이달의 보안 동향 및 대응

- 북한 김수키 해킹그룹의 유형별 스피어피싱 공격사례 분석해 보니
- 뻥뻥 터지는 보안사고에 칼 빼든 KISA, 침해사고 기업 책임 강화 제도 강구중
- 극장형 보안, 즉 '보여주기식 보안'이 판을 치는 이유와 끝내는 방법
- 복지부 산하 기관, 해킹 공격 받아… "135만명 개인정보 유출 의심"
- 한국 사이트 해킹 예고 중국 해커, 숙명여대·순천향대 등 교육·기관 무차별 공격
- 제로데이·공급망 공격으로 인한 데이터 유출, 2023년 최고치 기록
- 중국 해커, S2W 보고서에 앙심 품고 한국 여러 사이트 해킹…국방부 공격도 주장

보안뉴스 요약

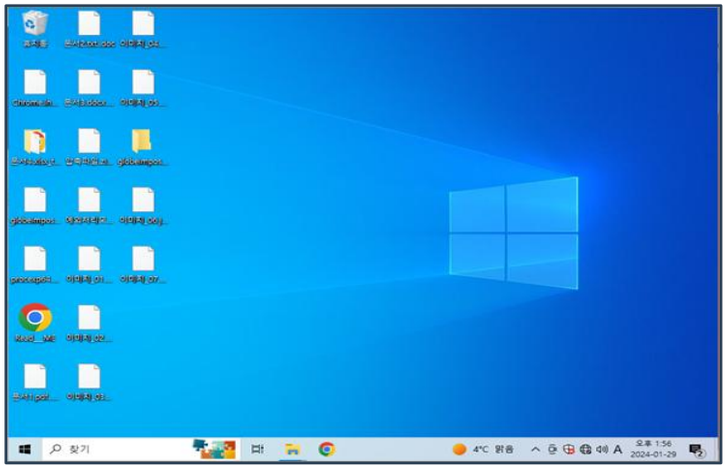
보안뉴스 24.01.06
2023년 12월 랜섬웨어 공격 및 피해사례 집계해보니...

데일리시큐 24.01.22
유명 프랜차이즈 '서브웨이', 락빗 랜섬웨어 공격 받아 수백기가 정보 유출…랜섬머니 요구중

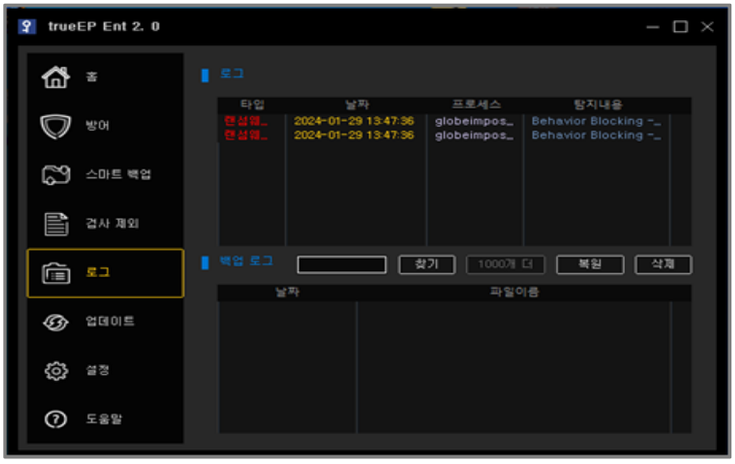
글로벌비즈 24.01.25
에퀴렌드, 랜섬웨어 공격받아… ' 거래 시스템 일부 정지

보안뉴스 24.01.26
글로브임포스터 랜섬웨어, '파일명.확장자.doc'로 암호화하며 확산중

이달의 랜섬웨어 GlobeImposter



< 공격에 성공한 화면 >



< trueEP의 차단 화면 >

침투

RDP를 이용한 랜섬웨어 설치

- 원격 데스크톱 프로토콜(RDP)를 통해 유포
- 스캐닝과정에서 무차별 대입 공격 및 사전 공격 수행

» 침투단계에서 trueEP의 대응

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

공격준비

네트워크 스캐닝 및 측면 이동

- 스캐너 및 계정 자격 증명 도용 도구 설치
- 네트워크 스캐닝 및 계정 정보 수집
- 볼륨 섀도우 복사본 및 이벤트/RDP로그 삭제

» 공격준비단계에서 trueEP의 대응

- 준비 단계에서의 행위가 trueEP 행위기반 알고리즘에 위배될 경우 차단
- 공격대상 폴더 및 파일 목록 식별 행위 차단
- MS백업 무력화 공격 차단 (옵션)

공격

유포된 악성코드 실행

- "<filename>. doc"으로 데이터 암호화
- 볼륨 섀도우 복사본 및 이벤트/RDP로그 삭제
- "Read__ME.html" 랜섬노트 생성

» 공격단계에서 trueEP의 대응

- 사용자입력 없는 암호화 행위 차단
- 행위 차단 시 프로세스 킬

랜섬웨어 상세 분석

GlobeImposter

단계	사용된 기법	trueEP의 대응
침투(유포)	1) 외부에서 접근 가능한 시스템을 대상으로 원격 데스크탑 서비스(Remote Desktop Protocol, RDP)를 이용하여 랜섬웨어 설치 2) 사용자 인증 자격 증명 탈취를 위한 스캐닝 과정에서 찾은 시스템들에 대해서 무차별 대입 공격 및 사전 공격을 수행	**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) 감염된 시스템의 네트워크를 타깃하기 위한 스캐너 및 계정 자격 증명 도용 도구 설치, 네트워크 내의 다른 시스템도 암호화하기 위해 내부 정찰 및 측면 이동 수행 2) 네트워크 스캐닝 및 계정 정보 수집, 권한 상승 3) RunOnce 키에 등록하기 전에 %LOCALAPPDATA% 경로에 자신을 복사하여 시스템 재부팅 후에도 작동	**trueEP는 계정을 탈취하고, 권한을 상승 등 일련의 진행 과정에서 trueEP 행위기반 알고리즘에 위배될 경우, 이를 탐지하여 차단함** 1) MS백업 무력화 공격 차단 (옵션) 2) 파일 유출진행 시 유출차단 알고리즘에 의한 이중방어 진행
공격	1) “<filename>.doc”으로 데이터 암호화 2) 배치 파일 생성 및 실행하여 볼륨 섀도 복사본 및 이벤트 로그, RDP관련 로그 삭제 3) “Read__ME.html” 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

LockBit

단계	사용된 기법	trueEP의 대응
침투(유포)	1) 국내에서는 저작권 위반, 입사지원서 등을 사칭하며, ₩word₩_rels₩settings.xml.rels’파일에는 ‘External Link’가 포함되어 외부 URL에서 추가 악성코드 설치 2) 분석을 회피하기 위해 다양한 분석 방지 기술 사용	**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) 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** • MS백업 무력화 행위 차단(옵션) 1) %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** • 사용자입력 없는 파일 암호화 행위 차단 • 행위 차단 시 프로세스 킬