Contenido

Introducción

Este documento describe cómo determinar si los archivos que se procesan con la protección avanzada de Malware (amperio) en el dispositivo de seguridad del email de Cisco (ESA) están enviados para el análisis del archivo, y también qué los archivos del registro asociados proporcionan.

Determine si los archivos están cargados para el análisis

Cuando se habilita el análisis del archivo, los archivos se pudieron enviar automáticamente con el amperio a la nube para el análisis adicional. Esto proporciona el del más alto nivel de la protección contra el zero-day y las amenazas apuntadas. El análisis del archivo está solamente disponible cuando se habilita la filtración de la reputación del archivo.

Utilice las opciones de los tipos de archivo para limitar los tipos de archivos que se pudieron enviar a la nube. Los archivos específicos se envían que se basan siempre en las peticiones de la nube de los servicios del análisis del archivo, que apunta esos archivos para los cuales el análisis adicional sea necesario. El análisis del archivo para los tipos de archivo determinados pudo ser inhabilitado temporalmente en que el análisis del archivo mantiene la capacidad de los alcances de la nube.

> Nota: Refiera a los criterios del archivo para los servicios de protección avanzados de Malware para el documento de Cisco de los productos de seguridad del contenido de Cisco para la información adicional.

> Nota: Revise los Release Note y el guía del usuario para la revisión específica de AsyncOS que se ejecute en su dispositivo, pues los tipos de archivo del análisis del archivo variarán basado en la versión.

Tipos de archivo que pueden ser enviados para el análisis del archivo:

- Todas las versiones que soportan el análisis y Windows del archivo ejecutables, por ejemplo: archivos del **.exe**, del **.dll**, **.sys**, y **.scr**.

- Las configuraciones de los tipos de archivo que usted ha seleccionado para la carga en el anti-Malware y de la reputación paginan (para la Seguridad de la red) o página del archivo de las configuraciones de la reputación y del análisis (para la Seguridad del correo electrónico). El soporte inicial incluye el PDF y Microsoft Office los archivos.

  Nota: Si la carga en el servicio del análisis del archivo excede la capacidad, algunos archivos no pudieron ser analizados incluso si seleccionan al tipo de archivo para el análisis. Usted recibe una alerta cuando el servicio no puede temporalmente procesar los archivos de un tipo determinado.

Aquí están algunas NOTAS IMPORTANTES:

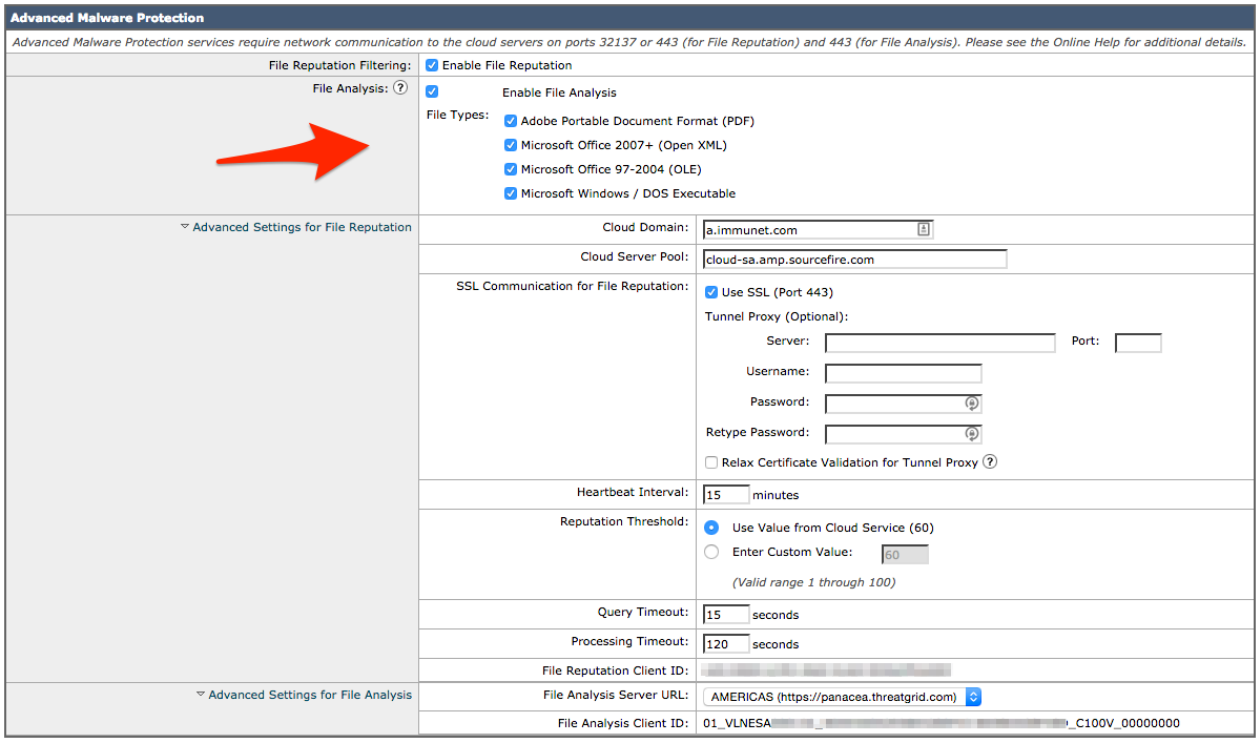
- Los criterios del tamaño del archivo son establecidos dinámicamente por el servicio del análisis del archivo basado en las tendencias actuales de la amenaza, y puede cambiar en cualquier momento. Los cambios de los criterios toman el efecto automáticamente, así que le no requieren tomar ningunas medidas.

- Si un archivo ha estado cargado recientemente de cualquier fuente, el archivo no está cargado otra vez. Para obtener los resultados del análisis del archivo para este archivo, búsqueda para el **SHA-256 de la** página de la información del análisis del archivo.

- El dispositivo intenta cargar el archivo una vez; si la carga no es acertada (por ejemplo, debido a los problemas de conectividad), el archivo no pudo ser cargado. Si el error es debido a una sobrecarga del servidor del análisis del archivo, la carga se intenta una vez más.

Configuración amperio para el análisis del archivo

Para configurar el amperio para el análisis del archivo vía el GUI, navegue a los **Servicios de seguridad > a la reputación del archivo y el análisis > edita las configuraciones globales…**:



Para configurar el amperio para el análisis del archivo vía el CLI, ingrese el **ampconfig > el comando setup** y el movimiento a través del Asisitente de la respuesta. Usted debe seleccionar **Y** cuando le presentan con esta pregunta: **¿Usted quiere modificar los tipos de archivo para el análisis del archivo?**

De acuerdo con esta configuración, analizan y se envían a los tipos de archivo se habilitan que para el análisis, como aplicable.

Registros amperio del estudio para el análisis del archivo

Cuando los archivos aplicables son analizados por el amperio, se registran en el registro amperio. Para revisar este registro para todas las acciones amperio, ingrese el comando **amperio de la cola** en el CLI, o muévase a través del Asisitente de la respuesta para la **cola** o el **comando grep**. **El comando grep** es útil si usted conoce el archivo específico u otros detalles para los cuales usted desea de buscar en el registro amperio.

Aquí tiene un ejemplo:

El archivo de **amp_watchdog.txt** se visualiza cada diez minutos en los registros. Este archivo es parte del señal de mantenimiento para el amperio.

Con los archivos procesados para la reputación, tienen el **upload_action** marcados con etiqueta en el final de la interrogación de la reputación del archivo. Hay tres respuestas para la acción de la carga:

Esta respuesta dicta si un archivo está enviado para el análisis. Una vez más debe cumplir los criterios de los tipos de archivo configurados para ser sometido con éxito.

Explicación de la acción el "0" de la carga contra la acción el "2" de la carga

Para el "0," esto significa que el archivo “no está necesitado para ser enviado para la carga”. O, una mejor manera de mirarlo es, el archivo *se puede* enviar para que la carga clasifíe el análisis *si procede*. Sin embargo, si el archivo entonces no se requiere el archivo no se envía.

Para el "2," que éste es un estricto “no envíe” el archivo para la carga. Esta acción es final y decisiva, y se hace el proceso del análisis del archivo.

“Situaciones de ejemplo”

Esta sección describe tres escenarios posibles en los cuales los archivos estén cargados para el análisis correctamente, o no es cargado debido a una razón específica.

Archivo cargado para el análisis

Este ejemplo muestra un archivo DOCX que cumpla los criterios y se marque con etiqueta con el **upload_action = 1.** En la línea siguiente, el **archivo cargado para el** Secure Hash Algorithm (SHA) del **análisis** se registra al registro amperio también.

Archivo no cargado para el análisis debido al tipo de archivo

Este ejemplo muestra a archivo zip que es analizado por el amperio y marcado con etiqueta con el **upload_action = 1** añadido al final del fichero al registro de la reputación del archivo, pero el análisis del archivo amperio no soporta los archivos ZIP. Por lo tanto, no hay un SHA registrado al registro amperio para este archivo.

Archivo no cargado para el análisis porque el archivo se sabe ya

Este ejemplo muestra un archivo PDF que es analizado por el amperio con el **upload_action = 2** añadido al final del fichero al registro de la reputación del archivo. Este archivo se sabe a la nube y no se requiere ya para ser cargado para el análisis, así que no está cargado otra vez.

Información Relacionada

- Guías del usuario de AsyncOS
- Criterios del archivo para los servicios de protección avanzados de Malware para los productos de seguridad del contenido de Cisco
- Prueba avanzada de la protección ESA Malware (amperio)
- Soporte Técnico y Documentación - Cisco Systems