Supplementary

Reverse Engineering: Towards Malware Analysis

Lecture – pefile (and Python APIs you should know about)

Computer Science Practice

SPRING 2023

Python Arsenal

- Less known libraries
  - pefile
    - Ero Carrera
  - Vivisect (more on this later)
    - Invisigoth Kenshoto
- Have many security applications
- Good libraries to have in your arsenal

pefile

- Parses the PE file format
- Freely available
  - http://code.google.com/p/pefile/
- Robust API
- Can be used to modify the PE file quickly
- PEiD integration & signatures

pefile: How to Initialize?

- Easy for raw data

```
import pefile
try:
    pe = self.pefile.PE(data=data)
except self.pefile.PEFormatError as e:
    print "pefile error %s" % str(e)
```

- Easy for executable pathname too

```
pe = pefile.PE("/path/to/yourfile.exe")
```

pefile: Accessing PE Header

- Accessing PE header
  - `pe.dump_info()`
- Accessing individual fields
  - `pe.DOS_HEADER.e_magic`
  - `pe.FILE_HEADER.NumberOfSections`
- Why would you do the following?

```
ep = pe.OPTIONAL_HEADER.AddressOfEntryPoint
ep_ava = ep+pe.OPTIONAL_HEADER.ImageBase
```

pefile: Iterating

```
for section in pe.sections:

for entry in pe.DIRECTORY_ENTRY_IMPORT:
  for imp in entry.imports:

for exp in pe.DIRECTORY_ENTRY_EXPORT.symbols:
```

pefile: Section & Miscellaneous

`section.get_entropy()` – returns entropy of a section

`section.get_data()` – returns the data contents of a section

`section/export/import.name` – returns name of instance

peutils: Using PEiD Signatures

```
import peutils

signatures =
peutils.SignatureDatabase(self.sigfile)

try:
    pe = self.pefile.PE(data=data)
except self.pefile.PEFormatError:
    return ret

matches = signatures.match(pe,ep_only=True)
```