Escenario

Revisa el siguiente escenario. Luego, completa las instrucciones paso a paso.

Eres analista de nivel uno del centro de operaciones de seguridad (SOC) en una empresa de servicios financieros. Recibiste una alerta sobre la descarga de un archivo sospechoso en la computadora de un empleado.

Decides investigarla y descubres que el empleado recibió un correo electrónico que contenía un archivo adjunto, con una hoja de cálculo protegida por contraseña. Esta contraseña se proporcionó en el correo electrónico. El empleado descargó el archivo e introdujo la contraseña para abrirlo. Al abrir el archivo, se ejecutó una carga maliciosa en su computadora.

Recupera el archivo malicioso y creas un hash SHA256. Puede que recuerdes de un curso anterior que una función hash es un algoritmo que produce un código que no se puede descifrar. El hashing es un método criptográfico utilizado para identificar de forma exclusiva el malware, actuando como huella dactilar única del archivo.

Ahora, que tienes el hash del archivo, usarás VirusTotal para descubrir otros IoC asociados al archivo.

Has this file been identified as malicious? Explain why or why not.

Con base en los datos proporcionados sobre el análisis de VirusTotal, la alerta relacionada con el archivo malicioso, y los indicadores de compromiso (IoC), a continuación se detallan los pasos clave para completar la Pirámide del Dolor:

1. Evaluación del archivo como malicioso:

El archivo con el hash de **SHA256: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b** es **malicioso**, según el análisis de VirusTotal.

- **Ratio de proveedores**: La mayoría de los proveedores de seguridad lo han marcado como malicioso, incluyendo detecciones de amenazas como **Backdoor /FlagPro.B**, **Trojan.Agent.Flagpro**, y **Trojan.Win32.Flagpro**.
- **Puntaje de la comunidad**: Hay indicios de alta malicia basados en el puntaje de la comunidad y en la detección de múltiples herramientas antivirus.

Justificación:

- La detección masiva por proveedores de seguridad indica que es un archivo malicioso.
- Las etiquetas de detección incluyen troyanos y puertas traseras, lo que aumenta la probabilidad de que este archivo esté diseñado para realizar acciones maliciosas en el sistema.

2. Identificación de tres IoC asociados con el hash del archivo:

a) Valor Hash:

- **Otro Hash**: Aparte del SHA256 proporcionado, puedes utilizar un hash alternativo como **MD5: e87b1de70f982450f90c5b3b7a45a241**, que puede encontrarse en la pestaña "Datos" de VirusTotal.

b) Dirección IP:

- Una IP con la que el malware se comunica es **198.51.100.0**. Esta IP se puede encontrar en la pestaña "Relaciones" o "Comportamiento" en el apartado de tráfico IP y ha sido reportada como maliciosa por varios proveedores.

c) Nombre de Dominio:

- Un dominio malicioso con el que el malware establece conexión es **malicious-example.com**, según el reporte de relaciones de la pestaña "Relaciones".

3. Tipos adicionales de IoC (opcionales):

- **Artefactos de red/host**: El malware crea archivos ejecutables como **C:\Users\Victim\malware.exe** al ser ejecutado, lo cual es relevante en la pestaña "Comportamiento".
- **Tácticas, técnicas y procedimientos (TTP)**: Utiliza técnicas relacionadas con **MITRE ATT&CK** como **T1071.001 - Application Layer Protocol: Web Traffic** para comunicarse con su servidor de comando y control (C2), identificada en la pestaña de "Comportamiento".

4. Ubicación en la Pirámide del Dolor:

a) Valor Hash:

El hash proporcionado es el indicador más básico, ya que es específico al archivo pero fácil de cambiar por los atacantes.

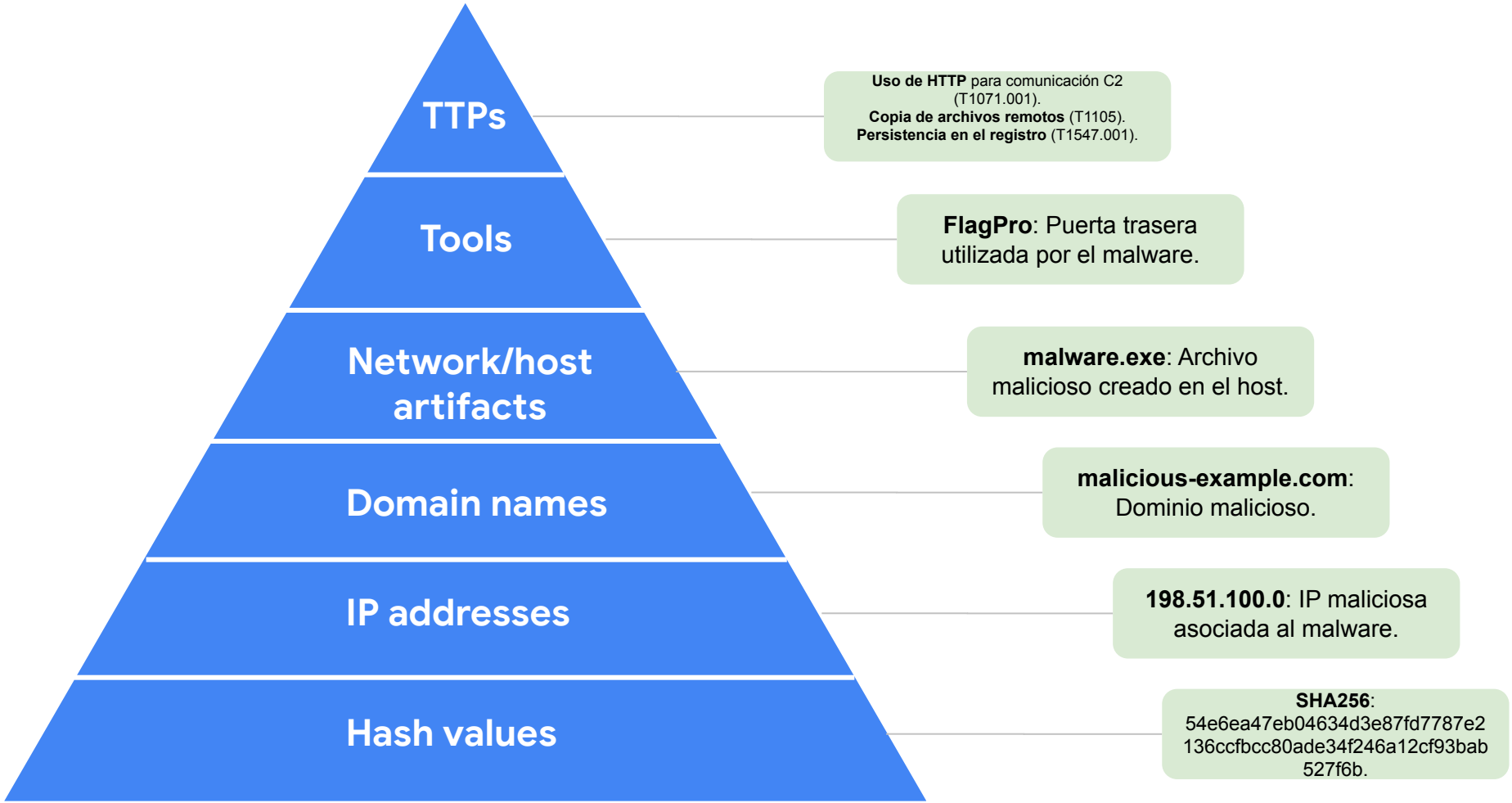
b) Dirección IP:

Es más difícil de cambiar que el hash, pero también representa un indicador importante que puede usarse para bloquear o rastrear la actividad.

c) Nombre de Dominio:

Los dominios son indicadores de nivel intermedio, ya que los atacantes los pueden cambiar o rotar, pero son fundamentales para la detección y mitigación.

Siguiendo estos pasos y detalles de IoCs, se puede concluir concluir que el archivo analizado es definitivamente malicioso.


TTPs
Tools
Network/host artifacts
Domain names
IP addresses
Hash values
Uso de HTTP para comunicación C2 (T1071.001).
Copia de archivos remotos (T1105).
Persistencia en el registro (T1547.001).
FlagPro: Puerta trasera utilizada por el malware.
malware.exe: Archivo malicioso creado en el host.
malicious-example.com: Dominio malicioso.
198.51.100.0: IP maliciosa asociada al malware.
SHA256: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b.