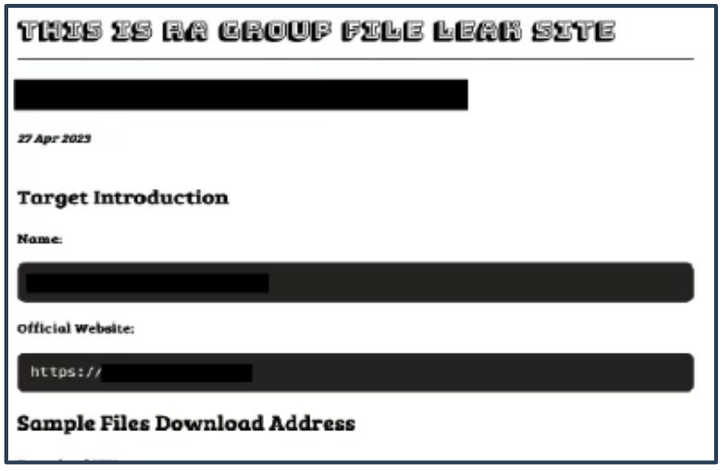
보안뉴스 23.06.01
Prestige 랜섬웨어, 피해자에게 감염 사실 알리지 않는 게 특징

보안뉴스 23.06.15
랜섬웨어 감염 후 복구하지 못해 결국 문 닫은 미국의 120년된 병원

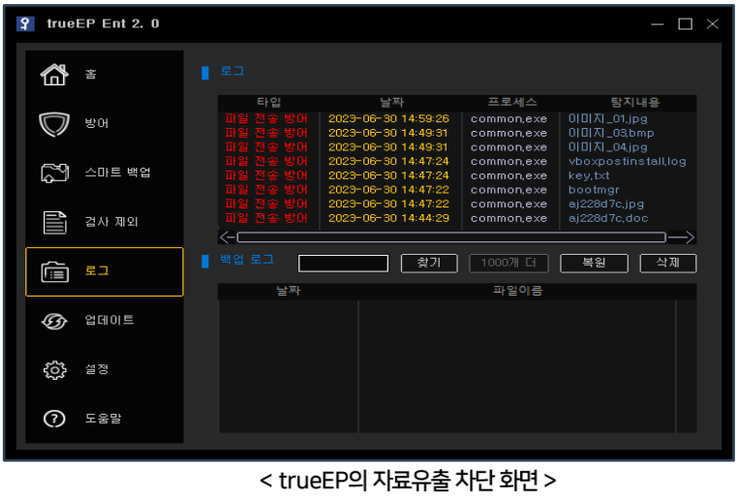
ITDAILY 23.06.20
랜섬웨어 조직, 역할 분담하며 공격 세분화…

보안뉴스 23.06.27
의료AI 1세대 '딥노이드', 랜섬웨어 공격으로 대규모 데이터 유출

이달의 랜섬웨어 RA GROUP



< 데이터 유출 공개 사이트 >



< trueEP의 자료유출 차단 화면 >

침투

직접 침투

- 공격자가 직접 악성코드 설치 및 악의적인 명령 실행

» 침투단계에서 trueEP의 대응

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

공격준비

기업 내 데이터 수집 후 외부 유출

- 피해자 시스템의 휴지통 내용을 삭제
- 시스템 복원 기능 무력화

» 공격준비단계에서 trueEP의 대응

- 자료유출 프로세스를 중단시켜 악성행위 차단
- MS백업 무력화 행위 차단(옵션)

공격

유포된 악성코드 실행

- 공격 대상 폴더 및 파일 목록 식별
- ‘*.GAGUP’ 파일명으로 변경

» 공격단계에서 trueEP의 대응

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

랜섬웨어 상세 분석

RA GROUP

단계	사용된 기법	trueEP의 대응
침투(유포)	1) 공격자가 직접 악성코드 설치 및 악의적인 명령 실행	**trueEP는 인바운드 영역에는 개입하지 않음** • 시그니처 기반 제품들의 방어 영역 • 악성코드가 파일형태로 존재하는 실공격 이전의 단계 trueEP는 악성코드가 프로세스로 실행되어 실공격 행위를 하는 단계에서 탐지하고 차단하는 원리임.
공격준비	1) 기업 내 데이터 수집 후 외부 유출 2) vssadmin.exe를 실행하여 볼륨 섀도 복사본을 삭제	**trueEP는 사용자 행위 없는 레지스트리 접근 행위를 탐지 시 해당 프로세스를 중단시켜 악성행위 차단** 1) 자료유출 프로세스를 중단시켜 악서행위 차단 2) MS백업 무력화 행위 차단(옵션)
공격	1) 공격 대상 폴더 및 파일 목록 식별 2) '<File Name>.GAGUP' 파일명으로 변경 3) 각 감염 경로 폴더에 How To Restore Your Files.txt 를 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

LockBit3.0

단계	사용된 기법	trueEP의 대응
침투(유포)	1) 국내에서는 저작권 위반, 입사지원서 등을 사칭 2) 분석을 회피하기 위해 다양한 분석 방지 기술 사용	**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) 복구를 막기 위해 윈도우 백업을 삭제 2) 자신의 복사본을 %programdata% 디렉터리에 쓴 후 이 프로세스에서 시작	**trueEP는 사용자 행위 없는 레지스트리 접근 행위를 탐지 시 해당 프로세스를 중단시켜 악성행위 차단** 1) MS백업 무력화 행위 차단(옵션) 2) %programdata% 디렉토리 선감시
공격	1) 공격 대상 폴더 및 파일 목록 식별 2) 자료 탈취와 암호화 공격을 동시에 실행 3) 확장자는 캠페인 또는 샘플마다 다르게 변경("HLJkNskOq" 및 "futRjC7nx" 확인)	**trueEP 사용자 입력이 없는 파일 암호화 행위를 탐지하는 순간에 프로세스를 중단시켜 악성행위를 차단** 1) 자료유출 및 식별행위 프로세스를 중단시켜 악성행위 차단 2) 디스크 드라이브의 루트 또는 개인 폴더(바탕화면,내 문서 등)의 폴더의 파일리스트 접근 수집 시 차단