Cisco 보안 엔드포인트 포렌식 스냅샷 정보

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[일반 정보](#)

소개

이 문서에서는 포렌식 스냅샷이 엔드포인트에서 수집할 수 있는 권한 있는 정보에 대해 설명합니다
.

기고자: Cisco 소프트웨어 엔지니어 Pedro Medina.

사전 요구 사항

.

- Cisco "보안 엔드포인트" 콘솔
- Cisco "궤도"

요구 사항

- 관리자 또는 비관리자 사용자로 "보안 엔드포인트"에 액세스
- Cisco "Orbital" 액세스

  참고: 사용자가 비관리자인 경우 TAC 지원 팀을 통해 "비관리자를 위한 포렌식 스냅샷" 기능 활성화를 요청해야 합니다.

일반 정보

포렌식 스냅샷이 요청되면 사용자가 이 설명 테이블을 기반으로 필요한 정보를 찾을 수 있는 필수 정보에 따라 테이블 형식으로 정보가 표시됩니다.

이름	의미	개인 정보 보호 문제
Autoexec 항목	시스템 시작 시 실행되는 항목	없음
Bitlocker 암호화 모니터링	마운트된 모든 드라이브의 암호화 상태	암호화되지 않은 파일 버전에 대한 일부 성
DNS 캐시 테이블 모니터링	최근에 검색한 도메인	최근 브라우저 기록
호스트 파일 데이터	호스트 파일의 항목	없음

호스트에 설치된 프로그램	설치된 애플리케이션	없음
수신 포트	네트워크 리스너를 여는 프로그램을 나열합니다.	없음
로드된 모듈 해시	실행 중인 DLL(Dynamic Link Library) 파일의 해시 값	없음
로드된 모듈 프로세스	실행 중인 프로세스의 이름, 경로 및 PID	없음
로드된 모듈과 프로세스 비교	로드된 모듈의 모듈 ID를 프로세스의 PID에 매핑 테이블	없음
로그온 세션	로그인한 사용자(시스템 사용자 포함)	없음
매핑된 드라이브	로컬 및 원격 마운트 지점, 파일 시스템 유형, 부트 파티션 정보, 암호화 정보.	없음
네트워크 연결 - 프로세스	내부 및 아웃바운드 네트워크 연결을 특정 PID에 매핑하고 프로세스를 시작한 시작 명령줄을 표시합니다.	프라이빗 상태일 수 있는 특정 애플리케의 네트워크 연결이 노출될 수 있습니다
네트워크 인터페이스	디바이스의 모든 물리적 및 가상 네트워크 인터페이스 목록	없음
네트워크 프로파일 레지스트리	시스템이 연결된 네트워크 목록입니다.	WIFI SSID가 노출될 수 있습니다.
OS 버전	운영 체제 버전	없음
Powershell 기록	디바이스에서 실행되고 시스템에 저장된 모든 Powershell 명령 목록입니다.	스크립트로 코딩된 비밀번호, 비밀 API 기타 민감한 데이터를 공개할 수 있는 잠 .
프리페치 디렉토리	메모리 관리 기능 - OS는 시작 시간을 절약하기 위해 자주 로드되는 실행 파일을 미리 로드하려고 시도합니다.	사용자 습관의 노출.
최근 파일 데이터	가장 최근에 사용/액세스한 파일	사용자 습관 및 개인 파일 이름의 노출
파일 해시 실행	실행 중인 모든 실행 파일의 이름, 경로, 명령줄, PID, 소유자	없음
서비스 모니터링 실행	실행 중인 모든 서비스의 이름, 서비스 유형, PID 및 시작 유형	없음
예약된 작업	시스템에서 주기적으로 실행되도록 설정된 모든 자동화된 작업 목록	없음
공유 리소스	시스템에서 공유 열기	없음
시작 항목	시스템 시작 시 실행되는 항목이며, 레지스트리 키에 저장된다는 점에서 autoexec과 다릅니다.	없음
시스템 네트워크 상태 모니터링	네트워크 통계	없음
임시 디렉토리 파일 데이터	프로세스에 의해 생성된 임시 파일	사용자 검색 기록이 노출될 수 있습니다

신뢰할 수 있는 루트 인증서	신뢰할 수 있는 루트 인증서 저장소 데이터 덤프	없음
UBSTOR 레지스트리 키	연결된 USB 장치의 기록	장치 일련 번호 노출
사용자 그룹	시스템의 로컬 그룹	없음
UserAssist 모니터링	최근에 실행된 파일을 표시합니다.	암호화 실행 또는 도구 삭제와 같은 숨기 동작이 노출될 수 있습니다.
사용자	디바이스의 로컬 사용자	없음
사용자 - 로그인됨	현재 디바이스에 로그인한 로컬 사용자	없음
WMI 이벤트 필터 모니터링	특정 항목에 대한 이벤트 로그 감시	없음
Windows AV 제품 모니터링	시스템에 설치된 안티바이러스(있는 경우)	없음
Windows BAM 항목 모니터링	파일 실행에 대한 증거 제공	동작 노출 가능
Windows 환경 변수	경로 정보, 시스템 변수 등을 표시합니다.	없음
Windows 핫픽스	설치된 모든 패치 목록	없음
Windows NT 도메인 검색	컴퓨터가 인증할 수 있는 도메인 목록	없음
Windows ShellBags 모니터링	폴더에 대한 사용자 액세스, 해당 폴더를 보기 위한 기본 설정 등에 대한 정보를 제공합니다.	사용자 습관의 노출.
Windows ShimCache 모니터링	실행 파일과의 호환성 추적	사용자 행동 노출.
Chrome 확장 모니터링	Chrome 확장 목록	사용자 행동 노출.
Windows Office MRU	각 Office 응용 프로그램에 대해 가장 최근에 사용한 파일을 나열합니다.	민감한 파일 이름, 사용자 행동 노출