

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 definition 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
5         Disney Plus"
6         leak = 1
7     strings:
8         $a = "gmail.com:"
9         $b = "DISNEY_PLUS"
10        $c = "Disney Plus"
11    condition:
12        $a and ($b or $c)
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:

```
00000000: 7f45 4c46 0201 0100 0000 0000 0000 0000 .ELF.....00000000: 7f45 4c46 0201 0100 0000 0000 0000 0000 .ELF.....
00000010: 0200 3e00 0100 0000 2872 4c00 0000 0000 ..>....(rL...00000010: 0200 3e00 0100 0000 486a 4000 0000 0000 ..>....HJ@....
00000020: 4000 0000 0000 0000 0000 0000 0000 0000 @.....00000020: 4000 0000 0000 0000 0000 0000 0000 0000 @.....
00000030: 0000 0000 4000 3800 0300 4000 0000 0000 ....@.8...@....00000030: 0000 0000 4000 3800 0300 4000 0000 0000 ....@.8...@....
00000040: 0100 0000 0500 0000 0000 0000 0000 0000 ..@.....@....00000040: 0100 0000 0500 0000 0000 0000 0000 0000 ..@.....@....
00000050: 0000 4000 0000 0000 0000 4000 0000 0000 ..@.....@....00000050: 0000 4000 0000 0000 0000 4000 0000 0000 ..@.....@....
00000060: 4284 0c00 0000 0000 4284 0c00 0000 0000 B.....B.....00000060: 2d7c 0000 0000 0000 2d7c 0000 0000 0000 -|.....|.....
00000070: 0000 2000 0000 0000 0100 0000 0600 0000 ..@.....@....00000070: 0000 2000 0000 0000 0100 0000 0600 0000 ..@.....@....
00000080: 0000 0000 0000 0000 0090 4c00 0000 0000 .....L.....00000080: 0000 0000 0000 0000 0080 4000 0000 0000 .....L.....
00000090: 0090 4c00 0000 0000 0000 0000 0000 0000 ..@.....@....00000090: 0080 4000 0000 0000 0000 0000 0000 0000 ..@.....@....
000000a0: 7845 4500 0000 0000 0010 0000 0000 0000 xEE.....000000a0: 7893 2000 0000 0000 0010 0000 0000 0000 x.....
000000b0: 51e5 7464 0600 0000 0000 0000 0000 0000 Q.td.....000000b0: 51e5 7464 0600 0000 0000 0000 0000 0000 Q.td.....
000000c0: 0000 0000 0000 0000 0000 0000 0000 0000 .....000000c0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000d0: 0000 0000 0000 0000 0000 0000 0000 0000 .....000000d0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000e0: 10b9 0000 0000 0000 0000 0000 0000 0000 ....._..A.....000000e0: 10b9 39c1 dfdd 3033 .....9...03
#!/usr/bin/env python
import sys

def main(srcFilename):
    f = open(srcFilename, 'rb')
    s = open(srcFilename+'_00ff9941', 'wb+')
    header = f.read(0xea)
    s.write(header)
    bindata = f.read()
    f.close()
    bindata = bindata.replace(b'\x00\xff\x99\x41', 'UPX!')
    s.write(bindata)
    f.close()

if __name__ == '__main__':
    main(sys.argv[1])

#!/usr/bin/env python
import sys

def main(srcFilename):
    f = open(srcFilename, 'rb')
    s = open(srcFilename+'_dfdd3033', 'wb+')
    header = f.read(0xea)
    s.write(header)
    bindata = f.read()
    f.close()
    bindata = bindata.replace(b'\xdf\xdd\x30\x33', 'UPX!')
    s.write(bindata)
    f.close()

if __name__ == '__main__':
    main(sys.argv[1])
```

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
```