¿Cómo se envía un archivo en Threat Grid desde el portal de AMP para terminales?

Contenido

Introducción

Este documento describe el proceso para enviar muestras a la nube de Threat Grid (TG) desde el portal de protección frente a malware avanzado (AMP) para terminales.

Colaborado por Yeraldin Sánchez, Ingeniero del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- AMP de Cisco para terminales
- Nube TG

Componentes Utilizados

La información de este documento se basa en la versión 5.4.20190709 de la consola de Cisco AMP para terminales.

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.

Antecedentes

Estos son los requisitos para el escenario descrito en este documento:

- Acceso al portal de Cisco AMP para terminales
- Tamaño del archivo no superior a 20 MB
- Menos de 100 envíos al día

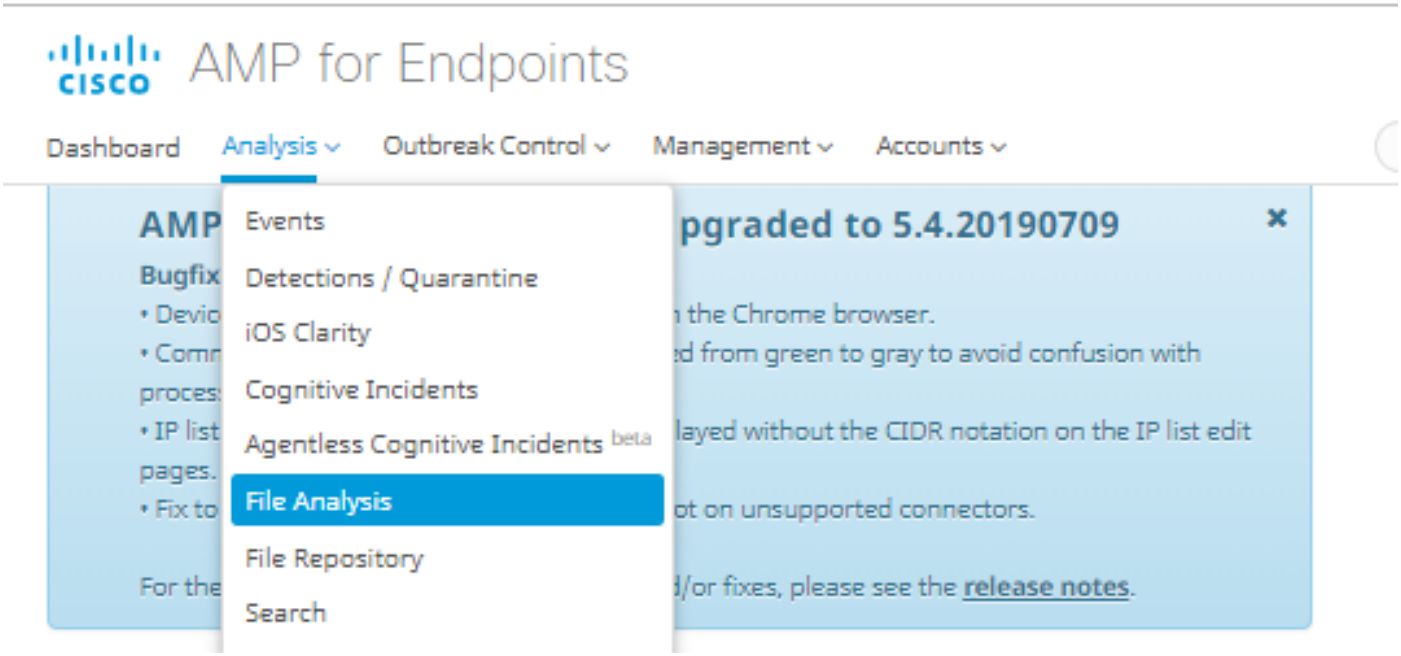
Limitaciones del análisis de archivos:

- Los nombres de archivo están limitados a 59 caracteres Unicode.
- Los archivos no pueden tener menos de 16 bytes o más de 20 MB
- Tipos de archivo admitidos: **.exe, .dll, .jar, .swf, .pdf, .rtf, .doc(x), .xls(x), .ppt(x), .zip, .vbn y .sep**

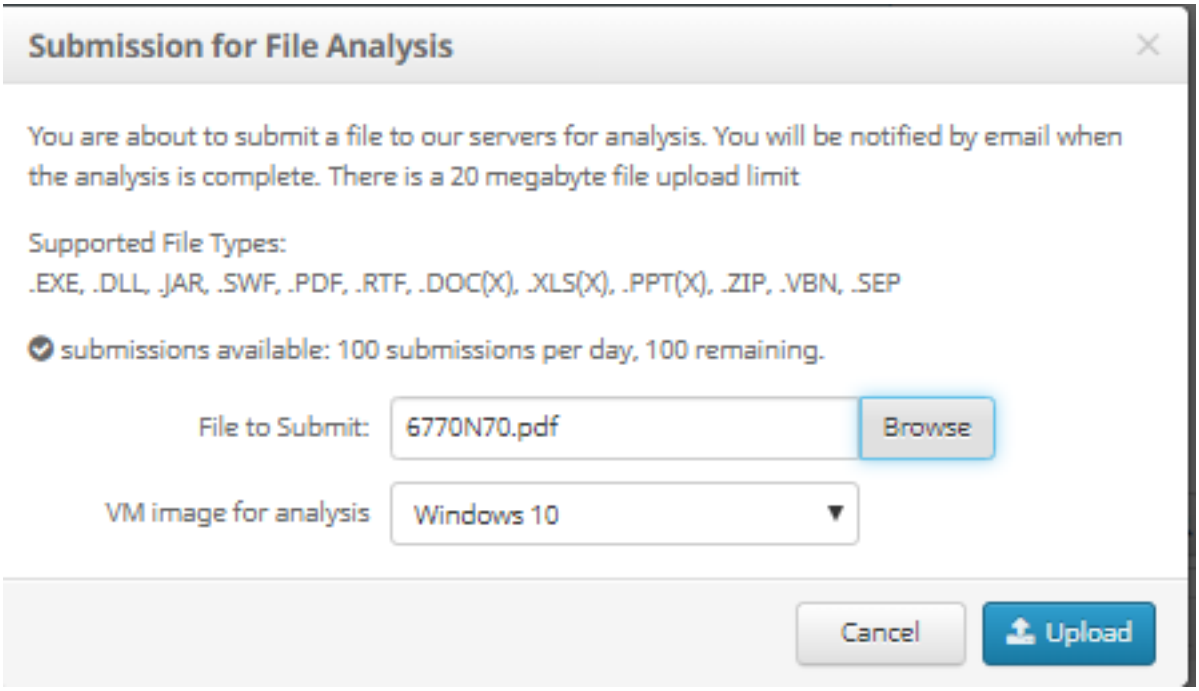
¿Cómo se envía un archivo en Threat Grid desde el portal de AMP para terminales?

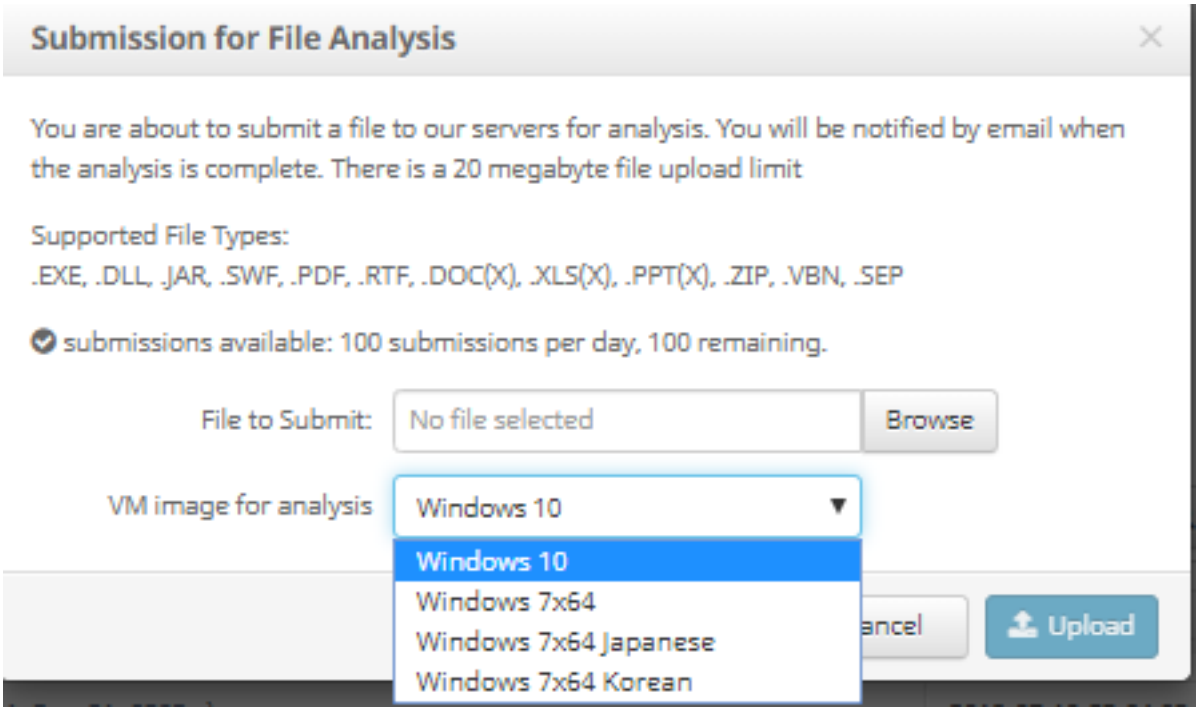
Estos son los pasos a seguir para enviar una muestra a la nube de TG desde el portal de AMP.

Paso 1. En el portal de AMP, navegue hasta **Análisis > Análisis de archivos**, como se muestra en la imagen.



Paso 2. Seleccione el archivo y la versión de imagen de Windows que desea enviar para su análisis, como se muestra en las imágenes.

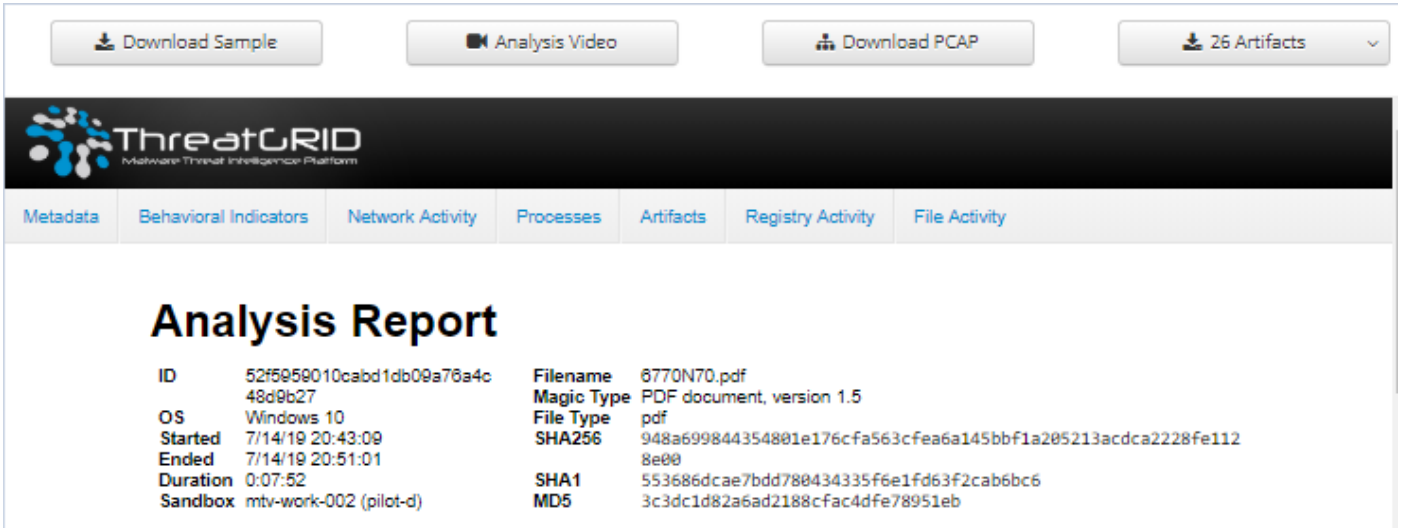




Paso 3. Una vez que se carga el ejemplo, el análisis tarda aproximadamente de 30 a 60 minutos en finalizar, depende de la carga del sistema, una vez finalizado este proceso, se envía una notificación por correo electrónico a su correo electrónico.

Paso 4. Cuando el análisis de archivos esté listo, haga clic en el botón **Report** para obtener información detallada sobre la puntuación de amenazas obtenida, como se muestra en las imágenes.

6770N70.pdf (948a6998...e1128e00)		2019-07-14 20:43:04 UTC	Report 56
Fingerprint (SHA-256)	948a6998...e1128e00		
File name	6770N70.pdf		
Threat Score	56		
Behavioral Indicators	Name	Score	
	pdf-uri-action	56	
	pdf-contains-uris	25	



Para obtener más información, puede encontrar opciones adicionales para el análisis de archivos:

Ejemplo de descarga: Esta opción permite descargar el ejemplo.

Vídeo de análisis: Esta opción le proporciona el ejemplo de vídeo obtenido en el análisis.

Descargar PCAP: Esta opción le proporciona un análisis de conectividad de red.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

> **Advertencia:** Los archivos descargados del análisis de archivos suelen ser malware activo y deben tratarse con extrema precaución.

> **Nota:** El análisis de un archivo específico se divide en varias secciones. Algunas secciones no pueden estar disponibles para todos los tipos de archivo.

Información Relacionada

- Cisco AMP para terminales: guía del usuario
- Soporte Técnico y Documentación - Cisco Systems