Consola de AMP para terminales y el último filtro visto

Contenido

Introducción

Este documento describe la explicación del error de filtro "Last Seen" al que se hace referencia en CSCvh31177 en protección frente a malware avanzado (AMP) para terminales.

Colaborado por Caly Hess, Ingeniero de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Acceso al panel de Cisco AMP para terminales

Componentes Utilizados

La información de este documento se basa en el software:

- Cisco AMP para terminales, consola 5.4.20190917

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Problema

El filtro "Last Seen" (Última vista) de la página de ordenadores de la consola muestra los conectores que se vieron en las últimas 24 horas y que aparecen en la lista.

Causa

La extracción actual de datos "Últimos visto" es un trabajo singular cada 24 horas. Aunque los datos que se reflejan en la página Computers (Ordenadores) y el resultado de Exportar a CSV para "Último visto" es en tiempo real, el propio filtro se ejecuta con los datos por lotes de ese trabajo único. Esto se implementó para aumentar la velocidad de los resultados, ya que el análisis en tiempo real de los sellos de tiempo para entornos empresariales de gran tamaño podría llevar a tiempos de espera y bloqueo de bases de datos.

Explicación de ordenadores "recientemente vistos" en un filtro de más de 7 días

La máquina estuvo fuera de línea durante más de 7 días hasta después de que se ejecutara el trabajo "Last Seen".

Ejemplo Real-World

- HostA.randomdomain.net sufrió un lamentable accidente con una taza de café completa y la placa madre no se recuperó completamente el 10 de agosto
- HostA.randomdomain.net está ahora sentado en el almacén de reparaciones hasta el 20 de setiembre del
- El 21 de septiembre st, HostA.randomdomain.net regresa a la red 4 horas después de que se ejecutara el trabajo "Last Seen", pero 2 horas antes de que el Auditor realice una exportación a CSV de los ordenadores que no se han visto en los últimos 30 días
- HostA.randomdomain.net aún se encuentra en la lista del trabajo "Last Seen" como no se ha visto más de 30 días. A pesar de que en la actualidad funciona plenamente y está libre de café, el auditor lo aprovecha en su exportación "inactiva"

Solución a corto plazo

El trabajo en sí no tarda 24 horas en ejecutarse, pero puede tomar al menos 12 horas. Con el fin de aumentar la precisión del filtro, se está desarrollando la reprogramación automática para el trabajo después de que el anterior finalice, que se espera corte entre 7 y 12 horas de tiempo de la ventana del lote.

Solución a largo plazo

Una reversión total del mecanismo "Última vista" que se acerca más al tiempo real cuando se extraen los datos. Esta solución requiere la implementación de una estructura de base de datos completamente nueva que se está desarrollando con la versión propuesta en el próximo año civil.