Como enviar um arquivo no Threat Grid a partir do portal do AMP for Endpoints?

Contents

Introduction

Este documento descreve o processo para enviar amostras para a nuvem do Threat Grid (TG) do Portal de Proteção Avançada contra Malware (AMP) para Endpoints.

Contribuído por Yeraldin Sánchez, Engenheiro do TAC da Cisco.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco AMP para endpoints
- Nuvem TG

Componentes Utilizados

As informações neste documento são baseadas no console Cisco AMP para endpoints versão 5.4.20190709.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Estes são os requisitos para o cenário descrito neste documento:

- Acesso ao portal Cisco AMP para endpoints
- Tamanho do arquivo não superior a 20 MB
- Menos de 100 envios por dia

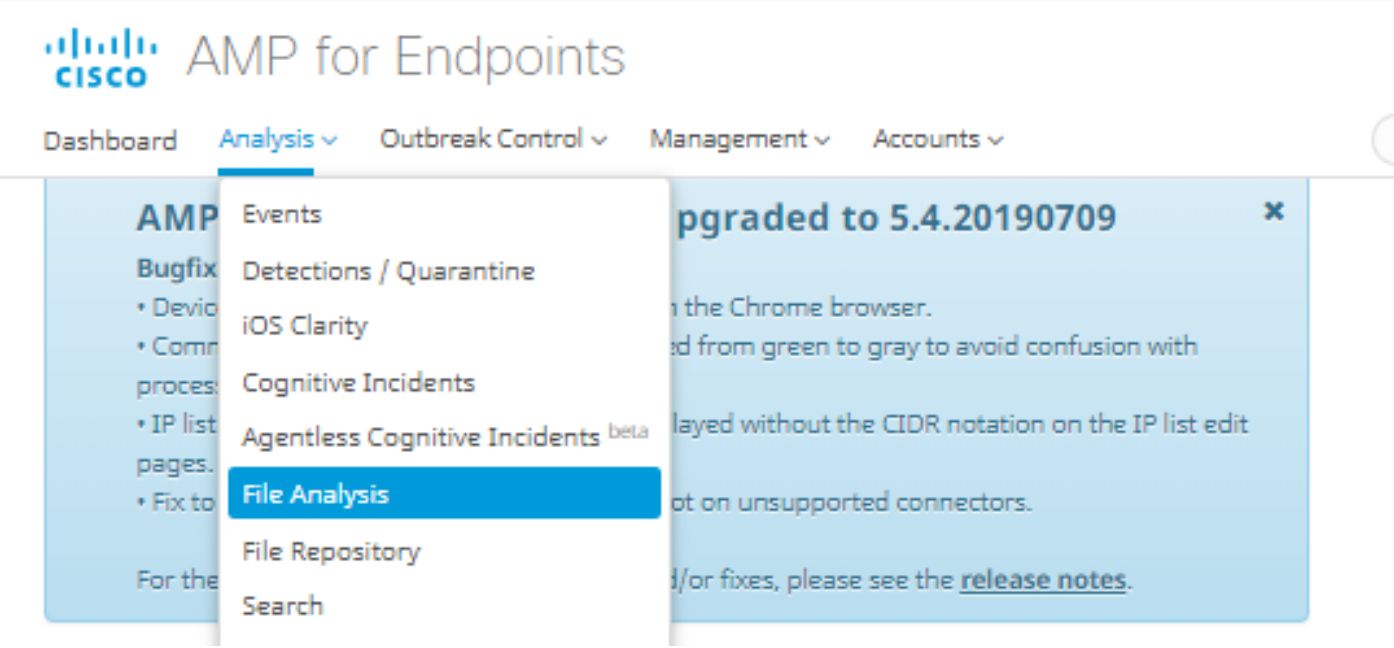
Limitações de análise de arquivo:

- Os nomes de arquivos são limitados a 59 caracteres Unicode.
- Os arquivos não podem ser menores que 16 bytes ou maiores que 20 MB
- Tipos de arquivos suportados: **.exe, .dll, .jar, .swf, .pdf, .rtf, .doc(x), .xls(x), .ppt(x), .zip, .vbn e .sep**

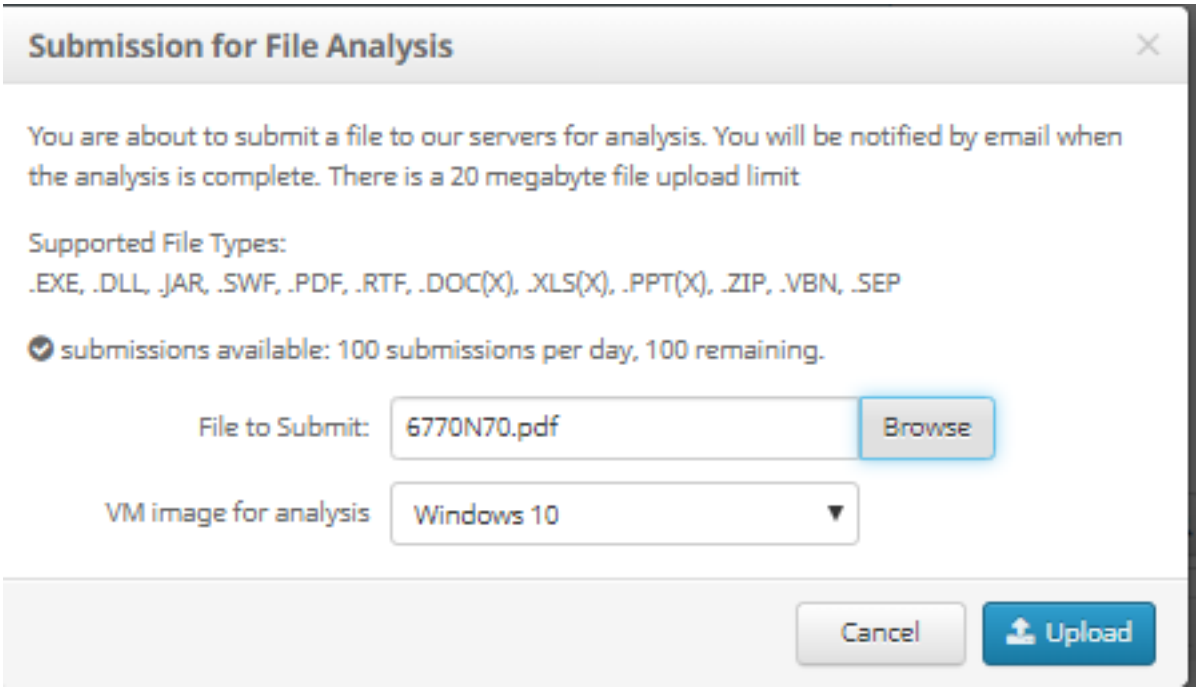
Como enviar um arquivo no Threat Grid a partir do portal do AMP for Endpoints?

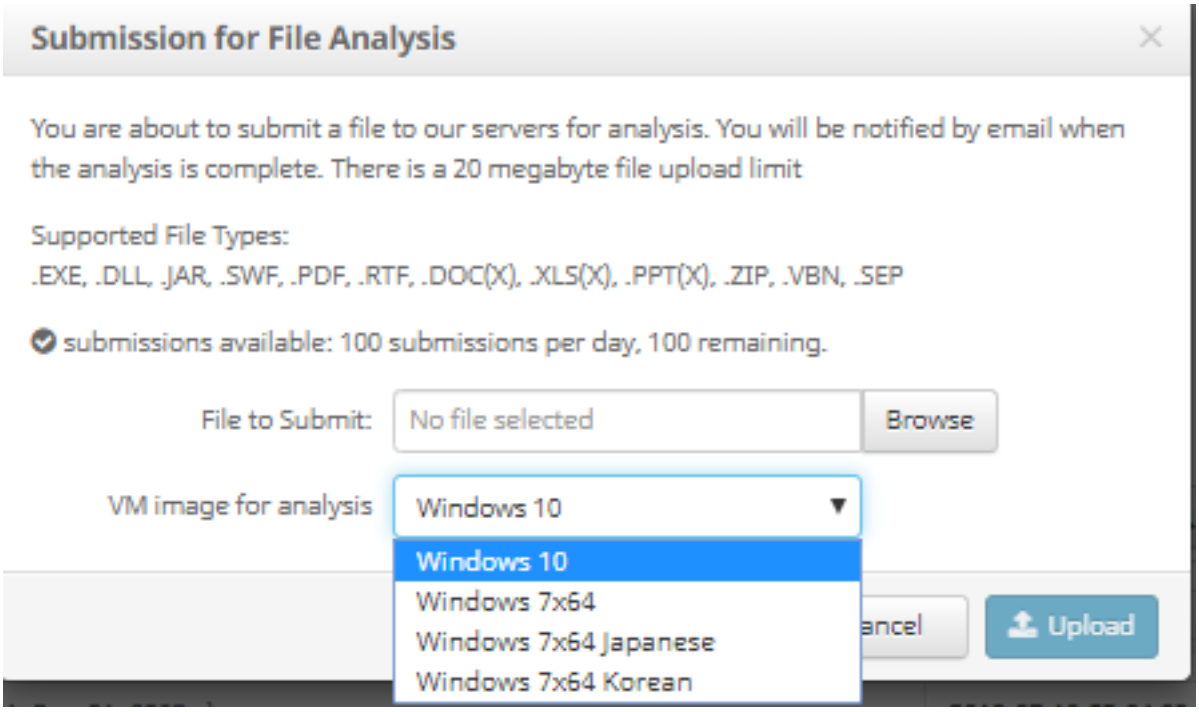
Aqui estão as etapas a seguir para enviar um exemplo para a nuvem TG do portal AMP.

Etapa 1. No portal AMP, navegue para **Analysis > File Analysis**, como mostrado na imagem.



Etapa 2. Selecione o arquivo e a versão da imagem do Windows que deseja enviar para análise, como mostrado nas imagens.

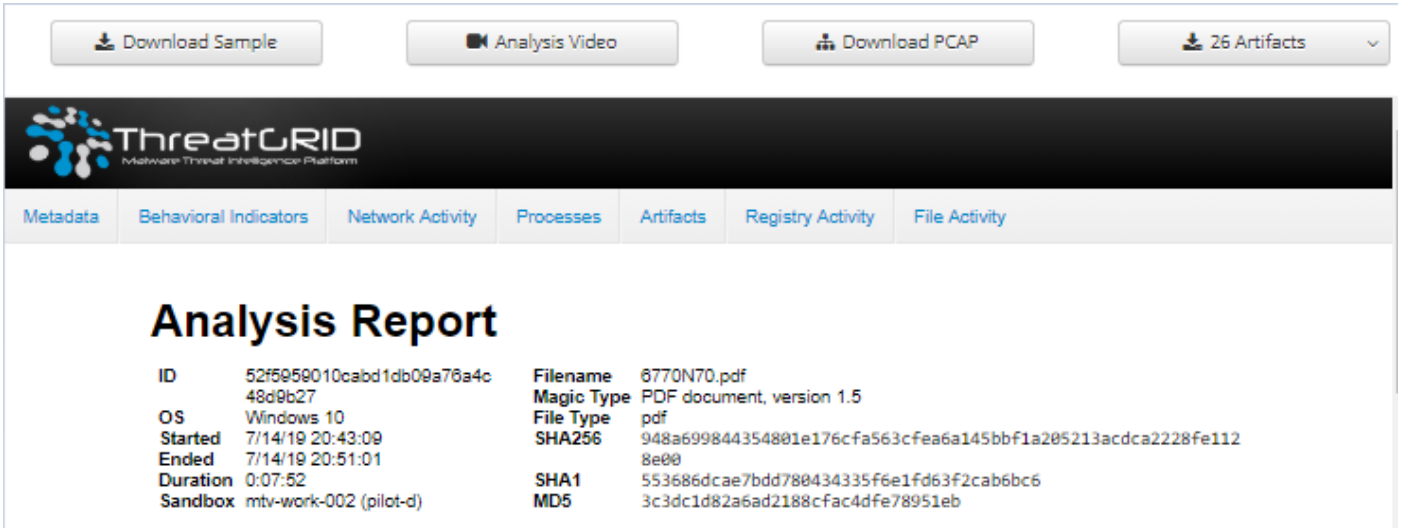




Etapa 3. Depois que a amostra é carregada, a análise leva aproximadamente de 30 a 60 minutos para ser concluída, depende da carga do sistema, depois que esse processo é concluído, uma notificação de e-mail é enviada ao seu e-mail.

Etapa 4. Quando a análise do arquivo estiver pronta, clique no botão **Report** para obter informações detalhadas sobre a pontuação da ameaça, como mostrado nas imagens.

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 obter mais informações, você pode encontrar opções adicionais para a análise do arquivo:

Exemplo de download: Esta opção permite que você faça o download do exemplo.

Vídeo de análise: Esta opção fornece o vídeo de exemplo obtido na análise.

Baixar PCAP: Essa opção fornece uma análise de conectividade de rede.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

> **aviso:** Os arquivos baixados da Análise de arquivo são geralmente malware ao vivo e devem ser tratados com extrema cautela.

> **Note**: A análise de um arquivo específico é dividida em várias seções. Algumas seções não podem estar disponíveis para todos os tipos de arquivos.

Informações Relacionadas

- Cisco AMP para endpoints - Guia do usuário
- Suporte Técnico e Documentação - Cisco Systems