이달의 보안 동향 및 대응

- KISIA, 제조업 랜섬웨어 대응 위한 민관 협력 강화한다
- 北 해커 김수키, 이번엔 '짝퉁 쿠팡 앱' 제작
- 랜섬웨어로 34억 뜯어낸 IT회사, 北해커와 한패였다
- 사이버공격 헬스케어에 심각한 위협

보안뉴스 요약

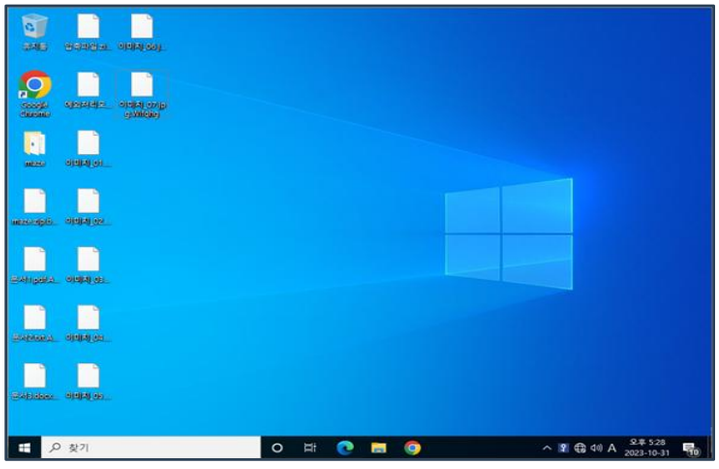
ITbiznews 23.10.13
北 해킹그룹, 랜섬웨어 공격으로 수익 창출 집중

ITbiznews 23.10.17
랜섬웨어 5년간 14배 늘었다…"피해 대부분 中企"

보안뉴스 23.10.26
일본의 시계 제조사 세이코, 랜섬웨어 공격에 당해 주요 정보 유출

매일경제 23.10.27
암호 못풀면 공장 못돌려 … 영세업체 돈 뜯어 北 보냈다

이달의 랜섬웨어 MAZE



< 공격에 성공한 화면 >

< trueEP의 차단 화면 >

침투

스팸 이메일 캠페인을 통한 배포

1) 익스플로잇 킷(Fallout Exploti Kit)과 스팸 이메일 캠페인을 통한 배포

» 침투단계에서 trueEP의 대응

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

공격준비

RDP접근 및 권한상승

- 공격자의 RDP접근 및 권한상승
- 시스템 백업 및 섀도우 복사본 삭제

» 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
- MS백업 무력화 공격 차단 (옵션)

공격

유포된 악성코드 실행

- 임의의 확장 명으로 데이터 암호화
- "DECRYPT-FILES.txt" 랜섬노트 생성

» 공격단계에서 trueEP의 대응

- 사용자입력 없는 암호화 행위 차단
- 행위 차단 시 프로세스 킬

랜섬웨어 상세 분석

Maze

단계	사용된 기법	trueEP의 대응
침투(유포)	1) 익스플로잇 킷(Fallout Exploti Kit)과 스팸 이메일 캠페인을 통한 배포 2) 사용자가 악성파일 다운로드 시 문서에 포함된 IcedID페이로드 매크로가 실행됨	**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) 공격자는 RDP연결을 통해 피해자 시스템에 로그인 2) 네트워크 침투에 필요한 도구 배포 및 액세스 권한 확보 후 새 도메인 계정 생성 3) 공유 폴더 존재시 두개의 링크 폴더 생성, 추가적으로 C&C서버 연결 시도 4) 시스템 복원 무력화WMIC(Windows Management Instrumentation 명령줄)를 사용하여 모든 VSS(볼륨 섀도 복사본)제거	**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) 임의의 확장 명으로 데이터 암호화 3) 감염사실 통보를 위한 바탕화면 변경 및 랜섬 노트 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

Blackcat

단계	사용된 기법	trueEP의 대응
공격준비	1) 사용자의 개인정보 파일 유출 2) 백업 및 섀도 복사본 제거 3) UUID(Universally Unique Identifiers) 수집 및 “ACCESS_KEY”생성 • 피해자의 고유 TOR주소 ‘액세스 토큰’을 생성하는데 사용 4) PsExec를 이용하여 레지스트리에 접근, 제한된 원격 관리 기능 비활성화(관리 권한 상승 시도)	**trueEP는 사용자 행위 없는 레지스트리 접근 행위를 탐지 시 해당 프로세스를 중단시켜 악성행위 차단** • 파일 유출 진행시 trueEP의 유출차단 알고리즘에 의한 이중방어 진행 • 윈도우 백업 삭제 행위 차단(옵션) • 시스템 레지스트리 접근 시 차단
공격	1) 네트워크 공유를 통해 전파된 악성코드 실행 2) 공격 대상 폴더 및 파일 목록 식별	**trueEP 사용자 입력이 없는 파일 암호화 행위를 탐지하는 순간에 프로세스를 중단시켜 악성행위를 차단** • 폴더 및 파일 목록 식별 행위 차단 • 사용자 입력 없는 암호화 행위 차단 • 디스크 드라이브의 루트 또는 개인폴더(바탕화면, 내문서 등)의 폴더의 파일리스트 접근 수집시 차단