Cisco Secure Endpoint forensische snapshot-informatie

Inhoud

Inleiding

Dit document beschrijft de geprivilegieerde informatie die een forensische snapshot kan verzamelen op eindpunten.

Bijgedragen door Pedro Medina, Cisco Software Engineer.

Voorwaarden

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco "Secure Endpoint"-console
- Cisco "Orbital"

Vereisten

- Toegang tot "Secure Endpoint" met beheerder of niet-beheerder.
- Toegang tot Cisco "Orbital"

  Opmerking: Als uw gebruiker een Non-Admin is, moet u vragen om de functie "Forensische Snapshots voor Non-Admins" via TAC-ondersteuningsteam in te schakelen.

Algemene informatie

Zodra een Forensische Snapshot is gevraagd, wordt de informatie gepresenteerd in een tabelformaat, gebaseerd op de vereiste informatie kan de gebruiker elke vereiste informatie vinden op basis van deze beschrijvingstabel:

Name	Wat het betekent	Privacyproblemen
Automatisch exec-items	Items die worden uitgevoerd bij opstarten machine	None
Bewaking van bitlocker-encryptie	Versleutelingsstatus van elk gekoppeld station	Enige zichtbaarheid in unencrypted ver van bestanden
DNS-	Recent doorzochte domeinen	Recente browser geschiedenis.

cachetabelbewaking		
Hosts-bestandsgegevens	Items in het hostbestand	None
Geïnstalleerde programma's op host	Geïnstalleerde toepassingen	None
Luisterpoorten	Maakt een lijst van programma's die netwerkluisteraars openen	None
Hashes voor geladen modules	Hashwaarden van het uitvoeren van DLL-bestanden (Dynamic Link Library)	None
Beladen modulaire processen	Naam, pad en PID van lopende processen	None
Geladen modules versus processen	Toewijzing van module-ID van geladen modules aan PID uit de tabel Processen	None
Aanmeldingssessies	Aangemelde gebruikers, inclusief systeemgebruikers	None
Gekoppelde stations	Lokale en externe koppelpunten, type bestandssysteem, informatie over opstartpartitie, coderingsinformatie.	None
Netwerkverbindingen - processen	Kaarten in- en uitgaande netwerkverbindingen met specifieke PID's en geeft de opstartopdrachtregel weer die het proces heeft gestart.	Mogelijke blootstelling van netwerkverbindingen van bepaalde toepassingen, die privé kunnen zijn.
Netwerkinterfaces	Lijst van alle fysieke en virtuele netwerkinterfaces op het apparaat	None
Registratie van netwerkprofielen	Lijst van netwerken waarmee de machine verbinding heeft gemaakt.	Mogelijke blootstelling van WIFI SSID's
Versie besturingssysteem	Versie van het besturingssysteem	None
Powershell History	Lijst van alle Powershell-opdrachten die op het apparaat worden uitgevoerd en op het systeem zijn opgeslagen.	Potentieel om wachtwoorden, geheime sleutels, en andere gevoelige gegeven bloot te stellen die in scripts worden gecodeerd.
Prefetch-map	Geheugenbeheerfunctie - het besturingssysteem zal proberen vaak geladen uitvoerbare bestanden voor te laden om opstarttijd te besparen.	Publiciteit van gewoontes.
Recente bestandsgegevens	Meest recent gebruikte / benaderde bestanden	Blootstelling aan gebruikersgewoonten persoonlijke bestandsnamen.
Bestandshashes uitvoeren	Naam, pad, opdrachtregel, PID, eigenaar van alle actieve executables.	None
Bewaking van operationele services	Naam, servicetype, PID en opstarttype van alle actieve services	None
Geplande taken	Lijst met alle geautomatiseerde taken die zijn ingesteld om periodiek op het systeem te worden uitgevoerd	None

Gedeelde bronnen	Open aandelen op het systeem	None
Opstartitems	Items die draaien bij het opstarten van de machine - anders dan autoexec in die zin dat deze worden opgeslagen in registersleutels	None
Statusbewaking van systeemnetwerk	Netwerkstatistieken	None
Temperatuur Directory File Data	Tijdelijke bestanden gemaakt door processen	Mogelijke belichting van gebruiker brow geschiedenis.
Trusted Root-certificaten	Trusted Root Certificate Store data dump	None
UBSTOR-registersleutel	Geschiedenis van aangesloten USB apparaten	Blootstelling van serienummers van de apparatuur.
Gebruikersgroepen	Lokale groepen op de machine	None
UserAssist-bewaking	Toont recent uitgevoerde bestanden	Mogelijke belichting van verborgen gec zoals het uitvoeren van encryptie- of wisgereedschappen.
Gebruikers	Lokale gebruikers op het apparaat	None
Gebruikers - ingelogd	Lokale gebruikers die momenteel op het apparaat zijn aangemeld	None
Bewaking van WMI-gebeurtenisfilters	Logboek voor gebeurtenissen voor specifieke items	None
Windows AV-productbewaking	Welke anti-virus is geïnstalleerd op het systeem, als er	None
Windows BAM-bewaking van vermeldingen	Bewijs van de uitvoering van bestanden	Kan gedrag blootstellen
Windows-omgevingsvariabelen	Geeft padinformatie, systeemvariabelen, etc. weer.	None
Windows-hotfixes	Lijst met alle geïnstalleerde patches	None
Zoeken op Windows NT-domeinen	Lijst met domeinen waaraan de machine kan authenticeren	None
Windows Shell-taakbewaking	Hier vindt u informatie over de toegang van gebruikers tot mappen, voorkeuren voor het weergeven van die map, enzovoort.	Publiciteit van gewoontes.
Windows ShimCache-bewaking	Compatibiliteit met uitvoerbare bestanden	Blootstelling aan gebruikersgedrag.
Chrome-uitbreidingsbewaking	Lijsten Chrome-uitbreidingen	Blootstelling aan gebruikersgedrag.
Windows Office-MRU	Toont de meest recente gebruikte bestanden voor elke Office-toepassing	Blootstelling aan gevoelige bestandsna gebruikersgedrag