YARA RULES CHEATSHEET

INSTALLATION

Download the source code, then:

```
> tar -zxf yara-4.0.0.tar.gz
> cd yara-4.0.0
> ./bootstrap.sh
```

Install dependencies:

```
> sudo apt-get install automake libtool
  make gcc pkg-config
```

Compile and install:

```
> ./configure
> make
> sudo make install
```

Run tests:

```
> make check
```

METADATA

Useful meta information examples to add:

- description = "Short description about rule"
- author = "The Author"
- reference = "http://www.somereference.com"
- date = "2020-09"
- md5 = "7b1311d460b8e04ab4d550a9f5233203"

STRINGS

Available modifiers:

- fullword //not substrings
- ascii //ascii values
- wide //unicode values
- nocase //ignore case
- xor //find xored strings
- base64 //find base64 encoded strings
- base64wide //same but for unicode

Types of strings:

- $text_string = "text here"
- $hex_string = { EB FE [2-4] ?? (13 37 | 73 31 }
  - ? wild card, [2-4] arbitrary bytes, (x | y) = (x or y)
- $regex_string = /md5: [0-9a-zA-Z]{32}/

SPECIAL RULES

Global Rule:

It will be evaluated before the rest of the rules, which in turn will be evaluated only if all global rules are satisfied.

Private Rule:

These are not reported by YARA when they match on a given file.

CONDITIONS

- Boolean operators and, or, not
- Relational operators >=, <=, <, >, ==, !=
- Arithmetic operators +,-,*,\, %
- Bitwise operators &, |, <<, >>, ~, ^

Available keywords:

- all of them //all strings in the rule
- any of them // any string in the rule
- 3 of them //at least 3 strings in the rule
- all of ($a*) //all strings whose identifier starts by $a
- any of ($a,$b,$c) // any of $a, $b or $c
- 1 of ($*) // same that "any of them"

Useful conditions:

- uint16(0) == 0x5A4D // MZ signature at offset 0
- filesize < 2MB //to check filesize
- for expression of string_set : (boolean_expression)

```
rule example_rule: banker {
  meta:
    description = "This is just an example"
  strings:
    $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
    $b = "Some string"
  condition:
    $a or $b
}
```

Ayelen Torello @cyb3rhuskys & Fernanda Billordo Zini @cyb3rR4v3n

YARA RULES CHEATSHEET

INSTALLATION

Download the source code, then:

```
> tar -zxf yara-4.0.0.tar.gz
> cd yara-4.0.0
> ./bootstrap.sh
```

Install dependencies:

```
> sudo apt-get install automake libtool
make gcc pkg-config
```

Compile and install:

```
> ./configure
> make
> sudo make install
```

Run tests:

```
> make check
```

METADATA

Useful meta information examples to add:

- **description = "Short description about rule"**
- **author = "The Author"**
- **reference = "http://www.somereference.com"**
- date = "2020-09"
- **md5 = "7b1311d460b8e04ab4d550a9f5233203"**

STRINGS

Available modifiers:

- **fullword** //not substrings
- **ascii** //ascii values
- **wide** //unicode values
- **nocase** //ignore case
- **xor** //find xored strings
- **base64** //find base64 encoded strings
- **base64wide** //same but for unicode

Types of strings:

- **$text_string** = "text here"
- **$hex_string** = { EB FE [2-4] ?? (13 37 | 73 31 }
  - **? wild card, [2-4] arbitrary bytes, (x | y) = (x or y)**
- **$regex_string** = /md5: [0-9a-zA-Z]{32}/

SPECIAL RULES

Global Rule:

It will be evaluated before the rest of the rules, which in turn will be evaluated only if all global rules are satisfied.

Private Rule:

These are not reported by YARA when they match on a given file.

CONDITIONS

- Boolean operators **and**, **or**, **not**
- Relational operators **>=**, **<=**, **<**, **>**, **==**, !=
- Arithmetic operators **+**,**-**,*,\, %
- Bitwise operators **&**, |, **<<**, **>>**, ~, **^**

Available keywords:

- **all of them** //all strings in the rule
- **any of them** // any string in the rule
- **3 of them** //at least 3 strings in the rule
- **all of ($a*)** //all strings whose identifier starts by $a
- **any of ($a,$b,$c)** // any of $a, $b or $c
- **1 of ($*)** // same that "any of them"

Useful conditions:

- **uint16(0)** == 0x5A4D // MZ signature at offset 0
- **filesize** < 2MB //to check filesize
- **for** expression **of** string_set **:** (boolean_expression)

```
rule example_rule: banker {
   meta:
      description = "This is just an example"
   strings:
      $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
      $b = "Some string"
   condition:
      $a or $b
}
```

Ayelen Torello @cyb3rhuskys & Fernanda Billordo Zini @cyb3rR4v3n