REVERSING 2020

CLOSING

TOMISLAV PERIČIN

Chief Software Architect &
Co-Founder, ReversingLabs

QUALITY WRITTEN YARA RULES - DETECTION RULES WORTH THEIR WEIGHT IN GOLD

TOMISLAV PERIČIN

Chief Software Architect at ReversingLabs

One of the founders of **ReversingLabs**
Presenter at conferences: BlackHat, ReCon, CARO Workshop, SAS and TechnoSecurity.

Developer on such projects as TitaniumCore, TitanEngine, NyxEngine and RLPack.

@ap0x

{YARA at ReversingLabs

2013 - 2015

Integrated YARA into TitaniumCore

Started including YARA threat detection rules in our products

Patch contributions to YARA code base

2016

Showing YARA match information

Automatic YARA ruleset versioning

Included .NET and hash modules

2017

Enabled suspicious classifications

2018

Integrated with TitaniumCore format identification and unpacking

2019

Using YARA metadata to name detected threats

Extended YARA to support more than 32 threads

2020

Explainable YARA rules

{YARA dilemma: Threat detection or hunting?

Detection

- **Goal:** Malware detection & blocking
- Pro:
  - Can accurately detect malware threats
  - Can block for malware based on artifacts
  - Can be deployed to scan files or memory
- Con:
  - Requires time to write & test correctly
  - Can be bypassed with pattern breaking

Hunting

- **Goal:** Proactive analysis & detection
- Pro:
  - Can find new interesting things to analyze
  - Can be broad to cover multiple formats
  - Can look for things other than malware
- Con:
  - Requires time consuming human analysis
  - Can generate lots of false positives

{YARA threat detection rule goals

1. Clean written YARA rules with well labeled conditions

```
    strings:
        $find_files = {
...
        }
        $encrypt_files = {
...
        }
        $enum_shares = {
...
        }
    condition:
        uint16(0) == 0x5A4D and
        (
            $find_files and
            $encrypt_files and
            $enum_shares
        )
```

{YARA threat detection rule goals

2. Matching on unique malware type functionality

```
    strings:
        $find_files = {
...
        }
        $encrypt_files = {
...
        }
        $enum_shares = {
...
        }
    condition:
        uint16(0) == 0x5A4D and
        (
            $find_files and
            $encrypt_files and
            $enum_shares
        )
```

{YARA threat detection rule goals

3. Preferring code byte pattern matching over strings

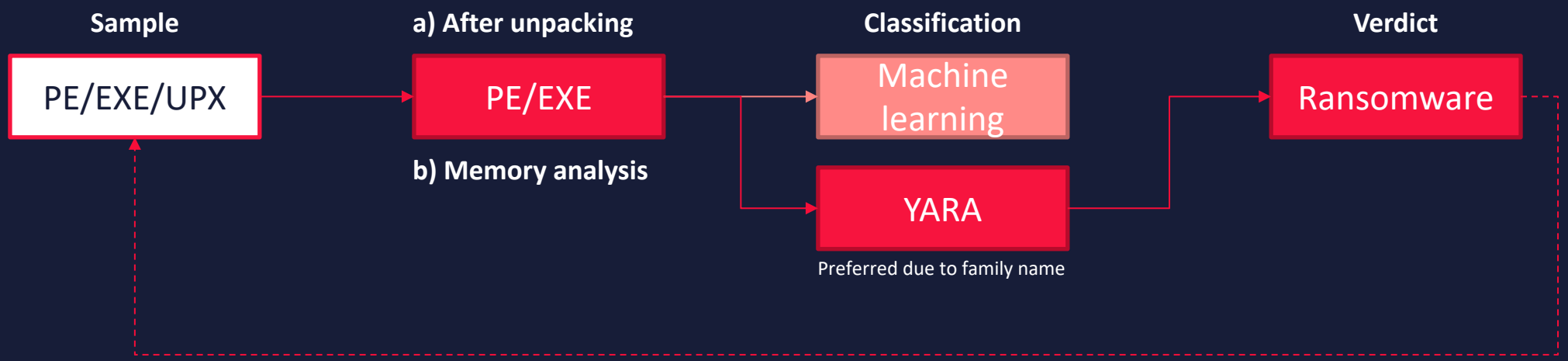
```
    strings:

        $find_files = {
            8B FF 55 8B EC 51 8B 4D ?? 8D 51 ?? 8A 01 41 84 C0 75 ?? 57 8B 7D ?? 2B CA 8B C7 41
...
        }

        $encrypt_files = {
            55 8B EC 83 E4 ?? B8 ?? ?? ?? ?? E8 ?? ?? ?? ?? A1 ?? ?? ?? ?? 33 C4 89 84 24 ?? ??
...
        }

        $enum_shares = {
            55 8B EC 6A ?? 68 ?? ?? ?? ?? 64 A1 ?? ?? ?? ?? 50 83 EC ?? A1 ?? ?? ?? ?? 33 C5 89
...
        }

    condition:
        uint16(0) == 0x5A4D and
        (
            $find_files and
            $encrypt_files and
            $enum_shares
        )
```

{YARA threat detection rule goals

4. Native classification pipeline integration

```
rule Win32_Ransomware_DesuCrypt : tc_detection malicious
{
    meta:

        tc_detection_type   = "Ransomware"
        tc_detection_name   = "DesuCrypt"
        tc_detection_factor = 5

    strings:

        $find_files = {
...
        }

...

    condition:
        uint16(0) == 0x5A4D and
        (
            $find_files and
            $encrypt_files and
            $enum_shares
        )
}
```

{YARA threat detection within layered objects



{YARA threat detection results

{YARA threat detection results

JoeSandbox Ultimate

Overview ▾ | Startup | Dropped | Domains / IPs | Static | Network | Hooks | Stats | Behavior ▾ | Disassembly ▾

Yara Overview

Memory Dumps

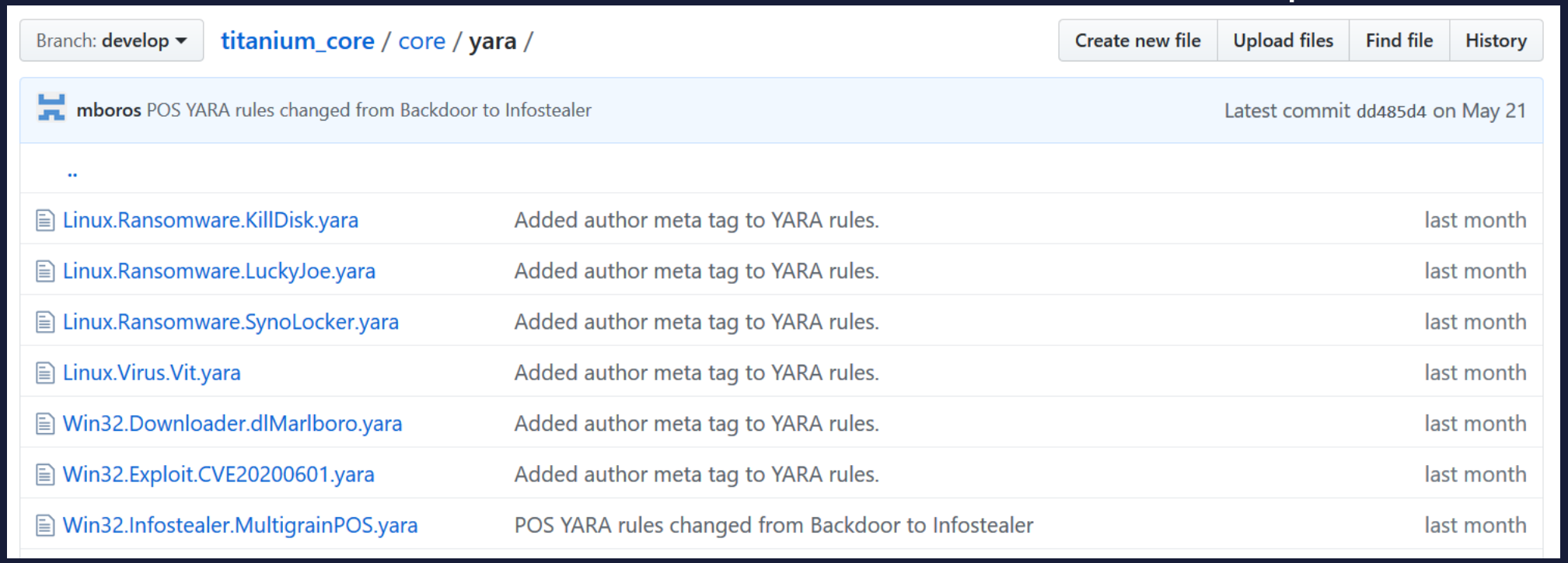
Source	Rule	Description	Author	Strings
00000000.00000002.267216487.0000000000271000.00000020.00000001.sdmp	Win32_Trojan_Emotet	unknown	ReversingLabs	• 0x1b70:$decrypt_resource_v2: 55 8B EC 83 EC 0C 8B 41 04 8B 11 33 C2 53 56 8D 71 04 89 55 FC 8D 58 01 89 45 F8 83 C6 04 F6 C3 ... • 0x6bb0:$generate_filename_v2: 55 8B EC 81 EC 08 02 00 00 8D 85 F8 FD FF FF 50 6A 00 6A 00 51 6A 00 B9 01 E9 E7 C0 E8 5F B9 FF ...
00000000.00000002.267199670.0000000000260000.00000040.00000001.sdmp	Win32_Trojan_Emotet	unknown	ReversingLabs	• 0x24af:$decrypt_resource_v2: 55 8B EC 83 EC 0C 8B 41 04 8B 11 33 C2 53 56 8D 71 04 89 55 FC 8D 58 01 89 45 F8 83 C6 04 F6 C3 ... • 0x74ef:$generate_filename_v2: 55 8B EC 81 EC 08 02 00 00 8D 85 F8 FD FF FF 50 6A 00 6A 00 51 6A 00 B9 01 E9 E7 C0 E8 5F B9 FF ...
00000003.00000002.507867622.0000000000270000.00000040.00000001.sdmp	Win32_Trojan_Emotet	unknown	ReversingLabs	• 0x24af:$decrypt_resource_v2: 55 8B EC 83 EC 0C 8B 41 04 8B 11 33 C2 53 56 8D 71 04 89 55 FC 8D 58 01 89 45 F8 83 C6 04 F6 C3 ... • 0x74ef:$generate_filename_v2: 55 8B EC 81 EC 08 02 00 00 8D 85 F8 FD FF FF 50 6A 00 6A 00 51 6A 00 B9 01 E9 E7 C0 E8 5F B9 FF ...
00000003.00000002.508160792.0000000000461000.00000020.00000001.sdmp	Win32_Trojan_Emotet	unknown	ReversingLabs	• 0x1b70:$decrypt_resource_v2: 55 8B EC 83 EC 0C 8B 41 04 8B 11 33 C2 53 56 8D 71 04 89 55 FC 8D 58 01 89 45 F8 83 C6 04 F6 C3 ... • 0x6bb0:$generate_filename_v2: 55 8B EC 81 EC 08 02 00 00 8D 85 F8 FD FF FF 50 6A 00 6A 00 51 6A 00 B9 01 E9 E7 C0 E8 5F B9 FF ...

Unpacked PEs

No yara matches

ReversingLabs Open Source {YARA rules

https://github.com/reversinglabs/reversinglabs-yara-rules 128 YARA Rules published



ReversingLabs Open Source rules require **YARA** version **3.2.0** or newer to be installed. Additionally, the following YARA modules need to be enabled: **PE** and **ELF**.

Q/A

TOMISLAV PERIČIN

Chief Software Architect &
Co-Founder, ReversingLabs

QUALITY WRITTEN YARA RULES - DETECTION RULES WORTH THEIR WEIGHT IN GOLD

TRIVIA

1. Which version of YARA introduced the "pdb_path" function to the "pe" module which can match a string that contains the Program Database path?

- **a.** 4.0.0
- **b.** 3.9.0
- **c.** 3.11.0
- **d.** 3.7.0

2. What are two of the three hash algorithm functions in YARA's hash module that are not based on a version of SHA?

- **a.** MD5, Checksum32, crc32 (any two of these)
- **b.** SHA3

3. Which version of YARA introduced the "time" module which allows the rule writer to make time comparisons in a rule's conditions?

- **a.** 3.7.0
- **b.** 1.4.0
- **c.** 2.5.0
- **d.** 3.11.0

4. Which condition should be used today in the current version of YARA to signify the entry point of a PE file?

- **a.** pe.entry_point
- **b.** entrypoint

5. According to YARA's documentation, how many modules are included with YARA?

- **a.** 8
- **b.** 6
- **c.** 10
- **d.** 4

6. If you want to match a string which has null bytes interleaved between the bytes of the string one wishes to match, which string modifier does one use?

- **a.** wide
- **b.** xor
- **c.** ascii
- **d.** base64

7. Which operator should be used in the condition to match a substring in a condition that evaluates to a string?

- **a.** contains
- **b.** in
- **c.** under
- **d.** at

REVERSING 2020

THANK YOU

REVERSING 2020