

scanner

PE static analysis platform

PE static analysis platform

- CLI && GUI
- Plugins
- Analysis database
- Developer oriented

Show me the code interface

FILE SCANNER

UploadLast results

Drag & Drop to upload file

OR

Browse file

Last results

Last update	SHA1	Filename	Analyse
2023-05-10 09:15:24	f2cd2b349341094854c5806f617a746dd50a74eb	pe-Windows-x86-cmd	GO
2023-04-06 10:38:16	0f3c4ff28f354aede202d54e9d1c5529a3bf87d8	pe-Windows-x64-cmd	GO
2023-04-05 17:48:51	7376306ef191b557b00a125c850139c4252b44b9	pe-mingw32-strip.exe	GO
2023-04-05 17:48:47	e293ef359ff13b46ec4e1faac11487828879614c	ntdll.dll	GO
2023-04-05 17:48:45	e64fc056cae8b7882cdd2fdd1786f4bb3a5af408	pe-cygwin-ls.exe	GO
2023-04-05 17:48:40	7c52f22d92b7feb8a115e31710584c611fc6a51c	pe-Windows-ARMv7-Thumb2LE-HelloWorld	GO
2023-04-05 17:44:53	ca0c223888eb85c15fd9592119e128c2ec055c88	Backdoor.Win32.Hupigon.nzlf_6f76.exe	GO
2023-04-05 17:44:51	57e780430688b4113959c9f8659ee9300e0af72	Backdoor.Win32.Poison.cmoefab6.exe	GO

FILE SCANNER

UploadInfosExtractorsActions

Analysis results

Infos

- Filename: pe-Windows-x86-cmd
- Last update: 2023-05-10 09:15:24
- Hash: f2cd2b349341094854c5806f617a746dd50a74eb
- Analysis duration: 3.05 seconds

Extractors

CAPA/FLARE_CAPA/STDOUT.LOG

C

🔗

md5

e52110456ec302786585656f220405eb

sha1

f2cd2b349341094854c5806f617a746dd50a74eb

sha256

785c974152976525e46b032c30378e457d069f30ac3f0fe9613e5e142ce7e8b2

path

/home/user/workspace/scanner/scanner/results/f2cd2b349341094854c5806f617a746dd50a74eb/pe-Windows-x86-cmd

CHECKSUMS/CHECKSUMS/STDOUT.LOG

C

🔗

algorithm,value

md5sum,e52110456ec302786585656f220405eb

sha1sum,f2cd2b349341094854c5806f617a746dd50a74eb

sha256sum,785c974152976525e46b032c30378e457d069f30ac3f0fe9613e5e142ce7e8b2

sha512sum,0e4b7e5407ae55bd37b7b19576d1467e5bab1e81457613bbab28ce6e8f0bdf96c158c4409d126a9eb4d77048b86e8444810663c6b3982398ed43ea596d7bd992

ENTROPY/ENTROPY/STDOUT.LOG

C

🔗

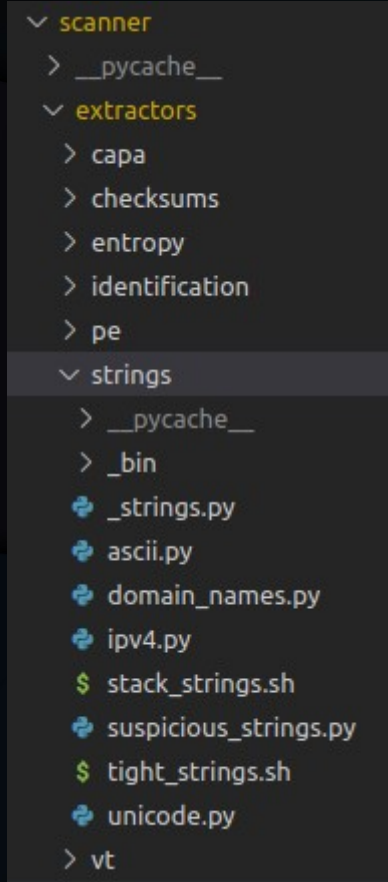
algorithm,value

shannon,4.590256737929562

natural,3.1817235159421693

hartley,1.3818049659154965

Extractors



- Drop your exec
- Categorize with folders
- Write to stdout / stderr
- Prefix deps with _

Extractors full list

capa	capa -vv
checksums	Md5, sha1, sha256
entropy	Calcul shannon, natural, hartley
identification	file (1)
pe/authenticode	Authenticode display
pe/debug	PE debug infos (e.g. pdb path)
pe/exports	Exports listing
pe/features	Has suspicious imphash, has native subsystem, ...
pe/header	PE header infos (addr of entrypoint, size of code, ...)
pe/imports_hash	Imports hash computation (pefile / lief based)
pe/imports	Imports listing
pe/packers	Packer detection

pe/resources	Rsrc listing
pe/rich_header	rich header infos (vs2022 up to date!)
pe/sections	Pe section infos
pe/stamps	PE timestamps
pe/subsystem	PE subsystem output
pe/suspicious_imports	Suspicious imports listing (e.g. antidebug)
pe/suspicious_modules	Suspicious modules listing (e.g. libraries)
pe/suspicious_sections	Suspicious sections listing (e.g. packers)
strings/ascii	Ascii strings listing
strings/domain_names	Domain names listing
strings/ipv4	Ipv4 listing

strings/stack_strings	Stack strings listing
strings/suspicious_strings	Suspicious strings (e.g. cmd.exe)
strings/tight_strings	Tight strings listing
strings/unicode	Utf16le strings listing
vt/by_hash	VT hash report download

Example

Write extractor ...

```
#!/usr/bin/env python3
import sys
from _strings import get_description, get_strings

if __name__ == "__main__":
    """/usr/bin/strings -es $1"""
    if (
        strings_infos := get_strings(
            sys.argv[1], ascii=True, unicode=False, offsets=True
        ) == []:
        sys.exit(1)

    print("offset,string,description")
    for offset, content in strings_infos:
        string = content.decode("ascii")
        print(f"{offset:#08x}", string, get_description(string), sep=",")

    sys.exit(0)
```

```
user@user:~/workspace/scanner$ poetry run scanner cli --file files/pe-Windows-x64-cmd
Handle files/pe-Windows-x64-cmd
pe-Windows-x64-cmd -- 0f3c4ff28f354aede202d54e9d1c5529a3bf87d8
[OK] Process ascii.py ran in 0.12 second(s)
[OK] Process unicode.py ran in 0.13 second(s)
[OK] Process ipv4.py ran in 0.13 second(s)
[OK] Process file.sh ran in 0.01 second(s)
[OK] Process checksums.sh ran in 0.05 second(s)
[OK] Process imports.hash.py ran in 0.23 second(s)
[OK] Process suspicious_strings.py ran in 0.4 second(s)
[OK] Process domain_names.py ran in 0.45 second(s)
[OK] Process packers.py ran in 0.33 second(s)
[OK] Process sections.py ran in 0.3 second(s)
[OK] Process suspicious_modules.py ran in 0.28 second(s)
[OK] Process suspicious_sections.py ran in 0.28 second(s)
[OK] Process exports.py ran in 0.24 second(s)
[OK] Process rich_header.py ran in 0.25 second(s)
[OK] Process subsystem.py ran in 0.24 second(s)
[OK] Process suspicious_imports.py ran in 0.28 second(s)
[OK] Process stamps.py ran in 0.49 second(s)
[OK] Process resources.py ran in 0.31 second(s)
[OK] Process authenticcode.py ran in 0.25 second(s)
```

... run the scanner ...

```
[OK] Process features.py ran in 2.87 second(s)
[OK] Process tight_strings.sh ran in 45.45 second(s)
[OK] Process stack_strings.sh ran in 48.69 second(s)
[OK] Process flare_caps.py ran in 68.91 second(s)
Extractors ran in 69.06 second(s) for 0f3c4ff28f354aede202d54e9d1c5529a3bf87d8
```

... under extractors/ ...

```
▼ strings
> __pycache__
> _bin
+ _strings.py
+ ascii.py
```

... collect output.

STRINGS/ASCII/STDOUT.LOG

```
offset,string,description
0x00004d,!This program cannot be run in DOS mode.,string in dos stub
0x0001d0,.text,
0x0001f7,.data,
0x000220,.rsrc,
0x000247,@.reloc,
0x0002a8,msvcrt.dll,
```


Installation

- `Python -m venv .env`
- `..env/bin/activate`
- `Pip install scanner.tar.gz`
- `Poetry run scanner`

