

如何从面向终端的AMP门户提交Threat Grid中的文件？

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[如何从面向终端的AMP门户提交Threat Grid中的文件？](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍从面向终端的高级恶意软件防护(AMP)门户向Threat Grid(TG)云提交样本的流程。

作者：思科TAC工程师Yeraldin Sánchez。

先决条件

要求

Cisco 建议您了解以下主题：

- 面向终端的思科AMP
- TG云

使用的组件

本文档中的信息基于面向终端的思科AMP控制台版本5.4.20190709。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

本文档中描述的场景要求如下：

- 访问面向终端的思科AMP门户
- 文件大小不超过20MB
- 每天不到100次提交

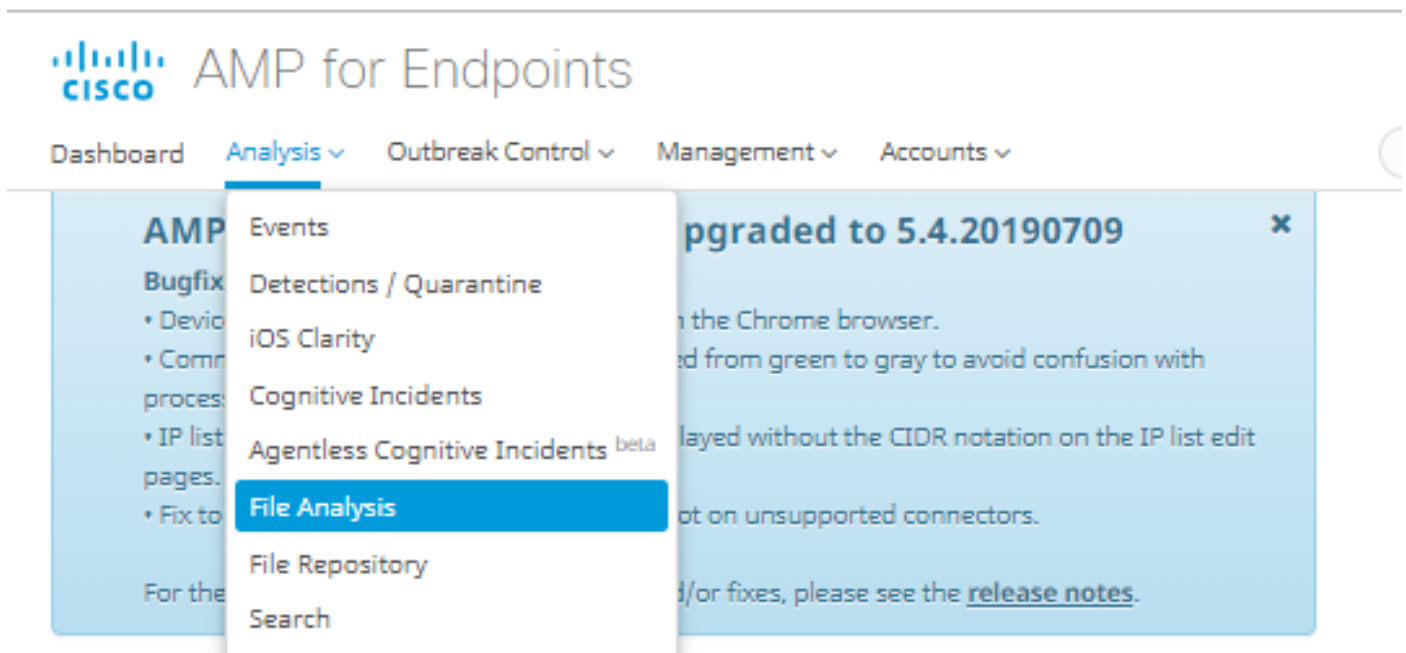
文件分析限制：

- 文件名限制为59个Unicode字符。
- 文件不得小于16字节或大于20 MB
- 支持的文件类型：.exe、.dll、.jar、.swf、.pdf、.rtf、.doc(x)、.xls(x)、.ppt(x)、.zip、.vbn和 .sep

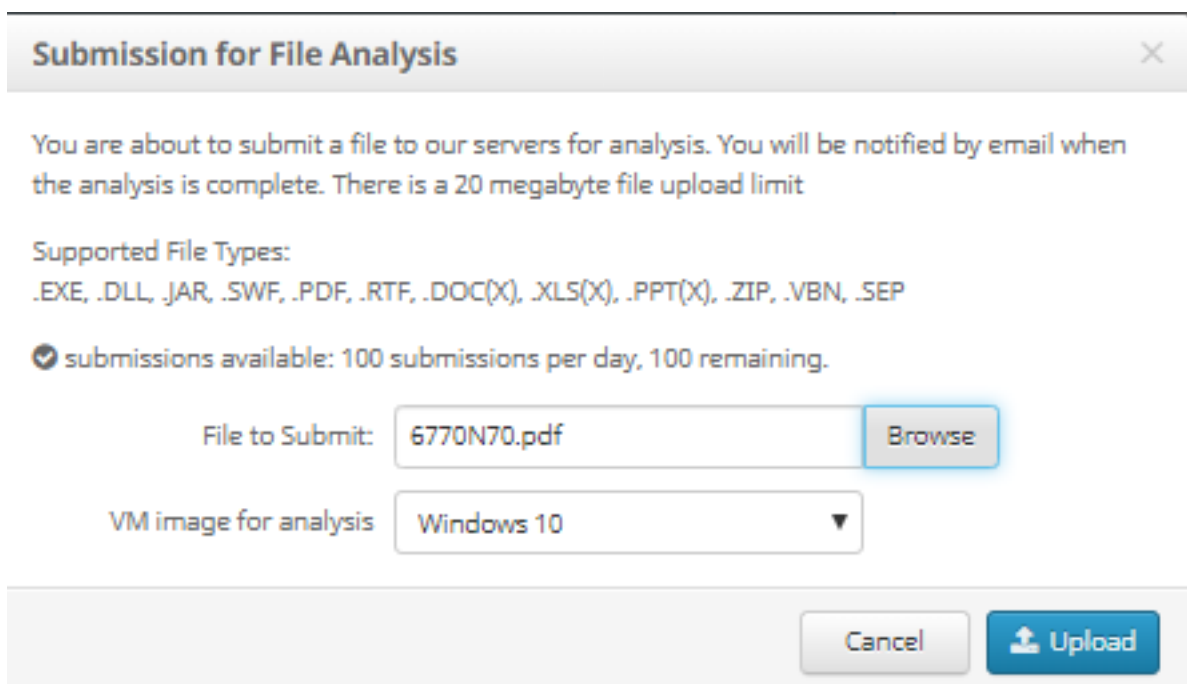
如何从面向终端的AMP门户提交Threat Grid中的文件？

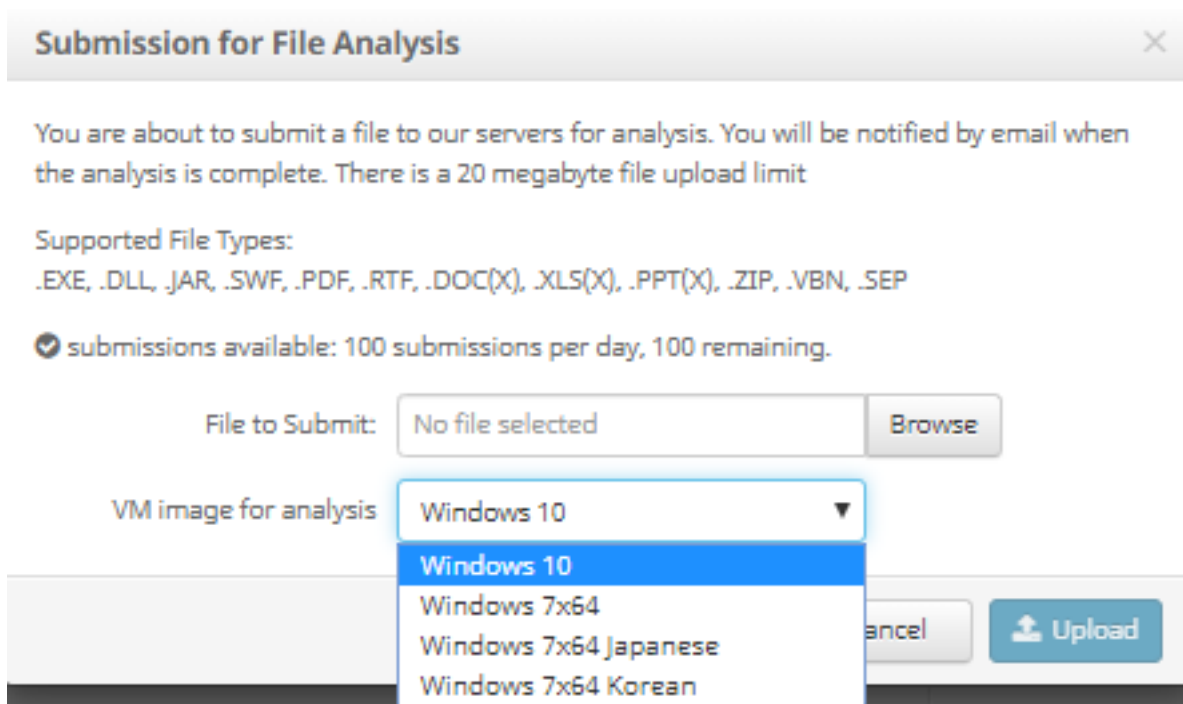
以下是从AMP门户向TG云提交示例的步骤。

步骤1.在AMP门户上，导航至**Analysis > File Analysis**，如图所示。



步骤2.选择要发送以供分析的文件和Windows映像版本，如图所示。





步骤3.上传样本后，分析大约需要30到60分钟才能完成，具体取决于系统负载，此过程完成后，系统会向您的电子邮件发送电子邮件通知。

步骤4.文件分析准备就绪后，单击**Report**按钮，获取有关威胁评分的详细信息，如图所示。

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	

Download Sample
Analysis Video
Download PCAP
26 Artifacts

ThreatGRID
Malware Threat Intelligence Platform

Metadata
Behavioral Indicators
Network Activity
Processes
Artifacts
Registry Activity
File Activity

Analysis Report

ID	52f5959010cabd1db09a76a4c48d9b27	Filename	6770N70.pdf
OS	Windows 10	Magic Type	PDF document, version 1.5
Started	7/14/19 20:43:09	File Type	pdf
Ended	7/14/19 20:51:01	SHA256	948a699844354801e176cfa563cfea6a145bbf1a205213acdca2228fe1128e00
Duration	0:07:52	SHA1	553686dcae7bdd780434335f6e1fd63f2cab6bc6
Sandbox	mtv-work-002 (pilot-d)	MD5	3c3dc1d82a6ad2188cfac4dfe78951eb

要了解更多信息，可以找到文件分析的其他选项：

下载示例：此选项允许您下载示例。

分析视频：此选项提供分析中获得的示例视频。

下载PCAP:此选项提供网络连接分析。

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。

警告：从文件分析下载的文件通常是活生生的恶意软件，必须极其谨慎地处理。

注意：对特定文件的分析分为几个部分。某些部分不能用于所有文件类型。

相关信息

- [面向终端的思科AMP — 用户指南](#)
- [技术支持和文档 - Cisco Systems](#)