이달의 보안 동향 및 대응

- “이중·삼중 갈취는 기본” 몸값을 받기 위해 새로운 전술 펼치는 해커들
- “랜섬웨어의 93%, 백업 저장소 노려”
- “언제적 해킹 기법인데”…당하고 또 당하는 이유는?
- 알라딘 전자책 해킹 사고, “출판업 근간 뿌리째 흔들 만한 역대급 사건”

보안뉴스 요약

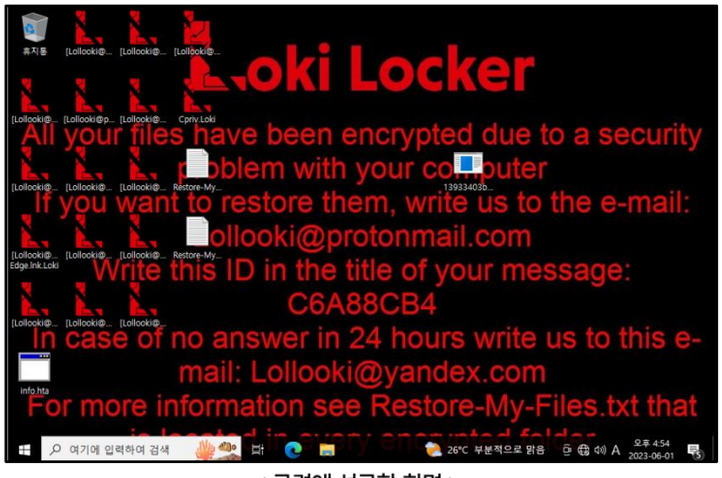
SecuN CCTV NEWS
CCTV뉴스 23.05.09
웨스턴디지털, 3월 발생한 사이버 공격으로 고객 개인정보도 유출

전자신문 The Electronic Times
전자신문 23.05.12
랜섬웨어 ‘로키로커’ 국내 유포…“블랙빗과 유사”

보안뉴스
보안뉴스 23.05.18
비안리안 랜섬웨어, 원격 데스크톱 기능 통해 들어온다

보안뉴스
보안뉴스 23.05.19
오리온, 블랙캣 랜섬웨어 공격으로 1테라 데이터 탈취당했나

이달의 랜섬웨어 Loki Locker



< 공격에 성공한 화면 >

< trueEP의 차단 화면 >

침투

원격제어(RDP) 접근 방식 침투

- 공격자가 직접 침투하여 악성코드 설치 및 악의적인 명령 실행

» 침투단계에서 trueEP의 대응

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

공격준비

레지스트리 등록 및 보안 해제

- 작업관리자 비활성화 레지스트리 등록
- Windows방화벽 및 디펜더 기능 해제

» 공격준비단계에서 trueEP의 대응

- 시스템 레지스트리 접근 차단
- MS방화벽 무력화 행위 차단(옵션)
- MS백업 무력화 행위 차단(옵션)

공격

유포된 악성코드 실행

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

» 공격단계에서 trueEP의 대응

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

랜섬웨어 상세 분석

Loki Locker

단계	사용된 기법	trueEP의 대응
침투(유포)	1) 원격 제어(RDP) 접근 방식으로 시스템에 침투하여 랜섬웨어를 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) 프로세스 종료를 방해를 위한 작업 관리자 무력화(레지스트리 접근) 2) Windows방화벽, 디펜더 기능 해제, 시스템 복원 무력화 3) Recycle.bin에 존재하는 파일 및 볼륨쉐도우 삭제	**trueEP는 사용자 행위 없는 레지스트리 접근 행위를 탐지 시 해당 프로세스를 중단시켜 악성행위 차단** 1) 시스템 레지스트리 접근 시 차단 2) MS방화벽 무력화 행위 차단(옵션) 3) MS백업 무력화 행위 차단(옵션)
공격	1) 공격 대상 폴더 및 파일 목록 식별 2) '[Lollooki@protonmail.com][Random]<File Name>.LOKI' 파일명으로 변경 3) 각 감염 경로 폴더에 Restore-My-Files.txt를 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

BianLian

단계	사용된 기법	trueEP의 대응
침투(유포)	1) 무작위 살포 유형의 공격(네트워크 침투) 2) 주요 피해 산업군(미디어, 엔터테인먼트, 각종 전문직 서비스, 제조, 의료, 에너지, 교육 등)	**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) 다음 명령줄을 사용하여 랜섬웨어 파일 삭제 ➢ *cmd /c del C:₩Users₩<관리자>₩Desktop₩new_one.exe* 2) API함수(FindFirstFileW() 및 FindNextFileW())를 사용하여 파일과 디렉터리를 열거하며, 암호화를 위해 파일과 디렉터리 검색	**trueEP는 사용자 행위 없는 레지스트리 접근 행위를 탐지 시 해당 프로세스를 중단시켜 악성행위 차단** 1) 공격대상 폴더 및 파일 목록 식별행위 차단
공격	1) 시스템 드라이브(A:₩에서 Z:₩까지)를 식별하고 연결된 드라이브에서 사용 가능한 모든 파일을 암호화 2) 백업 드라이브 암호화 3) '<File Name>.bianlian'파일명으로 변경	**trueEP 사용자 입력이 없는 파일 암호화 행위를 탐지하는 순간에 프로세스를 중단시켜 악성행위를 차단** 1) 해당 프로세스를 중단시켜 악성행위 차단 2) 디스크 드라이브의 루트 또는 개인 폴더(바탕화면,내 문서 등)의 폴더의 파일리스트 접근 수집 시 차단 3) MS백업 무력화 행위 차단(옵션)