Informazioni sulle istantanee forensi di Cisco Secure Endpoint

Sommario

Introduzione

In questo documento vengono descritte le informazioni privilegiate che uno snapshot forense può raccogliere dagli endpoint.

Contributo di Pedro Medina, Cisco Software Engineer.

Prerequisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Console Cisco "Secure Endpoint"
- Cisco "Orbital"

Requisiti

- Accesso a "Secure Endpoint" con un utente amministratore o non amministratore
- Accesso a Cisco "Orbital"

  Nota: Se l'utente non è un amministratore, è necessario richiedere di abilitare la funzione "Forensic Snapshots for Non-Admins" tramite il team di supporto TAC.

Informazioni generali

Una volta richiesta una copia istantanea forense, le informazioni verranno presentate in formato tabellare, in base alle informazioni richieste che l'utente può trovare in base a questa tabella di descrizione:

Nome	Cosa significa	Problemi di privacy
Elementi Autoexec	Elementi eseguiti all'avvio del computer	Nessuna
Monitoraggio Crittografia Bitlocker	Stato di crittografia di ogni unità montata	Visibilità delle versioni non crittografate file
Monitoraggio tabella	Domini cercati di recente	Cronologia recente del browser.

cache DNS		
Dati file host	Elementi nel file hosts	Nessuna
Programmi installati sull'host	Applicazioni installate	Nessuna
Porte di ascolto	Elenca i programmi che aprono listener di rete	Nessuna
Hash moduli caricati	Valori hash dei file DLL in esecuzione	Nessuna
Processi dei moduli caricati	Nome, percorso e PID dei processi in esecuzione	Nessuna
Moduli caricati e processi	Mappatura dell'ID modulo dai moduli caricati al PID dalla tabella dei processi	Nessuna
Sessioni di accesso	Utenti connessi, inclusi gli utenti di sistema	Nessuna
Unità mappate	Punti di montaggio locali e remoti, tipo di file system, informazioni sulla partizione di avvio, informazioni sulla crittografia.	Nessuna
Connessioni di rete - Processi	Esegue il mapping delle connessioni di rete in entrata e in uscita a PID specifici e visualizza la riga di comando di avvio che ha avviato il processo.	Possibile esposizione delle connession rete di alcune applicazioni, che posson essere private.
Interfacce di rete	Elenco di tutte le interfacce di rete fisiche e virtuali nel dispositivo	Nessuna
Registro di sistema dei profili di rete	Elenco delle reti a cui il computer si è connesso.	Possibile esposizione di SSID WIFI.
Versione sistema operativo	Versione del sistema operativo	Nessuna
Cronologia di Powershell	Elenco di tutti i comandi PowerShell eseguiti sul dispositivo e archiviati nel sistema.	Possibilità di esporre password, chiavi segrete e altri dati riservati codificati ne script.
Directory di prelettura	Funzionalità di gestione della memoria: il sistema operativo tenterà di precaricare gli eseguibili caricati di frequente per risparmiare tempo all'avvio.	Esposizione alle abitudini degli utenti.
Dati file recenti	File utilizzati/utilizzati più di recente	Esposizione alle abitudini degli utenti e nomi di file privati.
Esecuzione hash file	Nome, percorso, riga di comando, PID, proprietario di tutti gli eseguibili in esecuzione.	Nessuna
Esecuzione monitoraggio servizi	Nome, tipo di servizio, PID e tipo di avvio di tutti i servizi in esecuzione	Nessuna
Operazioni pianificate	Elenco di tutte le operazioni automatiche impostate per l'esecuzione periodica nel sistema	Nessuna
Risorse condivise	Apri condivisione nel sistema	Nessuna
Elementi di avvio	Elementi che vengono eseguiti all'avvio del computer - diversi da autoexec in quanto	Nessuna

	sono archiviati nelle chiavi del Registro di sistema	
Monitoraggio dello stato della rete del sistema	Statistiche di rete	Nessuna
Dati file di directory temporanei	File temporanei creati dai processi	Possibile esposizione della cronologia esplorazioni utente.
Certificati radice attendibili	Dump dati archivio certificati radice attendibile	Nessuna
Chiave del Registro di sistema USTOR	Cronologia dei dispositivi USB collegati	Esposizione dei numeri di serie dei dispositivi.
Gruppi di utenti	Gruppi locali nel computer	Nessuna
Monitoraggio di UserAssist	Mostra i file eseguiti di recente	Possibile esposizione di comportament nascosti, ad esempio l'esecuzione di strumenti di crittografia o cancellazione
Utenti	Utenti locali sul dispositivo	Nessuna
Utenti - Accesso	Utenti locali attualmente connessi al dispositivo	Nessuna
Monitoraggio dei filtri eventi WMI	Controlla il registro eventi per individuare elementi specifici	Nessuna
Monitoraggio dei prodotti AV Windows	L'eventuale antivirus installato nel sistema	Nessuna
Monitoraggio voci BAM di Windows	Prova dell'esecuzione dei file	Potrebbe esporre i comportamenti
Variabili di ambiente di Windows	Mostra informazioni percorso, variabili di sistema e così via.	Nessuna
Aggiornamenti rapidi di Windows	Elenco di tutte le patch installate	Nessuna
Ricerca domini Windows NT	Elenco dei domini a cui il computer può eseguire l'autenticazione	Nessuna
Monitoraggio di Windows ShellBags	Fornisce informazioni sull'accesso degli utenti alle cartelle, sulle preferenze per la visualizzazione della cartella e così via.	Esposizione alle abitudini degli utenti.
Monitoraggio di Windows ShimCache	Verifica la compatibilità con gli eseguibili	Esposizione dei comportamenti degli u
Monitoraggio estensioni Chrome	Elenca le estensioni di Chrome	Esposizione dei comportamenti degli u
Windows Office MRU	Elenca gli ultimi file utilizzati per ogni applicazione di Office	Esposizione dei nomi di file sensibili, comportamento dell'utente