Truecut Security News Letter
24년 3월 간추린 보안 이슈
Truecut Security, LAB

이달의 보안 동향 및 대응

- “반도체 장비업체들 조심하세요” 서버 비상등 켜졌다…북한의 ‘표적 해킹’ 주의보
- 북한에 해킹 당한 사법부 전산망... 대법원, 압수수색 후 마지 못해 인정했다
- ‘내부자 데이터 유출, 사고당 비용 1,500만 달러에 달해’… 코드42 조사
- "AI, 보안 빠지면 흉기"…LG '투트랙' 인재 선점 나섰다
- [긴급] 설치파일로 위장한 정보탈취형 악성코드 ‘스틸C’ 대량 유포중

보안뉴스 요약

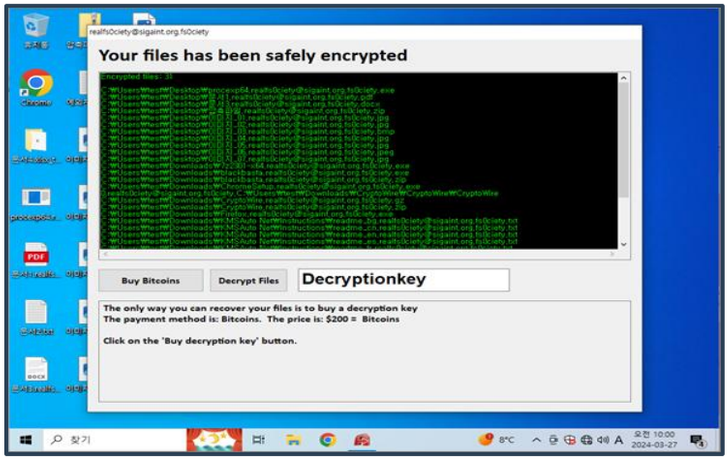
보안뉴스 24.03.17
복호화 키를 포함한 크립토와이어 랜섬웨어 유포

보안뉴스 24.03.20
"그놈이 돌아왔다"…록빗 랜섬웨어 조직 활동 재개

news1 24.03.20
'정보 탈취 후 몸값 협박' 랜섬웨어 그룹 록빗…무력화 5일 만에 활동 재개

INSIDE VINA 24.03.29
‘랜섬웨어 피해' VND증권, 거래중단 4일째…재개시점 '안갯속'

이달의 랜섬웨어 CryptoWire



< 공격에 성공한 화면 >

< trueEP의 차단 화면 >

침투

피싱 메일을 통해 유포

- 피싱 메일의 첨부파일
- 파일 공유 사이트 등

» 침투단계에서 trueEP의 대응

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

공격준비

네트워크 스캐닝 및 측면 이동

- 파일 암호화 확장을 위해 로컬 및 연결된 네트워크 환경 탐색

» 공격준비단계에서 trueEP의 대응

- 준비 단계에서의 행위가 trueEP 행위기반 알고리즘에 위배될 경우 차단
- 바탕화면 및 시스템 레지스트리 접근 시 차단

공격

유포된 악성코드 실행

- “<filename>.realfs0ciety@sigaint.org.fs0ciety”으로 데이터 암호화
- 섀도우 복사본 삭제
- 복호화 키가 포함된 랜섬노트 생성

» 공격단계에서 trueEP의 대응

- 사용자입력 없는 암호화 행위 차단
- 행위 차단 시 프로세스 킬

랜섬웨어 상세 분석

CryptoWire

단계	사용된 기법	trueEP의 대응
침투(유포)	1) 피싱 메일을 통해 유포 2) “C₩Program Files₩Common Files” 경로에 자가 복제를 하고, 지속성 유지를 위해 작업 스케줄러를 등록	**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) 파일 암호화의 확장을 위해서 로컬과 연결된 네트워크 환경을 탐색하여 바탕화면의 domaincheck.txt로 저장하고, 생성된 계정을 탐색	**trueEP는 계정을 탈취하고, 권한을 상승 등 일련의 진행 과정에서 trueEP 행위기반 알고리즘에 위배될 경우, 이를 탐지하여 차단함** 1) 바탕화면 및 시스템 레지스트리 접근 시 차단
공격	1) “<filename>.realfs0ciety@sigaint.org.fs0ciety”으로 데이터 암호화 2) 복구방지를 위해 휴지통 삭제 및 볼륨쉐도우 카피 삭제를 수행 3) 복호화 키가 포함된 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