

¿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.

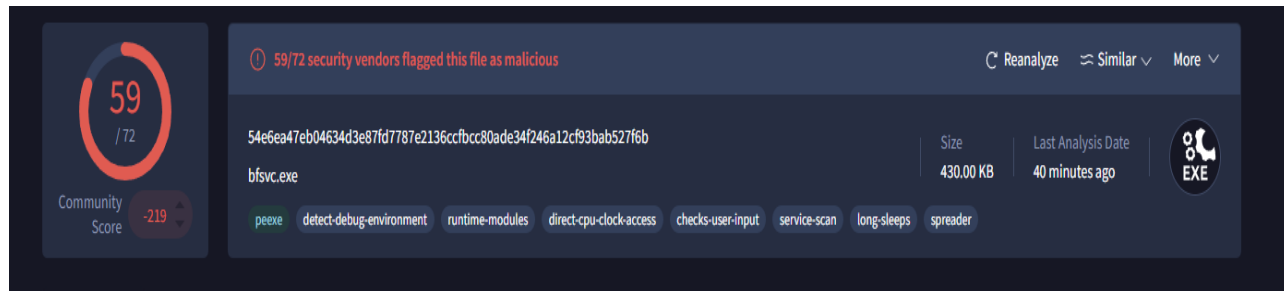
•**1:13 p.m.:** El empleado descarga y abre el archivo.

•**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:

Popular threat label	Threat categories	Family labels	Signatures	Feeds	Source
Security researcher analysis					
Do you want to automate checks?					
Win32.ps-3	Malware:Win32/Generic.CRM0000	Abtulus	Backdoor-Win32/Agent, Malware-3		
ARCCloud	Malware:Win32/Agent.6	Abtuls	Traps.Agent/Traps		
Avast.Ant	Traps:W32/Black.Blood	Avast	Traps.Agent.256001		
Avast	Win32-Malware-gen	Avs	W32/Malware-gen		
Avira (free cloud)	HEUR:KDR/133398	BitDefender	Gen.Variant/Traps.171985		
Avira Pro	W32-KDR/malware	Cybereason/Falcon	Win32/malware_confidence_100%_0%		
CTB	Win32:Traps	Cybereason	Traps		
Cyren	Malware:Generic.98	Dynatrace	WML/C005		
DrWeb	Backdoor/Traps	Elastic	Malware-PHP-Confidence		
Emnarak	Gen.Variant/Traps.171985.86	Exotic	Gen.Variant/Traps.171985		
ESRT-NOISE	A Variant Of Win32/Traps-3	Foxitsoft	W32/Generic.BK-36		
GData	Gen.Variant/Traps.171985	Google	Traps		
GridinSoft (free cloud)	Traps:Win32.Agent.1000	Norma	Traps-Win32/Traps		
Kingpin	Traps-Generic.gen	KillnetWin	Traps.1700000001.1		
KISW	Traps.1700000001.2	Kaspersky	W32/Traps-Win32/Traps-gen		



TTP

Herramientas

**Artefactos de
red/host**

Nombres de dominio

Direcciones IP

Valores hash

<http://org.misecure.com/index.html>

104.115.151.81

54e6ea47eb04634d3e87fd778
7e2136ccfbcc80ade34f246a12
cf93bab527f6b