De Mecánica a Software

Una breve investigación sobre malware y un canal de YouTube comprometido.

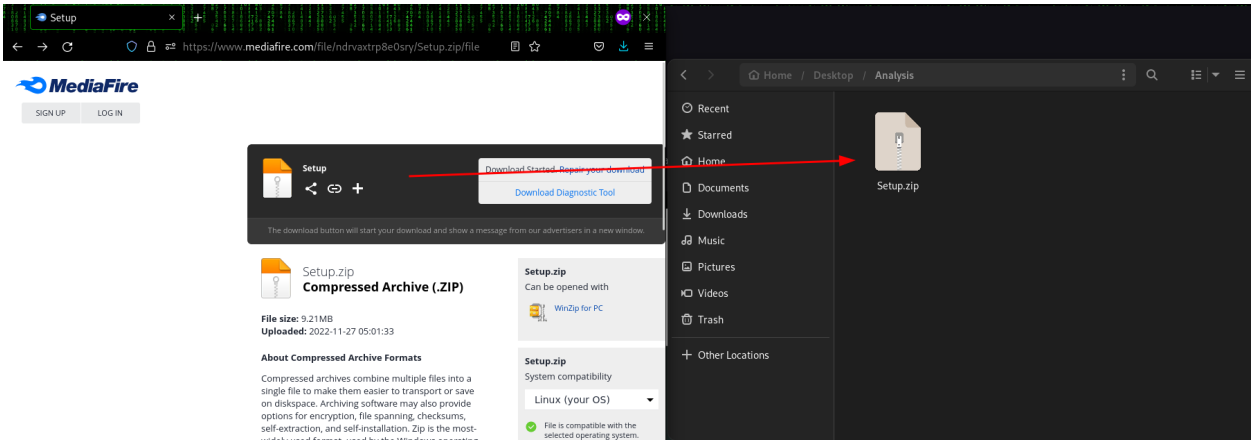
Es un extracto de la publicación del blog, pero en formato PDF y solo se centra en el análisis de la muestra.

Contenido

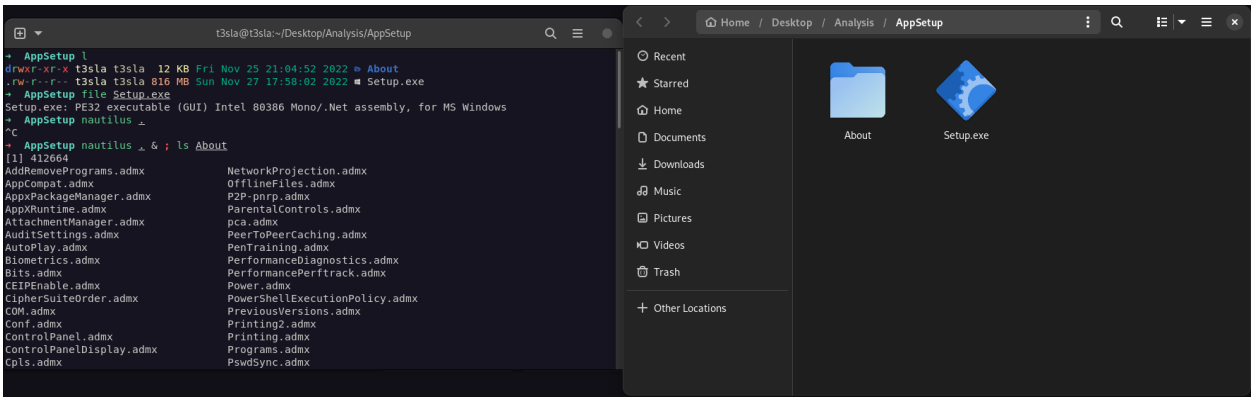
1. Herramientas;

1. Virus Total (VT).
2. Intezer Analyze.
3. VirtualBox.
4. Windows 10.
5. PEView.
6. HxD.
7. File.

2. Descarga de la muestra y comparación;



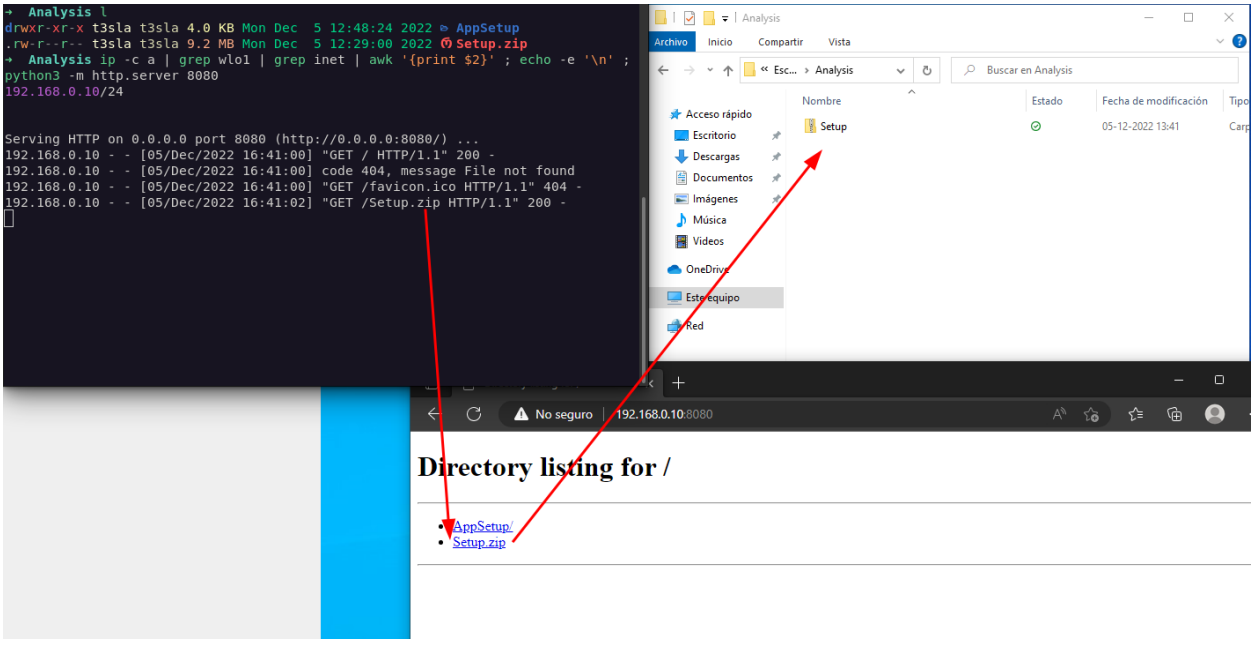
```
→  Analysis l
.rw-r--r-- t3sla t3sla 9.2 MB Mon Dec  5 12:29:00 2022  Setup.zip
→  Analysis file Setup.zip
Setup.zip: Zip archive data, at least v1.0 to extract, compression method=store
→  Analysis unzip Setup.zip
Archive:  Setup.zip
   creating: AppSetup/
   creating: AppSetup/About/
[Setup.zip] AppSetup/About/AddRemovePrograms.admx password:
  inflating: AppSetup/About/AddRemovePrograms.admx
  inflating: AppSetup/About/AppCompat.admx
  inflating: AppSetup/About/AppxPackageManager.admx
  inflating: AppSetup/About/AppXRuntime.admx
  inflating: AppSetup/About/AttachmentManager.admx
  inflating: AppSetup/About/AuditSettings.admx
  inflating: AppSetup/About/AutoPlay.admx
  inflating: AppSetup/About/Biometrics.admx
  inflating: AppSetup/About/Bits.admx
  inflating: AppSetup/About/CEIPEnable.admx
  inflating: AppSetup/About/CipherSuiteOrder.admx
  inflating: AppSetup/About/COM.admx
  inflating: AppSetup/About/Conf.admx
  inflating: AppSetup/About/ControlPanel.admx
  inflating: AppSetup/About/ControlPanelDisplay.admx
  inflating: AppSetup/About/Cpls.admx
```



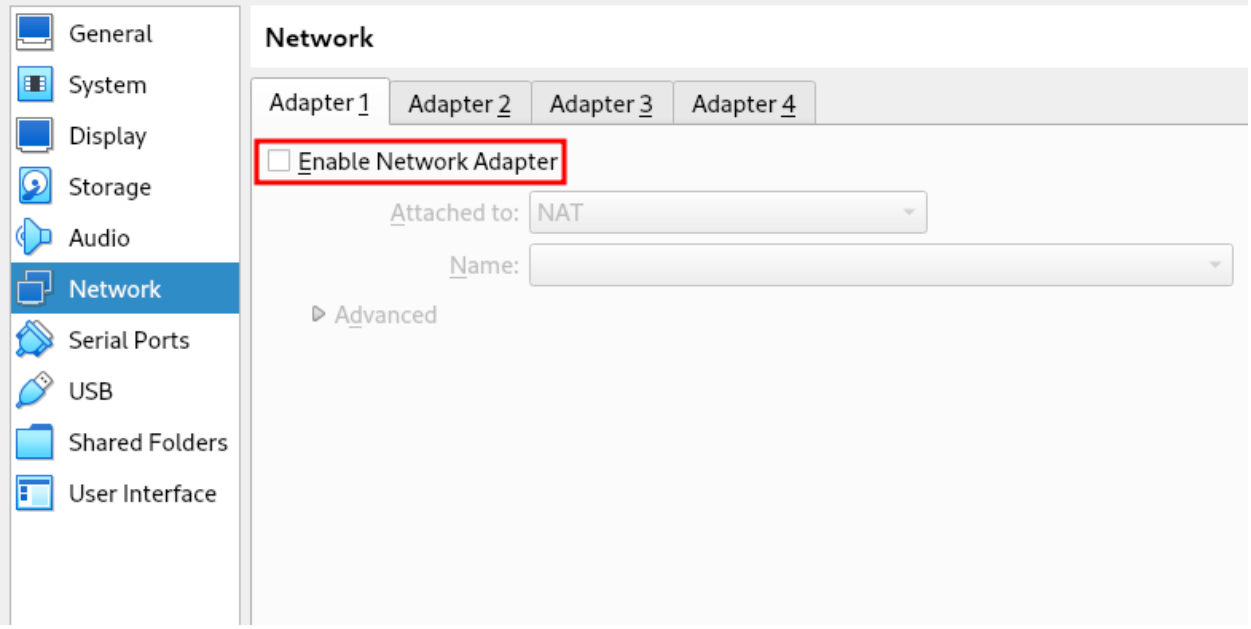
La primera alerta que obtenemos es el tamaño del binario, si comparamos con el instalador legítimo no concuerdan.

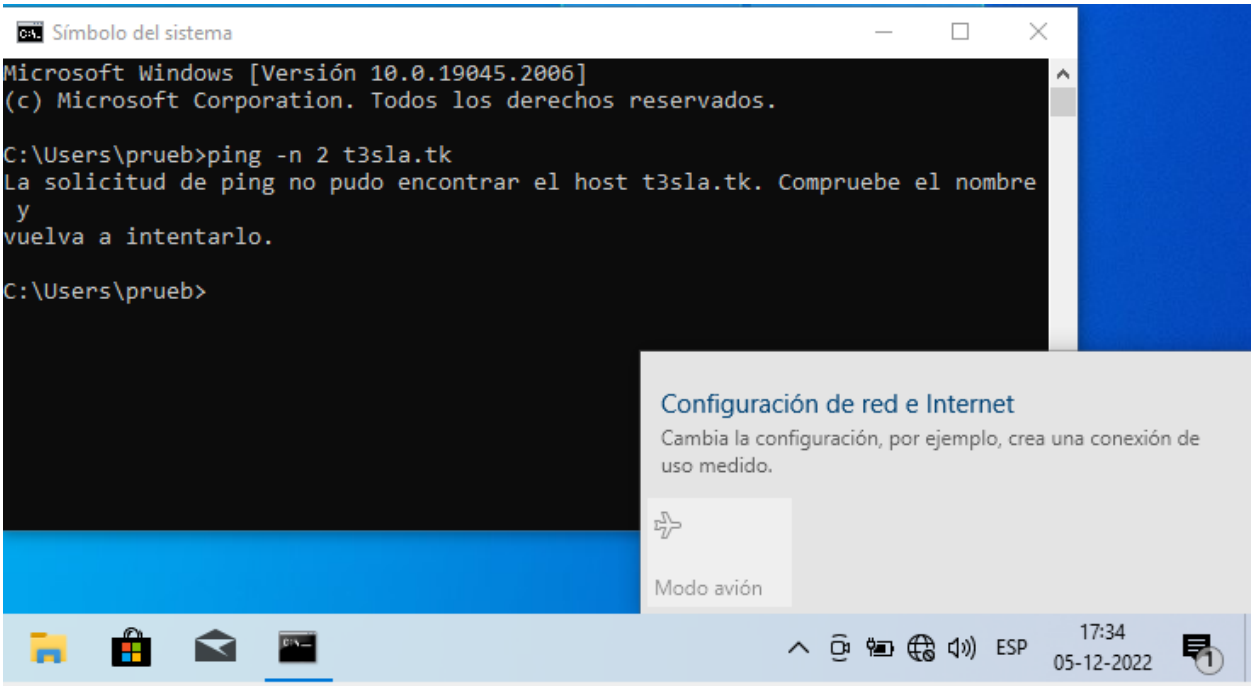
3. Configuración de la VM;

Por precaución y mini laboratorio de análisis utilizaré una máquina virtual empleando el sistema operativo Windows 10 Home (x64).



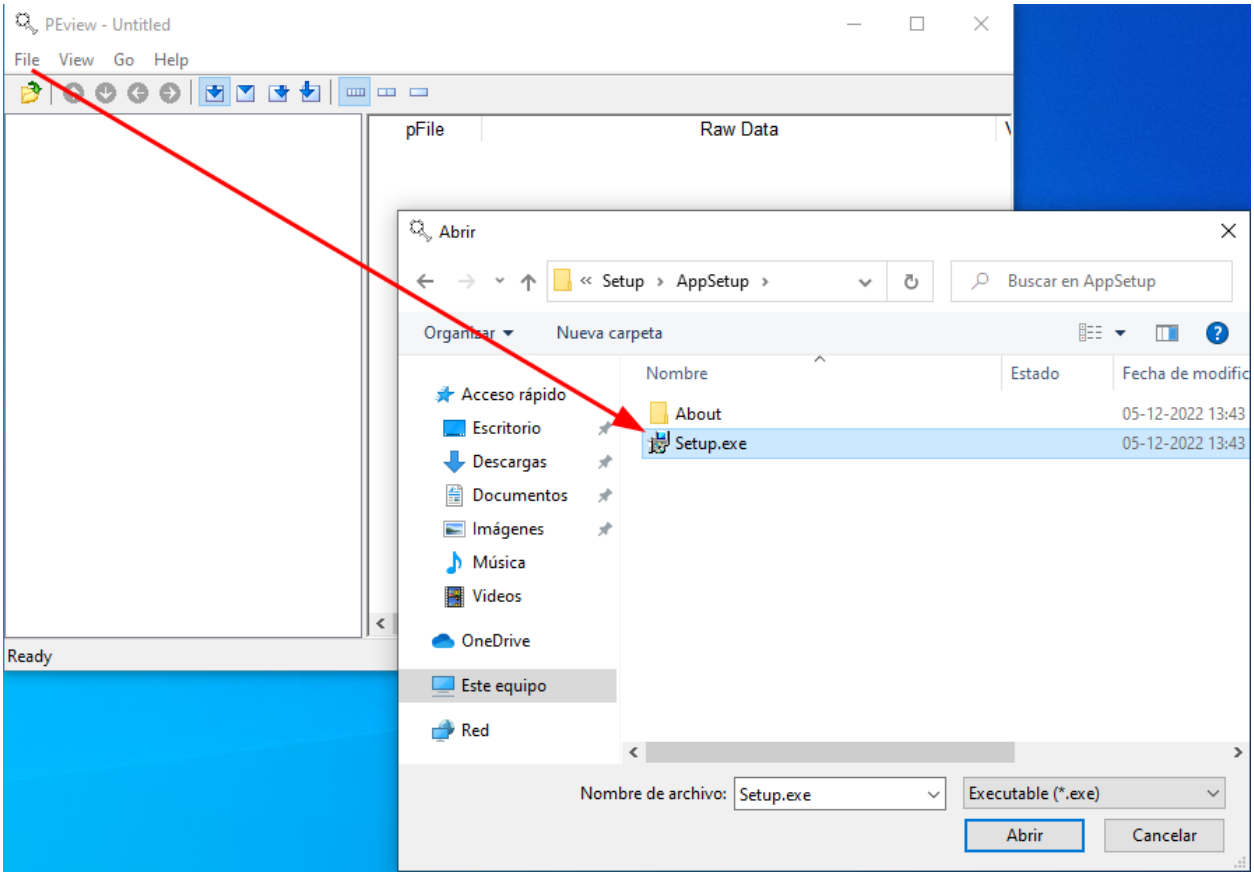
Como medida extra, ante cualquier error que puede provenir de mi persona, también se desactivará el adaptador de red para evitar la comunicación de la máquina a internet y mi red.

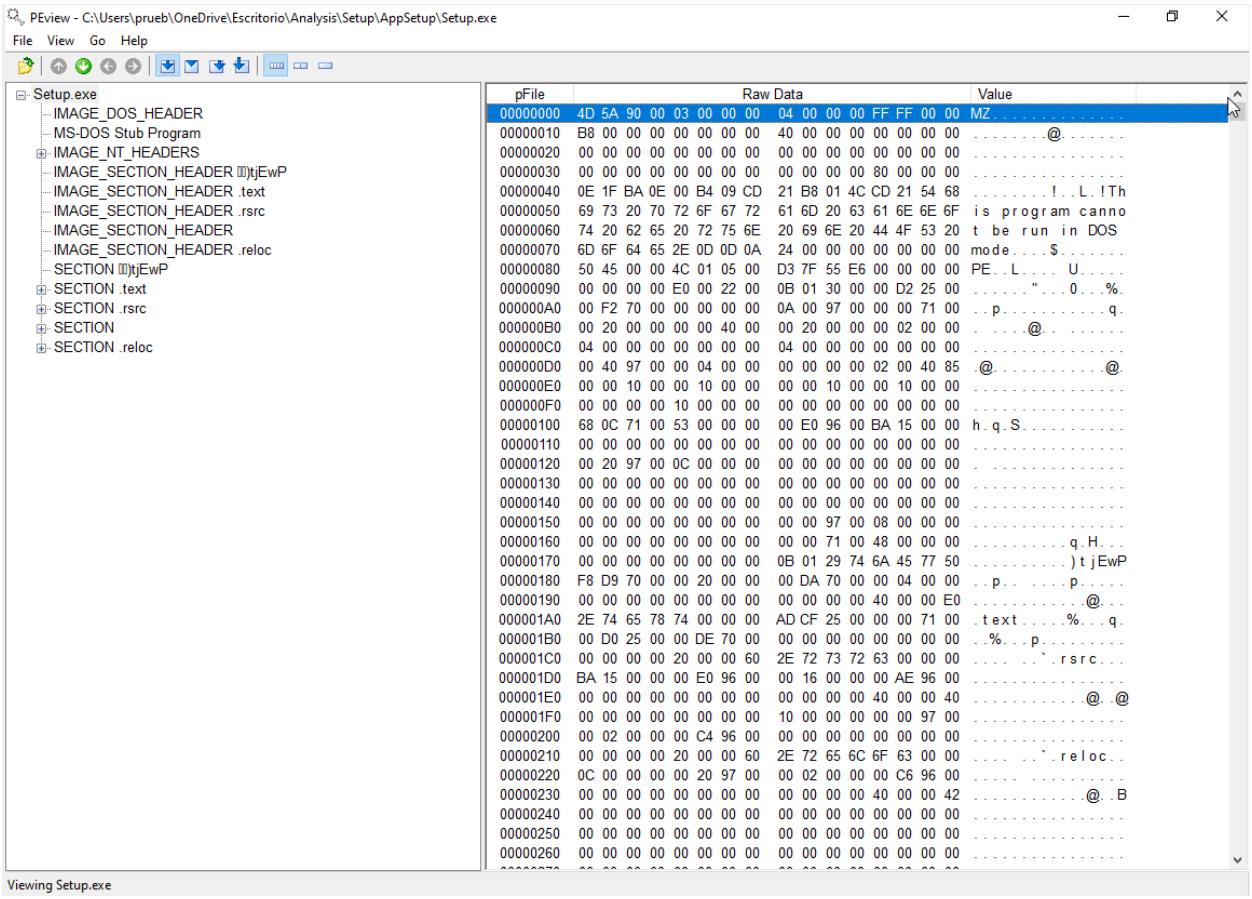




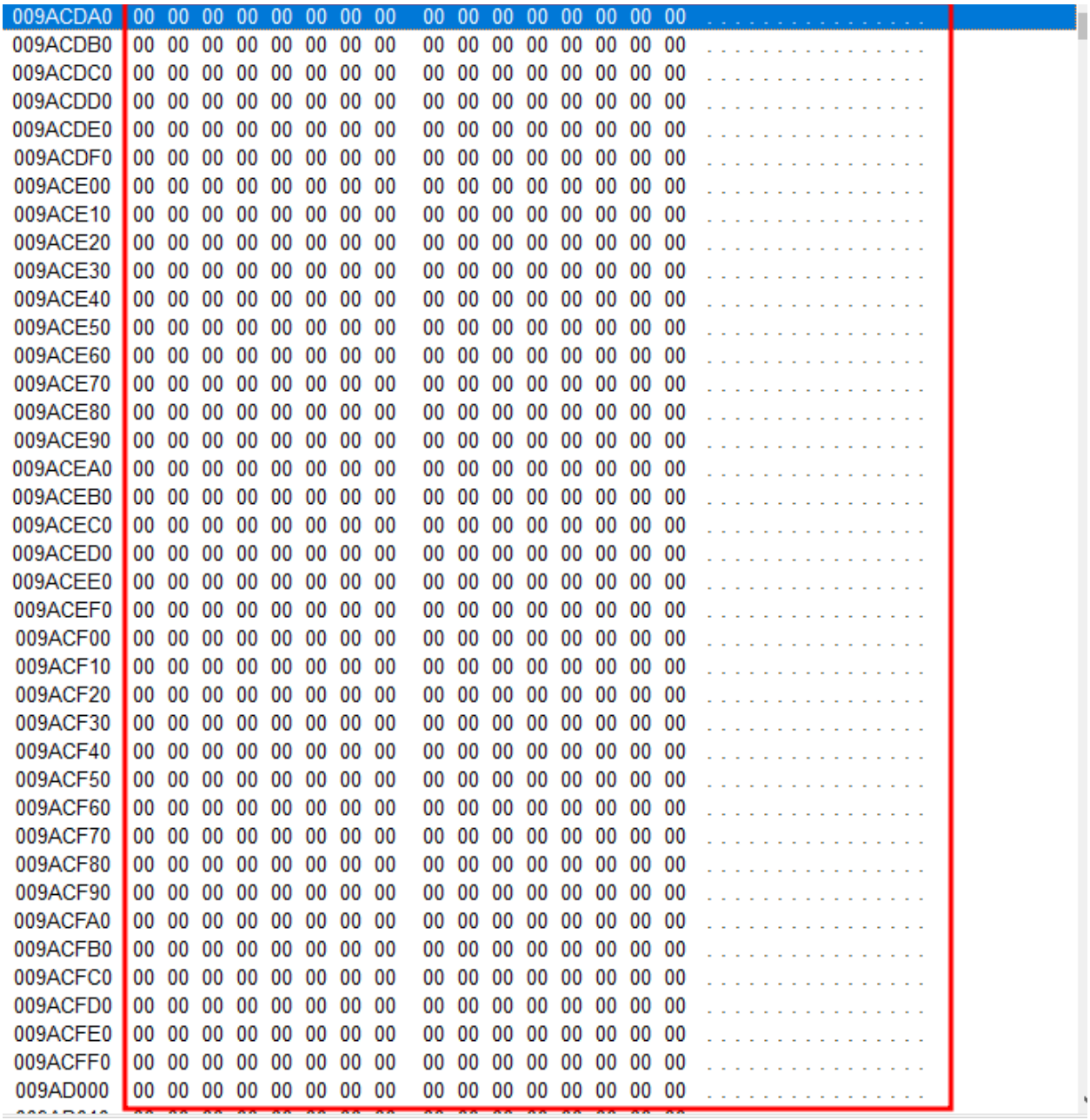
4. Análisis del PE.

Empleando PEView para obtener la estructura del Portable Executable.


PEview - Untitled
File View Go Help
pFile
Raw Data
Ready
Abrir
Setup › AppSetup ›
Buscar en AppSetup
Organizar
Nueva carpeta
Nombre
Estado
Fecha de modific
Acceso rápido
Escritorio
Descargas
Documentos
Imágenes
Música
Videos
OneDrive
Este equipo
Red
About
05-12-2022 13:43
Setup.exe
05-12-2022 13:43
Nombre de archivo: Setup.exe
Executable (*.exe)
Abrir
Cancelar

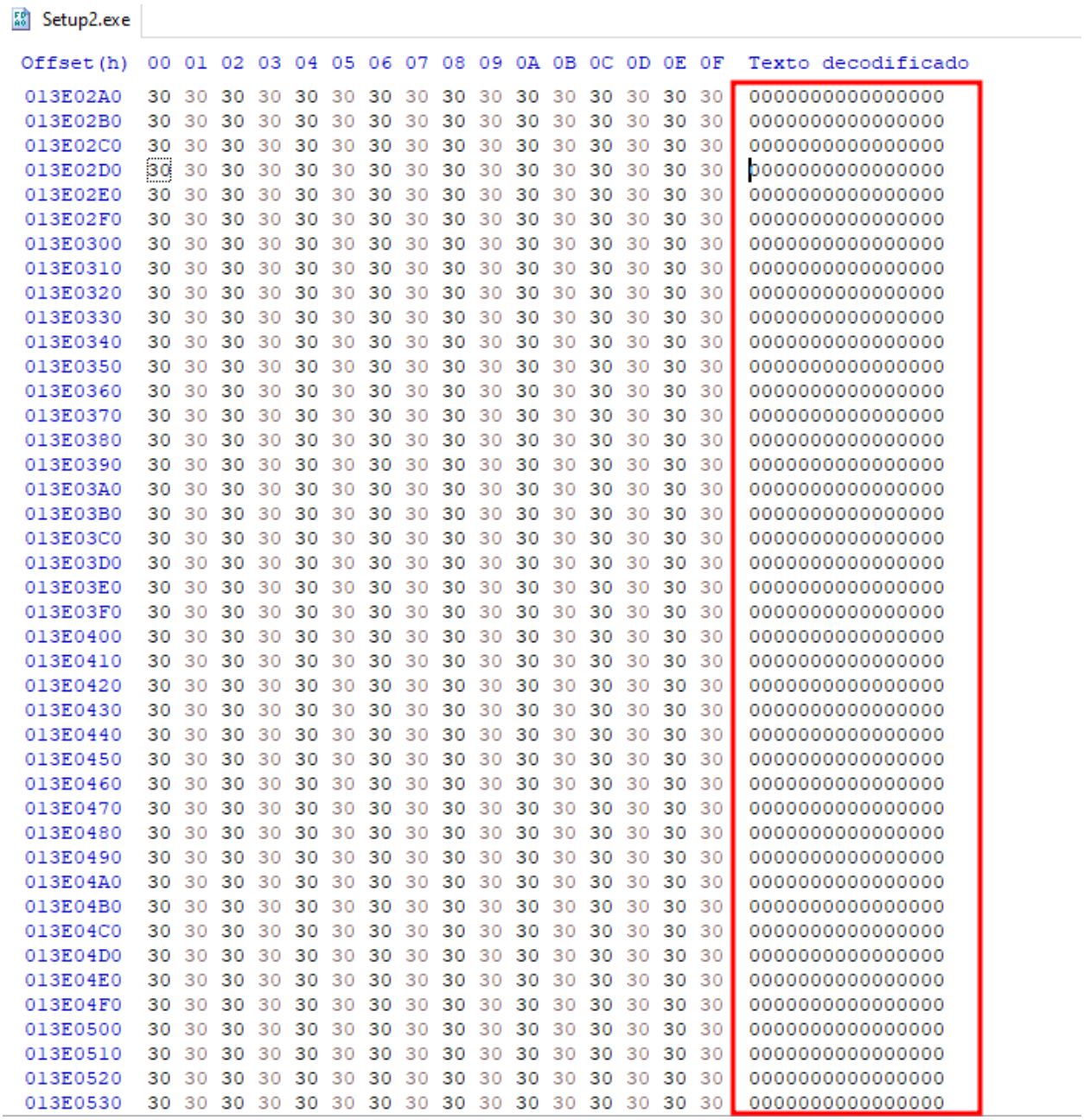


Si realizamos algo de **scroll** podemos ver que no hay ninguna **data (NULL - 00).**

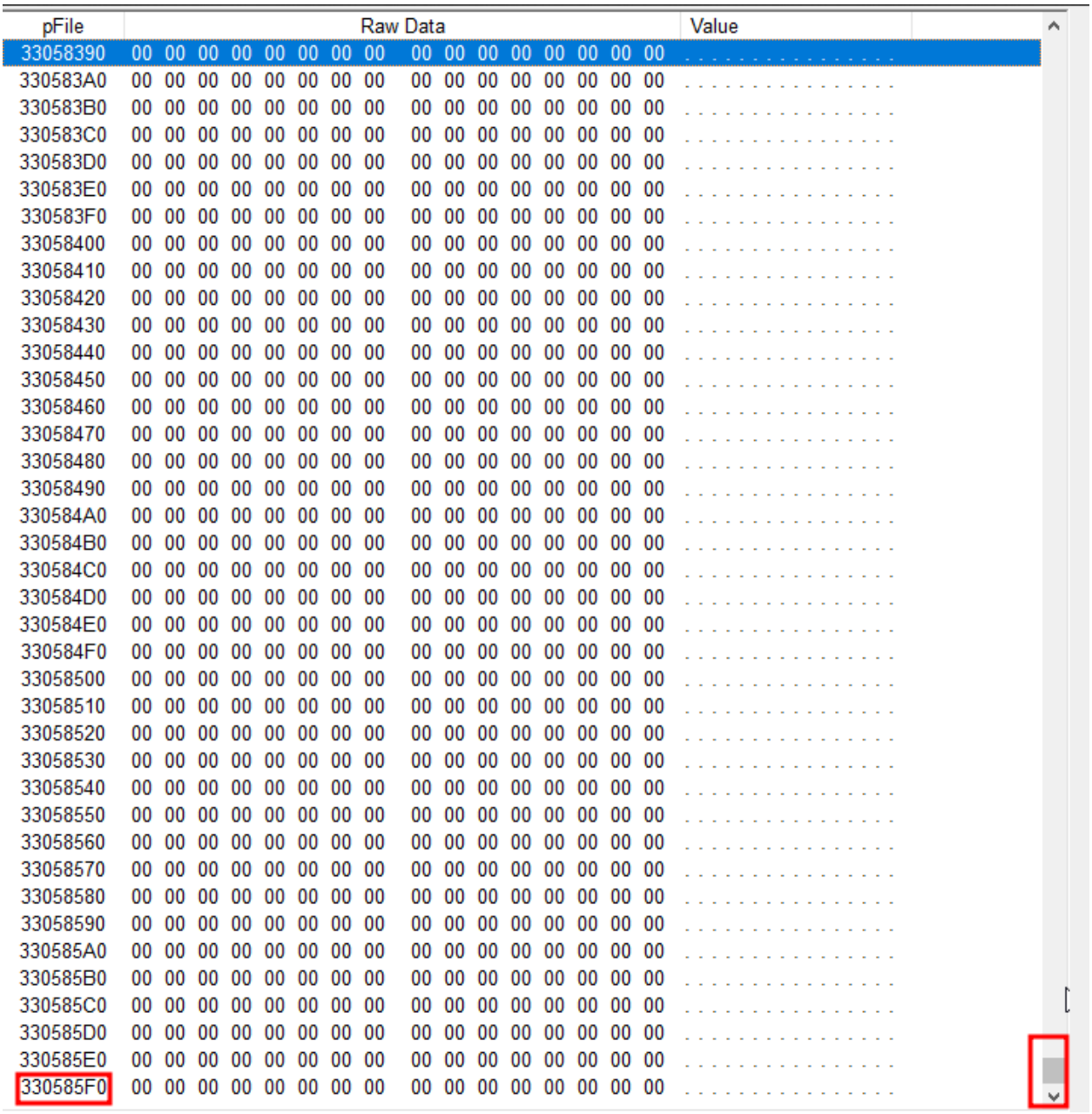


009ACDA0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009ACDB0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009ACDC0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009ACDD0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009ACDE0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009ACDF0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009ACE00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009ACE10	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009ACE20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009ACE30	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009ACE40	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009ACE50	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009ACE60	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009ACE70	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009ACE80	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009ACE90	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009ACEA0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009ACEB0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009ACEC0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009ACED0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009ACEE0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009ACEF0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009ACF00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009ACF10	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009ACF20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009ACF30	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009ACF40	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009ACF50	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009ACF60	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009ACF70	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009ACF80	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009ACF90	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009ACFA0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009ACFB0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009ACFC0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009ACFD0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009ACFE0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009ACFF0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009AD000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

También se observan algunos ceros.



Una práctica bastante común para aumentar el tamaño de un fichero (aunque es más común utilizar ceros que NULL) esto es una exageración:

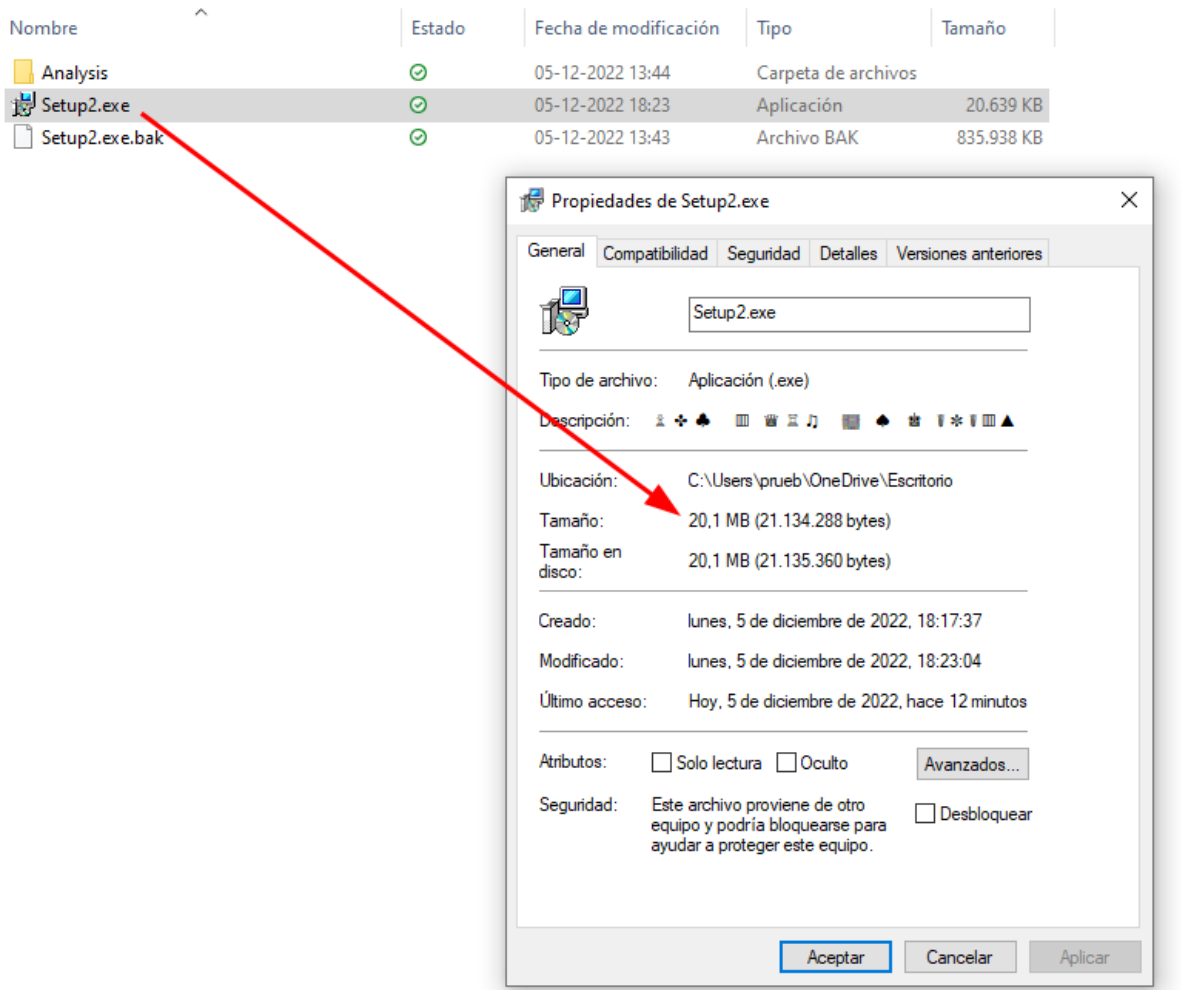


pFile	Raw Data	Value
33058390	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
330583A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
330583B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
330583C0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
330583D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
330583E0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
330583F0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
33058400	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
33058410	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
33058420	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
33058430	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
33058440	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
33058450	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
33058460	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
33058470	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
33058480	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
33058490	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
330584A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
330584B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
330584C0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
330584D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
330584E0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
330584F0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
33058500	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
33058510	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
33058520	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
33058530	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
33058540	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
33058550	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
33058560	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
33058570	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
33058580	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
33058590	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
330585A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
330585B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
330585C0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
330585D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
330585E0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .
330585F0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	. . . . .

5. Eliminado la data;

Haciendo uso de **HxD** podemos indicar un **bloque** a eliminar.

Simplemente indicando una **posición inicial** y otra de **término**.



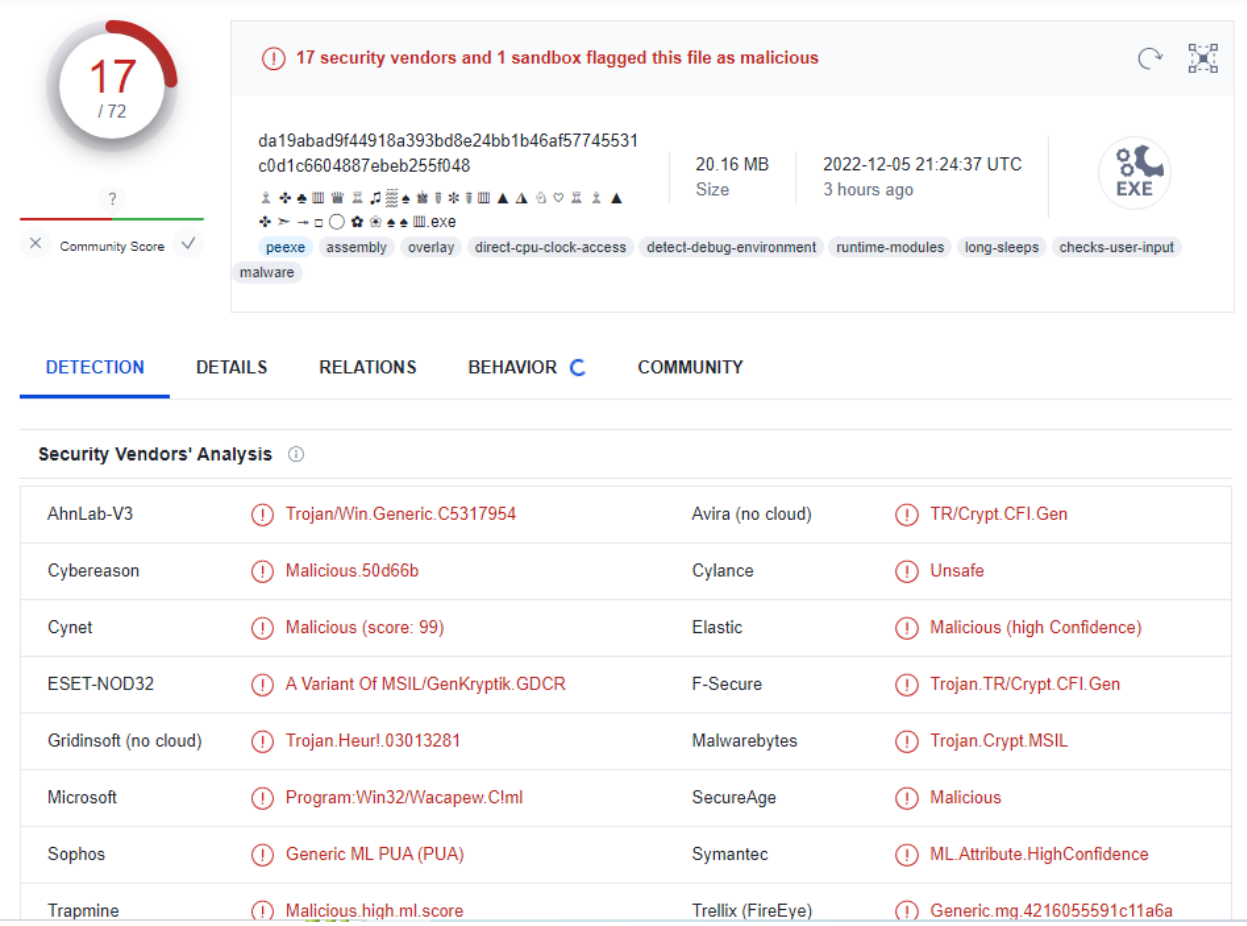
Se logra reducir drásticamente el tamaño del ejecutable.

> Agregar que se realizó una copia del instalador a otro directorio y se cambió el nombre a `Setup2.exe` por si se cometía algún error al momento de eliminar la data.

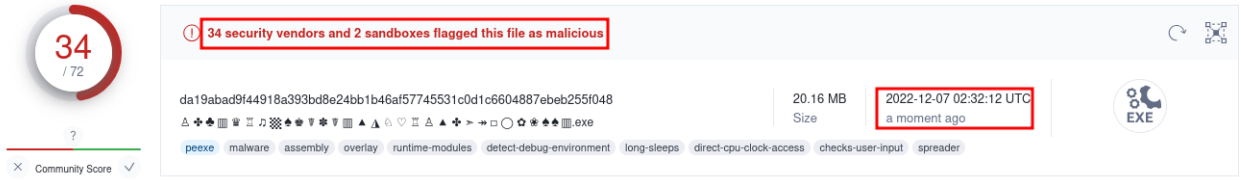
---

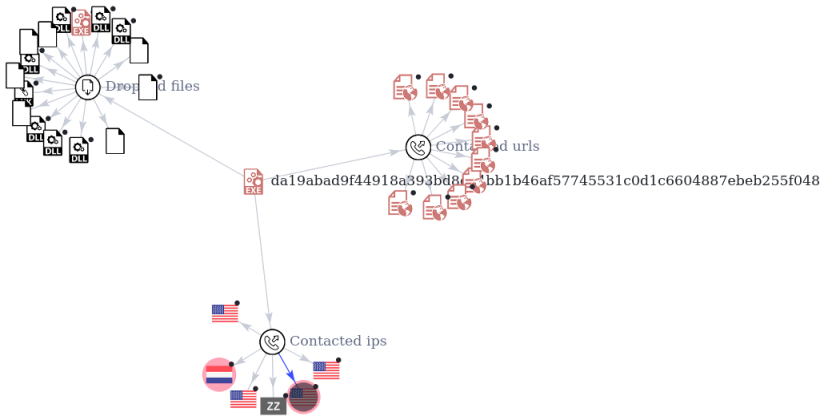
6. Virus Total;

Procedemos a subir el binario a VT para su análisis con los diferentes motores de antivirus que ofrece.

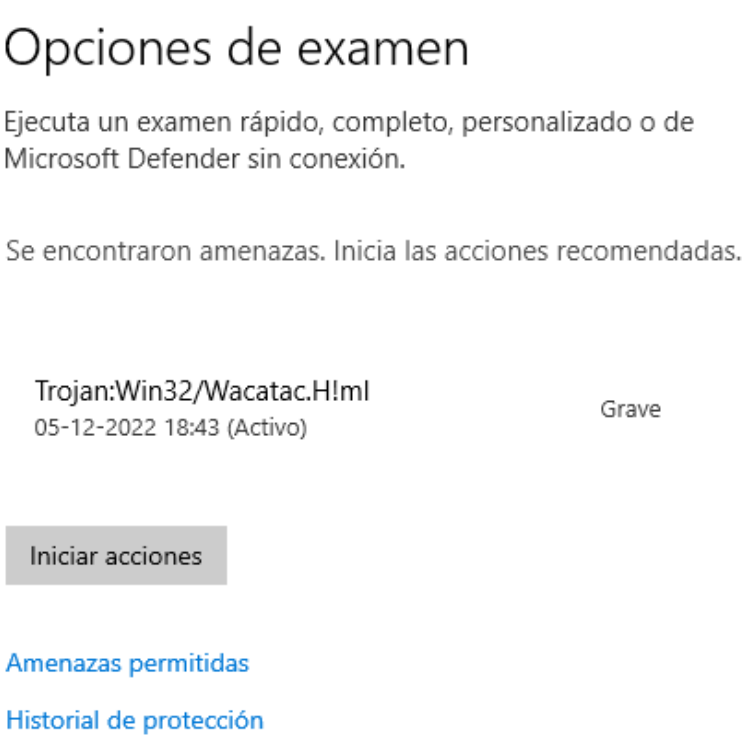


Obteniendo una detección por parte de 17 motores y un sandbox, una detección relativamente aceptable.



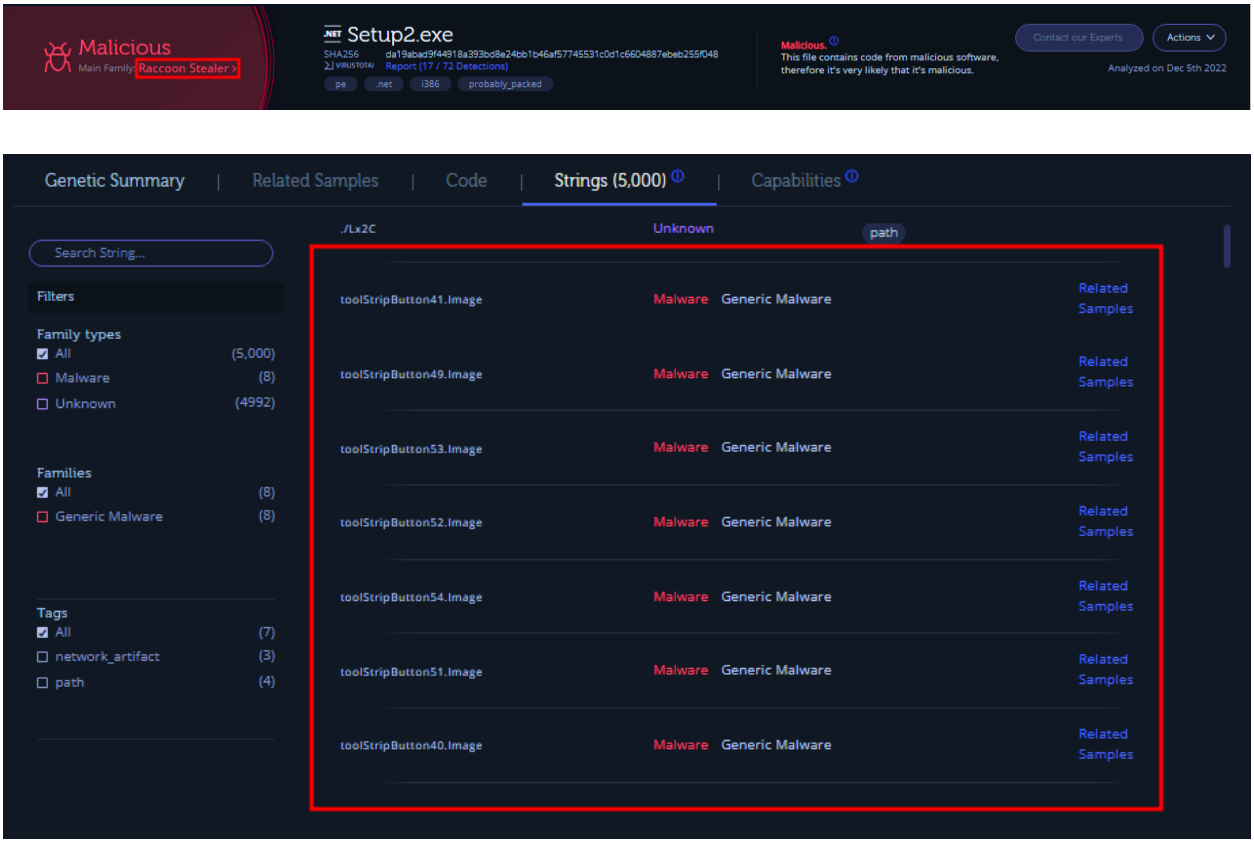


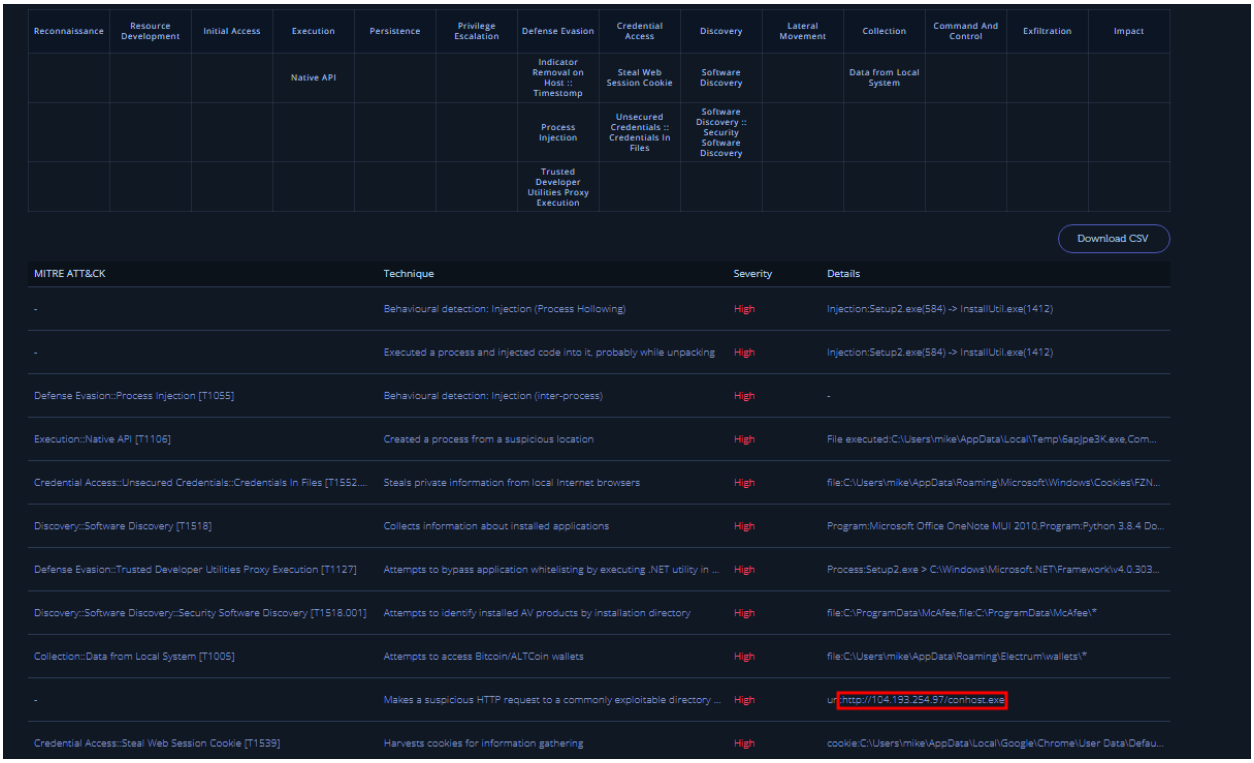
7. Windows Defender;



8. Intezer Analyze;

Con el fin de recolectar más antecedentes sobre el malware.





Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
			Native API			Indicator Removal on Host :: Timestomp	Steal Web Session Cookie	Software Discovery		Data from Local System			
						Process Injection	Unsecured Credentials :: Credentials In Files	Software Discovery :: Security Software Discovery					
						Trusted Developer Utilities Proxy Execution							

Download CSV

MITRE ATT&CK	Technique	Severity	Details
-	Behavioural detection: Injection (Process Hollowing)	High	Injection:Setup2.exe(584) -> InstallUtil.exe(1412)
-	Executed a process and injected code into it, probably while unpacking	High	Injection:Setup2.exe(584) -> InstallUtil.exe(1412)
Defense Evasion::Process Injection [T1055]	Behavioural detection: Injection (inter-process)	High	-
Execution::Native API [T1106]	Created a process from a suspicious location	High	File executed:C:\Users\mike\AppData\Local\Temp\6apjpe3K.exe,Com...
Credential Access::Unsecured Credentials::Credentials In Files [T1552....	Steals private information from local Internet browsers	High	file:C:\Users\mike\AppData\Roaming\Microsoft\Windows\Cookies\FZN...
Discovery::Software Discovery [T1518]	Collects information about installed applications	High	Program:Microsoft Office OneNote MUI 2010,Program:Python 3.8.4 Do...
Defense Evasion::Trusted Developer Utilities Proxy Execution [T1127]	Attempts to bypass application whitelisting by executing .NET utility in ...	High	Process:Setup2.exe > C:\Windows\Microsoft.NET\Framework\v4.0.303...
Discovery::Software Discovery::Security Software Discovery [T1518.001]	Attempts to identify installed AV products by installation directory	High	file:C:\ProgramData\McAfee,file:C:\ProgramData\McAfee*
Collection::Data from Local System [T1005]	Attempts to access Bitcoin/ALTCoin wallets	High	file:C:\Users\mike\AppData\Roaming\Electrum\wallets*
-	Makes a suspicious HTTP request to a commonly exploitable directory ...	High	url:http://104.193.254.97/conhost.exe
Credential Access::Steal Web Session Cookie [T1539]	Harvests cookies for information gathering	High	cookie:C:\Users\mike\AppData\Local\Google\Chrome\User Data\Defau...

9. IOCs;

```
4216055591c11a6ad41fa31ab03fa616 - MD5
```

```
705b62e50d66bbaced6ed2c963808a4d31be7a3d - SHA1
```

```
da19abad9f44918a393bd8e24bb1b46af57745531c0d1c6604887ebeb255f048 - SHA256
```

```
45.15.156.120 - C2
```

```
104.193.254.97 - C2
```

```
32a7337eb3f9e155c32e7bc0dc4d4cb5 - RAR MD5
```

```
806290abf68808cc970d7890778d7384f1e04cf26e6f3927ad19c68f24e421b5 - RAR SHA256
```

```
c481329f643ab66850409fb477c02247 - Setup.exe MD5
```

```
2424d04db21f6c9f36d9f243f92818044131177ad575136bd88638c416e705ffc - Setup.exe SHA256
```

```
https://telegra.ph/Wondershare-Filmora-12-04-2
```

```
https://telegra.ph/Wondershare-Filmora-11-11-04
```

```
https://www.mediafire.com/file/a29ccqwgoxosph5/InstallFilex64.rar/file
```

```
https://cdn.discordapp.com/attachments/1047653673217556562/1047985278662496256/SoftwareSetupFile.zip
```

```
https://www.mediafire.com/file/ndrvaxtrp8e0sry/Setup.zip/file
```

Detections	Status	URL
18 / 92	200	http://104.193.254.97/conhost.exe
14 / 92	404	http://45.15.156.120/
18 / 91	200	http://45.15.156.120/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/softokn3.dll
17 / 91	200	http://45.15.156.120/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/freebl3.dll
17 / 91	200	http://45.15.156.120/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/mozglue.dll
18 / 92	200	http://45.15.156.120/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/msvcp140.dll
17 / 91	200	http://45.15.156.120/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/vcruntime140.dll
17 / 91	200	http://45.15.156.120/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/sqlite3.dll
13 / 92	404	http://45.15.156.120/ff7b95a4f215508064d0c24fe6e4f0bf
17 / 91	200	http://45.15.156.120/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/nss3.dll

---

10. Scans;

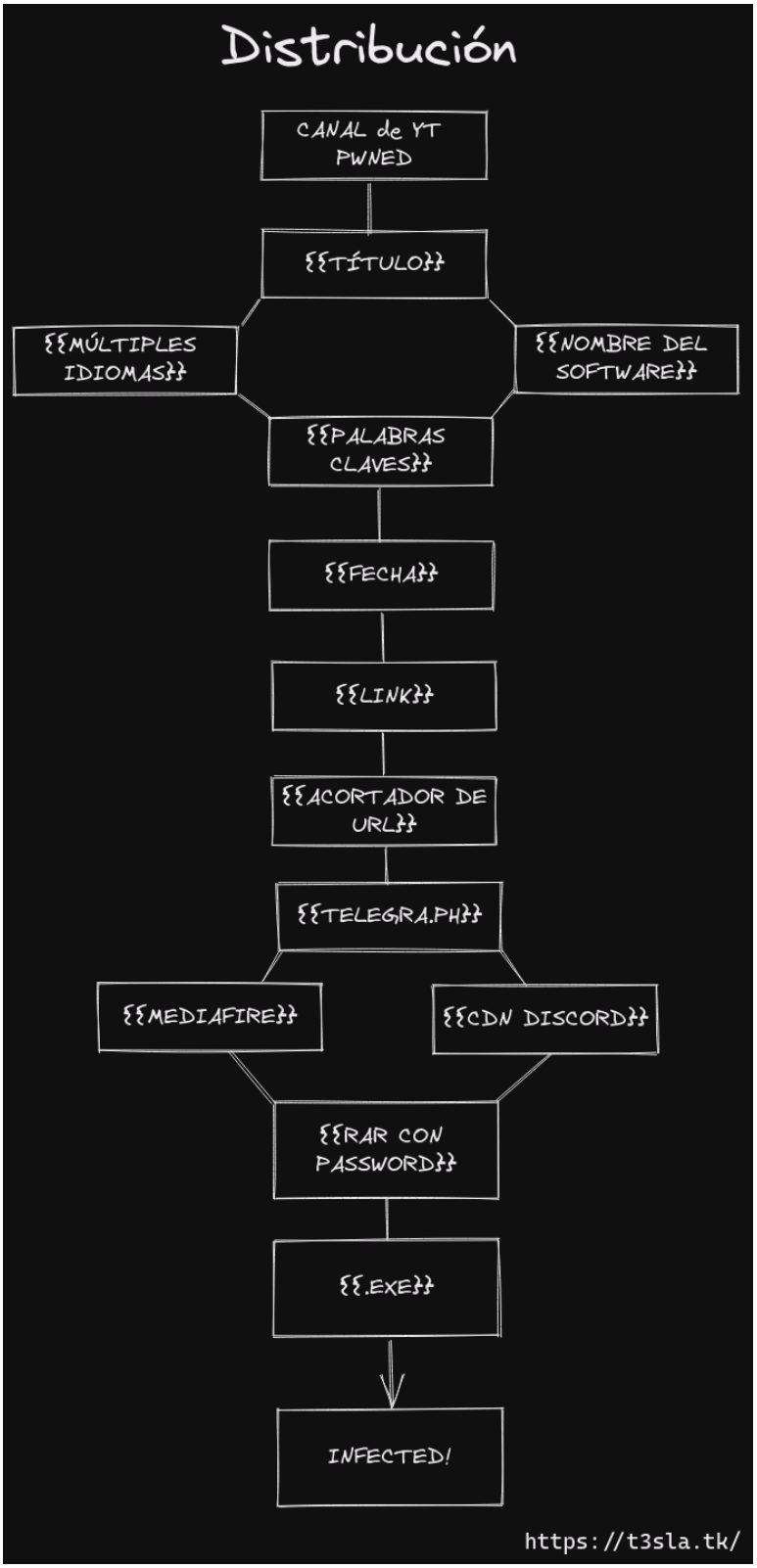
1. VT.

2. Intezer.

---

11. Diagrama;

Distribución del Malware y patrones reiterados.


Distribución
CANAL de YT PWNED
{{TÍTULO}}
{{MÚLTIPLES IDIOMAS}}
{{NOMBRE DEL SOFTWARE}}
{{PALABRAS CLAVES}}
{{FECHA}}
{{LINK}}
{{ACORTADOR DE URL}}
{{TELEGRA.PH}}
{{MEDIAFIRE}}
{{CDN DISCORD}}
{{RAR CON PASSWORD}}
{{.EXE}}
INFECTED!
https://t3sla.tk/


Red Team