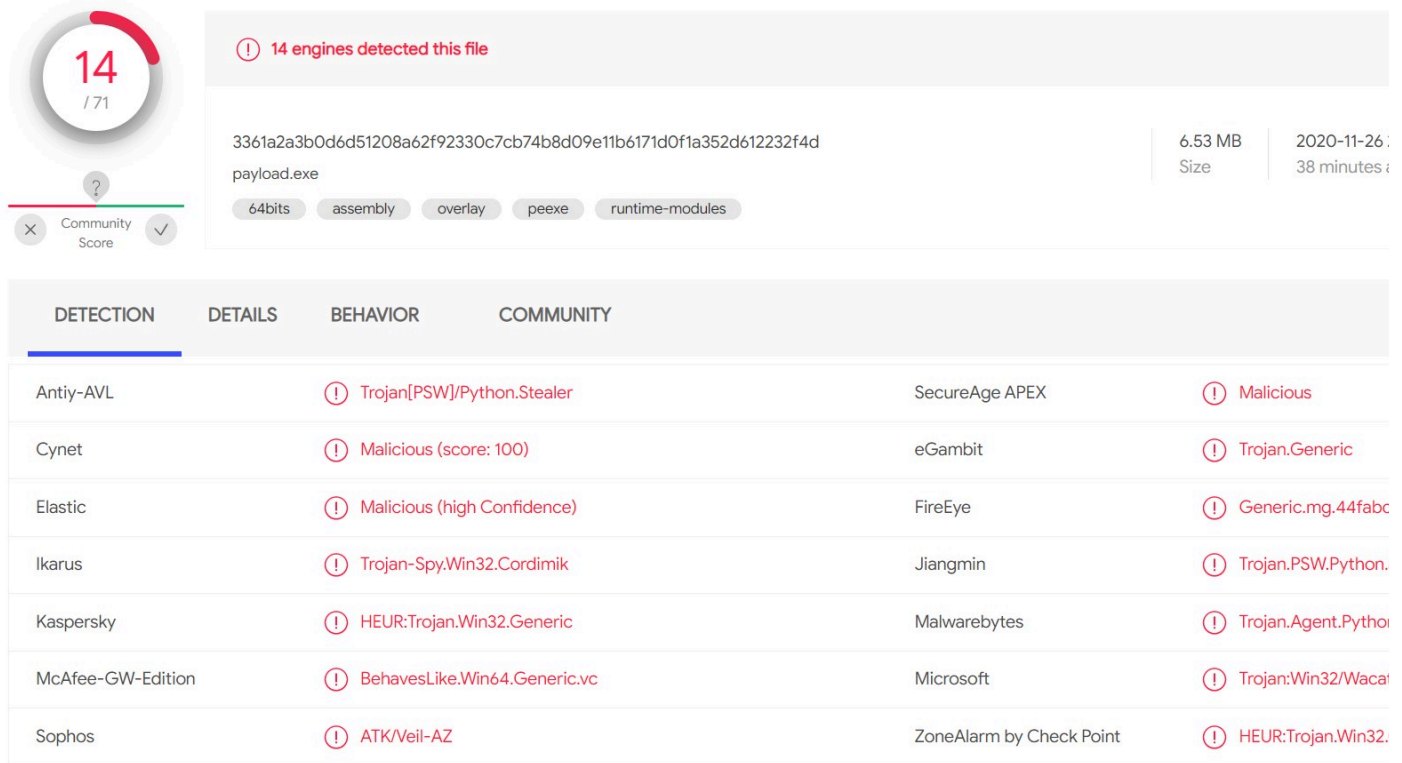


24. Evasión de antivirus

Thursday, November 26, 2020 5:48 PM

Crea un ejecutable con pyinstaller

1. Escribe tu script
2. Guárdalo como .pyw
3. Usa pyinstaller para crear tu ejecutable.
4. Súbelo a una página tipo 'Virus Total' para verificar si lo reconocen o no los antivirus.



The screenshot shows a VirusTotal scan interface. On the left, a circular progress indicator shows 14 out of 71 engines. Below it, a 'Community Score' section shows a question mark and a checkmark. The main area displays the file name 'payload.exe' and its hash '3361a2a3b0d6d51208a62f92330c7cb74b8d09e11b6171d0f1a352d612232f4d'. The file size is 6.53 MB and it was scanned on 2020-11-26 at 38 minutes. Below this, there are tabs for '64bits', 'assembly', 'overlay', 'peexe', and 'runtime-modules'. The 'DETECTION' tab is active, showing a table of results from various antivirus engines.

DETECTION	DETAILS	BEHAVIOR	COMMUNITY	
Antiy-AVL	!	Trojan[PSW]/Python.Stealer	SecureAge APEX	! Malicious
Cynet	!	Malicious (score: 100)	eGambit	! Trojan.Generic
Elastic	!	Malicious (high Confidence)	FireEye	! Generic.mg.44fab
Ikarus	!	Trojan-Spy.Win32.Cordimik	Jiangmin	! Trojan.PSW.Python.
Kaspersky	!	HEUR:Trojan.Win32.Generic	Malwarebytes	! Trojan.Agent.Pytho
McAfee-GW-Edition	!	BehavesLike.Win64.Generic.vc	Microsoft	! Trojan:Win32/Waca
Sophos	!	ATK/Veil-AZ	ZoneAlarm by Check Point	! HEUR:Trojan.Win32.

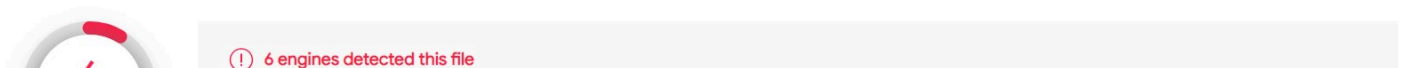
Crea un ejecutable con setup y py2exe

1. Instala el módulo py2exe
`pip install py2exe`
2. Escribe un script setup.py

```
from distutils.core import setup
import py2exe
setup(
    name = 'Payload',
    description = 'Python-based App',
    version = '1.0',
    console=['payload.pyw'],
    options = {'py2exe': {'bundle_files': 2,
                          'packages': 'ctypes',
                          'includes':
                          'base64,sys,socket,struct,time,code,platform,getpass,shutil'
                          }},
    zipfile = None,
)
```

3. Ejecuta el siguiente comando
`setup.py py2exe`
4. Sube el ejecutable a una página tipo 'Virus Total' para verificar si lo reconocen o no los antivirus.

Usando payload.py



The screenshot shows the top part of a VirusTotal scan interface. A circular progress indicator shows 6 out of 71 engines. Below it, a 'Community Score' section shows a question mark and a checkmark. The main area displays the file name 'payload.py' and its hash '3361a2a3b0d6d51208a62f92330c7cb74b8d09e11b6171d0f1a352d612232f4d'. The file size is 6.53 MB and it was scanned on 2020-11-26 at 38 minutes. Below this, there are tabs for '64bits', 'assembly', 'overlay', 'peexe', and 'runtime-modules'.

1 / 69

Community Score

a23f1ceb85b9ef498a7bea529e95d2ec79299f0e20d199d62cbfff6810db24b5

payload.exe

8.09 MB

2020-11-26 23:13 minutes ago

64bitsassemblyinvalid-rich-pe-linker-versionoverlaypeexe runtime-modules

DETECTION	DETAILS	BEHAVIOR	COMMUNITY
SecureAge APEX	Malicious	Cynet	Malicious (score: 100)
Jiangmin	Trojan.PSW.Python.x	Kaspersky	HEUR:Trojan.Win32.G
Zillya	Trojan.Disco.Script.95	ZoneAlarm by Check Point	HEUR:Trojan.Win32.G

Usando payload.pyw

6 / 66

Community Score

6 engines detected this file

c555cc70ba1d71b390a8d3b348a57390edcb271524e3b3d6db49e69ee432f0cd

payload.exe

8.09 MB

2020-11-26 23:1 minute ago

64bitsassemblyinvalid-rich-pe-linker-versionoverlaypeexe

DETECTION	DETAILS	BEHAVIOR	COMMUNITY
SecureAge APEX	Malicious	Cynet	Malicious (score: 100)
Jiangmin	Trojan.PSW.Python.x	Kaspersky	HEUR:Trojan.Win32.G
Zillya	Trojan.Disco.Script.95	ZoneAlarm by Check Point	HEUR:Trojan.Win32.G
Acronis	Undetected	Ad-Aware	Undetected
AegisLab	Undetected	AhnLab-V3	Undetected

Script



