Forensische Snapshot-Informationen zu Cisco Secure Endpoint

Inhalt

Einleitung

Dieses Dokument beschreibt die privilegierten Informationen, die ein forensischer Snapshot von Endpunkten sammeln kann.

Beitrag von Pedro Medina, Cisco Software Engineer.

Voraussetzungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Konsole "Sichere Endgeräte"
- Cisco Orbital

Anforderungen

- Zugriff auf "sichere Endgeräte" mit oder ohne Administratorbenutzer
- Zugang zu Cisco "Orbital"

> **Anmerkung:** Wenn Ihr Benutzer kein Administrator ist, müssen Sie die Aktivierung der Funktion "Forensische Snapshots für Nicht-Administratoren" über das TAC-Support-Team anfordern.

Allgemeine Informationen

Sobald ein forensischer Snapshot angefordert wurde, werden die Informationen in einem Tabellenformat angezeigt. Basierend auf den erforderlichen Informationen kann der Benutzer die erforderlichen Informationen anhand der folgenden Beschreibungstabelle finden:

Name	Vorteile	Datenschutzbedenken
AutoAusführen-Elemente	Elemente, die beim Systemstart ausgeführt werden	None
Überwachung der Bitlocker-Verschlüsselung	Verschlüsselungsstatus aller gemounteten Laufwerke	Gewisse Transparenz unverschlüsselte Dateiversionen

Überwachung der DNS-Cachetabelle	Kürzlich durchsuchte Domänen	Aktueller Browserverlauf.
Hosts-Dateidaten	Elemente in der Hosts-Datei	None
Installierte Programme auf dem Host	Installierte Anwendungen	None
Überwachungs-Ports	Listet Programme auf, die Netzwerklistener öffnen	None
Geladene Modulhashes	Hashwerte der ausgeführten DLL-Dateien (Dynamic Link Library)	None
Prozesse geladener Module	Name, Pfad und PID der laufenden Prozesse	None
Geladene Module und Prozesse	Zuordnung der Modul-ID von geladenen Modulen zu der PID aus der Prozesstabelle	None
Anmeldesitzungen	Angemeldete Benutzer, einschließlich Systembenutzer	None
Zugeordnete Laufwerke	Lokale und entfernte Bereitstellungspunkte, Dateisystemtyp, Informationen zur Bootpartition, Verschlüsselungsinformationen.	None
Netzwerkverbindungen - Prozesse	Ordnet ein- und ausgehende Netzwerkverbindungen bestimmten PIDs zu und zeigt die Startup-Befehlszeile an, die den Prozess initiiert hat.	Mögliche Exposition von Netzwerkverbindungen bestimmter Anwendungen, die privat sein können.
Netzwerkschnittstellen	Liste aller physischen und virtuellen Netzwerkschnittstellen auf dem Gerät	None
Registrierung von Netzwerkprofilen	Liste der Netzwerke, mit denen der Computer verbunden ist.	Mögliche Exposition von WIFI-SSIDs.
Betriebssystemversion	Version des Betriebssystems	None
Powershell-Verlauf	Liste aller auf dem Gerät ausgeführten und auf dem System gespeicherten Powershell-Befehle.	Möglichkeit zur Offenlegung von Passwörtern, geheimen API-Schlüsseln anderen vertraulichen Daten, die in Sk kodiert sind.
Prefetch-Verzeichnis	Speicherverwaltungsfunktion - Das Betriebssystem versucht, häufig geladene ausführbare Dateien vorzuladen, um die Startzeit zu sparen.	Offenlegung von Benutzergewohnheite
Daten der letzten Dateien	Zuletzt verwendete/aufgerufene Dateien	Offenlegung von Benutzergewohnheite privaten Dateinamen.
Ausgeführte Datei-Hashes	Name, Pfad, Befehlszeile, PID, Eigentümer aller ausgeführten ausführbaren Dateien.	None
Ausführen der Dienstüberwachung	Name, Diensttyp, PID und Starttyp aller ausgeführten Dienste	None
Geplante Aufgaben	Liste aller automatisierten Aufgaben, die auf dem System regelmäßig ausgeführt werden	None

Gemeinsam genutzte Ressourcen	Öffnen von Freigaben im System	None
Startelemente	Elemente, die beim Systemstart ausgeführt werden - unterscheiden sich von autoexec dadurch, dass diese in Registrierungsschlüsseln gespeichert werden	None
Überwachung des Systemnetzwerkstatus	Netzwerkstatistik	None
Temporäre Verzeichnisdateidaten	Temporäre Dateien, die von Prozessen erstellt wurden	Mögliche Offenlegung des Browserverl
Vertrauenswürdige Stammzertifikate	Datenspeicherauszug für vertrauenswürdige Stammzertifikate	None
UBSTOR-Registrierungsschlüssel	Verlauf der angeschlossenen USB-Geräte	Anzeige von Seriennummern der Gerä
Benutzergruppen	Lokale Gruppen auf dem Computer	None
UserAssist-Überwachung	Zeigt kürzlich ausgeführte Dateien an	Mögliche Offenlegung von verstecktem Verhalten, wie das Ausführen von Verschlüsselungs- oder Wischwerkzeu
Benutzer	Lokale Benutzer auf dem Gerät	None
Benutzer - Angemeldet	Lokale Benutzer, die derzeit am Gerät angemeldet sind	None
WMI-Ereignisfilterüberwachung	Überwacht das Ereignisprotokoll auf bestimmte Elemente	None
Überwachung von Windows AV-Produkten	Welche installierte Antivirus-Software ist auf dem System, falls vorhanden?	None
Überwachung von Windows BAM-Einträgen	Nachweise für die Ausführung von Dateien	Verhalten aufdecken könnten
Windows-Umgebungsvariablen	Zeigt Pfadinformationen, Systemvariablen usw. an	None
Windows-Hotfixe	Liste aller installierten Patches	None
Suche nach Windows NT-Domänen	Liste der Domänen, bei denen sich der Computer authentifizieren kann	None
Windows ShellBags-Überwachung	Enthält Informationen über den Benutzerzugriff auf Ordner, Einstellungen zum Anzeigen dieses Ordners usw.	Offenlegung von Benutzergewohnheite
Windows ShimCache-Überwachung	Nachverfolgung der Kompatibilität mit ausführbaren Dateien	Offenlegung des Benutzerverhaltens
Überwachung von	Listet Chrome-Erweiterungen auf	Offenlegung des Benutzerverhaltens

Chrome-Erweiterungen		
Windows Office MRU	Führt die zuletzt verwendeten Dateien für jede Office-Anwendung auf	Gefährdung empfindlicher Dateinamen Benutzerverhalten