Informações de instantâneo forense do Cisco Secure Endpoint

Contents

Introduction

Este documento descreve as informações privilegiadas que um Instantâneo Forense pode coletar de endpoints.

Contribuição de Pedro Medina, engenheiro de software da Cisco.

Prerequisites

A Cisco recomenda que você tenha conhecimento destes tópicos:

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

Requirements

- Acesso a "Endpoint seguro" com usuário Admin ou Não-Admin
- Acesso ao "Orbital" da Cisco

> **Note**: Se seu usuário for um Não-administrador, você deverá solicitar a ativação do recurso "Instantâneos forenses para Não-administradores" por meio da equipe de suporte do TAC.

Informações gerais

Depois que um Instantâneo Forense for solicitado, as informações serão apresentadas em um formato de tabela, com base nas informações necessárias, o usuário poderá encontrar qualquer informação necessária com base nesta tabela de descrição:

Nome	O que isso significa	Preocupações com privacidade
itens Autoexec	Itens executados na inicialização da máquina	Nenhum
Monitoramento de criptografia de bitlocker	Status de criptografia de cada unidade montada	Alguma visibilidade em versões não criptografadas de arquivos
Monitoramento de	Domínios pesquisados recentemente	Histórico recente do navegador.

Tabela de Cache DNS		
Dados do arquivo de hosts	Itens no arquivo de hosts	Nenhum
Programas instalados no host	Aplicativos instalados	Nenhum
Portas de escuta	Lista programas abrindo ouvintes de rede	Nenhum
Hashes de Módulos Carregados	Valores de hash de arquivos DLL em execução	Nenhum
Processos de módulos carregados	Nome, caminho e PID dos processos em execução	Nenhum
Módulos carregados versus processos	Mapeamento de ID de módulo de módulos carregados para PID da tabela Processos	Nenhum
Sessões de Logon	Usuários conectados, incluindo usuários do sistema	Nenhum
Unidades mapeadas	Pontos de montagem locais e remotos, tipo de sistema de arquivos, informações de partição de inicialização e informações de criptografia.	Nenhum
Conexões de Rede - Processos	Mapeia conexões de rede de entrada e saída para PIDs específicos e exibe a linha de comando de inicialização que iniciou o processo.	Possível exposição das conexões de r de certos aplicativos, que podem ser privados.
Interfaces de rede	Lista de todas as interfaces de rede físicas e virtuais no dispositivo	Nenhum
Registro de perfis de rede	Lista de redes às quais a máquina se conectou.	Possível exposição de SSIDs de Wi-Fi
Versão do SO	Versão do sistema operacional	Nenhum
Histórico do Powershell	Lista de todos os comandos do Powershell executados no dispositivo e armazenados no sistema.	Potencial para expor senhas, chaves d secretas e outros dados confidenciais codificados em scripts.
Diretório de pré-busca	Recurso de gerenciamento de memória - o SO tentará pré-carregar executáveis carregados com frequência para economizar tempo de inicialização.	Exposição dos hábitos do usuário.
Dados de arquivos recentes	Arquivos usados/acessados mais recentemente	Exposição de hábitos do usuário e nom de arquivos privados.
Executando hashes de arquivo	Nome, caminho, linha de comando, PID, proprietário de todos os executáveis em execução.	Nenhum
Executando monitoramento de serviços	Nome, tipo de serviço, PID e tipo de inicialização de todos os serviços em execução	Nenhum
Tarefas agendadas	Lista de todas as tarefas automatizadas definidas para execução periódica no sistema	Nenhum
Recursos compartilhados	Abrir compartilhamentos no sistema	Nenhum

Itens de inicialização	Itens executados na inicialização da máquina - diferentes do autoexec, pois são armazenados em chaves de registro	Nenhum
Monitoramento do estado da rede do sistema	Estatísticas de rede	Nenhum
Dados do arquivo de diretório temporário	Arquivos temporários criados por processos	Possível exposição do histórico de navegação do usuário.
Certificados raiz confiáveis	Despejo de dados do Repositório de Certificados Raiz Confiável	Nenhum
Chave do Registro UBSTOR	Histórico de dispositivos USB conectados	Exposição dos números de série dos dispositivos.
Grupos de usuários	Grupos locais na máquina	Nenhum
Monitoramento de assistênciado usuário	Mostra os arquivos executados recentemente	Possível exposição de comportamento oculto, como execução de criptografia ferramentas de limpeza.
Usuários	Usuários locais no dispositivo	Nenhum
Usuários - Conectados	Usuários locais que estão atualmente conectados ao dispositivo	Nenhum
Monitoramento de Filtros de Evento WMI	Inspeciona o log de eventos para itens específicos	Nenhum
Monitoramento de produtos Windows AV	Que antivírus instalado está no sistema, se houver	Nenhum
Monitoramento de Entradas BAM do Windows	Fornece evidência de execução de arquivos	Pode expor comportamentos
Variáveis de Ambiente do Windows	Mostra informações de caminho, variáveis de sistema etc.	Nenhum
Hotfixes do Windows	Lista de todos os patches instalados	Nenhum
Pesquisa de domínios do Windows NT	Lista de domínios nos quais a máquina pode se autenticar	Nenhum
Monitoramento de ShellBags do Windows	Fornece informações sobre o acesso do usuário a pastas, preferências para exibição dessa pasta etc.	Exposição dos hábitos do usuário.
Monitoramento do Windows ShimCache	Controla a compatibilidade com executáveis	Exposição de comportamentos do usu
Monitoramento de extensões do Chrome	Lista as extensões do Chrome	Exposição de comportamentos do usu
MRU do Windows Office	Lista os arquivos usados mais recentemente para cada aplicativo do Office	Exposição de nomes de arquivos confidenciais, comportamento do usuá