Información de instantánea de diagnóstico de Cisco Secure Endpoint

Contenido

Introducción

Este documento describe la información privilegiada que una instantánea forense puede recopilar de los terminales.

Colaboración de Pedro Medina, ingeniero de software de Cisco.

Prerequisites

Cisco recomienda que tenga conocimiento sobre estos temas:

- Consola "Secure Endpoint" de Cisco
- Cisco "Orbital"

Requirements

- Acceso a "terminal seguro" con usuario administrador o no administrador
- Acceso a Cisco "Orbital"

> **Nota:** Si su usuario no es administrador, debe solicitar que se habilite la función "Instantáneas de diagnóstico para no administradores" a través del equipo de asistencia del TAC.

Información general

Una vez que se haya solicitado una instantánea forense, la información se presentará en un formato de tabla, en función de la información necesaria, el usuario puede encontrar cualquier información necesaria en función de esta tabla de descripción:

Nombre	Qué significa	Preocupaciones sobre privacidad
elementos Autoexec	Elementos que se ejecutan al iniciar el equipo	Ninguno
Supervisión de cifrado Bitlocker	Estado de cifrado de cada unidad montada	Visibilidad de las versiones de archivos cifradas

Supervisión de tabla de caché DNS	Dominios buscados recientemente	Historial reciente del navegador.
Hosts Datos de archivo	Elementos del archivo de hosts	Ninguno
Programas instalados en host	Aplicaciones instaladas	Ninguno
Puertos de escucha	Enumera los programas que abren receptores de red	Ninguno
Hashes de módulos cargados	Valores hash de archivos DLL (biblioteca de vínculos dinámicos) en ejecución	Ninguno
Procesos de módulos cargados	Nombre, ruta y PID de los procesos en ejecución	Ninguno
Módulos cargados frente a procesos	Asignación de ID de módulo desde módulos cargados a PID desde la tabla Procesos	Ninguno
Sesiones de inicio	Usuarios conectados, incluidos los usuarios del sistema	Ninguno
Unidades asignadas	Puntos de montaje locales y remotos, tipo de sistema de archivos, información de partición de arranque, información de cifrado.	Ninguno
Conexiones de red - Procesos	Asigna conexiones de red entrantes y salientes a PID específicos y muestra la línea de comandos de inicio que inició el proceso.	Posible exposición de conexiones de re ciertas aplicaciones, que pueden ser privadas.
Interfaces de red	Lista de todas las interfaces de red físicas y virtuales del dispositivo	Ninguno
Registro de perfiles de red	Lista de redes a las que se ha conectado la máquina.	Posible exposición de SSID WIFI.
Versión de SO	Versión del sistema operativo	Ninguno
Historial de Powershell	Lista de todos los comandos PowerShell ejecutados en el dispositivo y almacenados en el sistema.	Posibilidad de exponer contraseñas, cl API secretas y otros datos confidencial codificados en scripts.
Obtener directorio previamente	Función de administración de memoria: el SO intentará cargar previamente los ejecutables cargados con frecuencia para ahorrar tiempo de inicio.	Exposición de los hábitos de los usuari
Datos de archivos recientes	Archivos utilizados/accedidos más recientemente	Exposición de hábitos de usuario y nor de archivo privados.
Ejecución de hashes de archivo	Nombre, ruta, línea de comandos, PID, propietario de todos los ejecutables en ejecución.	Ninguno
Ejecución de supervisión de servicios	Nombre, tipo de servicio, PID y tipo de inicio de todos los servicios en ejecución	Ninguno
Tareas programadas	Lista de todas las tareas automatizadas configuradas para ejecutarse periódicamente en el sistema	Ninguno
Recursos	Abrir recurso compartido en el sistema	Ninguno

compartidos		
Elementos de inicio	Elementos que se ejecutan al iniciar el equipo, distintos de autoexec en que se almacenan en claves del Registro	Ninguno
Supervisión del estado de red del sistema	Estadísticas de red	Ninguno
Datos del archivo de directorio temporal	Archivos temporales creados por procesos	Posible exposición del historial de navegación del usuario.
Certificados raíz de confianza	Volcado de datos del almacén de certificados raíz de confianza	Ninguno
Clave del Registro UBSTOR	Historial de dispositivos USB conectados	Exposición de los números de serie de dispositivo.
Grupos de usuarios	Grupos locales en el equipo	Ninguno
Supervisión de UserAssist	Muestra los archivos ejecutados recientemente	Posible exposición de comportamiento ocultos, como ejecutar herramientas de cifrado o borrado.
Usuarios	Usuarios locales en el dispositivo	Ninguno
Usuarios: conectados	Usuarios locales que han iniciado sesión en el dispositivo	Ninguno
Supervisión de filtros de eventos WMI	Observa el registro de eventos de elementos específicos	Ninguno
Supervisión de productos Windows AV	Qué antivirus instalado está en el sistema, si lo hay	Ninguno
Supervisión de entradas de BAM de Windows	Proporciona pruebas de la ejecución de archivos	Podría exponer comportamientos
Variables de entorno de Windows	Muestra información de ruta, variables del sistema, etc.	Ninguno
Revisiones de Windows	Lista de todos los parches instalados	Ninguno
Búsqueda de dominios de Windows NT	Lista de dominios en los que el equipo puede autenticarse	Ninguno
Supervisión de ShellBags de Windows	Proporciona información sobre el acceso de los usuarios a las carpetas, las preferencias para ver la carpeta, etc.	Exposición de los hábitos de los usuari
Supervisión de Windows ShimCache	Realiza un seguimiento de la compatibilidad con ejecutables	Exposición de comportamientos de los usuarios.
Supervisión de extensiones de Chrome	Muestra las extensiones de Chrome	Exposición de comportamientos de los usuarios.
MRU de Windows Office	Muestra los archivos utilizados más recientemente para cada aplicación de Office	Exposición de nombres de archivo confidenciales, comportamiento del us