Secure Endpoint Forensic Snapshot Information

Contents

Introduction

This document describes the privileged information that a Forensic Snapshot can gather from endpoints.

Contributed by Pedro Medina, Cisco Software Engineer.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Access to Secure Endpoint with either Admin or Non-Admin user
- Access to Cisco Orbital

Note: If your user is a Non-Admin, you must request to enable the feature Forensic Snapshots for Non-Admins via the TAC support team.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Secure Endpoint Forensic Snapshot Information

Once a Forensic Snapshot has been requested, the information is shown in a table format, based on the required information the user can find any required information based on this description table:

Name	**What it means**	**Privacy concerns**
Autoexec items	Items which run at machine startup	None

Bitlocker Encryption Monitoring	Encryption status of every mounted drive	Some visibility into unencrypted versions of files
DNS Cache Table Monitoring	Recently searched domains	Recent browser history.
Hosts File Data	Items in the hosts file	None
Installed Programs on the Host	Installed applications	None
Listen Ports	Lists programs that open up network listeners	None
Loaded Modules Hashes	Hash values of running Dynamic Link Library (DLL) files	None
Loaded Modules Processes	Name, path, and PID of running processes	None
Loaded Modules vs. Processes	Mapping of Module ID from Loaded Modules to PID from Processes table	None
Logon Sessions	Logged-in users, system users are included	None
Mapped Drives	Local and remote mount points, file system type, boot partition information, and encryption information.	None
Network Connections - Processes	Maps in- and outbound network connections to specific Process IDs (PIDs), and displays the startup command line which initiated the process.	Possible exposure of network connections of certain applications, which can be private.
Network Interfaces	List of all physical and virtual network interfaces on the device	None
Network Profiles	List of networks to which the machine	Possible exposure of WIFI Service Set

Registry	has connected.	Identifier (SSIDs).
OS Version	The version of the operating system	None
Powershell History	List of all Powershell commands run on the device and stored on the system.	Potential to expose passwords, secret API keys, and other sensitive data coded into scripts.
Prefetch Directory	Memory management feature - the OS attempts to preload frequently loaded executables to save startup time.	Exposure of user habits.
Recent files data	Most recently used/accessed files	Exposure of user habits and private filenames.
Running file hashes	Name, path, command line, PID, owner of all running executables.	None
Running services monitoring	Name, service type, PID, and startup type of all running services	None
Scheduled Tasks	List of all automated tasks set to run periodically on the system	None
Shared Resources	Open shares on the system	None
Startup Items	Items which run at machine startup - different from autoexec in that these are stored in registry keys	None
System Network State Monitoring	Network statistics	None
Temp Directory File Data	Temporary files created by processes	Possible exposure of user browse history.
Trusted Root Certificates	Trusted Root Certificate Store data dump	None

UBSTOR Registry Key	History of plugged-in USB devices	Exposure of device serial numbers.
User Groups	Local groups on the machine	None
UserAsssist Monitoring	Shows recently executed files	Possible exposure of hidden behavior, such as running encryption or wiping tools.
Users	Local users on the device	None
Users - Logged-in	Local users who are currently logged into the device	None
WMI Event Filters Monitoring	Watches event log for specific items	None
Windows AV Products Monitoring	Which installed antivirus is on the system, if any	None
Windows BAM Entries Monitoring	Provides evidence of the execution of files	Could expose behaviors
Windows Environment Variables	Shows path info, system variables, and so on.	None
Windows Hotfixes	List of all installed patches	None
Windows NT Domains Search	List of domains to which the machine can authenticate	None
Windows ShellBags Monitoring	Provides information about user access to folders, preferences for that folder, and so on.	Exposure of user habits.
Windows ShimCache Monitoring	Tracks compatibility with executables	Exposure of user behaviors.

Chrome Extensions Monitoring	Lists Chrome extensions	Exposure of user behaviors.
Windows Office MRU	Lists the most recently used files for each Office application	Exposure of sensitive filenames, user behavior