¿Se ha identificado este archivo como malicioso? Explica por qué sí o por qué no.

Eventos del incidente:

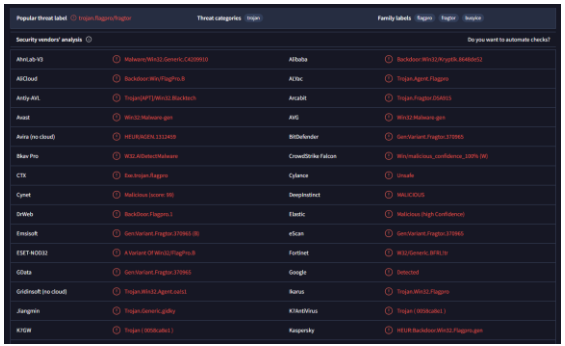
1:11 p.m.: Un empleado recibe un correo electrónico que contiene un archivo adjunto.

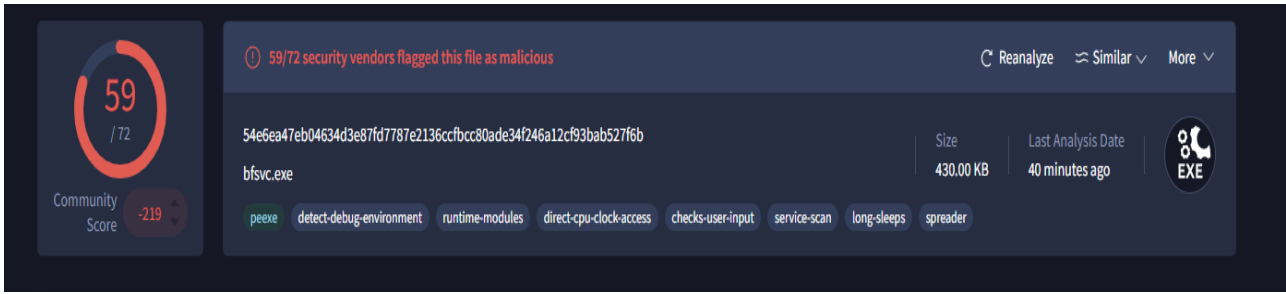
•**1:13 p.m.:** El empleado descarga y abre el archivo.

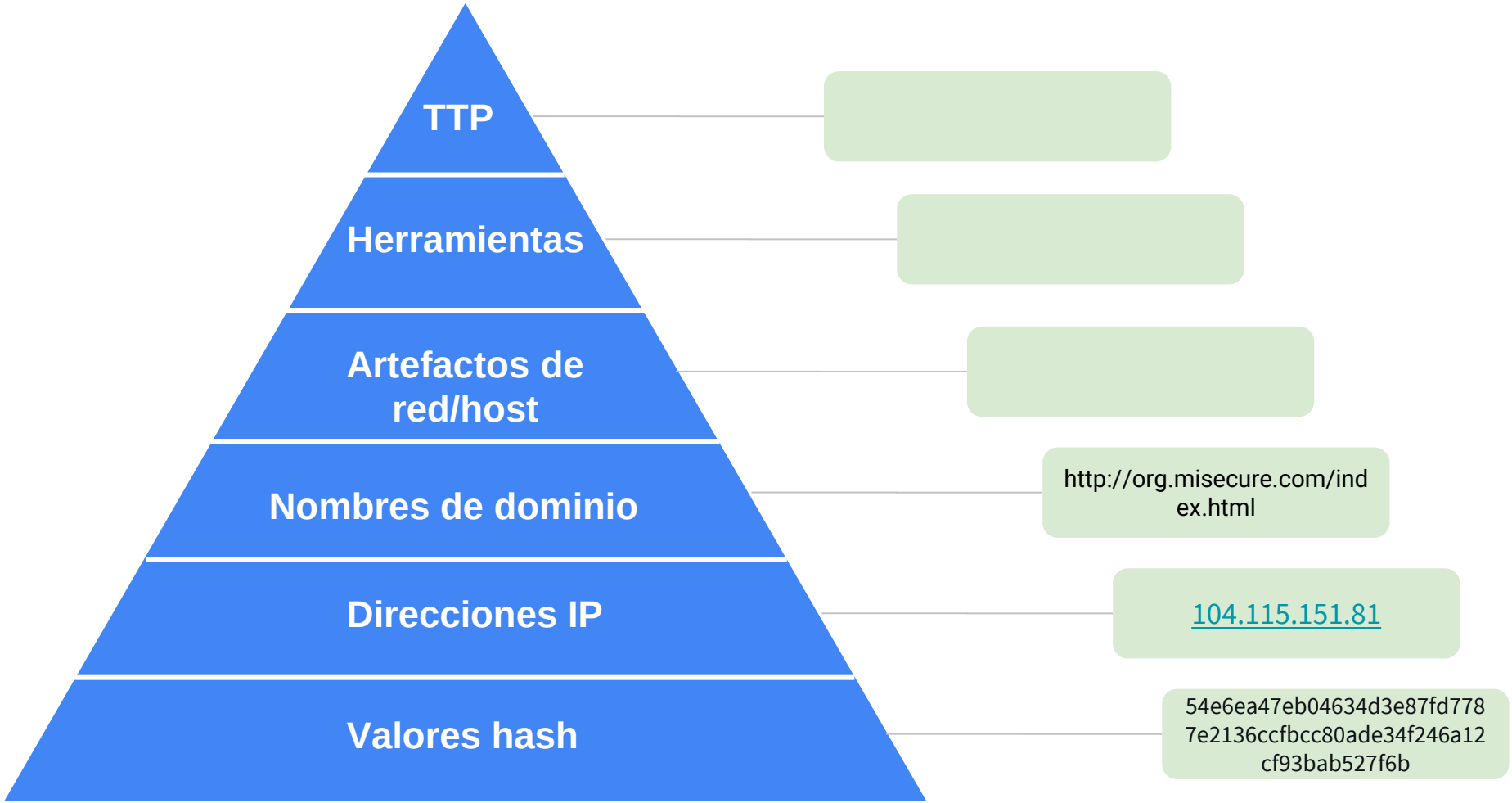
•**1:15 p.m.:** Se crean varios archivos ejecutables no autorizados en la computadora del empleado.

•**1:20 p.m.:** Un sistema de detección de intrusos detecta los archivos ejecutables y envía una alerta al SOC.

Debido e esto se encontró el hash del ejecutable y una vez analizado en virus total nos dio lo sig:






TTP
Herramientas
Artefactos de red/host
Nombres de dominio
Direcciones IP
Valores hash
http://org.misecure.com/index.html
104.115.151.81
54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b