이달의 보안 동향 및 대응

- “피싱은 여전히 가장 지배적인 인터넷 범죄”
- 지란지교데이터-하나시스, 키오스크·POS 이용자 정보보호 환경 구축 맞손
- 노골적으로 변하는 중국발 해킹… 기상청 장비에 악성코드 심어 납품?
- 개인정보뿐 아니라 계정 정보, PC 내 모든 정보 수집하는 피싱 공격 발견

보안뉴스 요약

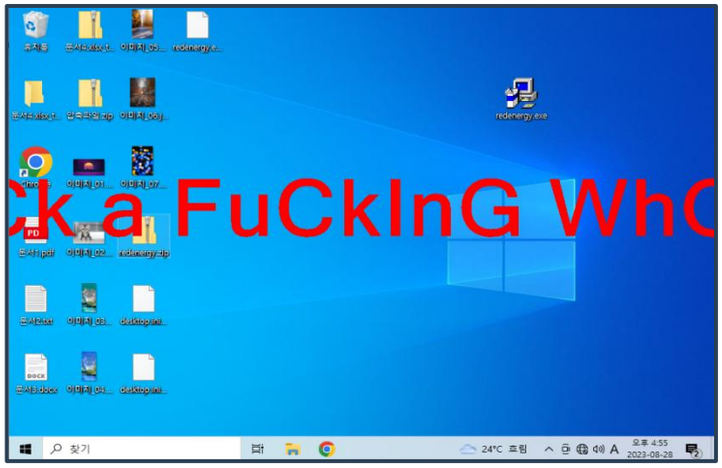
보안뉴스 23.08.08
새롭게 등장한 ‘하쿠나 마타타’ 랜섬웨어, 비트코인 대상 공격 시도…

HelloT 23.08.16
아카마이 “아태지역 랜섬웨어 피해자 1년새 204% 증가”

보안뉴스 23.08.24
레드에너지 인포스틸러, 웹 브라우저 업데이트로 위장해 유포돼

보안뉴스 23.08.28
모두의 위협으로 자리매김한 ‘랜섬웨어’, 공격 방식과 피해 사례…

이달의 랜섬웨어 RedEnergy



< 공격에 성공한 화면 >

< trueEP의 차단 화면 >

침투

브라우저 업데이트로 위장하여 클릭 유도

- 악성 웹사이트로 리디렉션
- 정식 업데이트 파일로 위장하여 침투

» 침투단계에서 trueEP의 대응

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

공격준비

DNS서버와 통신 및 추가 페이로드 다운

- 사용자 자격증명 탈취 후 액세스 권한 부여
- FTP상호 작용을 이용한 파일 유출 시도
- WMIC를 사용하여 볼륨 섀도 복사본 제거
- 공격대상 폴더 및 파일 목록 식별

» 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

공격

유포된 악성코드 실행

- <filename>.FACKOFF! 확장자로 데이터 암호화
- read_it.txt랜섬노트 생성

» 공격단계에서 trueEP의 대응

- 사용자입력 없는 암호화 행위 차단
- 행위 차단 시 프로세스 킬

랜섬웨어 상세 분석

RedEnergy

단계	사용된 기법	trueEP의 대응
침투(유포)	1) 사용자가 LinkedIn 프로필을 통해 대상 회사 웹사이트 방문 시도시 악성 웹사이트로 리디렉션 2) 정식 브라우저 업데이트로 위장한 악성 실행파일 다운로드	**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) DNS서버와 통신 후 악성 실행 파일 다운로드 및 사용자의 자격 증명 획득 2) FTP 상호 작용을 이용한 데이터 유출 시도 3) WMIC(Windows Management Instrumentation 명령줄)를 사용하여 모든 VSS(볼륨 섀도 복사본), 백업 카탈로그 및 섀도 복사본을 삭제 4) 공격 대상 폴더 및 파일 목록 식별	**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) • 공격대상 폴더 및 파일 목록 식별 행위 차단
공격	1) <filename>.FACKOFF! 확장자로 데이터 암호화 2) read_it.txt랜섬노트 생성	**trueEP는 사용자 입력이 없는 파일 암호화 행위를 탐지 시 해당 프로세스를 중단시켜 악성행위를 차단** • 사용자입력 없는 암호화 행위 차단 • 행위 차단 시 프로세스 킬

akira

단계	사용된 기법	trueEP의 대응
침투(유포)	1) VPN서비스(AnyDesk, WinRAR, and PCHunter등)를 이용하여 다중 인증을 활성화하지 않은 환경에 액세스	**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) 자료 탈취 시도 후 Akira랜섬웨어 실행 2) Windows 볼륨 섀도 복사본 삭제 3) 공격 대상 폴더 및 파일 목록 식별	**trueEP는 사용자 행위 없는 레지스트리 접근 행위를 탐지 시 해당 프로세스를 중단시켜 악성행위 차단** • 사용자입력 없는 자료유출 행위 차단 • %programdata% 디렉토리 선감시 • MS백업 무력화 공격 차단 (옵션) • 폴더 및 파일 목록 식별 행위 차단
공격	1) 공격대상 파일 암호화 실행 - '<File Name>.akira' 파일명으로 변경	**trueEP 사용자 입력이 없는 파일 암호화 행위를 탐지하는 순간에 프로세스를 중단시켜 악성행위를 차단** • 사용자입력 없는 파일 암호화 행위 차단