Writing YARA rules

An introduction to YARA for AIL usage

CIRCL
Computer Incident
Response Center
Luxembourg

Alexandre Dulaunoy
alexandre.dulaunoy@circl.lu
Jean-Louis Huynen
jean-louis.huynen@circl.lu

info@circl.lu

October 19, 2021

Links

- AIL project: `https://github.com/ail-project`
- AIL framework: `https://github.com/ail-project/ail-framework`
- Training materials: `https://github.com/ail-project/ail-training`
- YARA doc: `https://yara.readthedocs.io/en/stable/`
- YARA download: `http://virustotal.github.io/yara/`

What's YARA?

- *The pattern matching swiss knife for malware researchers (and everyone else)*;
- It's an improved **grep** to create pattern matching rule to search for **strings**, **binary patterns**, **regular expressions**;
- A YARA rule can be contextualised with metadata and tags describing a specific set of pattern matching rules.
- Easier definiton of conditions compared to regex.

A sample rule - disneyplus.yara

```
1   rule disney_plus : credential_leak
2 {
3       meta:
4           description = "Finding list of credentials for
      Disney Plus"
5           leak = 1
6       strings:
7           $a = "gmail.com:"
8           $b = "DISNEY_PLUS"
9           $c = "Disney Plus"
10      condition:
11          $a and ($b or $c)
12 }
13
```

Calling yara from command line

- Searching a single file

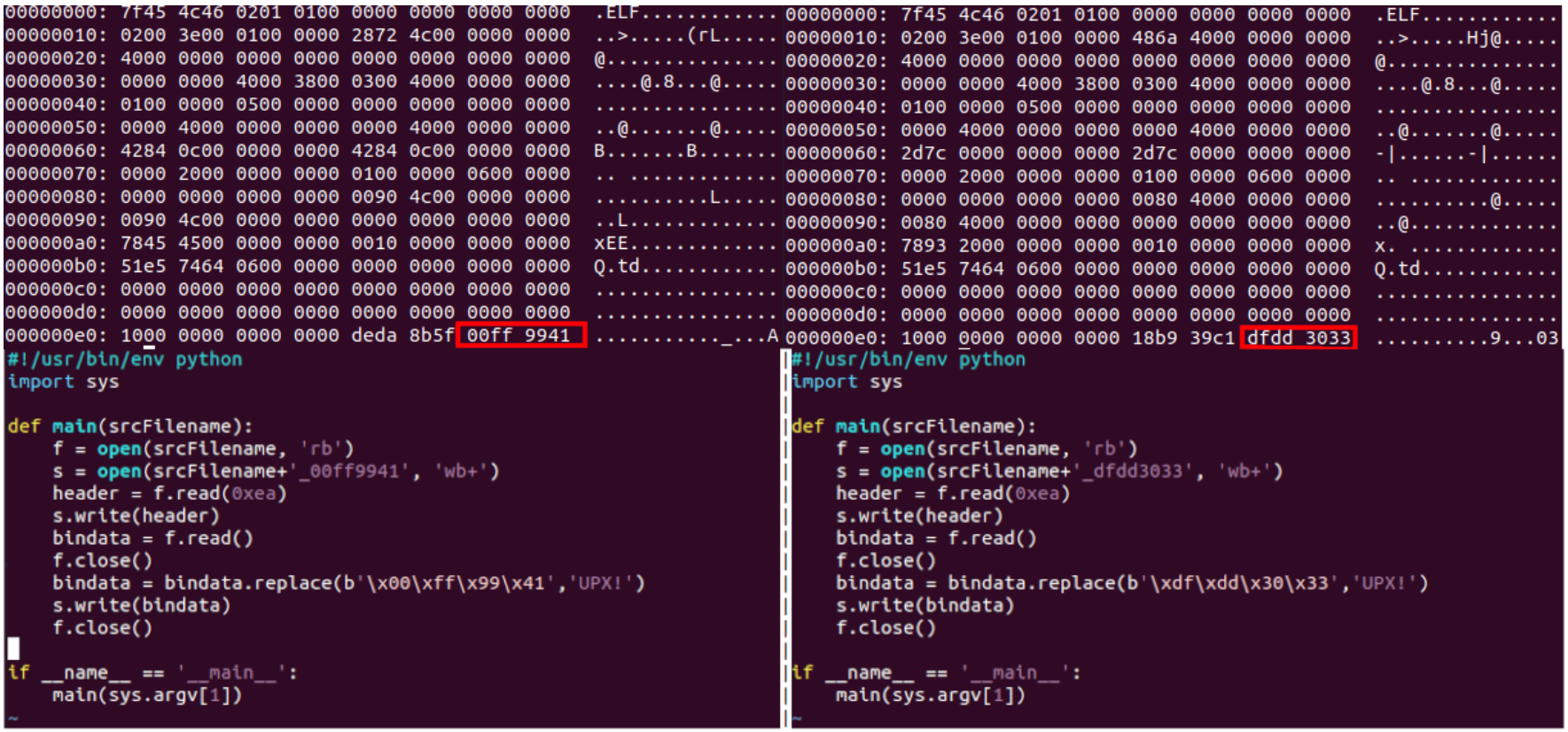
```
1 yara disneyplus.yara /home/adulau/dataset/2021/09/01/
      nv6RsKFm
2
```

- Searching a directory

```
1 yara disneyplus.yara -r /home/adulau/dataset
      /2021/09/01/
2
```

Searching in binaries

Binaries packed with UPX but made unusable by UPX -d by modifying the magic UPX string:



Searching in binaries

```
1 rule torcryptomining
2 {
3     strings:
4         $upx_erase = {(00 FF 99 41|DF DD 30 33)}
5     condition:
6   $upx_erase at 236
7 }
8
```