이달의 보안 동향 및 대응

- IAM 기업 옥타, 사이버공격으로 모든 고객 데이터 털렸다
- 영국, 랜섬웨어 공격으로 수십조 원 잃을 위기 처해
- 정부가 예측하는 2024년 사이버 보안 위협 4대 키워드는?
- 北 해킹 시도 하루 100만건, 레이저 기술까지 탈취했다니

보안뉴스 요약

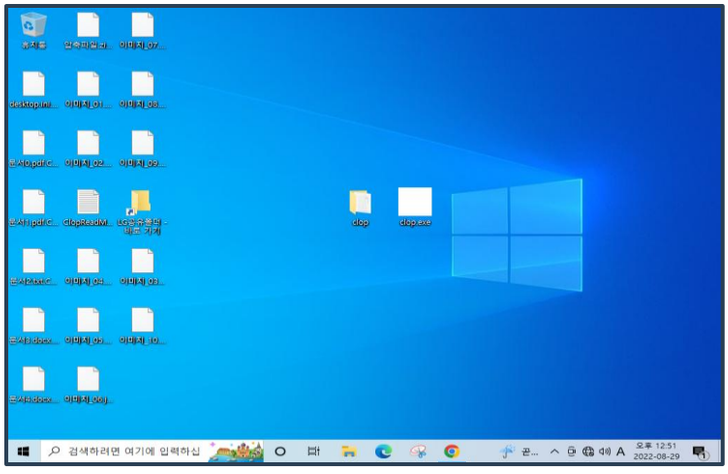
YTN 23.12.19
'랜섬웨어 해킹' 골프존 고객정보유출 은폐 의혹

zdnet 23.12.20
'마블 스파이더맨' 개발사, 랜섬웨어 해킹으로 출시 예정작 데이터 유출

데일리시큐 23.12.27
카바낙 뱅킹 멀웨어, 랜섬웨어로 진화해 재공격 시작…주의

머니투데이 23.12.28
내년 사이버 공격 심해질 것…'랜섬웨어·암호화폐 탈취' 주의해야

이달의 랜섬웨어 Clop



< 공격에 성공한 화면 >

< 트로이컷이 clop를 차단한 화면 >

침투

기관 사칭 메일에 HTML파일 첨부

- 문서 파일에 삽입된 매크로를 통한 원격 제어 멀웨어 다운로드
- 공유 폴더를 통한 악성코드 유포

» 침투단계에서 trueEP의 대응

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

공격준비

AD도메인 구성 정보 접근

- 취약점을 이용한 실행 권한 상승
- 각 도메인 컨트롤러 서버에 연결하여 연결된 시스템 장악
- 사용자의 개인정보 파일 유출

» 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
- AD접근 행위 차단(옵션)

공격

유포된 악성코드 실행

- “<filename>. clop”으로 데이터 암호화
- “ClopReadMe.txt” 랜섬노트 생성

» 공격단계에서 trueEP의 대응

- 사용자입력 없는 암호화 행위 차단
- 행위 차단 시 프로세스 킬

랜섬웨어 상세 분석

Clop

단계	사용된 기법	trueEP의 대응
침투(유포)	1) 기관 사칭 메일로 실행 유도, 문서가 아닌 HTML파일을 첨부하여 유포 2) 문서 파일에 삽입된 매크로를 통한 원격 제어 멀웨어 다운로드 3) 도메인 컨트롤러의 공유 폴더에 CLOP랜섬웨어 등 악성코드 유포	**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) AD도메인 구성 정보 확인 및 취약점을 이용한 실행 권한 상승 2) AD도메인 관리자 계정이 성공적으로 획득되면 도메인 컨트롤러 서버에 연결하여 각 연결된 시스템 장악 3) 사용자의 개인정보 파일 유출	**trueEP는 계정을 탈취하고, 권한을 상승 등 일련의 진행 과정에서 trueEP 행위기반 알고리즘에 위배될 경우, 이를 탐지하여 차단함** 1) AD접근 행위 차단(옵션) 2) 파일 유출 진행 시 유출차단 알고리즘에 의한 이중방어 진행
공격	1) AD도메인에 연결된 시스템에 작업 스케줄러 또는 원격 명령을 이용, CLOP Ransomware를 실행 2) “<filename>. clop”으로 데이터 암호화 3) “ClopReadMe.txt” 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

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 ➢피해자가 방문하는 고유한 Tor주소 ‘액세스 토큰’을 생성하는데 사용 4) PsExec를 이용하여 레지스트리에 접근, 제한된 원격 관리 기능 비활성화(관리 권한 상승 시도)	**trueEP는 계정을 탈취하고, 권한을 상승 등 일련의 진행 과정에서 trueEP 행위기반 알고리즘에 위배될 경우, 이를 탐지하여 차단함** 1) 파일 유출 진행 시 유출차단 알고리즘에 의한 이중방어 진행 2) 윈도우 백업 삭제 행위 차단(옵션) 3) 시스템 레지스트리 접근 시 차단
공격	1) 네트워크 공유를 통해 전파된 악성코드 실행 2) 공격 대상 폴더 및 파일 목록 식별 3) 7자의 랜덤한 영어,숫자 확장자로 데이터 암호화 4) “RECOVER-sykffle-FILES.TXT” 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