Informations sur les instantanés Cisco Secure Endpoint Forensic

Contenu

Introduction

Ce document décrit les informations privilégiées qu'un cliché d'analyse peut recueillir à partir de points de terminaison.

Contribution de Pedro Medina, ingénieur logiciel Cisco.

Conditions préalables

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Console « Secure Endpoint » de Cisco
- «Orbital » Cisco

Conditions requises

- Accès au « point de terminaison sécurisé » avec un utilisateur administrateur ou non administrateur
- Accès à Cisco « Orbital »

> **Note**: Si votre utilisateur n'est pas un administrateur, vous devez demander à activer la fonctionnalité « Forensic Snapshots for Non-Admins » via l'équipe d'assistance TAC.

Informations générales

Une fois qu'un instantané d'analyse a été demandé, les informations sont présentées sous forme de tableau, en fonction des informations requises. L'utilisateur peut trouver toutes les informations requises en fonction de ce tableau de description :

Name (nom)	Ce que cela signifie	Problèmes de confidentialité
Éléments Autoexec	Éléments exécutés au démarrage de la machine	Aucune
Surveillance du chiffrement Bitlocker	État de cryptage de chaque lecteur monté	Une certaine visibilité sur les versions chiffrées des fichiers

Surveillance de table de cache DNS	Domaines récemment recherchés	Historique récent du navigateur.
Données du fichier hôte	Éléments du fichier d'hôtes	Aucune
Programmes installés sur l'hôte	Applications installées	Aucune
Ports d'écoute	Répertorie les programmes ouvrant des écouteurs réseau	Aucune
Hachages des modules chargés	Valeurs de hachage des fichiers DLL (Dynamic Link Library) en cours d'exécution	Aucune
Processus des modules chargés	Nom, chemin et PID des processus en cours d'exécution	Aucune
Modules chargés et processus	Mappage de l'ID de module des modules chargés au PID de la table Processus	Aucune
Sessions de connexion	Utilisateurs connectés, y compris les utilisateurs système	Aucune
Lecteurs mappés	Points de montage locaux et distants, type de système de fichiers, informations de partition de démarrage, informations de chiffrement.	Aucune
Connexions réseau - Processus	Mappe les connexions réseau entrantes et sortantes à des PID spécifiques et affiche la ligne de commande de démarrage qui a lancé le processus.	Exposition possible des connexions rés de certaines applications, qui peuvent privées.
Interfaces réseau	Liste de toutes les interfaces réseau physiques et virtuelles sur le périphérique	Aucune
Registre des profils réseau	Liste des réseaux auxquels la machine est connectée.	Exposition possible des SSID WIFI.
Version du SE	Version du système d'exploitation	Aucune
Historique Powershell	Liste de toutes les commandes Powershell exécutées sur le périphérique et stockées sur le système.	Possibilité d'exposer des mots de pass des clés API secrètes et d'autres donn sensibles codées dans des scripts.
Répertoire de prélecture	Fonction de gestion de la mémoire : le système d'exploitation tente de précharger les fichiers exécutables fréquemment chargés pour gagner du temps au démarrage.	Exposition des habitudes des utilisateu
Données des fichiers récents	Fichiers les plus récemment utilisés/consultés	Exposition des habitudes des utilisateu des noms de fichiers privés.
Hachage des fichiers en cours	Nom, chemin, ligne de commande, PID, propriétaire de tous les exécutables en cours d'exécution.	Aucune
Exécution du contrôle des services	Nom, type de service, PID et type de démarrage de tous les services en cours d'exécution	Aucune
Tâches planifiées	Liste de toutes les tâches automatisées définies pour s'exécuter périodiquement sur le système	Aucune

Ressources partagées	Partages ouverts sur le système	Aucune
Éléments de démarrage	Éléments qui s'exécutent au démarrage de l'ordinateur, différents de autoexec en ce qu'ils sont stockés dans des clés de registre	Aucune
Surveillance de l'état du réseau	Statistiques réseau	Aucune
Données du fichier répertoire temporaire	Fichiers temporaires créés par des processus	Exposition possible de l'historique de navigation utilisateur.
Certificats racine approuvés	Vidage des données du magasin de certificats racine approuvé	Aucune
Clé de registre UBSTOR	Historique des périphériques USB branchés	Exposition des numéros de série des périphériques.
Groupes d'utilisateurs	Groupes locaux sur l'ordinateur	Aucune
Surveillance UserAssist	Affiche les fichiers récemment exécutés	Exposition possible d'un comportement masqué, tel que l'exécution d'outils de chiffrement ou d'effacement.
Utilisateurs	Utilisateurs locaux sur le périphérique	Aucune
Utilisateurs - Connectés	Utilisateurs locaux actuellement connectés au périphérique	Aucune
Surveillance des filtres d'événements WMI	Surveille le journal des événements pour des éléments spécifiques	Aucune
Surveillance des produits AV Windows	Quel antivirus installé se trouve sur le système, le cas échéant ?	Aucune
Analyse des entrées BAM Windows	Fournit une preuve de l'exécution des fichiers	Peut exposer des comportements
Variables d'environnement Windows	Affiche les informations de chemin, les variables système, etc.	Aucune
Correctifs Windows	Liste de tous les correctifs installés	Aucune
Recherche de domaines Windows NT	Liste des domaines auxquels la machine peut s'authentifier	Aucune
Surveillance Windows ShellBags	Fournit des informations sur l'accès utilisateur aux dossiers, les préférences d'affichage de ce dossier, etc.	Exposition des habitudes des utilisateu
Surveillance Windows ShimCache	Suit la compatibilité avec les exécutables	Exposition des comportements des utilisateurs.
Surveillance des extensions Chrome	Liste les extensions Chrome	Exposition des comportements des utilisateurs.
Windows Office MRU	Répertorie les derniers fichiers utilisés pour chaque application Office	Exposition des noms de fichiers sensib comportement des utilisateurs