Hunting Evil with YARA (Web Edition)

Unpac.Me is tool tailored for malware unpacking. The great thing about `Unpac.Me` is that it grants us the capability to run our YARA rules over their amassed database of malware submissions. Considering the hurdles of gaining access to commercialized malware datasets, Unpac.Me emerges as a prime asset for those dedicated SOC analysts and persistent malware enthusiasts.

Hunting for Evil Within Online Datasets with YARA

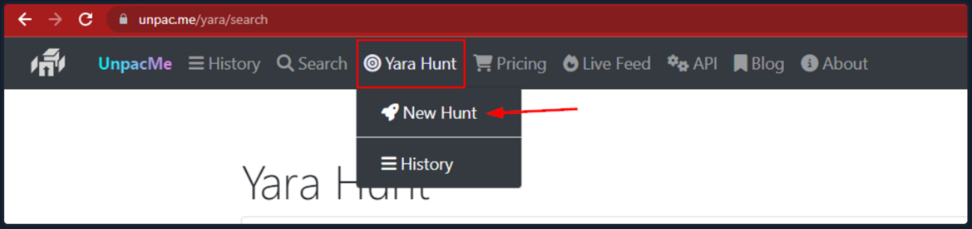
Suppose we want to test out the following YARA rule.

Code: yara

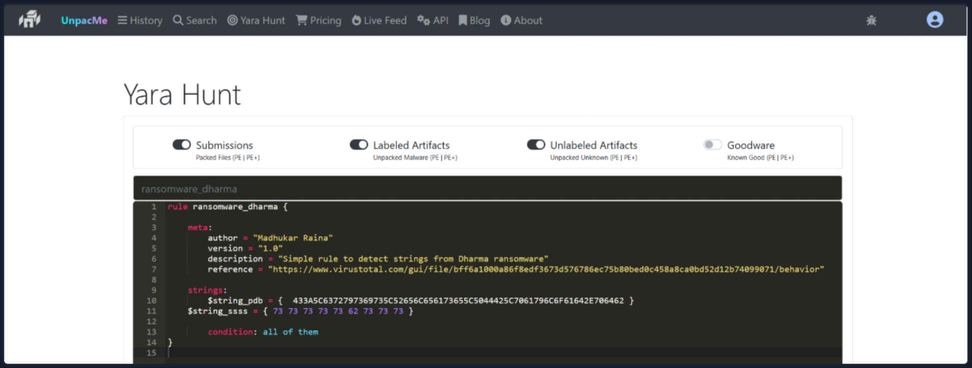
```
rule ransomware_dharma {

    meta:
        author = "Madhukar Raina"
        version = "1.0"
        description = "Simple rule to detect strings from Dharma ransomware"
        reference = "https://www.virustotal.com/gui/file/bff6a1000a86f8edf3673d576786ec75b80bed0c45

    strings:
        $string_pdb = {  433A5C6372797369735C52656C656173655C5044425C7061796C6F61642E706462 }
    $string_ssss = { 73 73 73 73 73 62 73 73 73 }

        condition: all of them
}
```

So, how do we get started?

- Register for zero-cost access and hop into the platform.
- Head over to `Yara Hunt` and choose `New Hunt`.



- Enter the YARA rule into the designated rule space.



Yara Hunt

● Submissions Packed Files (PE | PE+)
● Labeled Artifacts Unpacked Malware (PE | PE+)
● Unlabeled Artifacts Unpacked Unknown (PE | PE+)
○ Goodware Known Good (PE | PE+)

ransomware_dharma

```
rule ransomware_dharma {

    meta:
        author = "Madhukar Raina"
        version = "1.0"
        description = "Simple rule to detect strings from Dharma ransomware"
        reference = "https://www.virustotal.com/gui/file/bff6a1000a86f8edf3673d576786ec75b80bed0c458a8ca0bd52d12b74099071/behavior"

    strings:
        $string_pdb = {  433A5C6372797369735C52656C656173655C5044425C7061796C6F61642E706462 }
    $string_ssss = { 73 73 73 73 73 62 73 73 73 }

        condition: all of them
}
```

- First hit `Validate` and then `Scan`.

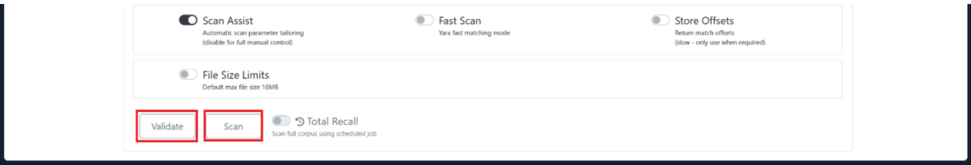
Table of Contents

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left



Scan Assist
Automatic scan parameter tailoring
(disable for full manual control)

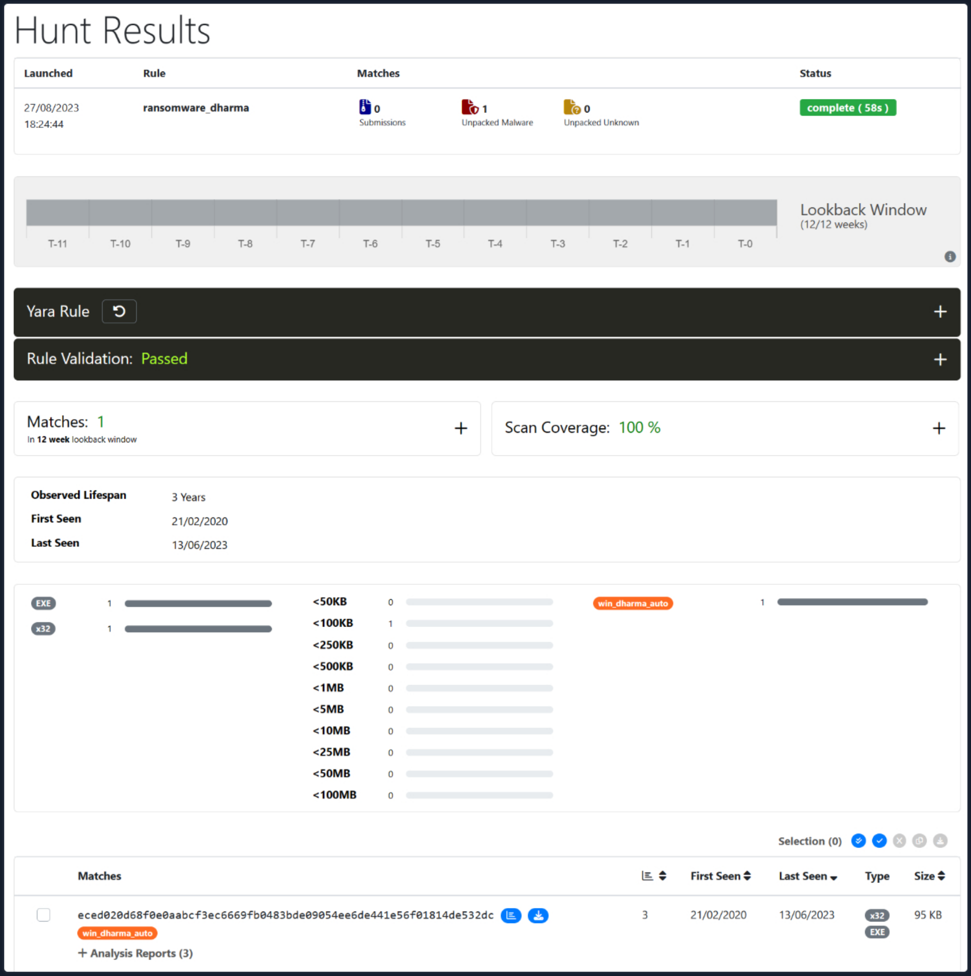
Fast Scan
Yara fast matching mode

Store Offsets
Return match offsets
(slow - only use when required)

File Size Limits
Default max file size 16MB

Total Recall
Scan full corpus using scheduled job

- Scan results get displayed right in front of our eyes. Taking a quick glance at our example, the system hustled through all malware submissions in a couple of minutes, spotting 1 match.



Hunt Results

Launched	Rule	Matches			Status
27/08/2023 18:24:44	ransomware_dharma	0 Submissions	1 Unpacked Malware	0 Unpacked Unknown	complete (58s)

Lookback Window
(12/12 weeks)

Yara Rule

Rule Validation: Passed

Matches: 1
In **12 week** lookback window

Scan Coverage: 100 %

Observed Lifespan	3 Years
First Seen	21/02/2020
Last Seen	13/06/2023

EXE	1
x32	1

<50KB	0
<100KB	1
<250KB	0
<500KB	0
<1MB	0
<5MB	0
<10MB	0
<25MB	0
<50MB	0
<100MB	0

win_dharma_auto	1

Selection (0)

	Matches		First Seen	Last Seen	Type	Size
□	eced020d68f0e0aabcf3ec6669fb0483bde09054ee6de441e56f01814de532dc win_dharma_auto + Analysis Reports (3)	3	21/02/2020	13/06/2023	x32 EXE	95 KB

For individuals and organizations with limited resources, Unpac.Me and similar platforms can serve as stepping stones to enhance their malware analysis and detection capabilities, enabling them to make meaningful contributions to the field of cybersecurity.

Previous   Next   Mark Complete & Next