



# 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

Contenido

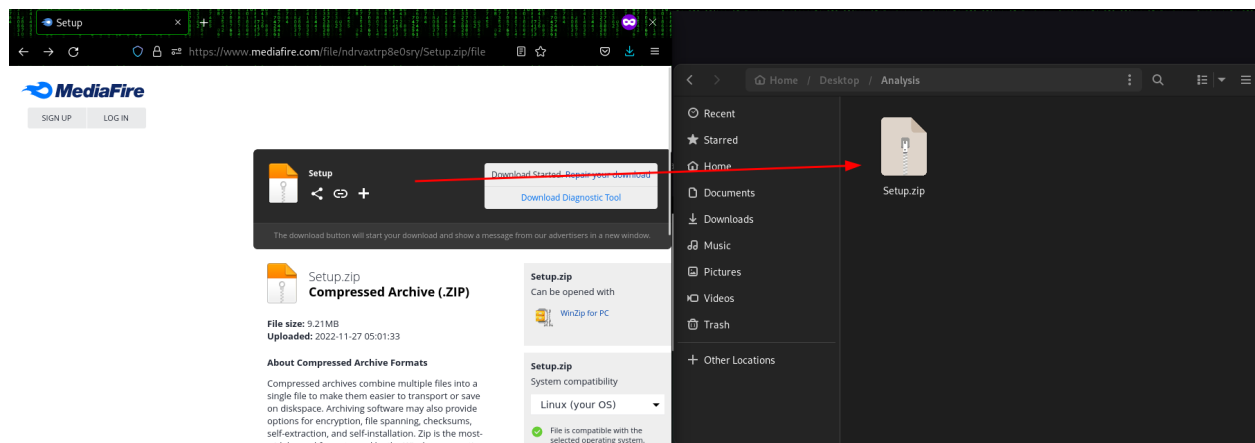
1. Herramientas;
2. Descarga de la muestra y comparación;
3. Configuración de la VM;

4. Análisis del PE.
  5. Eliminado la data;
  6. Virus Total;
  7. Windows Defender;
  8. Intezer Analyze;
  9. IOCs;
  10. Scans;
  11. Diagrama;
- 

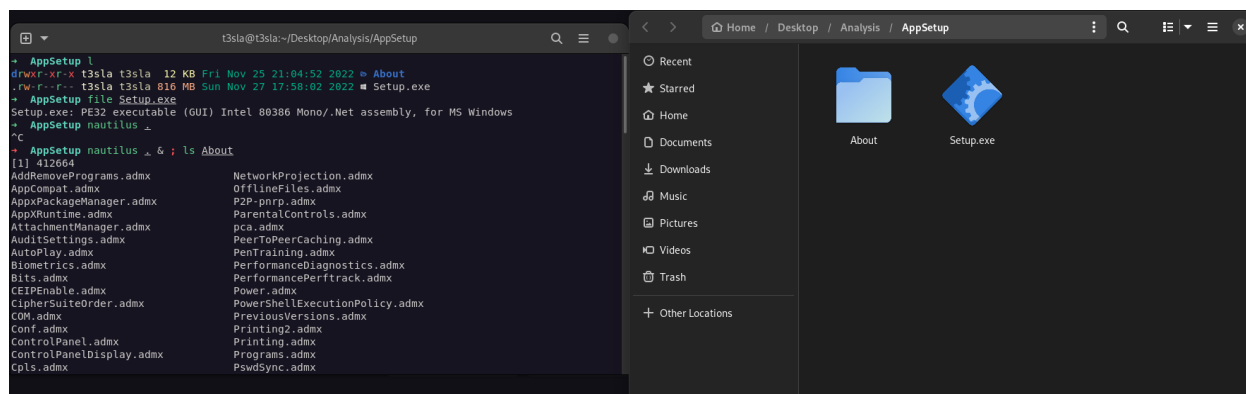
## 1. Herramientas;

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
```

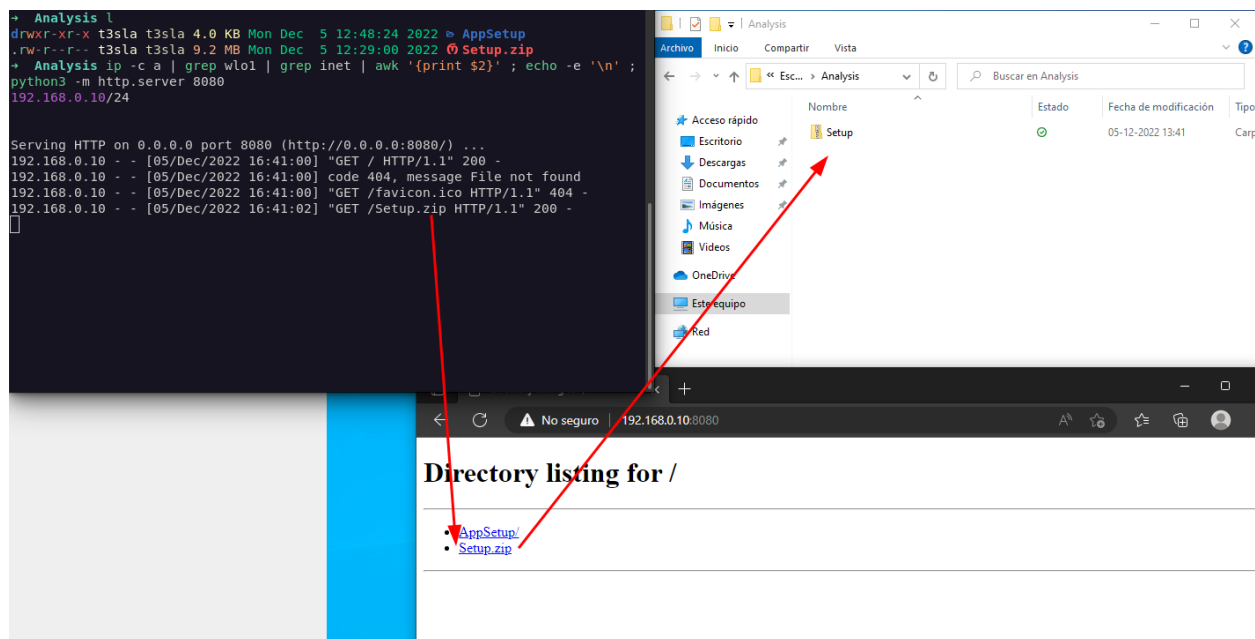


La primera alerta que obtenemos es el tamaño del binario, si lo comparamos con el instalador legítimo no concuerdan.

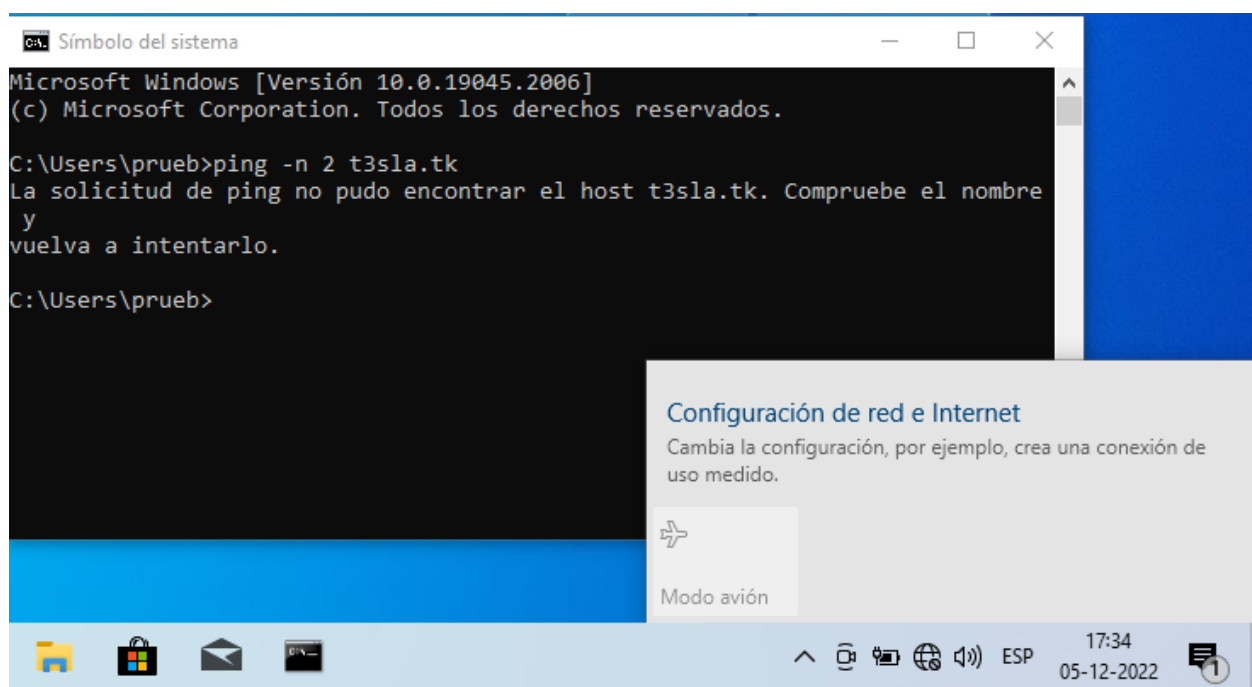
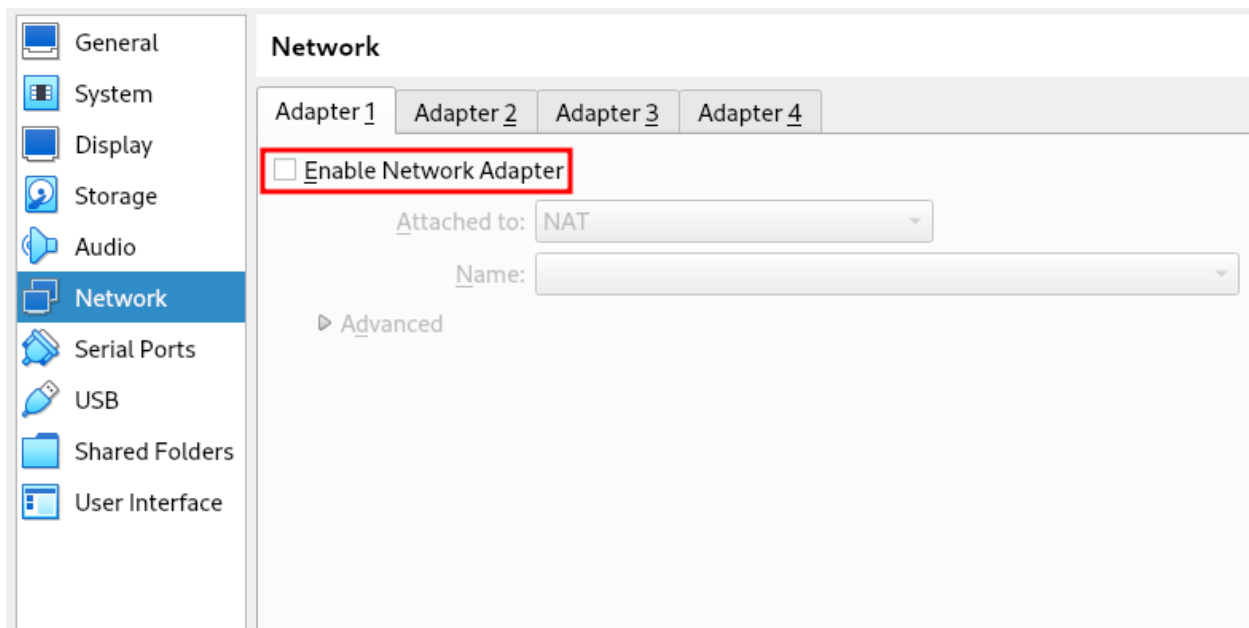
```
t3sla@t3sla:~/Downloads
→ Downloads
→ Downloads l filmora_setup_full846.exe
.rw-r--r-- t3sla t3sla 3.1 MB Mon Dec 12 03:33:45 2022 filmora_setup_full846.exe
→ Downloads file filmora_setup_full846.exe
filmora_setup_full846.exe: PE32 executable (GUI) Intel 80386, for MS Windows
→ Downloads
```

### 3. Configuración de la VM;

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

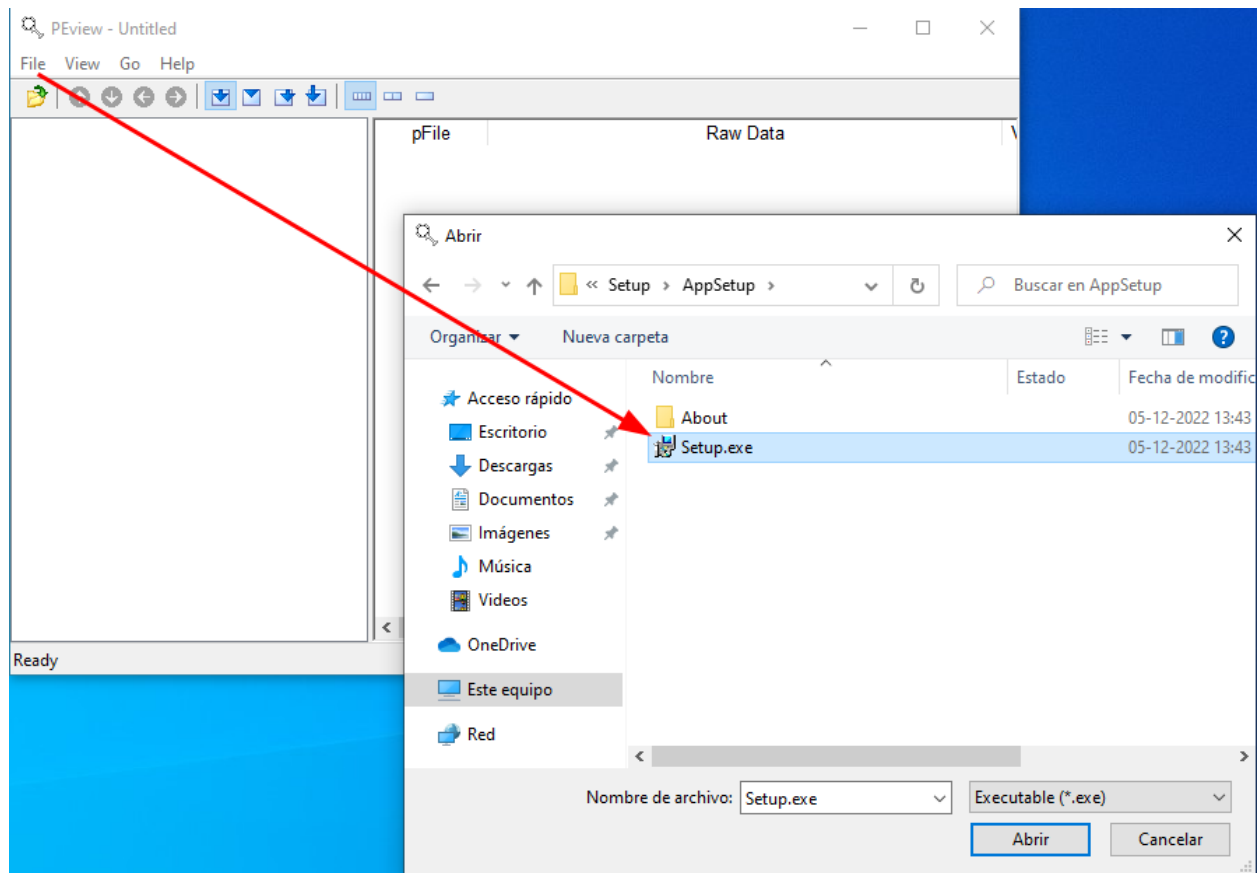


Como medida extra, ante cualquier error que puede provenir de mi persona, también se desactivará el adaptador de red para evitar la comunicación de la máquina a internet y mi red.



## 4. Análisis del PE.

Empleando PEView para obtener la estructura del Portable Executable.



PEView - C:\Users\prueb\OneDrive\Escritorio\Analysis\Setup\AppSetup\Setup.exe

File View Go Help

	pFile	Raw Data	Value
Setup.exe	00000000	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00	MZ
IMAGE_DOS_HEADER	00000010	B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00	.....@.....
MS-DOS Stub Program	00000020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
IMAGE_NT_HEADERS	00000030	00 00 00 00 00 00 00 00 00 00 00 80 00 00 00	.....
IMAGE_SECTION_HEADER .text	00000040	0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68	.....!..L..!Th
IMAGE_SECTION_HEADER .rsrc	00000050	69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6F	is program canno
IMAGE_SECTION_HEADER	00000060	74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20	t be run in DOS
IMAGE_SECTION_HEADER .reloc	00000070	6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00	mode...\$.....
SECTION .text	00000080	50 45 00 00 4C 01 05 00 D3 7F 55 E6 00 00 00 00	PE...L...U.....
SECTION .rsrc	00000090	00 00 00 00 E0 00 22 00 0B 01 30 00 00 D2 25 00	....."....0...%
SECTION	000000A0	00 F2 70 00 00 00 00 00 0A 00 97 00 00 00 71 00	..p.....q-
SECTION .reloc	000000B0	00 20 00 00 00 00 40 00 00 20 00 00 00 02 00 00	.....@.....
	000000C0	04 00 00 00 00 00 00 00 04 00 00 00 00 00 00	.....
	000000D0	00 40 97 00 00 04 00 00 00 00 00 02 00 40 85	..@.....@.....
	000000E0	00 00 10 00 00 10 00 00 00 00 10 00 00 10 00	.....
	000000F0	00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	.....
	00000100	68 0C 71 00 53 00 00 00 00 E0 96 00 BA 15 00 00	h.q.S.....
	00000110	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
	00000120	00 20 97 00 0C 00 00 00 00 00 00 00 00 00 00	.....
	00000130	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
	00000140	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
	00000150	00 00 00 00 00 00 00 00 00 97 00 08 00 00 00	.....
	00000160	00 00 00 00 00 00 00 00 00 00 71 00 48 00 00	.....q.H.....
	00000170	00 00 00 00 00 00 00 00 0B 01 29 74 6A 45 77 50	.....)tjEwP
	00000180	F8 D9 70 00 00 20 00 00 00 DA 70 00 00 04 00 00	..p.....p.....
	00000190	00 00 00 00 00 00 00 00 00 00 00 40 00 00 E0	.....@.....
	000001A0	2E 74 65 78 74 00 00 00 AD CF 25 00 00 00 71 00	..text....%...q.
	000001B0	00 D0 25 00 00 DE 70 00 00 00 00 00 00 00 00	..%...p.....
	000001C0	00 00 00 00 20 00 00 60 2E 72 73 72 63 00 00	.....\rsrc...
	000001D0	BA 15 00 00 00 E0 96 00 00 16 00 00 00 AE 96 00	.....
	000001E0	00 00 00 00 00 00 00 00 00 00 00 40 00 00 40	.....@..@.....
	000001F0	00 00 00 00 00 00 00 00 10 00 00 00 00 97 00	.....
	00000200	00 02 00 00 00 C4 96 00 00 00 00 00 00 00 00	.....
	00000210	00 00 00 00 20 00 00 60 2E 72 65 6C 6F 63 00	.....\reloc..
	00000220	0C 00 00 00 00 20 97 00 00 02 00 00 00 C6 96 00	.....
	00000230	00 00 00 00 00 00 00 00 00 00 00 40 00 00 42	.....@...B.....
	00000240	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
	00000250	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
	00000260	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....

Viewing Setup.exe

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





Setup2.exe																	
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Texto decodificado
013E02A0	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E02B0	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E02C0	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E02D0	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E02E0	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E02F0	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E0300	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E0310	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E0320	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E0330	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E0340	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E0350	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E0360	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E0370	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E0380	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E0390	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E03A0	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E03B0	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E03C0	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E03D0	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E03E0	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E03F0	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E0400	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E0410	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E0420	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E0430	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E0440	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E0450	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E0460	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E0470	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E0480	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E0490	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E04A0	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E04B0	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E04C0	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E04D0	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E04E0	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E04F0	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E0500	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E0510	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E0520	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000
013E0530	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	0000000000000000

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

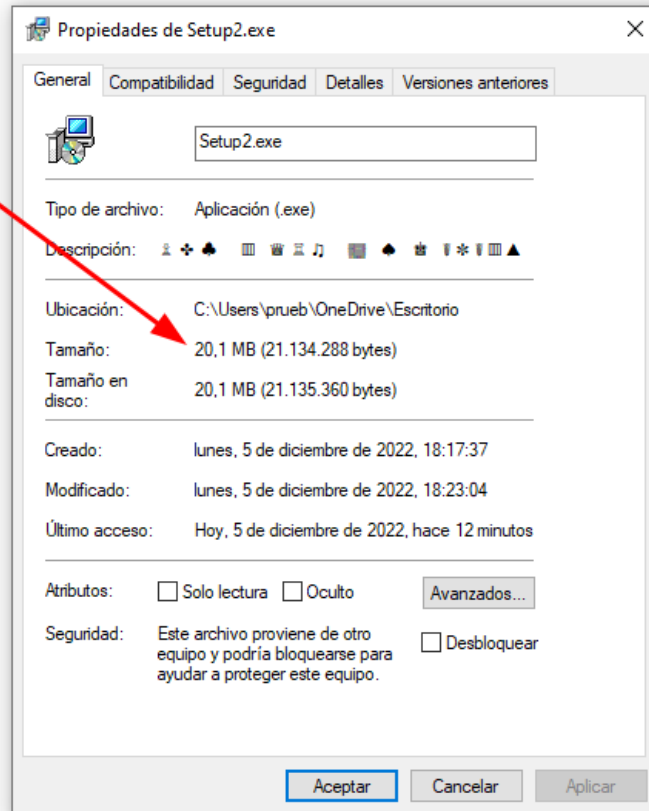
pFile	Raw Data																Value
33058390	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
330583A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
330583B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
330583C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
330583D0	00	00	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**.

Nombre	Estado	Fecha de modificación	Tipo	Tamaño
Analysis	✓	05-12-2022 13:44	Carpeta de archivos	
Setup2.exe	✓	05-12-2022 18:23	Aplicación	20.639 KB
Setup2.exe.bak	✓	05-12-2022 13:43	Archivo BAK	835.938 KB



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.

17

/ 72

?

Community Score

17 security vendors and 1 sandbox flagged this file as malicious

da19abad9f44918a393bd8e24bb1b46af57745531c0d1c6604887eb255f048

20.16 MB Size

2022-12-05 21:24:37 UTC 3 hours ago

EXE

peexe assembly overlay direct-cpu-clock-access detect-debug-environment runtime-modules long-sleeps checks-user-input malware

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY

Security Vendors' Analysis

AhnLab-V3	Trojan.Win.Generic.C5317954	Avira (no cloud)	TR/Crypt.CFI.Gen
Cybereason	Malicious.50d66b	Cylance	Unsafe
Cynet	Malicious (score: 99)	Elastic	Malicious (high Confidence)
ESET-NOD32	A Variant Of MSIL/GenKryptik.GDCR	F-Secure	Trojan.TR/Crypt.CFI.Gen
Gridinsoft (no cloud)	Trojan.Heur!.03013281	Malwarebytes	Trojan.Crypt.MSIL
Microsoft	Program:Win32/Wacapew.Clml	SecureAge	Malicious
Sophos	Generic ML PUA (PUA)	Symantec	ML.Attribute.HighConfidence
Trapmine	Malicious.high.ml.score	Trellix (FireEye)	Generic.mg.4216055591c11a6a

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

34

/ 72

?

Community Score

34 security vendors and 2 sandboxes flagged this file as malicious

da19abad9f44918a393bd8e24bb1b46af57745531c0d1c6604887eb255f048

20.16 MB Size

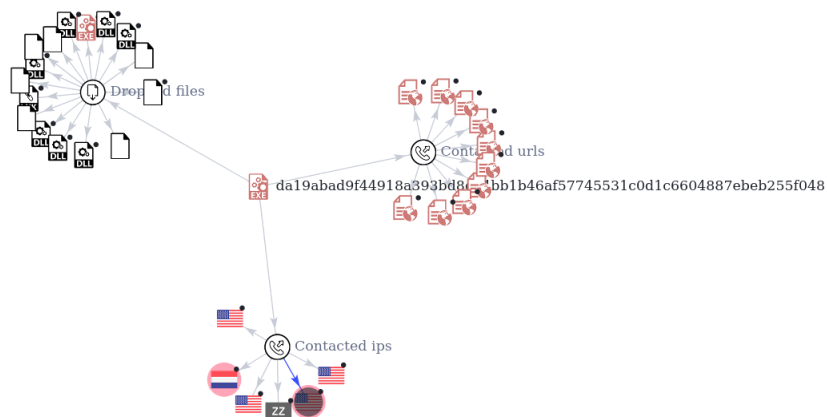
2022-12-07 02:32:12 UTC a moment ago

EXE

peexe malware assembly overlay runtime-modules detect-debug-environment long-sleeps direct-cpu-clock-access checks-user-input spreader

De Mecánica a Software

12



## 7. Windows Defender;

### Opciones de examen

Ejecuta un examen rápido, completo, personalizado o de Microsoft Defender sin conexión.

Se encontraron amenazas. Inicia las acciones recomendadas.

Trojan:Win32/Wacatac.H!ml

05-12-2022 18:43 (Activo)

Grave

Iniciar acciones

[Amenazas permitidas](#)

[Historial de protección](#)

## 8. Intezer Analyze;

Con el fin de recolectar más antecedentes sobre el malware.

**Malicious** Main Family: **Raccoon Stealer**

**Setup2.exe**  
SHA256: da19abac9f44918a393bd8e24be1b46a57745531cd1c6604887eb255f048  
VirusTotal Report (17 / 72 Detections)  
pe .net i386 probably\_packed

**Malicious**  
This file contains code from malicious software, therefore it's very likely that it's malicious.  
Analyzed on Dec 5th 2022

Contact our Experts Actions

Genetic Summary | Related Samples | Code | **Strings (5,000)** | Capabilities

Search String...

**Filters**

**Family types**

- ☒ All (5,000)
- ☐ Malware (8)
- ☐ Unknown (4992)

**Families**

- ☒ All (8)
- ☐ Generic Malware (8)

**Tags**

- ☒ All (7)
- ☐ network\_artifact (3)
- ☐ path (4)

.ILx2C	Unknown	path
toolStripButton41.Image	Malware	Generic Malware
toolStripButton49.Image	Malware	Generic Malware
toolStripButton53.Image	Malware	Generic Malware
toolStripButton52.Image	Malware	Generic Malware
toolStripButton54.Image	Malware	Generic Malware
toolStripButton51.Image	Malware	Generic Malware
toolStripButton40.Image	Malware	Generic 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 :: Timestamp	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\6apje3K.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	ur(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

2424d04db21f6c9f36d9f243f9281804413177ad575136bd88638c416e705ffc - 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.



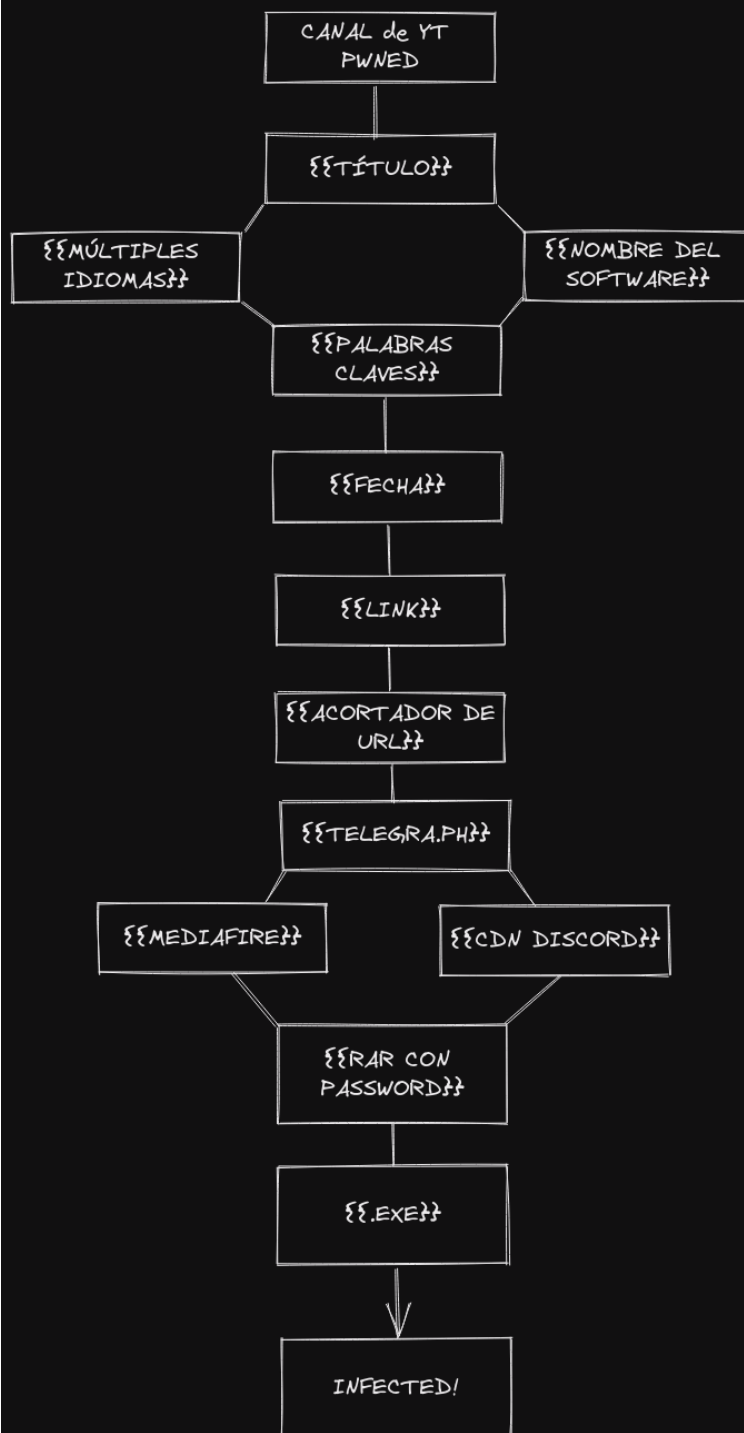
2. Intezer.

---

## **11. Diagrama;**

Distribución del Malware y patrones reiterados.

# Distribución



<https://t3sla.tk/>

