이달의 보안 동향 및 대응

- 연초부터 사이버 침해 기승...1월 기준 역대 최대
- 랜섬웨어 공격자들, 작년 한 해 대부분 오래된 취약점 공략했다
- "☒랜섬웨어 공격 증가"… 국정원, ☒정보기관과 첫 '합동보안 권고문' 발표
- 피해자가 지불하는 랜섬웨어 1건의 몸값, 향후 9건의 공격 원동력 된다
- 묻지마 테러 ☒, 코인털이 ☒… 사이버위협에 ☒ 골머리

보안뉴스 요약

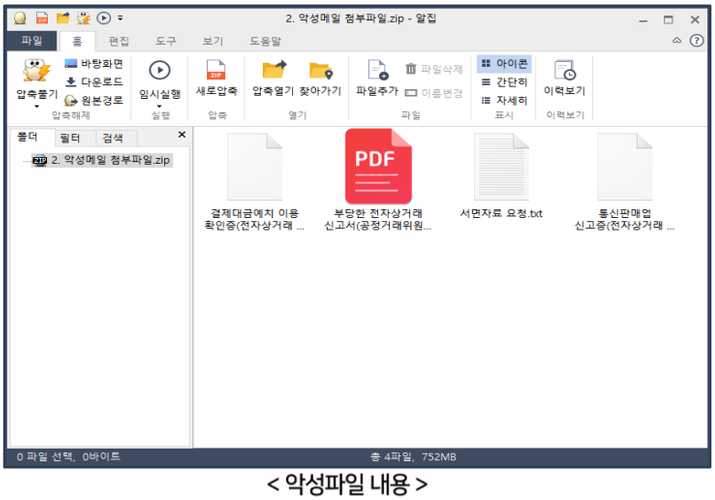
보안뉴스 23.02.06
중국 이어 북한? 北 해커조직, 공정거래위원회 사칭 피싱 공격

보안뉴스 23.02.12
검색 결과 노출 사이트 접속도 주의! 매그니베르 랜섬웨어 변형 유포

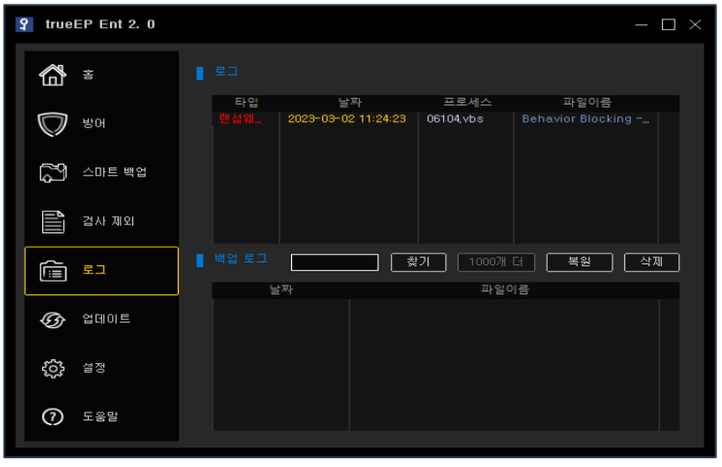
CIO 23.02.14
대학 공격한 이스라엘 새 해킹 그룹, 170만 달러 몸값 요구

CCTV뉴스 23.02.27
식품 대기업 Dole, 랜섬웨어 공격으로 북미 생산 중단

이달의 보안이슈 '코니(Konni)' 공정거래위원회 사칭 피싱 공격



< 악성파일 내용 >



< trueEP의 차단 화면 >

침투

피싱 메일에 악성파일을 첨부하여 유포

- 피싱 메일로 유포
- 메일 첨부 파일에 포함된 악성 스크립트 파일 실행

» 침투단계에서 trueEP의 대응

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

공격준비

한글(.hwp)파일을 위장한 바로가기(.lnk)

- 한글(.hwp)파일을 위장한 바로가기(.lnk)파일로 사용자가 한글 파일처럼 오인하도록 유도
- 공격 대상 폴더 및 파일 목록 식별

» 공격준비단계에서 trueEP의 대응

- 공격대상 폴더 및 파일 목록 식별행위 차단

공격

유포된 악성코드 실행

- 실행 중인 프로세스 목록, 호스트 정보, 다운로드 폴더 목록, 바탕화면 목록, 사용자IP 정보 등을 탈취

» 공격단계에서 trueEP의 대응

- 사용자행위 없는 자료 유출 행위 차단
- 해당 프로세스를 중단시켜 악성행위 차단

랜섬웨어 상세 분석

‘코니(Konni)’ 공정거래위원회 사칭 피싱 공격

단계	사용된 기법	trueEP의 대응
침투(유포)	1) 피싱 메일에 악성파일을 첨부하여 유포 2) ‘[공정거래위원회] 서면 실태조사 사전 예고 안내통지문’의 제목으로 유포됨 3) 공정거래법 조항을 언급하며 사용자 협조를 구하는 내용과 ‘소명자료 요청서류 ' 의 파일명을 가진 압축파일(.zip)첨부	**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) 한글(.hwp)파일을 위장한 바로가기(.lnk)파일로 사용자가 한글 파일처럼 오인하도록 유도 2) 해당 파일(.lnk)을 실행 시 악성 파일은 한글(.hwp)파일로 변경되며, 화면에는 정상 한글파일이 출력됨 3) 백그라운드에서 악성행위 동작 (공격 대상 폴더 및 파일 목록 식별)	trueEP는 사용자 행위 없는 레지스트리 접근 행위를 탐지 시 해당 프로세스를 중단시켜 악성행위 차단 1) 공격대상 폴더 및 파일 목록 식별행위 차단
공격	1) 실행 중인 프로세스 목록, 호스트 정보, 다운로드 폴더 목록, 바탕화면 목록, 사용자IP 정보 등을 탈취	trueEP 사용자 입력이 없는 파일 암호화 행위를 탐지하는 순간에 프로세스를 중단시켜 악성행위를 차단 1) 사용자행위 없는 자료 유출 행위 차단 2) 해당 프로세스를 중단시켜 악성행위 차단

Paradise

단계	사용된 기법	trueEP의 대응
침투(유포)	1) 스팸메일의 첨부파일을 통해 유포 2) 중국 원격 제어 프로그램 AweSun에 대한 취약점 공격을 이용하는 것으로 추정 3) AweSun 프로세스에 의해 생성된 cmd 및 파워쉘을 통해 “DP_Main.exe” 즉 Paradise 랜섬웨어가 설치됨.	**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) “%APPDATA%DP₩RunAsAdmin.dp” 파일을 사용하여 관리자 권한으로 실행 2) %APPDATA%DP₩DP_Main.exe복사본 생성 후 레지스트리Run Key에 등록 3) 복구 방지를 위한 볼륨 쉐도우 서비스 제거 4) 원격 비활성화를 위한 Windows 레지스트리 수정 시도	**trueEP는 아래의 행위를 탐지할 경우 차단함** 1) %programdata% 디렉토리 선감시 2) 시스템 레지스트리 접근 시 차단
공격	1) 공격 대상 폴더 및 파일 목록 식별 2) 특정 경로와 확장자를 제외한 모든 파일을 대상으로 암호화한 후 ‘*. [id-FEusom1c].[main@paradisenewgenshinimpact.top].honkai’ 파일명으로 변경	**trueEP는 아래의 행위를 탐지할 경우 차단함** • 사용자 행위 없는 프로세스 접근 행위 탐지시 해당 프로세스를 중단시켜 악성행위를 차단 1) 공격대상 폴더 및 파일 목록 식별 행위 차단 2) 사용자입력 없는 파일 암호화 행위 차단