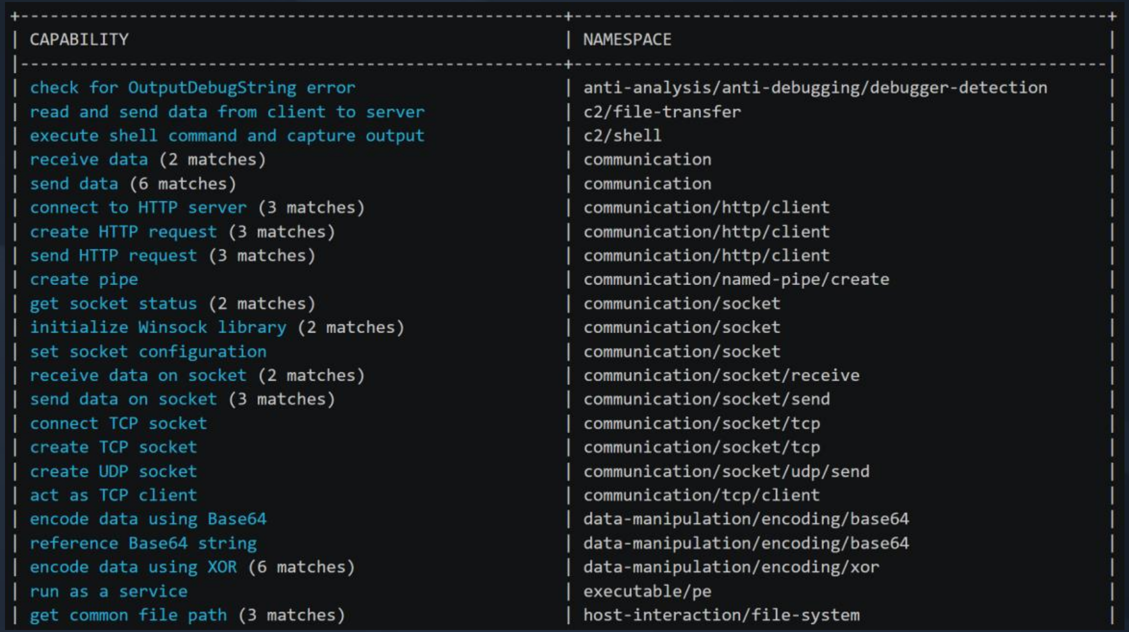
CAPA

Automatically Identify Malware Capabilities

Willi Ballenthin, Moritz Raabe
FLARE Reverse Engineers



```
+-------------------------------------------------------+-----------------------------------------------------+
| CAPABILITY                                            | NAMESPACE                                           |
|-------------------------------------------------------+-----------------------------------------------------|
| check for OutputDebugString error                     | anti-analysis/anti-debugging/debugger-detection     |
| read and send data from client to server              | c2/file-transfer                                    |
| execute shell command and capture output              | c2/shell                                            |
| receive data (2 matches)                              | communication                                       |
| send data (6 matches)                                 | communication                                       |
| connect to HTTP server (3 matches)                    | communication/http/client                           |
| create HTTP request (3 matches)                       | communication/http/client                           |
| send HTTP request (3 matches)                         | communication/http/client                           |
| create pipe                                           | communication/named-pipe/create                     |
| get socket status (2 matches)                         | communication/socket                                |
| initialize Winsock library (2 matches)                | communication/socket                                |
| set socket configuration                              | communication/socket                                |
| receive data on socket (2 matches)                    | communication/socket/receive                        |
| send data on socket (3 matches)                       | communication/socket/send                           |
| connect TCP socket                                    | communication/socket/tcp                            |
| create TCP socket                                     | communication/socket/tcp                            |
| create UDP socket                                     | communication/socket/udp/send                       |
| act as TCP client                                     | communication/tcp/client                            |
| encode data using Base64                              | data-manipulation/encoding/base64                   |
| reference Base64 string                               | data-manipulation/encoding/base64                   |
| encode data using XOR (6 matches)                     | data-manipulation/encoding/xor                      |
| run as a service                                      | executable/pe                                       |
| get common file path (3 matches)                      | host-interaction/file-system                        |
```

FIREEYE™ | MANDIANT®

FLARE

Willi Ballenthin
williballenthin

Moritz Raabe
m_r_tz

Contributors

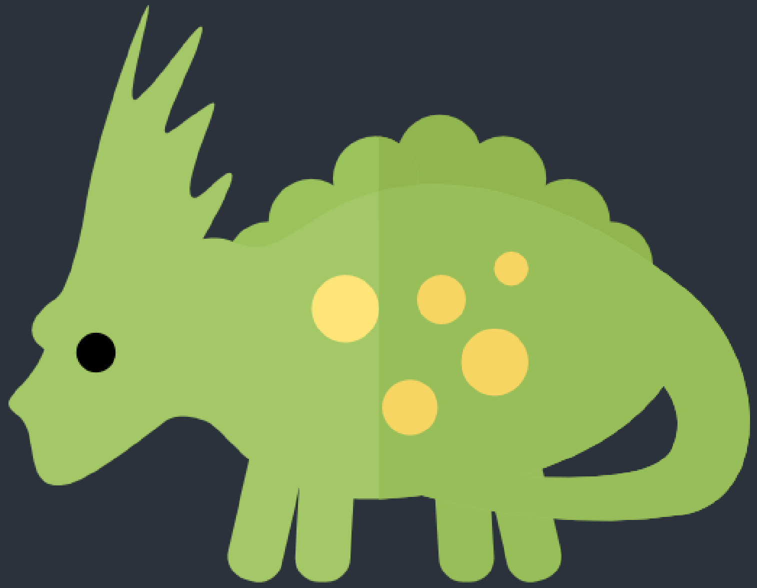
Ana Maria Martinez Gomez, Mike Hunhoff, Blaine Stancill,
Matt Williams, and rest of FLARE (~200 years RE experience)

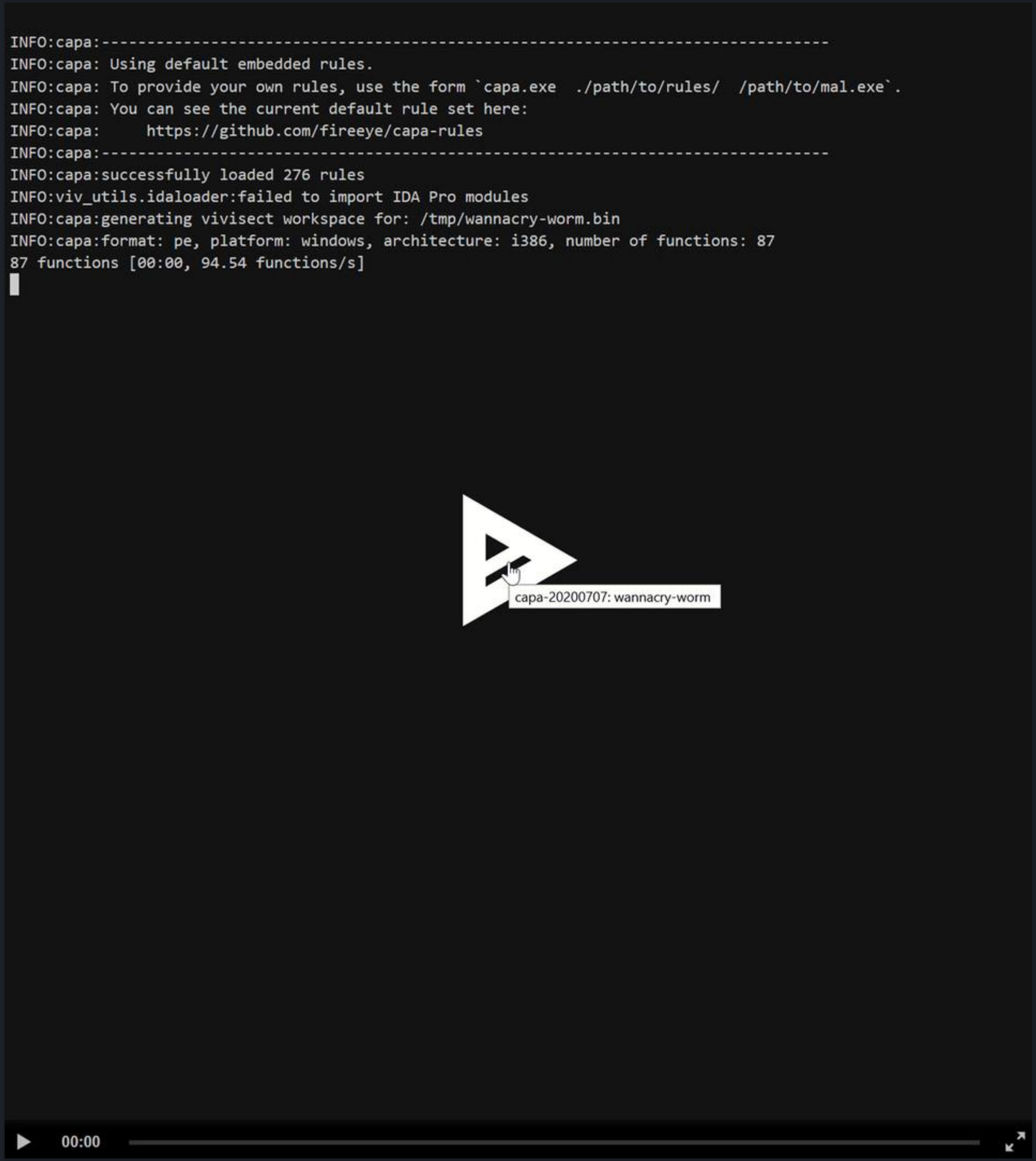
Welcome to #ballenthin-raabe!

CAPA analyzes a program and identifies things the program could do.

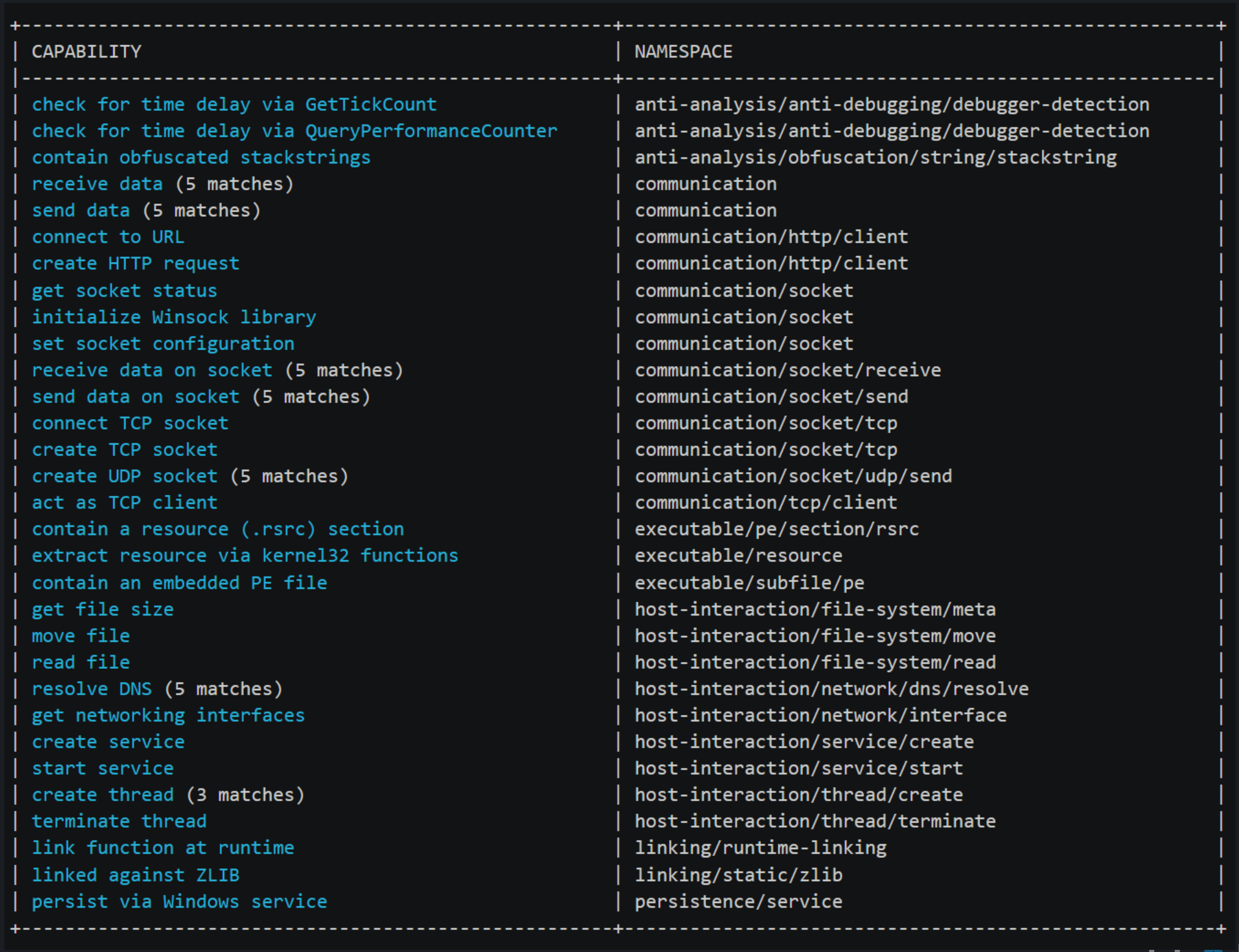
CAPA uses rules,
written by experts,
to recognize these capabilities.

CAPA vs Wannacry worm



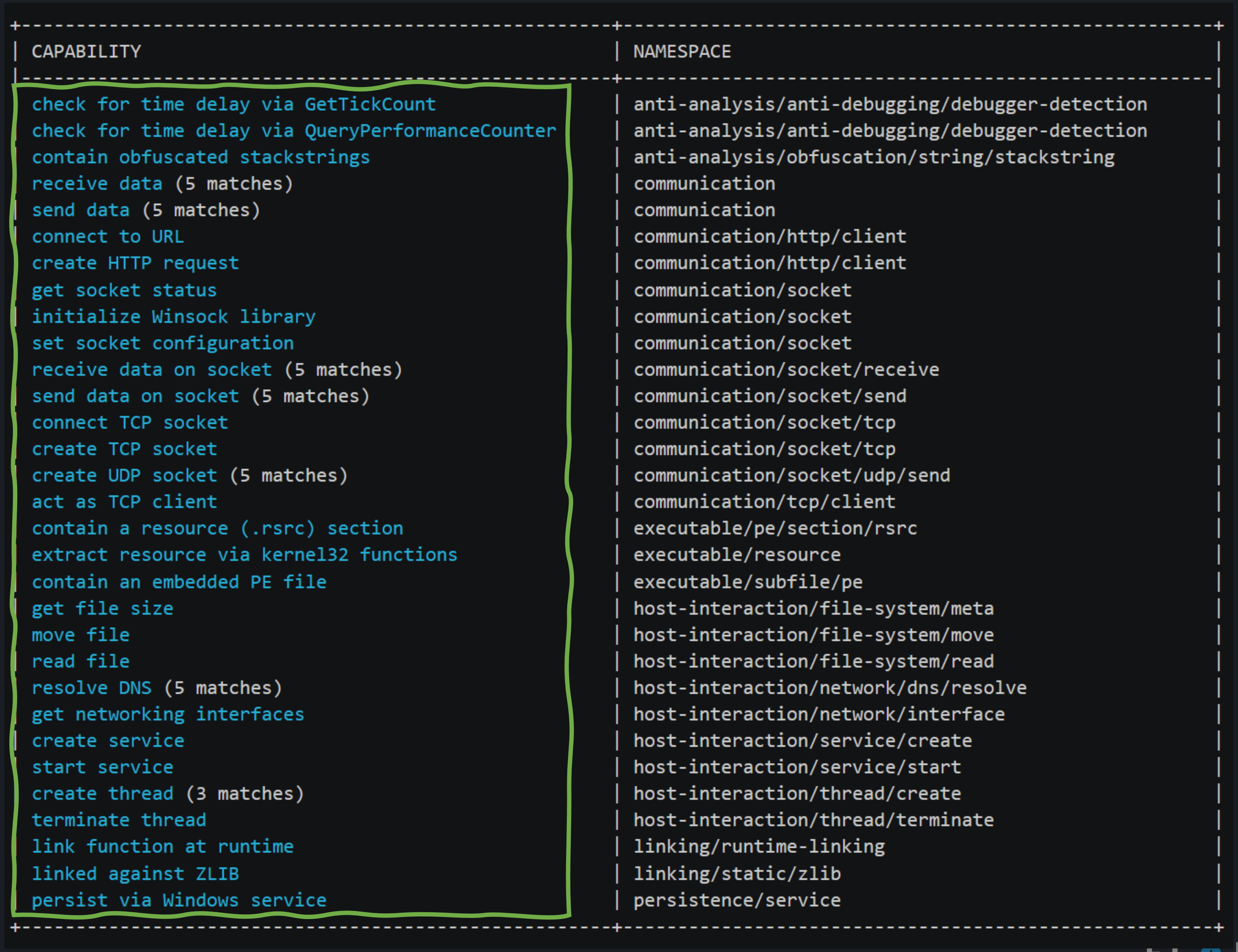


```
INFO:capa:--------------------------------------------------------------------------------
INFO:capa: Using default embedded rules.
INFO:capa: To provide your own rules, use the form `capa.exe  ./path/to/rules/  /path/to/mal.exe`.
INFO:capa: You can see the current default rule set here:
INFO:capa:     https://github.com/fireeye/capa-rules
INFO:capa:--------------------------------------------------------------------------------
INFO:capa:successfully loaded 276 rules
INFO:viv_utils.idaloader:failed to import IDA Pro modules
INFO:capa:generating vivisect workspace for: /tmp/wannacry-worm.bin
INFO:capa:format: pe, platform: windows, architecture: i386, number of functions: 87
87 functions [00:00, 94.54 functions/s]
```



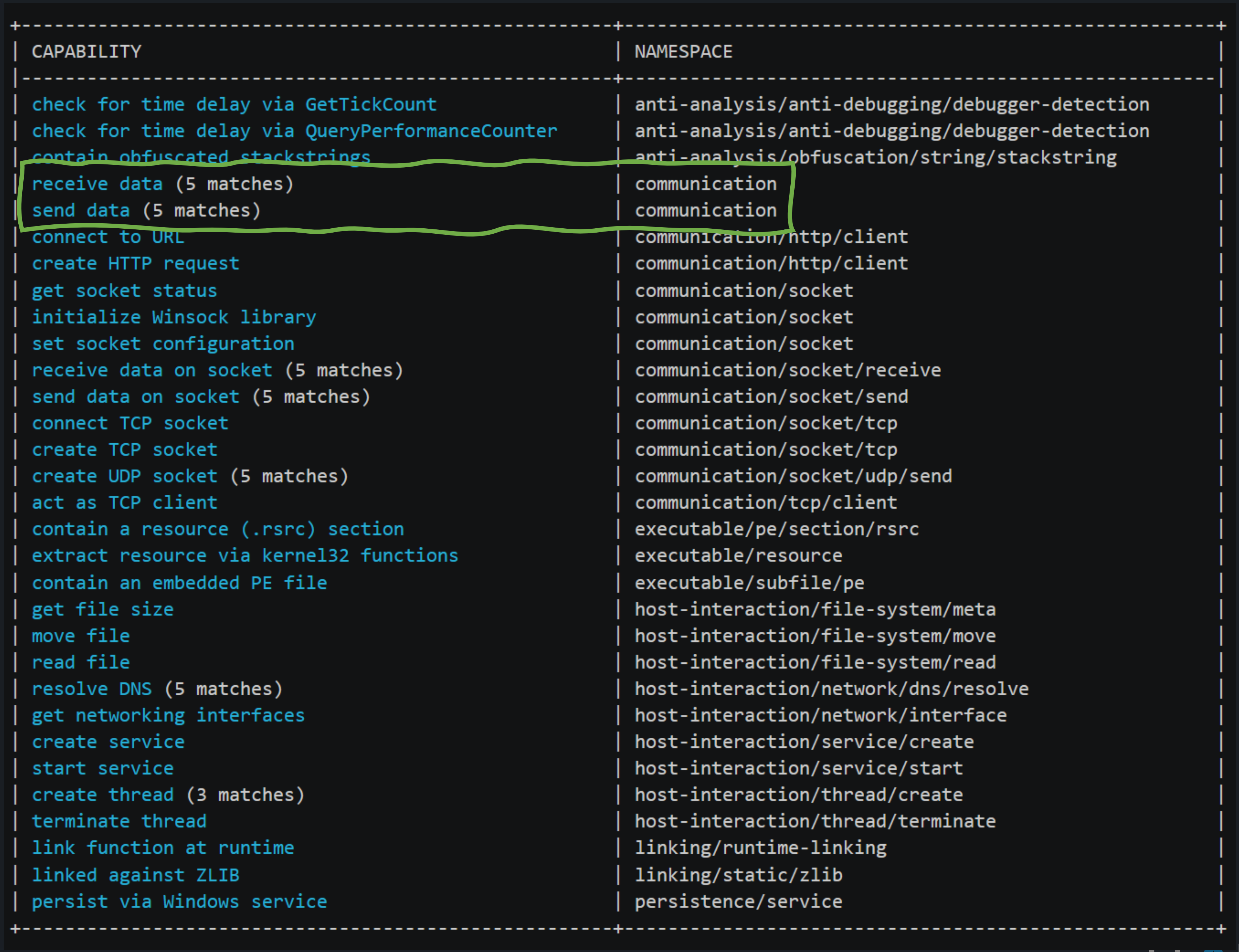
```
+------------------------------------------------------+------------------------------------------------------+
| CAPABILITY                                           | NAMESPACE                                            |
|------------------------------------------------------+------------------------------------------------------|
| check for time delay via GetTickCount                | anti-analysis/anti-debugging/debugger-detection      |
| check for time delay via QueryPerformanceCounter     | anti-analysis/anti-debugging/debugger-detection      |
| contain obfuscated stackstrings                      | anti-analysis/obfuscation/string/stackstring         |
| receive data (5 matches)                             | communication                                        |
| send data (5 matches)                                | communication                                        |
| connect to URL                                       | communication/http/client                            |
| create HTTP request                                  | communication/http/client                            |
| get socket status                                    | communication/socket                                 |
| initialize Winsock library                           | communication/socket                                 |
| set socket configuration                             | communication/socket                                 |
| receive data on socket (5 matches)                   | communication/socket/receive                         |
| send data on socket (5 matches)                      | communication/socket/send                            |
| connect TCP socket                                   | communication/socket/tcp                             |
| create TCP socket                                    | communication/socket/tcp                             |
| create UDP socket (5 matches)                        | communication/socket/udp/send                        |
| act as TCP client                                    | communication/tcp/client                             |
| contain a resource (.rsrc) section                   | executable/pe/section/rsrc                           |
| extract resource via kernel32 functions              | executable/resource                                  |
| contain an embedded PE file                          | executable/subfile/pe                                |
| get file size                                        | host-interaction/file-system/meta                    |
| move file                                            | host-interaction/file-system/move                    |
| read file                                            | host-interaction/file-system/read                    |
| resolve DNS (5 matches)                              | host-interaction/network/dns/resolve                 |
| get networking interfaces                            | host-interaction/network/interface                   |
| create service                                       | host-interaction/service/create                      |
| start service                                        | host-interaction/service/start                       |
| create thread (3 matches)                            | host-interaction/thread/create                       |
| terminate thread                                     | host-interaction/thread/terminate                    |
| link function at runtime                             | linking/runtime-linking                              |
| linked against ZLIB                                  | linking/static/zlib                                  |
| persist via Windows service                          | persistence/service                                  |
+------------------------------------------------------+------------------------------------------------------+
```

names of capabilities



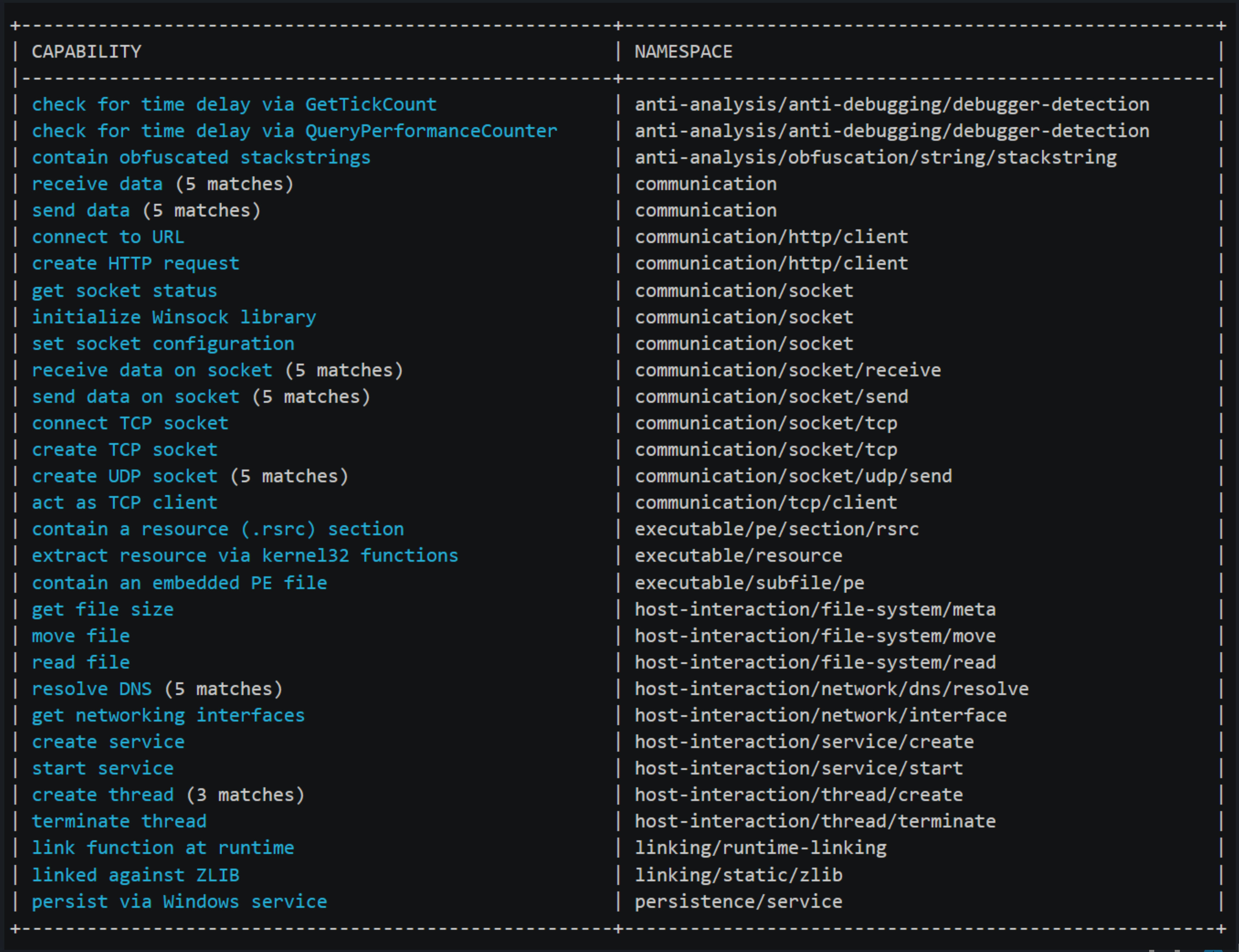
```
+------------------------------------------------------+------------------------------------------------------+
| CAPABILITY                                           | NAMESPACE                                            |
|------------------------------------------------------+------------------------------------------------------|
| check for time delay via GetTickCount                | anti-analysis/anti-debugging/debugger-detection      |
| check for time delay via QueryPerformanceCounter     | anti-analysis/anti-debugging/debugger-detection      |
| contain obfuscated stackstrings                      | anti-analysis/obfuscation/string/stackstring         |
| receive data (5 matches)                             | communication                                        |
| send data (5 matches)                                | communication                                        |
| connect to URL                                       | communication/http/client                            |
| create HTTP request                                  | communication/http/client                            |
| get socket status                                    | communication/socket                                 |
| initialize Winsock library                           | communication/socket                                 |
| set socket configuration                             | communication/socket                                 |
| receive data on socket (5 matches)                   | communication/socket/receive                         |
| send data on socket (5 matches)                      | communication/socket/send                            |
| connect TCP socket                                   | communication/socket/tcp                             |
| create TCP socket                                    | communication/socket/tcp                             |
| create UDP socket (5 matches)                        | communication/socket/udp/send                        |
| act as TCP client                                    | communication/tcp/client                             |
| contain a resource (.rsrc) section                   | executable/pe/section/rsrc                           |
| extract resource via kernel32 functions              | executable/resource                                  |
| contain an embedded PE file                          | executable/subfile/pe                                |
| get file size                                        | host-interaction/file-system/meta                    |
| move file                                            | host-interaction/file-system/move                    |
| read file                                            | host-interaction/file-system/read                    |
| resolve DNS (5 matches)                              | host-interaction/network/dns/resolve                 |
| get networking interfaces                            | host-interaction/network/interface                   |
| create service                                       | host-interaction/service/create                      |
| start service                                        | host-interaction/service/start                       |
| create thread (3 matches)                            | host-interaction/thread/create                       |
| terminate thread                                     | host-interaction/thread/terminate                    |
| link function at runtime                             | linking/runtime-linking                              |
| linked against ZLIB                                  | linking/static/zlib                                  |
| persist via Windows service                          | persistence/service                                  |
+------------------------------------------------------+------------------------------------------------------+
```

groups of similar capabilities

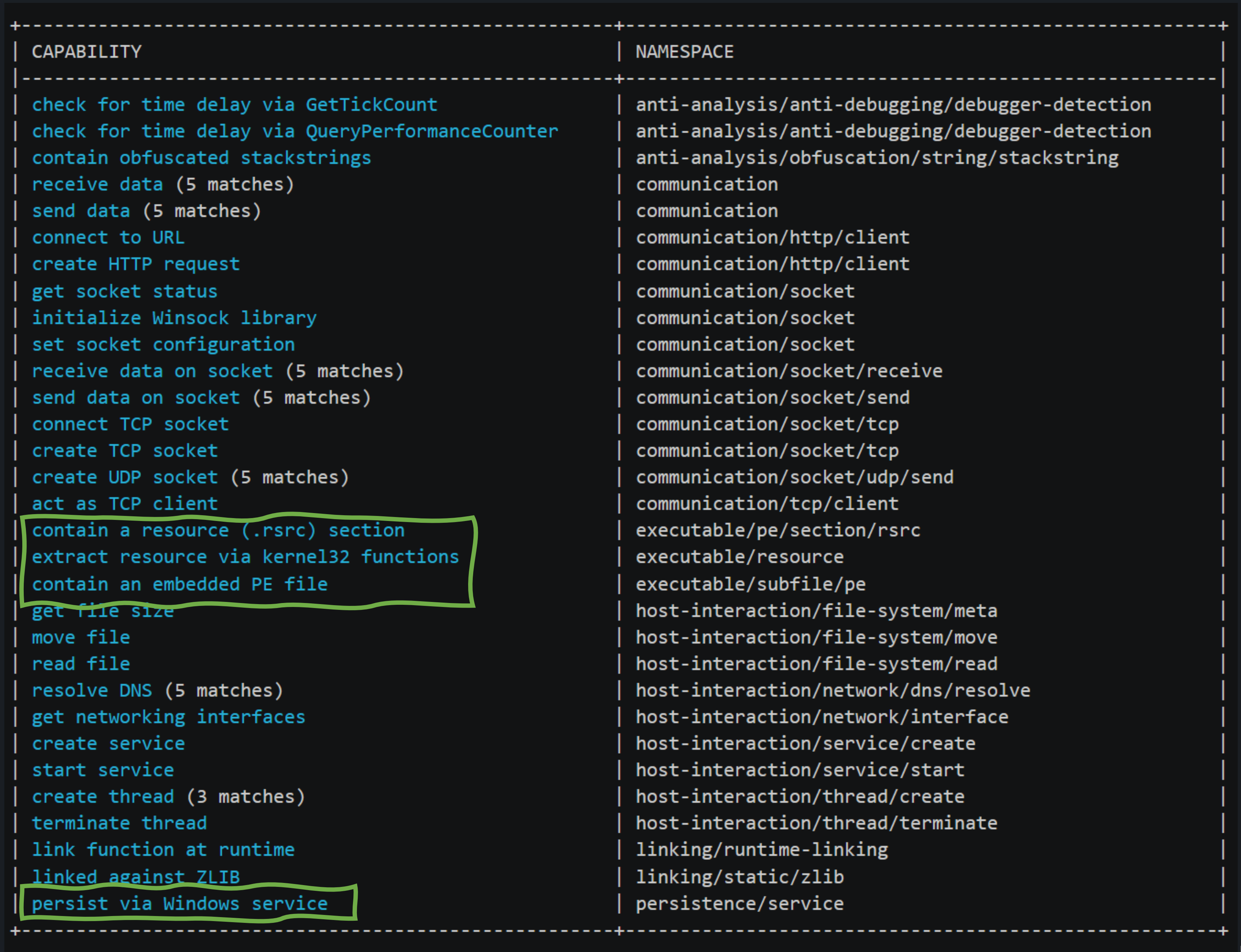


```
+------------------------------------------------------+------------------------------------------------------+
| CAPABILITY                                           | NAMESPACE                                            |
|------------------------------------------------------+------------------------------------------------------|
| check for time delay via GetTickCount                | anti-analysis/anti-debugging/debugger-detection      |
| check for time delay via QueryPerformanceCounter     | anti-analysis/anti-debugging/debugger-detection      |
| contain obfuscated stackstrings                      | anti-analysis/obfuscation/string/stackstring         |
| receive data (5 matches)                             | communication                                        |
| send data (5 matches)                                | communication                                        |
| connect to URL                                       | communication/http/client                            |
| create HTTP request                                  | communication/http/client                            |
| get socket status                                    | communication/socket                                 |
| initialize Winsock library                           | communication/socket                                 |
| set socket configuration                             | communication/socket                                 |
| receive data on socket (5 matches)                   | communication/socket/receive                         |
| send data on socket (5 matches)                      | communication/socket/send                            |
| connect TCP socket                                   | communication/socket/tcp                             |
| create TCP socket                                    | communication/socket/tcp                             |
| create UDP socket (5 matches)                        | communication/socket/udp/send                        |
| act as TCP client                                    | communication/tcp/client                             |
| contain a resource (.rsrc) section                   | executable/pe/section/rsrc                           |
| extract resource via kernel32 functions              | executable/resource                                  |
| contain an embedded PE file                          | executable/subfile/pe                                |
| get file size                                        | host-interaction/file-system/meta                    |
| move file                                            | host-interaction/file-system/move                    |
| read file                                            | host-interaction/file-system/read                    |
| resolve DNS (5 matches)                              | host-interaction/network/dns/resolve                 |
| get networking interfaces                            | host-interaction/network/interface                   |
| create service                                       | host-interaction/service/create                      |
| start service                                        | host-interaction/service/start                       |
| create thread (3 matches)                            | host-interaction/thread/create                       |
| terminate thread                                     | host-interaction/thread/terminate                    |
| link function at runtime                             | linking/runtime-linking                              |
| linked against ZLIB                                  | linking/static/zlib                                  |
| persist via Windows service                          | persistence/service                                  |
+------------------------------------------------------+------------------------------------------------------+
```

descriptive, not binary



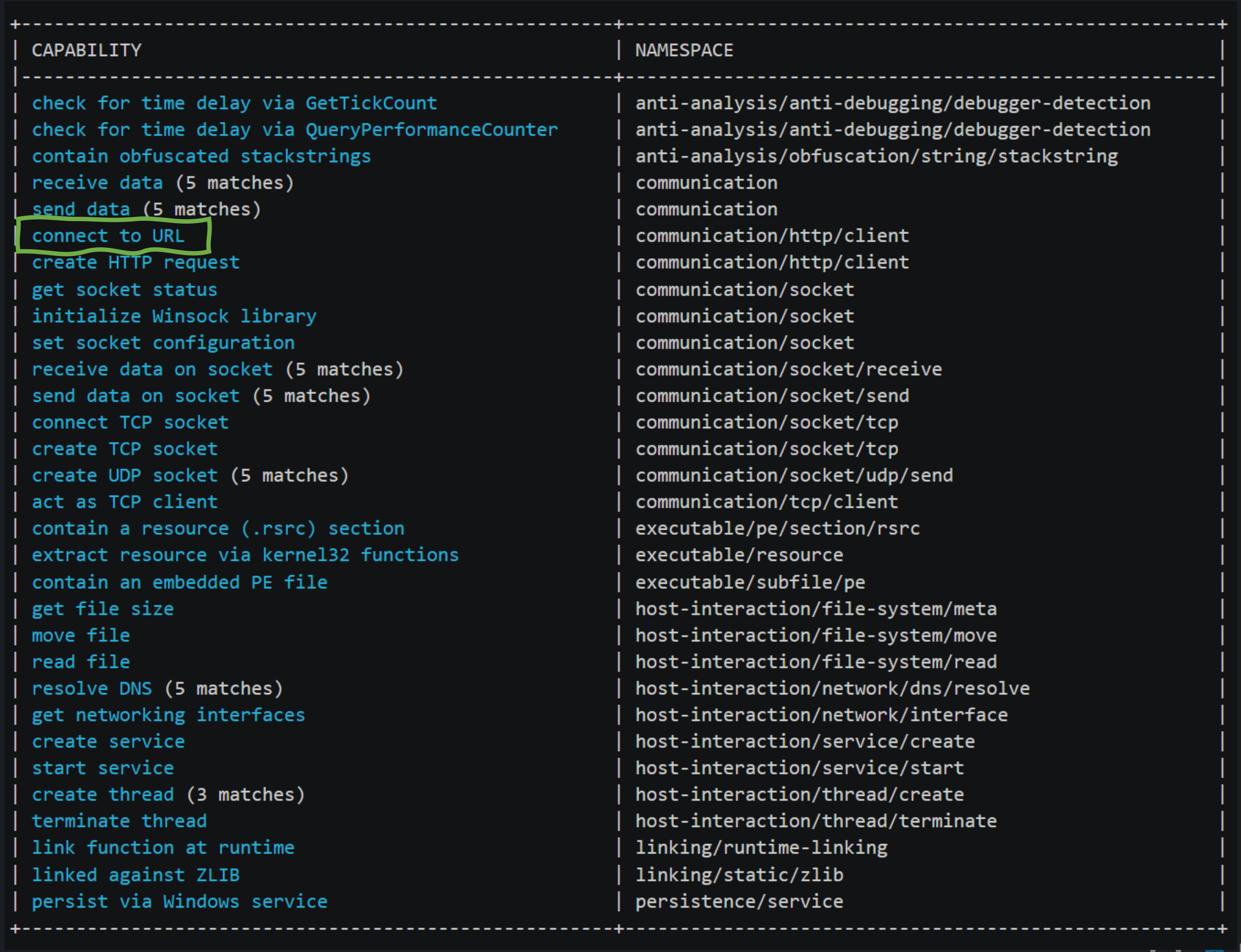
```
+------------------------------------------------------+------------------------------------------------------+
| CAPABILITY                                           | NAMESPACE                                            |
|------------------------------------------------------+------------------------------------------------------|
| check for time delay via GetTickCount                | anti-analysis/anti-debugging/debugger-detection      |
| check for time delay via QueryPerformanceCounter     | anti-analysis/anti-debugging/debugger-detection      |
| contain obfuscated stackstrings                      | anti-analysis/obfuscation/string/stackstring         |
| receive data (5 matches)                             | communication                                        |
| send data (5 matches)                                | communication                                        |
| connect to URL                                       | communication/http/client                            |
| create HTTP request                                  | communication/http/client                            |
| get socket status                                    | communication/socket                                 |
| initialize Winsock library                           | communication/socket                                 |
| set socket configuration                             | communication/socket                                 |
| receive data on socket (5 matches)                   | communication/socket/receive                         |
| send data on socket (5 matches)                      | communication/socket/send                            |
| connect TCP socket                                   | communication/socket/tcp                             |
| create TCP socket                                    | communication/socket/tcp                             |
| create UDP socket (5 matches)                        | communication/socket/udp/send                        |
| act as TCP client                                    | communication/tcp/client                             |
| contain a resource (.rsrc) section                   | executable/pe/section/rsrc                           |
| extract resource via kernel32 functions              | executable/resource                                  |
| contain an embedded PE file                          | executable/subfile/pe                                |
| get file size                                        | host-interaction/file-system/meta                    |
| move file                                            | host-interaction/file-system/move                    |
| read file                                            | host-interaction/file-system/read                    |
| resolve DNS (5 matches)                              | host-interaction/network/dns/resolve                 |
| get networking interfaces                            | host-interaction/network/interface                   |
| create service                                       | host-interaction/service/create                      |
| start service                                        | host-interaction/service/start                       |
| create thread (3 matches)                            | host-interaction/thread/create                       |
| terminate thread                                     | host-interaction/thread/terminate                    |
| link function at runtime                             | linking/runtime-linking                              |
| linked against ZLIB                                  | linking/static/zlib                                  |
| persist via Windows service                          | persistence/service                                  |
+------------------------------------------------------+------------------------------------------------------+
```



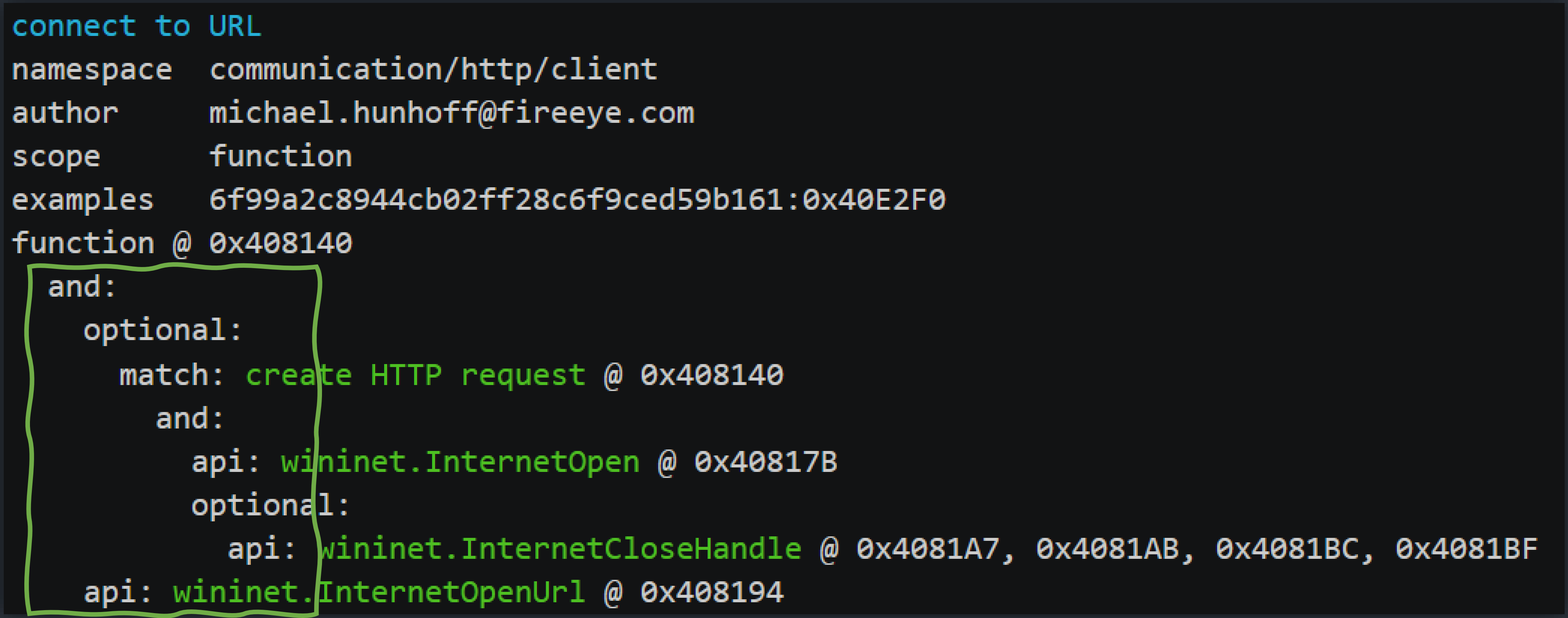
```
+------------------------------------------------------+------------------------------------------------------+
| CAPABILITY                                           | NAMESPACE                                            |
|------------------------------------------------------+------------------------------------------------------|
| check for time delay via GetTickCount                | anti-analysis/anti-debugging/debugger-detection      |
| check for time delay via QueryPerformanceCounter     | anti-analysis/anti-debugging/debugger-detection      |
| contain obfuscated stackstrings                      | anti-analysis/obfuscation/string/stackstring         |
| receive data (5 matches)                             | communication                                        |
| send data (5 matches)                                | communication                                        |
| connect to URL                                       | communication/http/client                            |
| create HTTP request                                  | communication/http/client                            |
| get socket status                                    | communication/socket                                 |
| initialize Winsock library                           | communication/socket                                 |
| set socket configuration                             | communication/socket                                 |
| receive data on socket (5 matches)                   | communication/socket/receive                         |
| send data on socket (5 matches)                      | communication/socket/send                            |
| connect TCP socket                                   | communication/socket/tcp                             |
| create TCP socket                                    | communication/socket/tcp                             |
| create UDP socket (5 matches)                        | communication/socket/udp/send                        |
| act as TCP client                                    | communication/tcp/client                             |
| contain a resource (.rsrc) section                   | executable/pe/section/rsrc                           |
| extract resource via kernel32 functions              | executable/resource                                  |
| contain an embedded PE file                          | executable/subfile/pe                                |
| get file size                                        | host-interaction/file-system/meta                    |
| move file                                            | host-interaction/file-system/move                    |
| read file                                            | host-interaction/file-system/read                    |
| resolve DNS (5 matches)                              | host-interaction/network/dns/resolve                 |
| get networking interfaces                            | host-interaction/network/interface                   |
| create service                                       | host-interaction/service/create                      |
| start service                                        | host-interaction/service/start                       |
| create thread (3 matches)                            | host-interaction/thread/create                       |
| terminate thread                                     | host-interaction/thread/terminate                    |
| link function at runtime                             | linking/runtime-linking                              |
| linked against ZLIB                                  | linking/static/zlib                                  |
| persist via Windows service                          | persistence/service                                  |
+------------------------------------------------------+------------------------------------------------------+
```

dropper?

wannacry killswitch

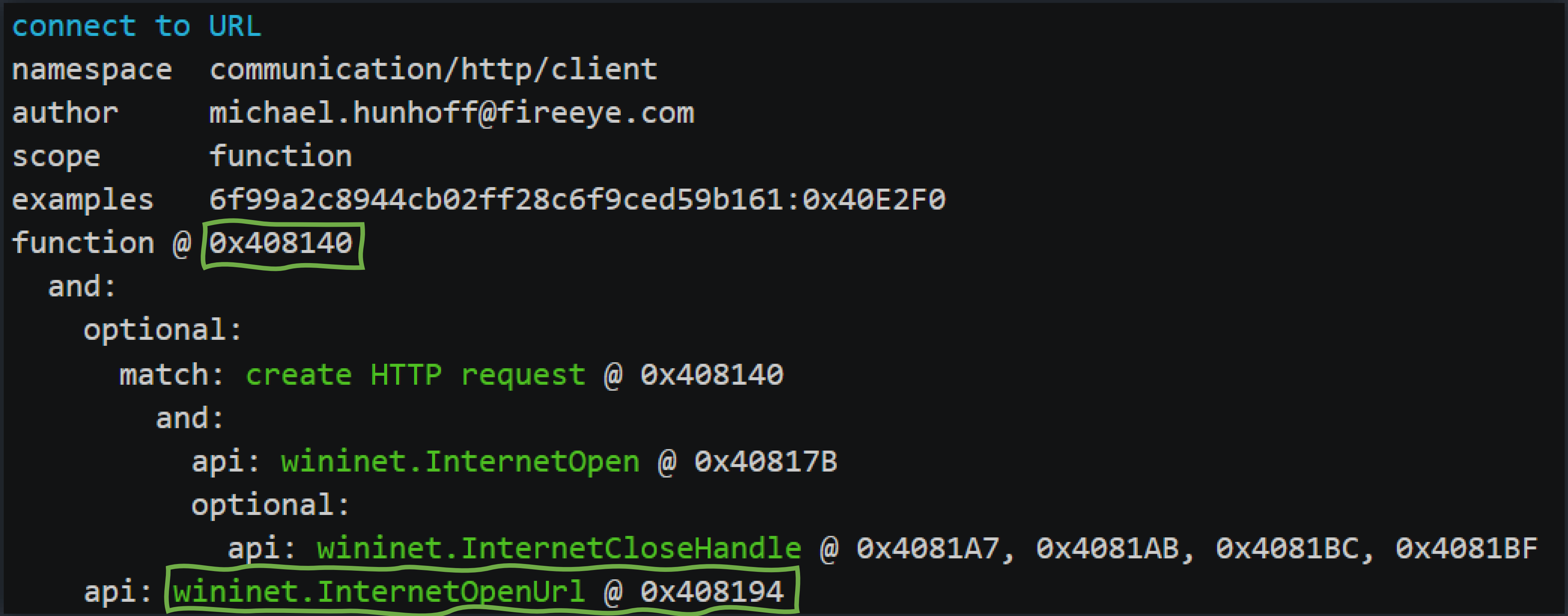


```
+-------------------------------------------------------+------------------------------------------------------+
| CAPABILITY                                            | NAMESPACE                                            |
|-------------------------------------------------------+------------------------------------------------------|
| check for time delay via GetTickCount                 | anti-analysis/anti-debugging/debugger-detection      |
| check for time delay via QueryPerformanceCounter      | anti-analysis/anti-debugging/debugger-detection      |
| contain obfuscated stackstrings                       | anti-analysis/obfuscation/string/stackstring         |
| receive data (5 matches)                              | communication                                        |
| send data (5 matches)                                 | communication                                        |
| connect to URL                                        | communication/http/client                            |
| create HTTP request                                   | communication/http/client                            |
| get socket status                                     | communication/socket                                 |
| initialize Winsock library                            | communication/socket                                 |
| set socket configuration                              | communication/socket                                 |
| receive data on socket (5 matches)                    | communication/socket/receive                         |
| send data on socket (5 matches)                       | communication/socket/send                            |
| connect TCP socket                                    | communication/socket/tcp                             |
| create TCP socket                                     | communication/socket/tcp                             |
| create UDP socket (5 matches)                         | communication/socket/udp/send                        |
| act as TCP client                                     | communication/tcp/client                             |
| contain a resource (.rsrc) section                    | executable/pe/section/rsrc                           |
| extract resource via kernel32 functions               | executable/resource                                  |
| contain an embedded PE file                           | executable/subfile/pe                                |
| get file size                                         | host-interaction/file-system/meta                    |
| move file                                             | host-interaction/file-system/move                    |
| read file                                             | host-interaction/file-system/read                    |
| resolve DNS (5 matches)                               | host-interaction/network/dns/resolve                 |
| get networking interfaces                             | host-interaction/network/interface                   |
| create service                                        | host-interaction/service/create                      |
| start service                                         | host-interaction/service/start                       |
| create thread (3 matches)                             | host-interaction/thread/create                       |
| terminate thread                                      | host-interaction/thread/terminate                    |
| link function at runtime                              | linking/runtime-linking                              |
| linked against ZLIB                                   | linking/static/zlib                                  |
| persist via Windows service                           | persistence/service                                  |
+-------------------------------------------------------+------------------------------------------------------+
```



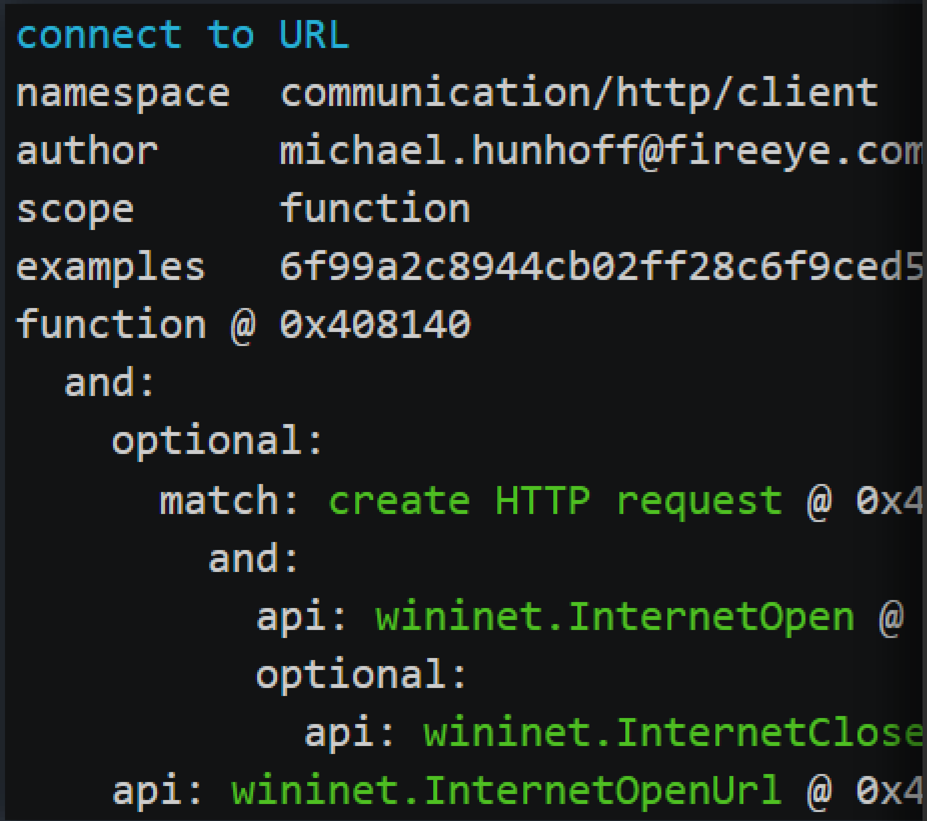
```
connect to URL
namespace  communication/http/client
author     michael.hunhoff@fireeye.com
scope      function
examples   6f99a2c8944cb02ff28c6f9ced59b161:0x40E2F0
function @ 0x408140
  and:
    optional:
      match: create HTTP request @ 0x408140
        and:
          api: wininet.InternetOpen @ 0x40817B
          optional:
            api: wininet.InternetCloseHandle @ 0x4081A7, 0x4081AB, 0x4081BC, 0x4081BF
    api: wininet.InternetOpenUrl @ 0x408194
```

why rule matched

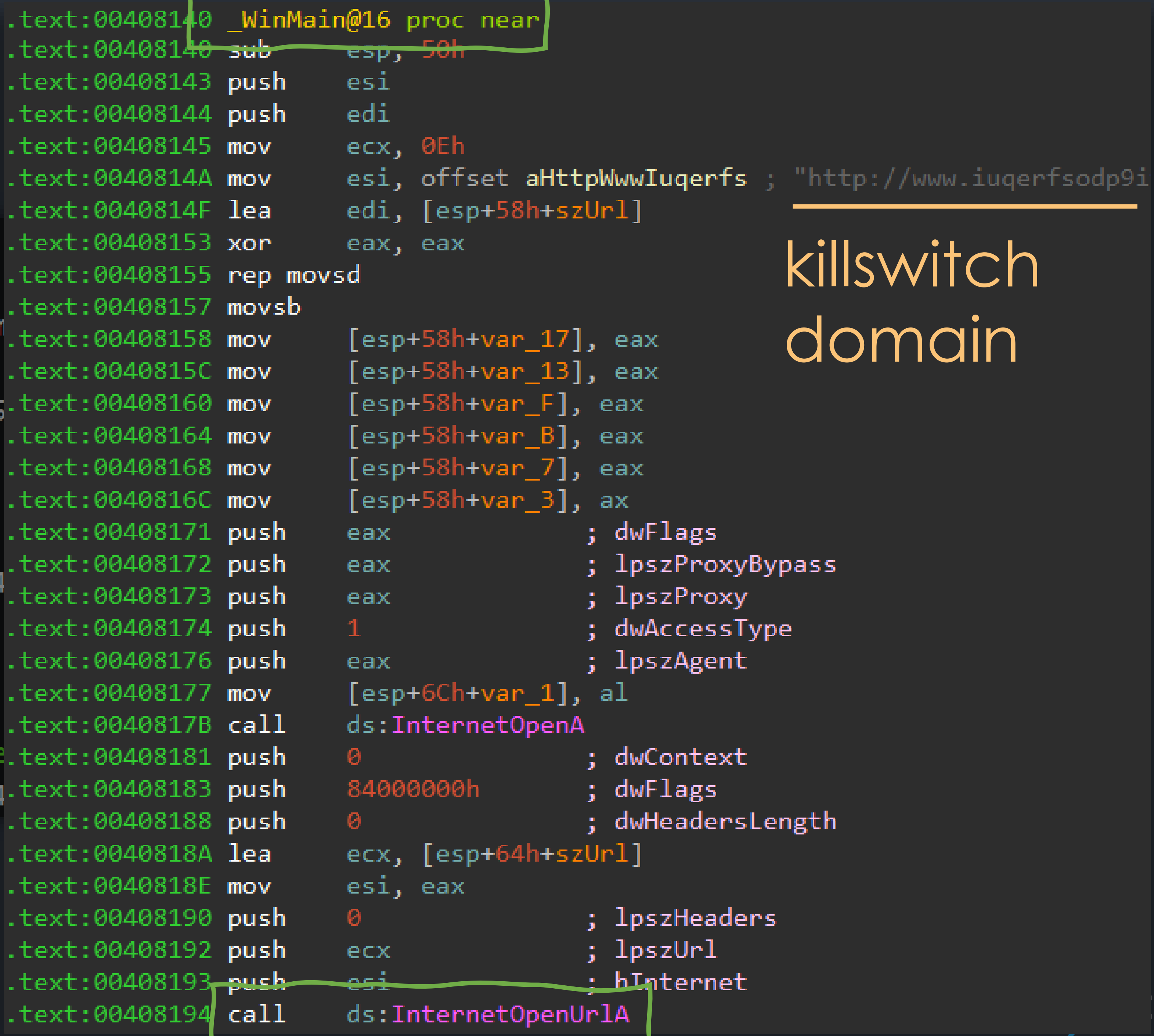


```
connect to URL
namespace  communication/http/client
author     michael.hunhoff@fireeye.com
scope      function
examples   6f99a2c8944cb02ff28c6f9ced59b161:0x40E2F0
function @ 0x408140
  and:
    optional:
      match: create HTTP request @ 0x408140
        and:
          api: wininet.InternetOpen @ 0x40817B
          optional:
            api: wininet.InternetCloseHandle @ 0x4081A7, 0x4081AB, 0x4081BC, 0x4081BF
    api: wininet.InternetOpenUrl @ 0x408194
```

where rule matched

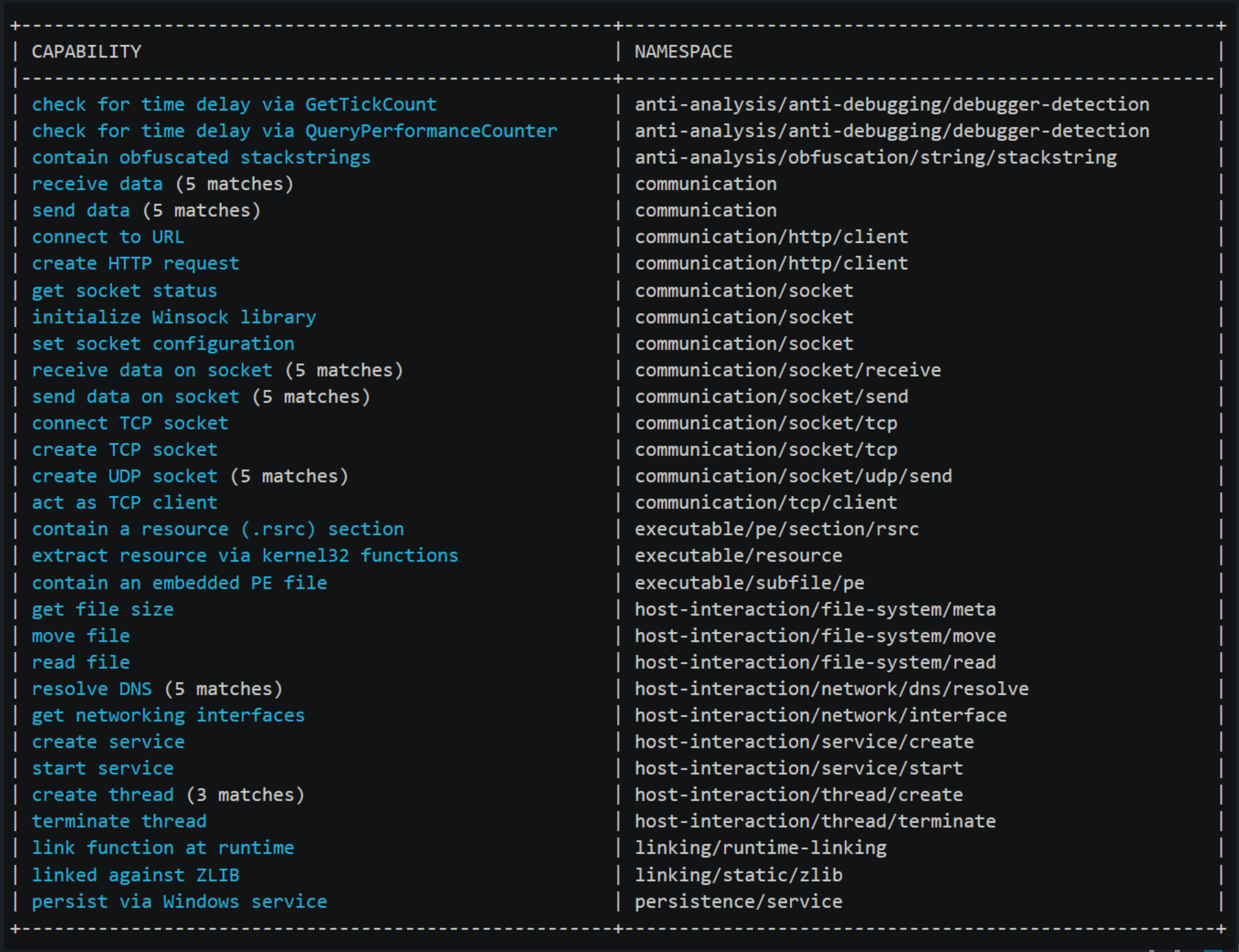


```
connect to URL
namespace  communication/http/client
author     michael.hunhoff@fireeye.com
scope      function
examples   6f99a2c8944cb02ff28c6f9ced5
function @ 0x408140
  and:
    optional:
      match: create HTTP request @ 0x4
        and:
          api: wininet.InternetOpen @
          optional:
            api: wininet.InternetClose
    api: wininet.InternetOpenUrl @ 0x4
```

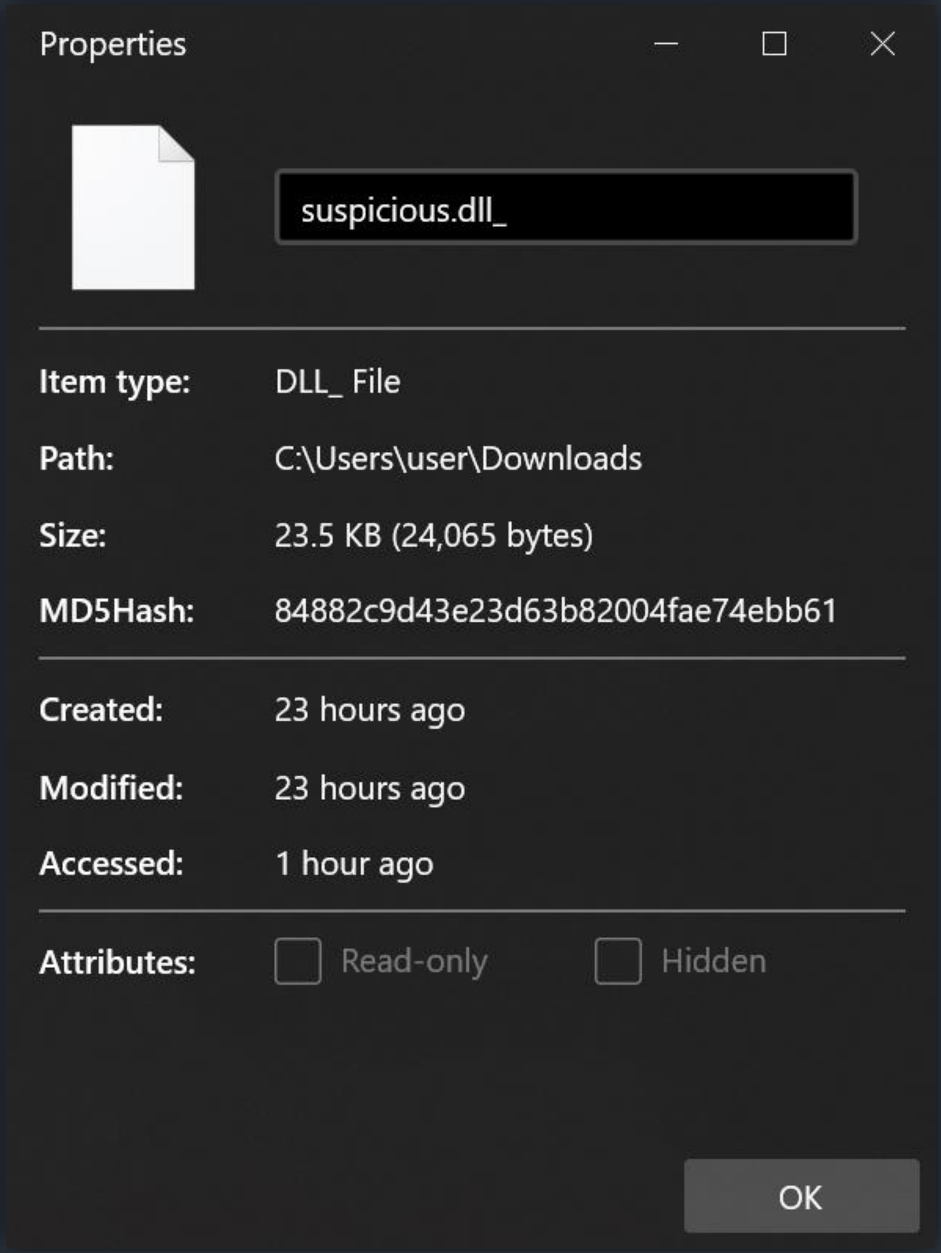


```
.text:00408140 _WinMain@16 proc near
.text:00408140 sub     esp, 50h
.text:00408143 push    esi
.text:00408144 push    edi
.text:00408145 mov     ecx, 0Eh
.text:0040814A mov     esi, offset aHttpWwwIuqerfs ; "http://www.iuqerfsodp9i
.text:0040814F lea     edi, [esp+58h+szUrl]
.text:00408153 xor     eax, eax
.text:00408155 rep movsd
.text:00408157 movsb
.text:00408158 mov     [esp+58h+var_17], eax
.text:0040815C mov     [esp+58h+var_13], eax
.text:00408160 mov     [esp+58h+var_F], eax
.text:00408164 mov     [esp+58h+var_B], eax
.text:00408168 mov     [esp+58h+var_7], eax
.text:0040816C mov     [esp+58h+var_3], ax
.text:00408171 push    eax                    ; dwFlags
.text:00408172 push    eax                    ; lpszProxyBypass
.text:00408173 push    eax                    ; lpszProxy
.text:00408174 push    1                      ; dwAccessType
.text:00408176 push    eax                    ; lpszAgent
.text:00408177 mov     [esp+6Ch+var_1], al
.text:0040817B call    ds:InternetOpenA
.text:00408181 push    0                      ; dwContext
.text:00408183 push    84000000h              ; dwFlags
.text:00408188 push    0                      ; dwHeadersLength
.text:0040818A lea     ecx, [esp+64h+szUrl]
.text:0040818E mov     esi, eax
.text:00408190 push    0                      ; lpszHeaders
.text:00408192 push    ecx                    ; lpszUrl
.text:00408193 push    esi                    ; hInternet
.text:00408194 call    ds:InternetOpenUrlA
```

killswitch domain



```
+------------------------------------------------------+------------------------------------------------------+
| CAPABILITY                                           | NAMESPACE                                            |
|------------------------------------------------------+------------------------------------------------------|
| check for time delay via GetTickCount                | anti-analysis/anti-debugging/debugger-detection      |
| check for time delay via QueryPerformanceCounter     | anti-analysis/anti-debugging/debugger-detection      |
| contain obfuscated stackstrings                      | anti-analysis/obfuscation/string/stackstring         |
| receive data (5 matches)                             | communication                                        |
| send data (5 matches)                                | communication                                        |
| connect to URL                                       | communication/http/client                            |
| create HTTP request                                  | communication/http/client                            |
| get socket status                                    | communication/socket                                 |
| initialize Winsock library                           | communication/socket                                 |
| set socket configuration                             | communication/socket                                 |
| receive data on socket (5 matches)                   | communication/socket/receive                         |
| send data on socket (5 matches)                      | communication/socket/send                            |
| connect TCP socket                                   | communication/socket/tcp                             |
| create TCP socket                                    | communication/socket/tcp                             |
| create UDP socket (5 matches)                        | communication/socket/udp/send                        |
| act as TCP client                                    | communication/tcp/client                             |
| contain a resource (.rsrc) section                   | executable/pe/section/rsrc                           |
| extract resource via kernel32 functions              | executable/resource                                  |
| contain an embedded PE file                          | executable/subfile/pe                                |
| get file size                                        | host-interaction/file-system/meta                    |
| move file                                            | host-interaction/file-system/move                    |
| read file                                            | host-interaction/file-system/read                    |
| resolve DNS (5 matches)                              | host-interaction/network/dns/resolve                 |
| get networking interfaces                            | host-interaction/network/interface                   |
| create service                                       | host-interaction/service/create                      |
| start service                                        | host-interaction/service/start                       |
| create thread (3 matches)                            | host-interaction/thread/create                       |
| terminate thread                                     | host-interaction/thread/terminate                    |
| link function at runtime                             | linking/runtime-linking                              |
| linked against ZLIB                                  | linking/static/zlib                                  |
| persist via Windows service                          | persistence/service                                  |
+------------------------------------------------------+------------------------------------------------------+
```



Properties

suspicious.dll_

Item type: DLL_ File

Path: C:\Users\user\Downloads

Size: 23.5 KB (24,065 bytes)

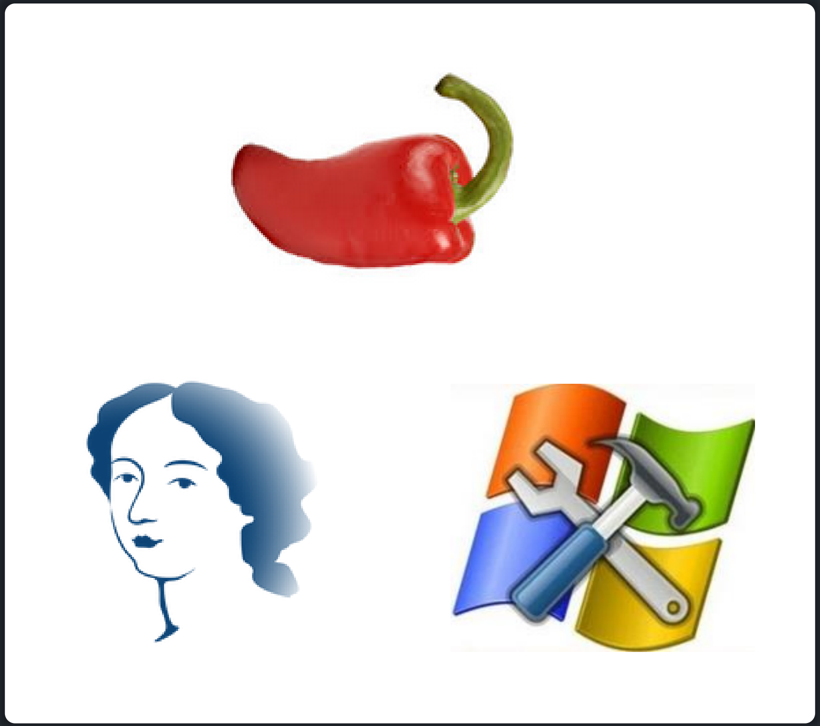
MD5Hash: 84882c9d43e23d63b82004fae74ebb61

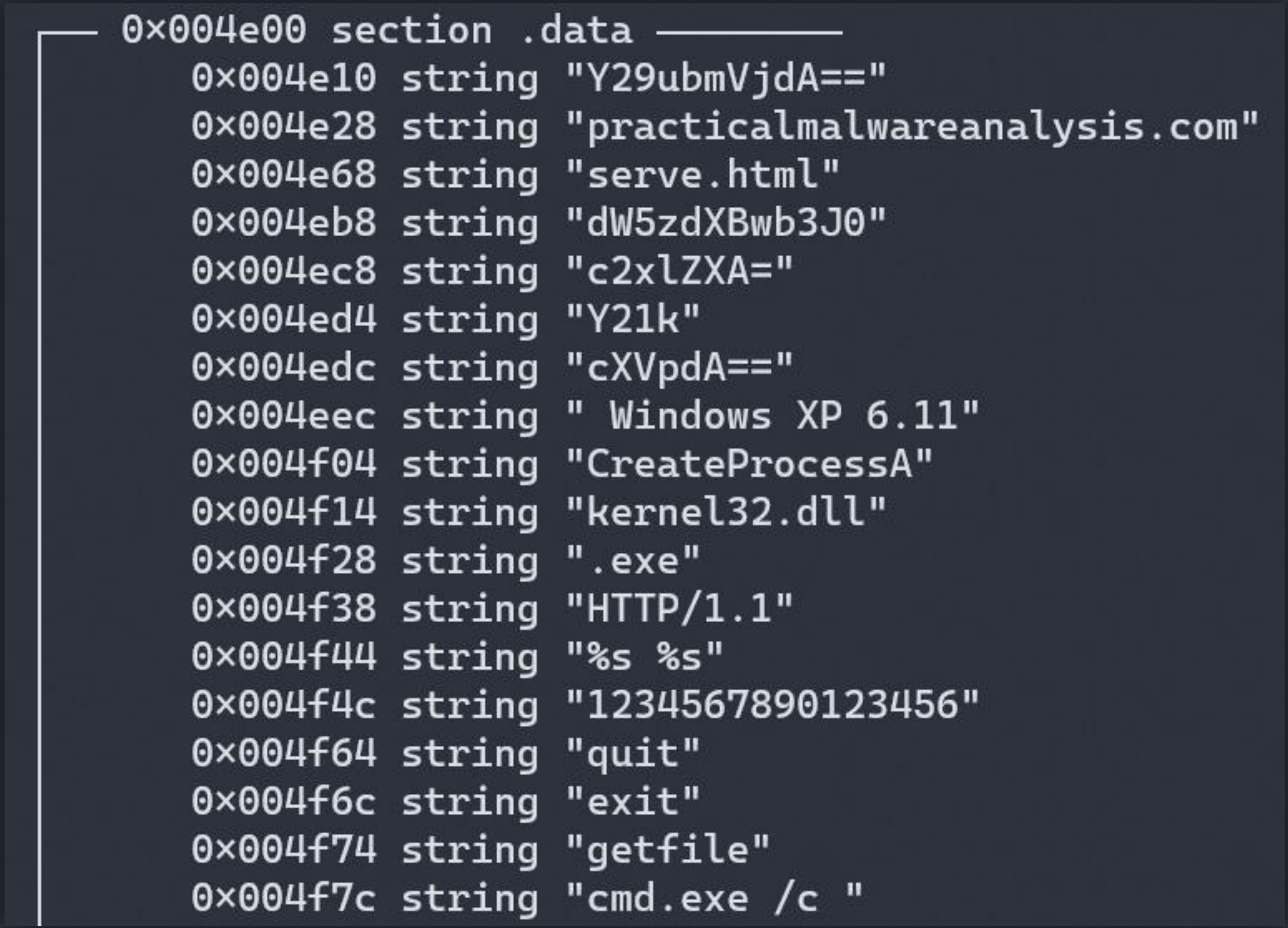
Created: 23 hours ago

Modified: 23 hours ago

Accessed: 1 hour ago

Attributes: ☐ Read-only ☐ Hidden





```
┌── 0x004e00 section .data ────────
│      0x004e10 string "Y29ubmVjdA=="
│      0x004e28 string "practicalmalwareanalysis.com"
│      0x004e68 string "serve.html"
│      0x004eb8 string "dW5zdXBwb3J0"
│      0x004ec8 string "c2xlZXA="
│      0x004ed4 string "Y21k"
│      0x004edc string "cXVpdA=="
│      0x004eec string " Windows XP 6.11"
│      0x004f04 string "CreateProcessA"
│      0x004f14 string "kernel32.dll"
│      0x004f28 string ".exe"
│      0x004f38 string "HTTP/1.1"
│      0x004f44 string "%s %s"
│      0x004f4c string "1234567890123456"
│      0x004f64 string "quit"
│      0x004f6c string "exit"
│      0x004f74 string "getfile"
│      0x004f7c string "cmd.exe /c "
│
```

the triage analysis “gap”

less experience → more ☹

- often good triage can avoid deeper analysis
- and thus, save time and money

more experience:

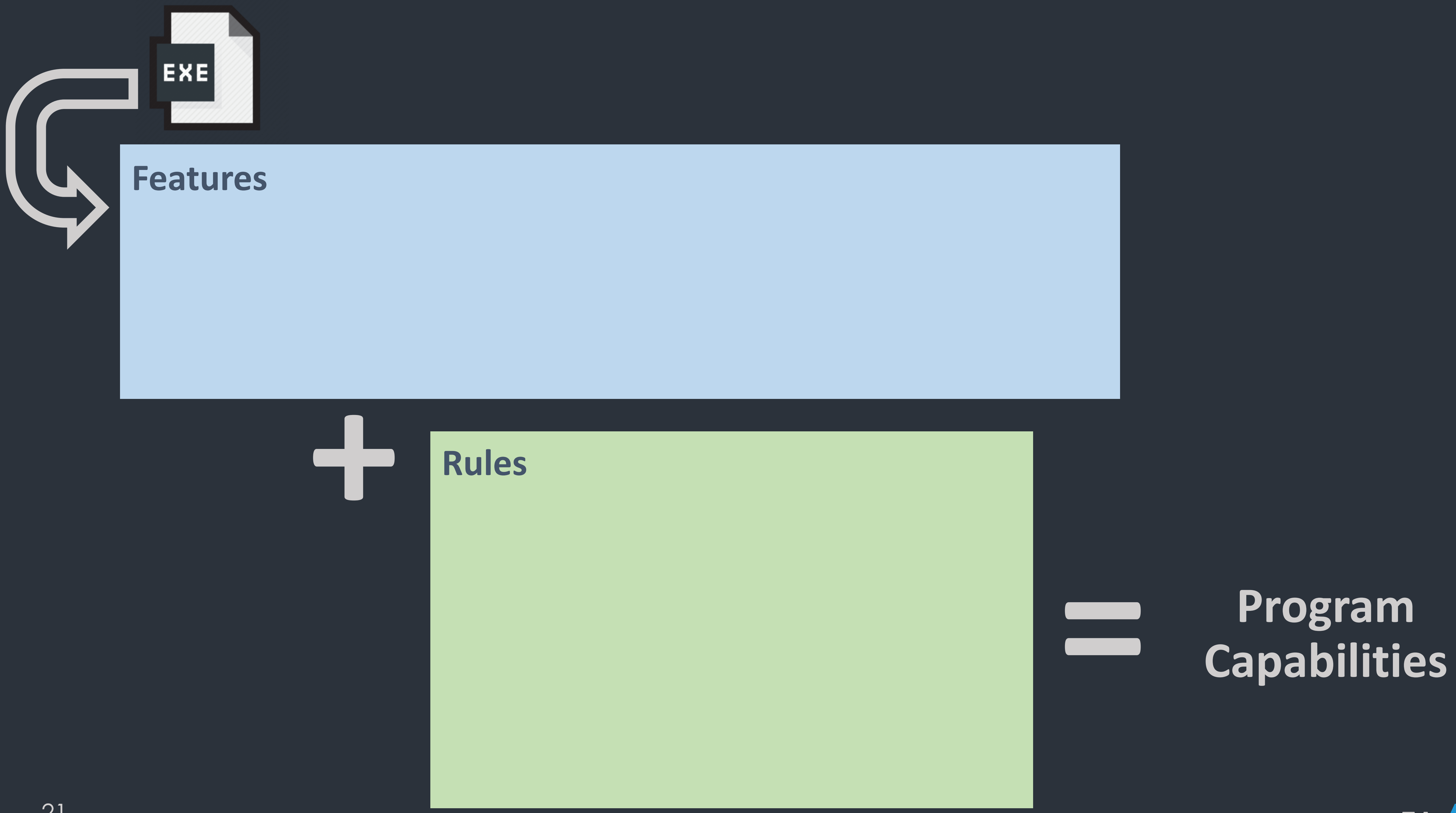
- know where to look
- know shortcuts
- know what’s common

the triage analysis “gap”

triage should be quick and *guide* further analysis steps

current triage tools

- strings / FLOSS: all strings in a binary, used or not, *without any context*
- PE header: e.g. imports, but *not how/why they’re used*
- sandbox detonation: limited to behavior seen on exercised code-paths



Features

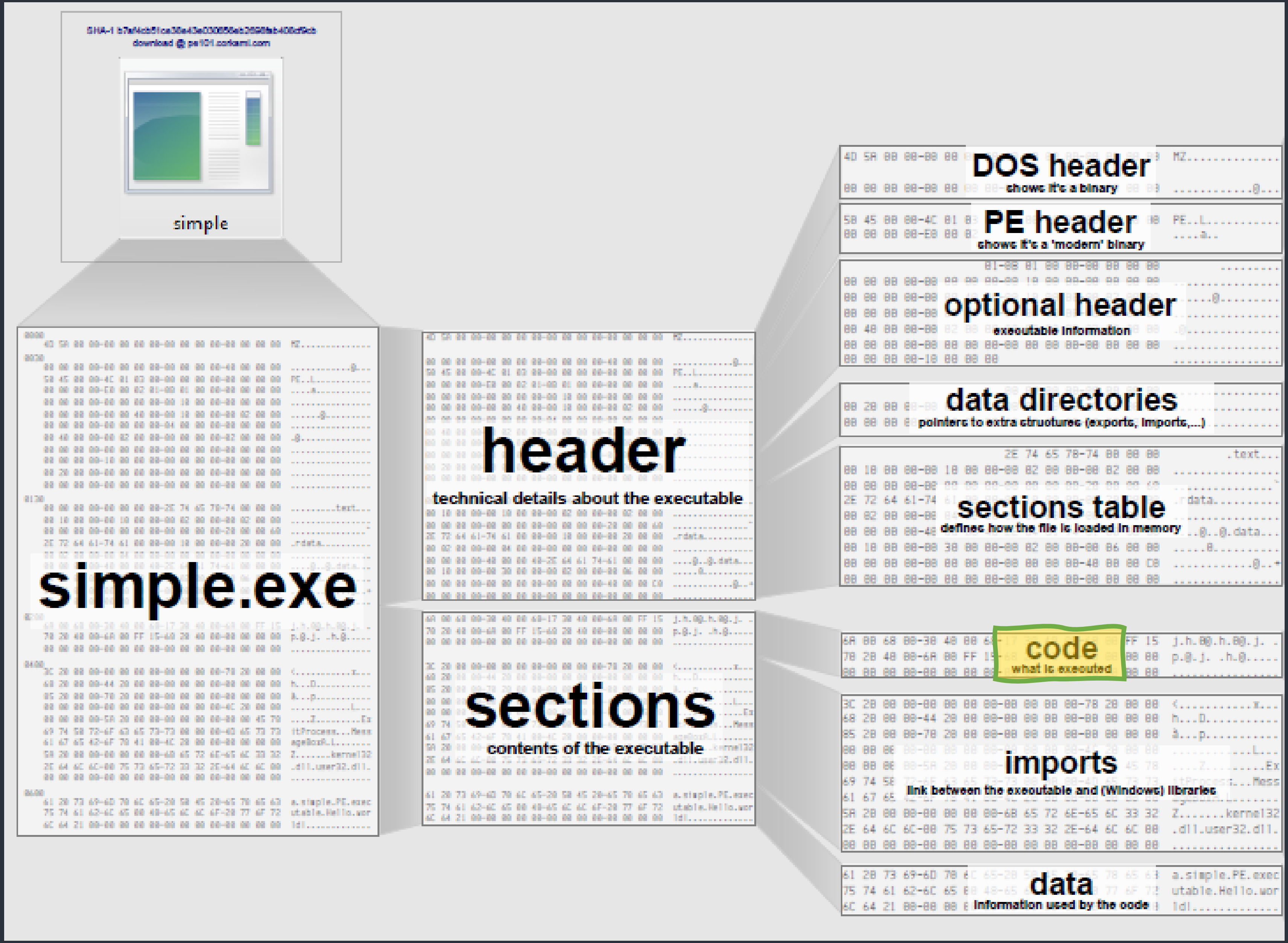
Rules

Program Capabilities

Features

+ Rules

Code

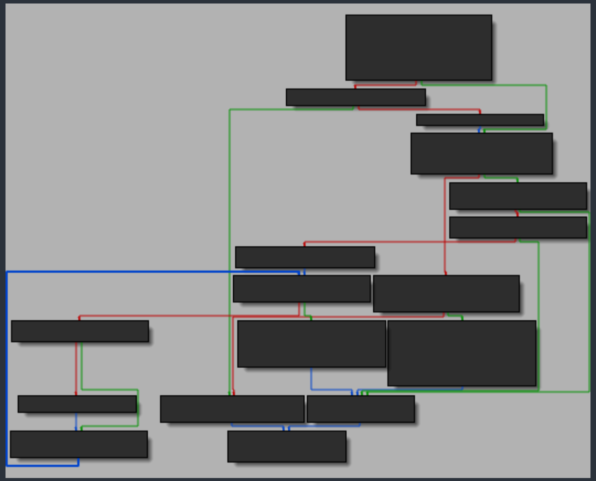

download @ pe101.corkami.com
simple
simple.exe
header
technical details about the executable
sections
contents of the executable
DOS header
shows it's a binary
PE header
shows it's a 'modern' binary
optional header
executable information
data directories
pointers to extra structures (exports, imports,...)
sections table
defines how the file is loaded in memory
code
what is executed
imports
link between the executable and (Windows) libraries
data
information used by the code

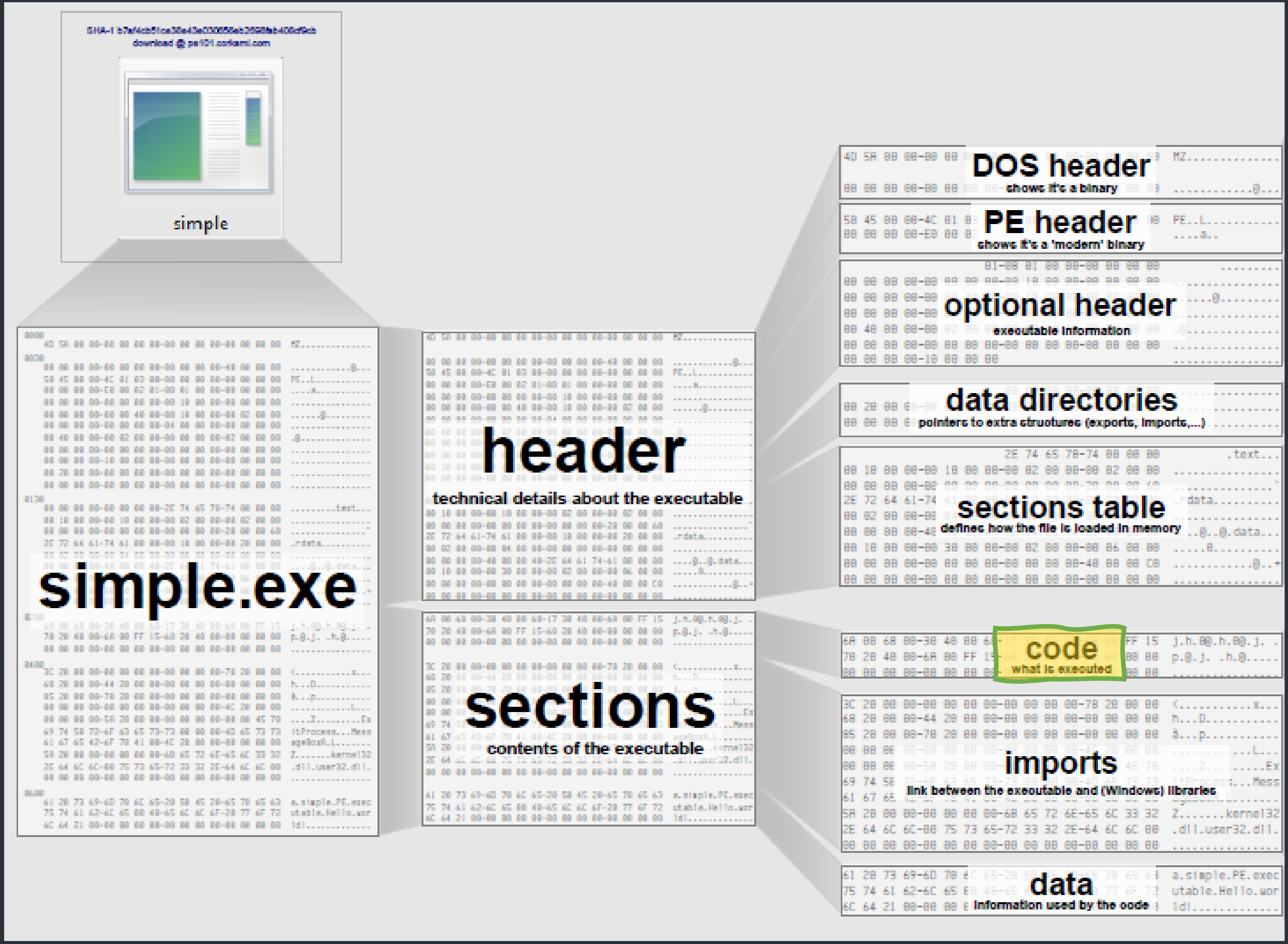
based on PE101 by Ange Albertini (CC BY 2.0)

Features

+ Rules

Code





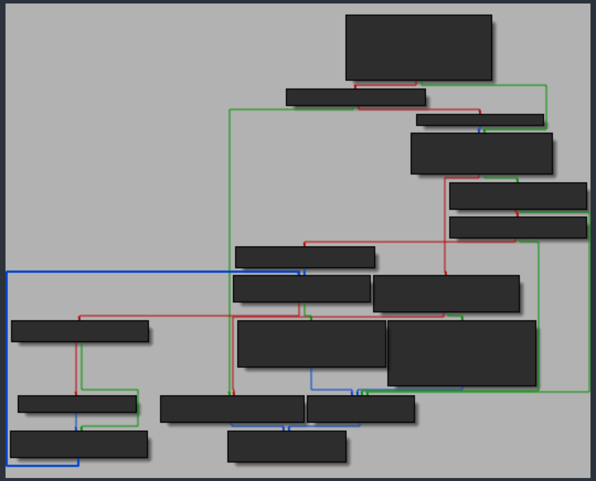
download @ pe101.corkami.com
simple
simple.exe
header
technical details about the executable
sections
contents of the executable
DOS header
shows it's a binary
PE header
shows it's a 'modern' binary
optional header
executable information
data directories
pointers to extra structures (exports, imports,...)
sections table
defines how the file is loaded in memory
code
what is executed
imports
link between the executable and (Windows) libraries
data
information used by the code

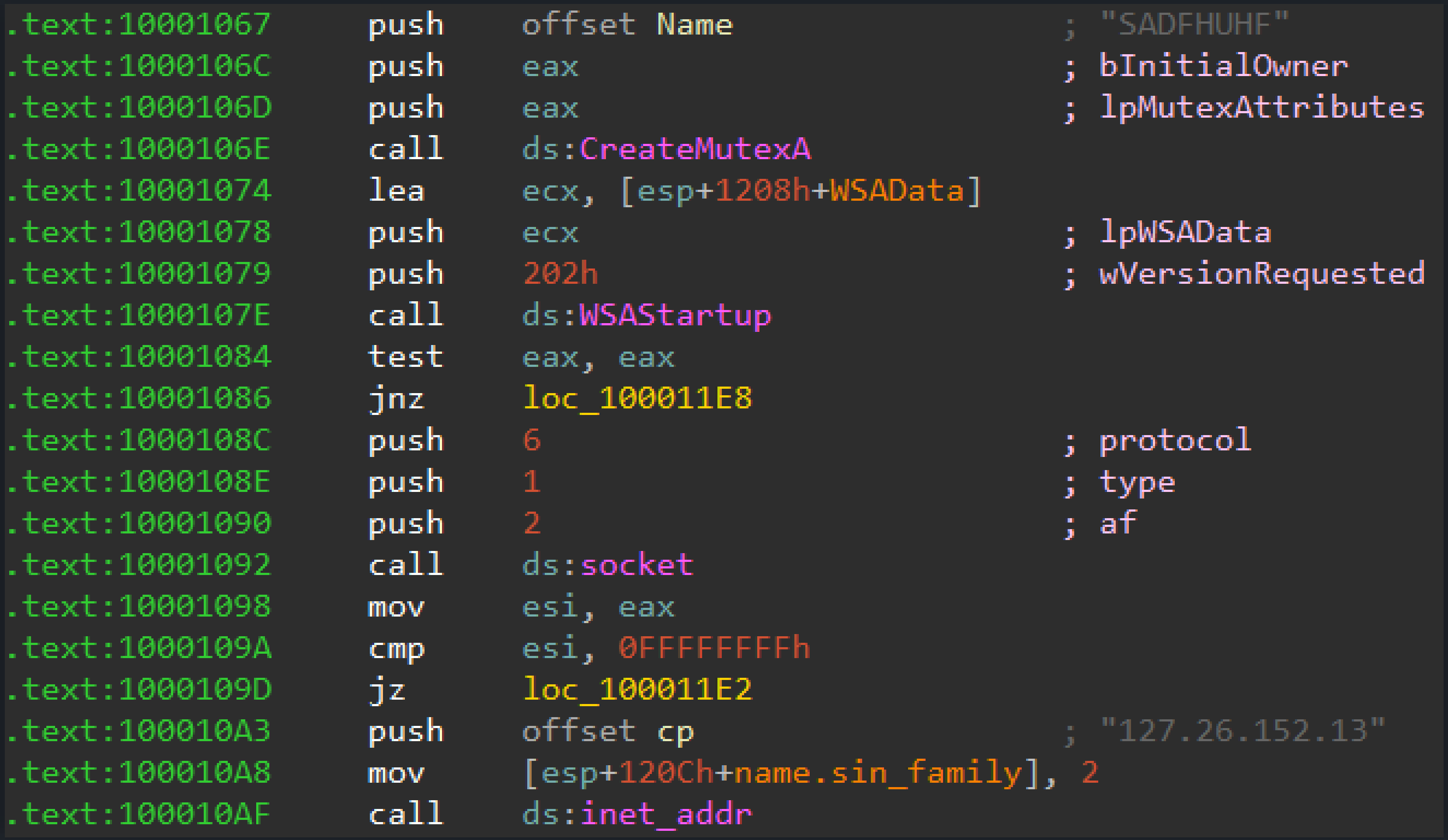
based on PE101 by Ange Albertini (CC BY 2.0)

Features

+ Rules

Code





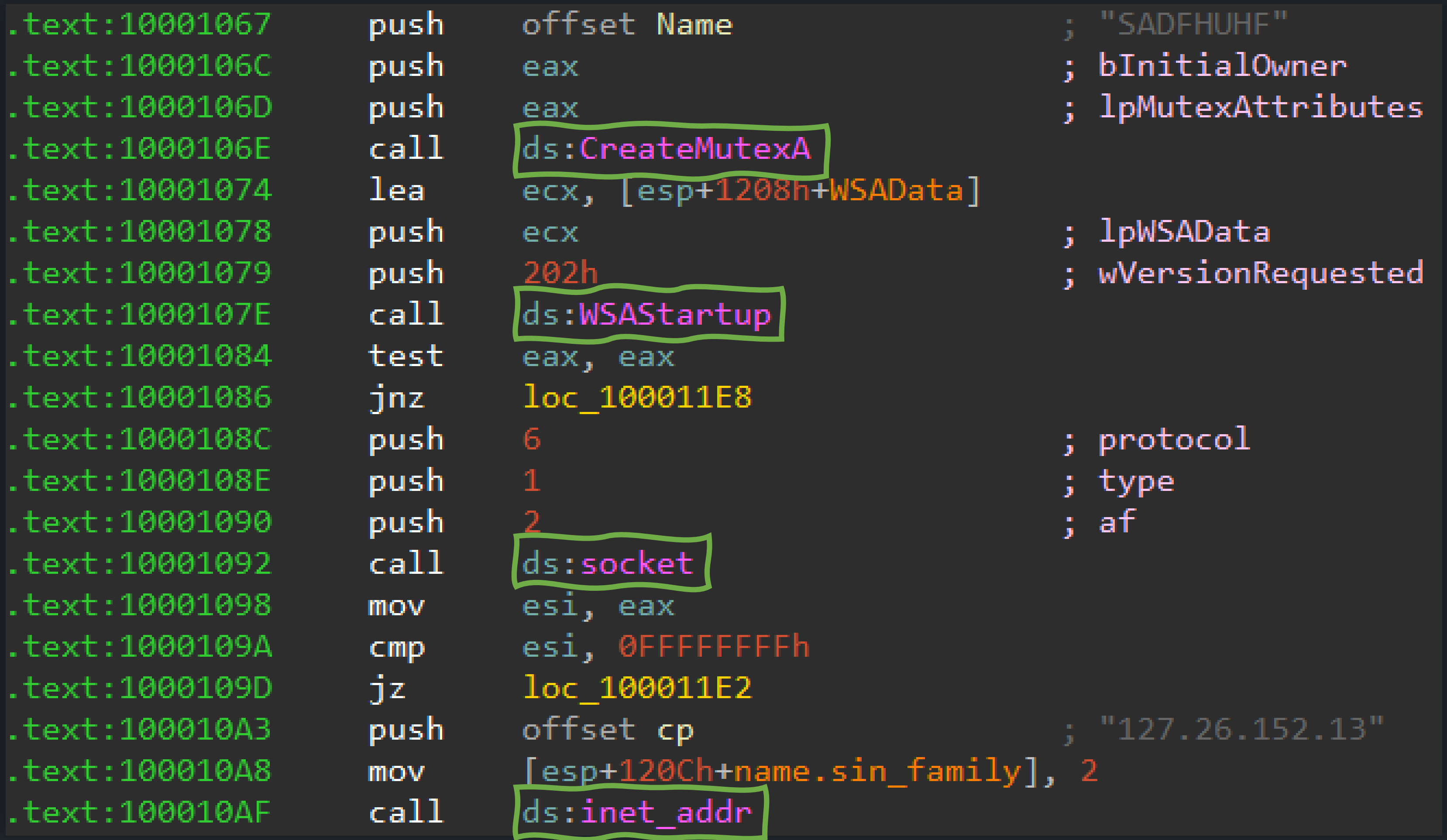
```
.text:10001067      push    offset Name             ; "SADFHUHF"
.text:1000106C      push    eax                     ; bInitialOwner
.text:1000106D      push    eax                     ; lpMutexAttributes
.text:1000106E      call    ds:CreateMutexA
.text:10001074      lea     ecx, [esp+1208h+WSAData]
.text:10001078      push    ecx                     ; lpWSAData
.text:10001079      push    202h                    ; wVersionRequested
.text:1000107E      call    ds:WSAStartup
.text:10001084      test    eax, eax
.text:10001086      jnz     loc_100011E8
.text:1000108C      push    6                       ; protocol
.text:1000108E      push    1                       ; type
.text:10001090      push    2                       ; af
.text:10001092      call    ds:socket
.text:10001098      mov     esi, eax
.text:1000109A      cmp     esi, 0FFFFFFFFh
.text:1000109D      jz      loc_100011E2
.text:100010A3      push    offset cp               ; "127.26.152.13"
.text:100010A8      mov     [esp+120Ch+name.sin_family], 2
.text:100010AF      call    ds:inet_addr
```

Features

+ Rules

Code

- API calls



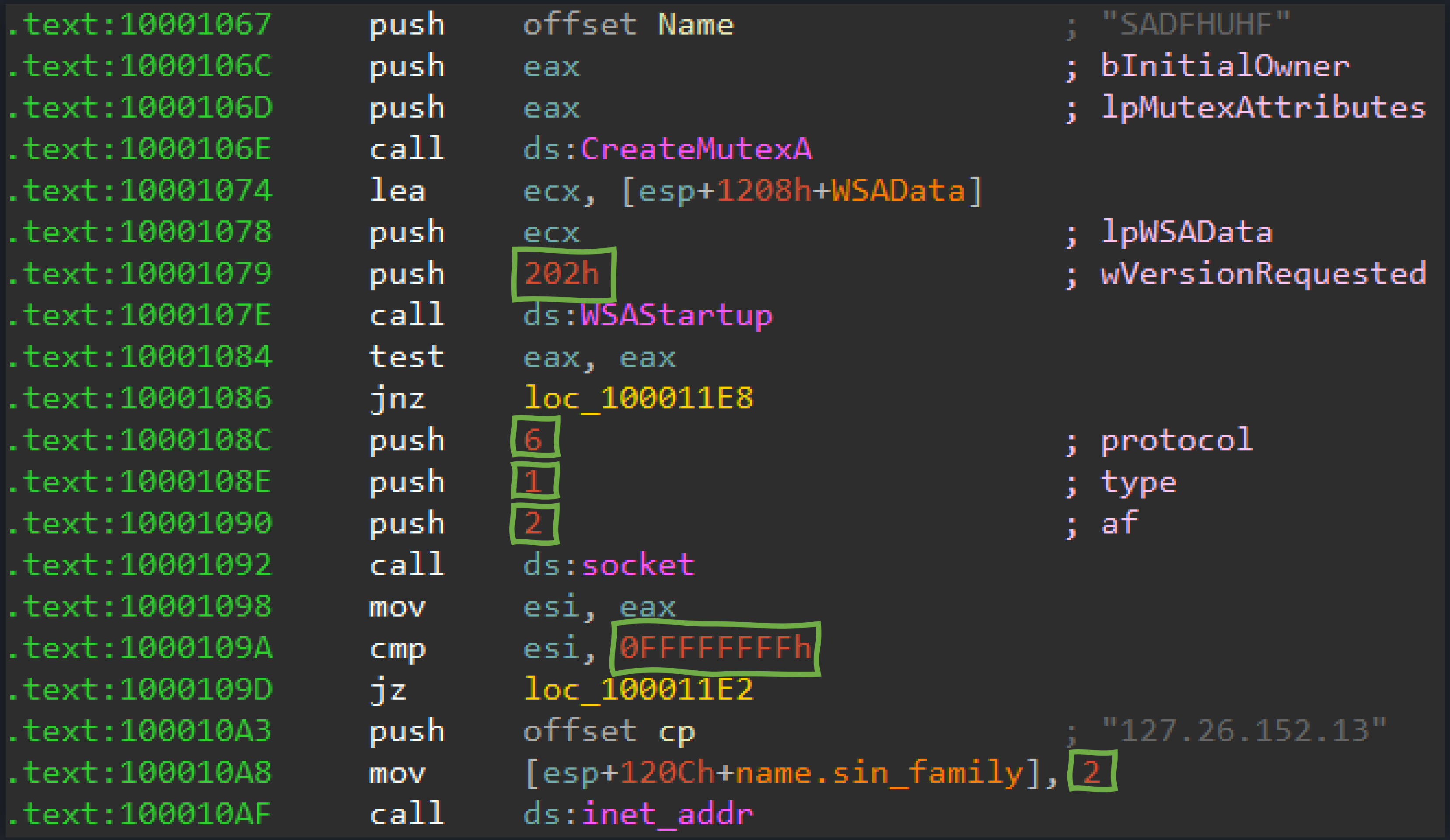
```
.text:10001067      push    offset Name                 ; "SADFHUHF"
.text:1000106C      push    eax                         ; bInitialOwner
.text:1000106D      push    eax                         ; lpMutexAttributes
.text:1000106E      call    ds:CreateMutexA
.text:10001074      lea     ecx, [esp+1208h+WSAData]
.text:10001078      push    ecx                         ; lpWSAData
.text:10001079      push    202h                        ; wVersionRequested
.text:1000107E      call    ds:WSAStartup
.text:10001084      test    eax, eax
.text:10001086      jnz     loc_100011E8
.text:1000108C      push    6                           ; protocol
.text:1000108E      push    1                           ; type
.text:10001090      push    2                           ; af
.text:10001092      call    ds:socket
.text:10001098      mov     esi, eax
.text:1000109A      cmp     esi, 0FFFFFFFFh
.text:1000109D      jz      loc_100011E2
.text:100010A3      push    offset cp                   ; "127.26.152.13"
.text:100010A8      mov     [esp+120Ch+name.sin_family], 2
.text:100010AF      call    ds:inet_addr
```

Features

+ Rules

Code

- API calls
- numbers



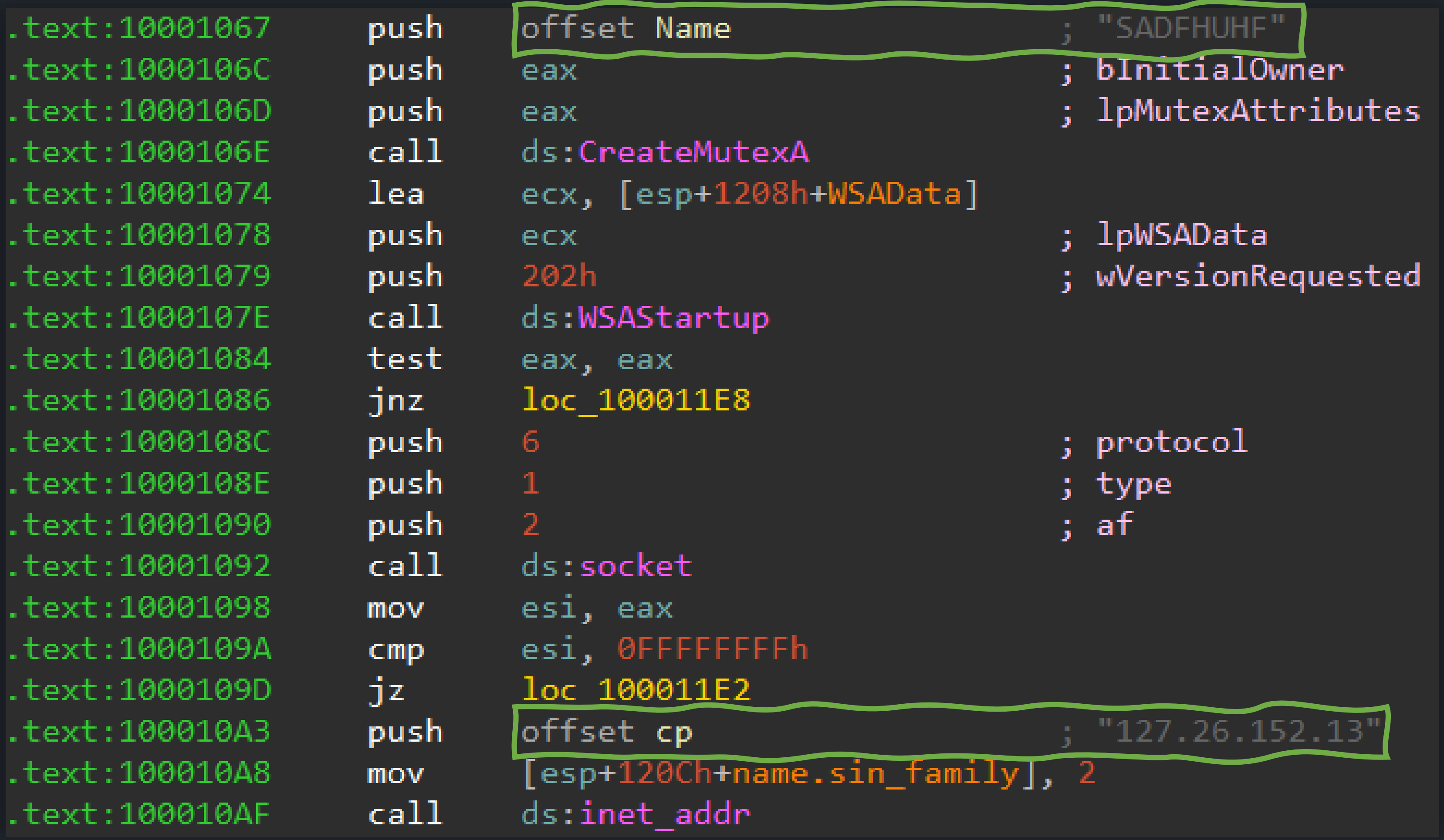
```
.text:10001067      push    offset Name                        ; "SADFHUHF"
.text:1000106C      push    eax                                ; bInitialOwner
.text:1000106D      push    eax                                ; lpMutexAttributes
.text:1000106E      call    ds:CreateMutexA
.text:10001074      lea     ecx, [esp+1208h+WSAData]
.text:10001078      push    ecx                                ; lpWSAData
.text:10001079      push    202h                               ; wVersionRequested
.text:1000107E      call    ds:WSAStartup
.text:10001084      test    eax, eax
.text:10001086      jnz     loc_100011E8
.text:1000108C      push    6                                  ; protocol
.text:1000108E      push    1                                  ; type
.text:10001090      push    2                                  ; af
.text:10001092      call    ds:socket
.text:10001098      mov     esi, eax
.text:1000109A      cmp     esi, 0FFFFFFFFh
.text:1000109D      jz      loc_100011E2
.text:100010A3      push    offset cp                          ; "127.26.152.13"
.text:100010A8      mov     [esp+120Ch+name.sin_family], 2
.text:100010AF      call    ds:inet_addr
```

Features

+ Rules

Code

- API calls
- numbers
- string references



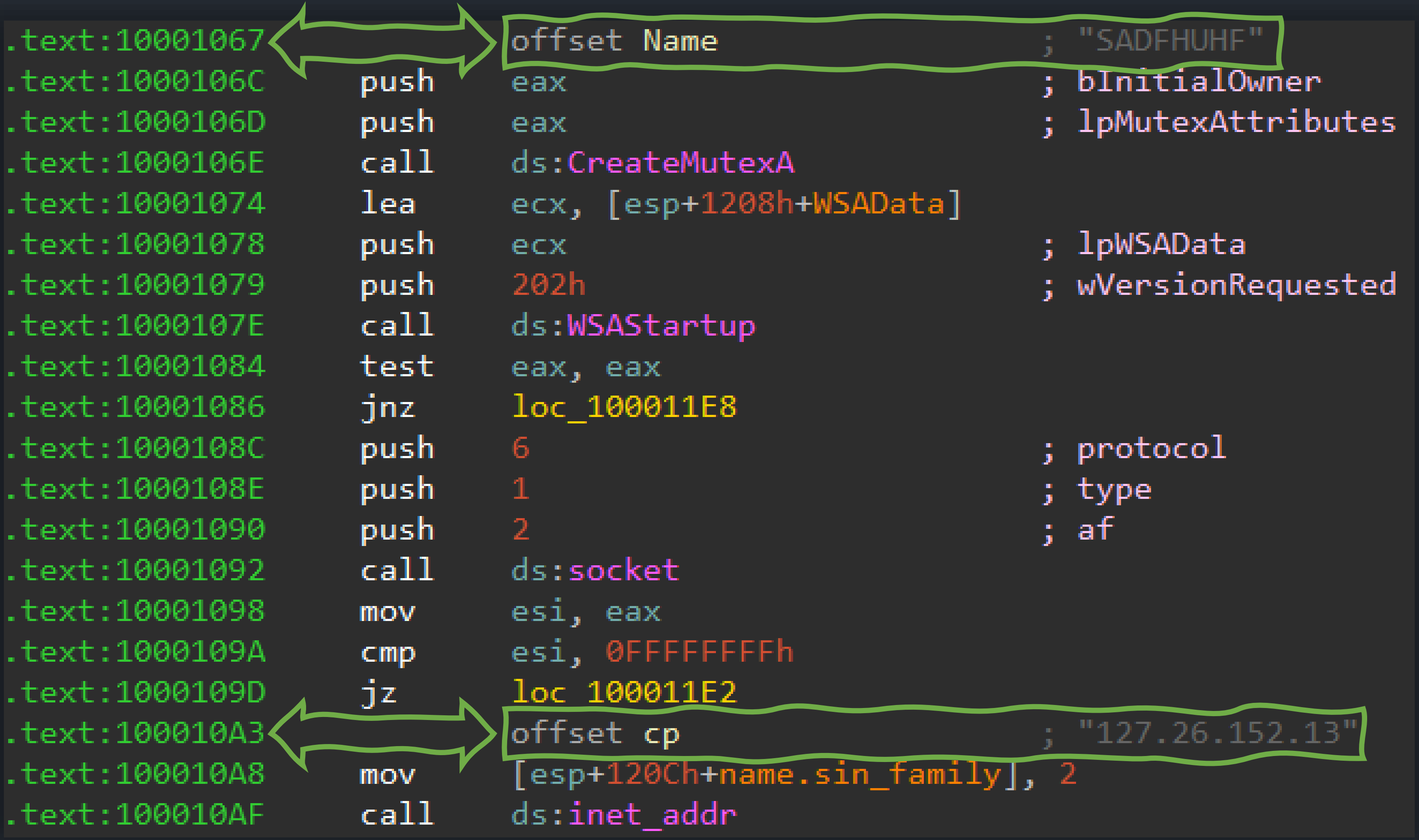
```
.text:10001067      push    offset Name                       ; "SADFHUHF"
.text:1000106C      push    eax                               ; bInitialOwner
.text:1000106D      push    eax                               ; lpMutexAttributes
.text:1000106E      call    ds:CreateMutexA
.text:10001074      lea     ecx, [esp+1208h+WSAData]
.text:10001078      push    ecx                               ; lpWSAData
.text:10001079      push    202h                              ; wVersionRequested
.text:1000107E      call    ds:WSAStartup
.text:10001084      test    eax, eax
.text:10001086      jnz     loc_100011E8
.text:1000108C      push    6                                 ; protocol
.text:1000108E      push    1                                 ; type
.text:10001090      push    2                                 ; af
.text:10001092      call    ds:socket
.text:10001098      mov     esi, eax
.text:1000109A      cmp     esi, 0FFFFFFFFh
.text:1000109D      jz      loc_100011E2
.text:100010A3      push    offset cp                         ; "127.26.152.13"
.text:100010A8      mov     [esp+120Ch+name.sin_family], 2
.text:100010AF      call    ds:inet_addr
```

Features

+ Rules

Code

- API calls
- numbers
- string references



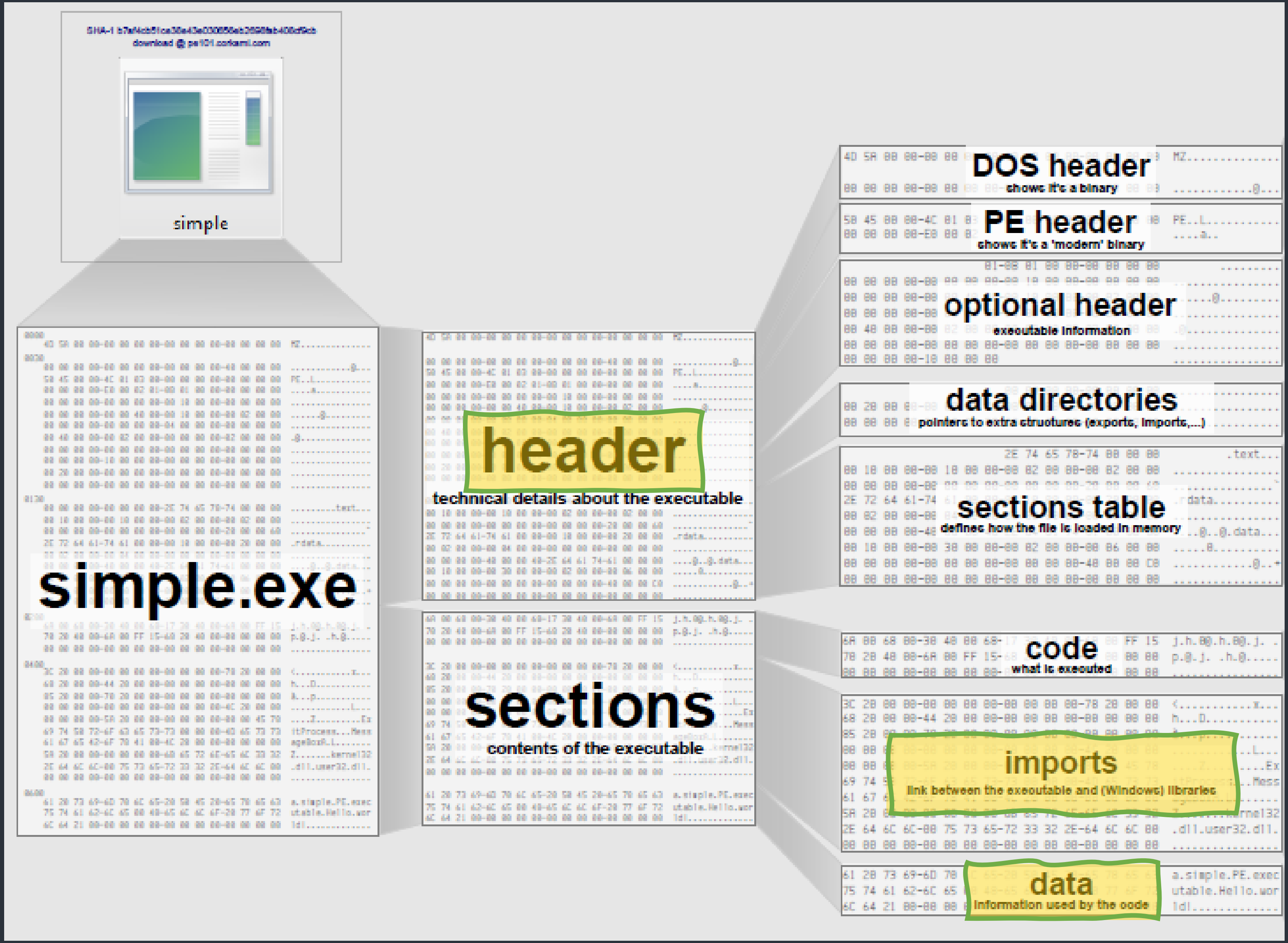
```
.text:10001067                 offset Name               ; "SADFHUHF"
.text:1000106C      push       eax                       ; bInitialOwner
.text:1000106D      push       eax                       ; lpMutexAttributes
.text:1000106E      call       ds:CreateMutexA
.text:10001074      lea        ecx, [esp+1208h+WSAData]
.text:10001078      push       ecx                       ; lpWSAData
.text:10001079      push       202h                      ; wVersionRequested
.text:1000107E      call       ds:WSAStartup
.text:10001084      test       eax, eax
.text:10001086      jnz        loc_100011E8
.text:1000108C      push       6                         ; protocol
.text:1000108E      push       1                         ; type
.text:10001090      push       2                         ; af
.text:10001092      call       ds:socket
.text:10001098      mov        esi, eax
.text:1000109A      cmp        esi, 0FFFFFFFFh
.text:1000109D      jz         loc_100011E2
.text:100010A3                 offset cp                 ; "127.26.152.13"
.text:100010A8      mov        [esp+120Ch+name.sin_family], 2
.text:100010AF      call       ds:inet_addr
```

Features

+ Rules

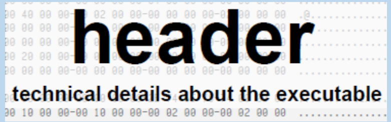
File

- header info
- imports
- strings


download @ pe101.corkami.com
simple
simple.exe
header
technical details about the executable
sections
contents of the executable
DOS header
shows it's a binary
PE header
shows it's a 'modern' binary
optional header
executable information
data directories
pointers to extra structures (exports, imports,...)
sections table
defines how the file is loaded in memory
code
what is executed
imports
link between the executable and (Windows) libraries
data
information used by the code

based on PE101 by Ange Albertini (CC BY 2.0)

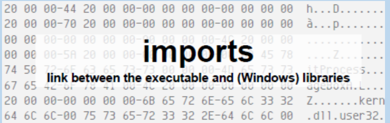
Features



header

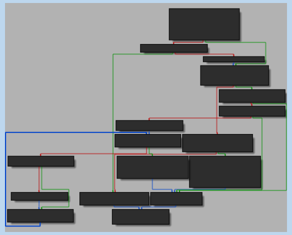
technical details about the executable

...



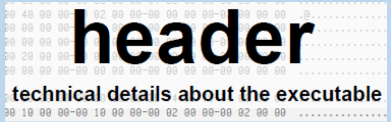
imports

link between the executable and (Windows) libraries



```
ds:CreateMutexA    ds:socket

0FFFFFFFFh  6  1  2

offset Name                                 ; "SADFHUHF"
offset cp                              ; "127.26.152.13"
```

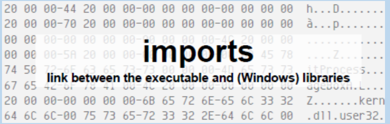
Features



header

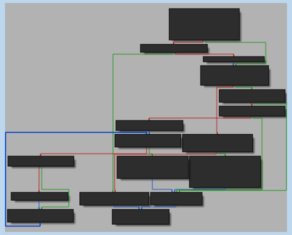
technical details about the executable

...



imports

link between the executable and (Windows) libraries



```
ds:CreateMutexA    ds:socket

0FFFFFFFFh  6  1  2

offset Name                    ; "SADFHUHF"
offset cp                      ; "127.26.152.13"
```

+

Rules

Features

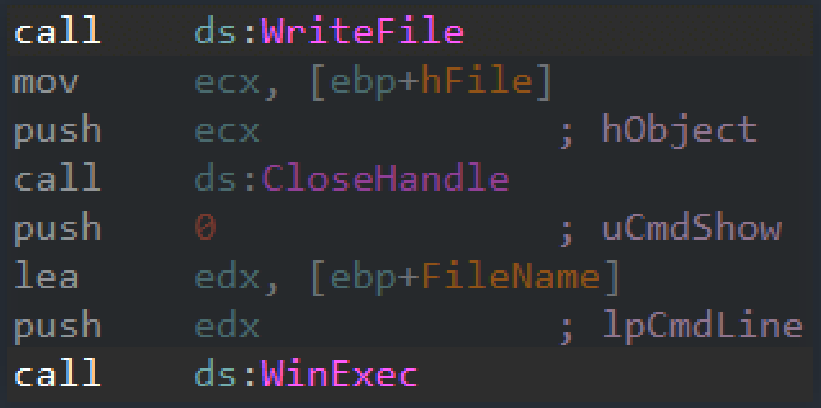
+ Rules

Feature combination → capability

Features

+ Rules

Feature combination → capability



```
call    ds:WriteFile
mov     ecx, [ebp+hFile]
push    ecx                     ; hObject
call    ds:CloseHandle
push    0                       ; uCmdShow
lea     edx, [ebp+FileName]
push    edx                     ; lpCmdLine
call    ds:WinExec
```

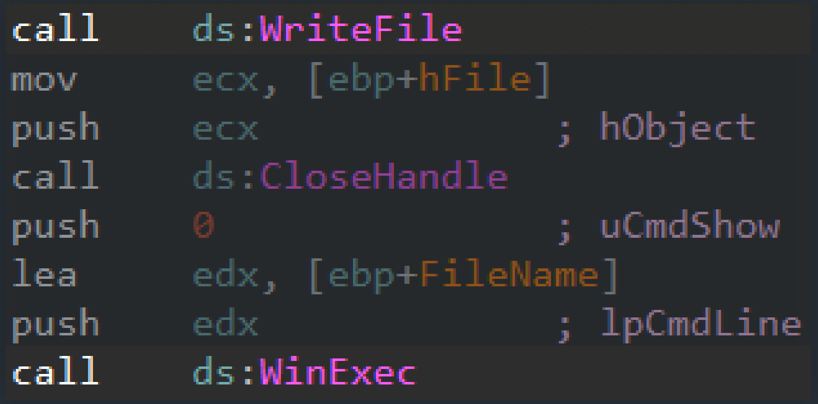
AND

Dropper

Features

+ Rules

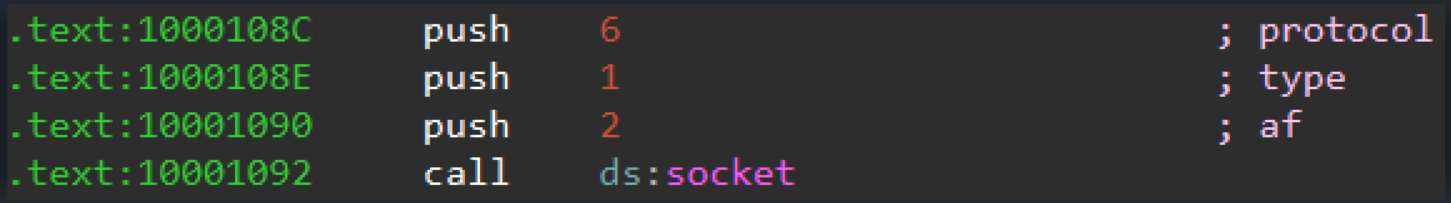
Feature combination → capability



```
call    ds:WriteFile
mov     ecx, [ebp+hFile]
push    ecx             ; hObject
call    ds:CloseHandle
push    0               ; uCmdShow
lea     edx, [ebp+FileName]
push    edx             ; lpCmdLine
call    ds:WinExec
```

AND

Dropper

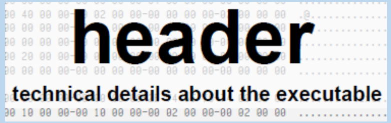


```
.text:1000108C      push    6                               ; protocol
.text:1000108E      push    1                               ; type
.text:10001090      push    2                               ; af
.text:10001092      call    ds:socket
```

AND

TCP socket

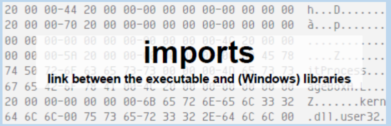
Features



header

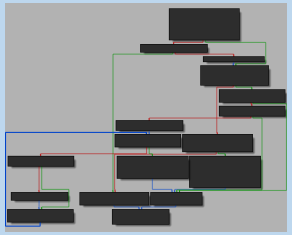
technical details about the executable

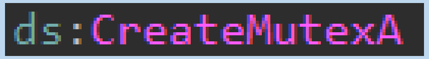
...



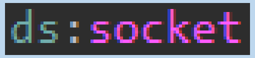
imports

link between the executable and (Windows) libraries

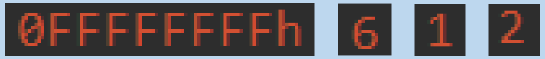




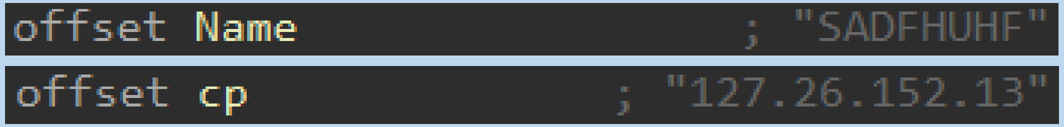
```
ds:CreateMutexA
```



```
ds:socket
```



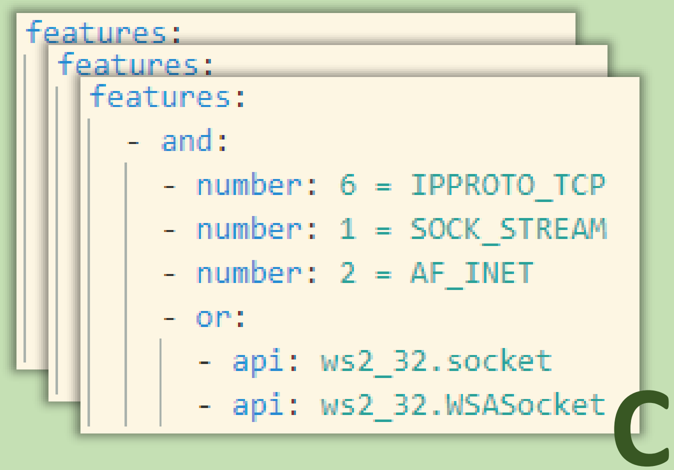
```
0FFFFFFFFh  6  1  2
```



```
offset Name                    ; "SADFHUHF"
offset cp                 ; "127.26.152.13"
```

+

Rules



```
features:
  - and:
    - number: 6 = IPPROTO_TCP
    - number: 1 = SOCK_STREAM
    - number: 2 = AF_INET
    - or:
      - api: ws2_32.socket
      - api: ws2_32.WSASocket
```

AND

OR

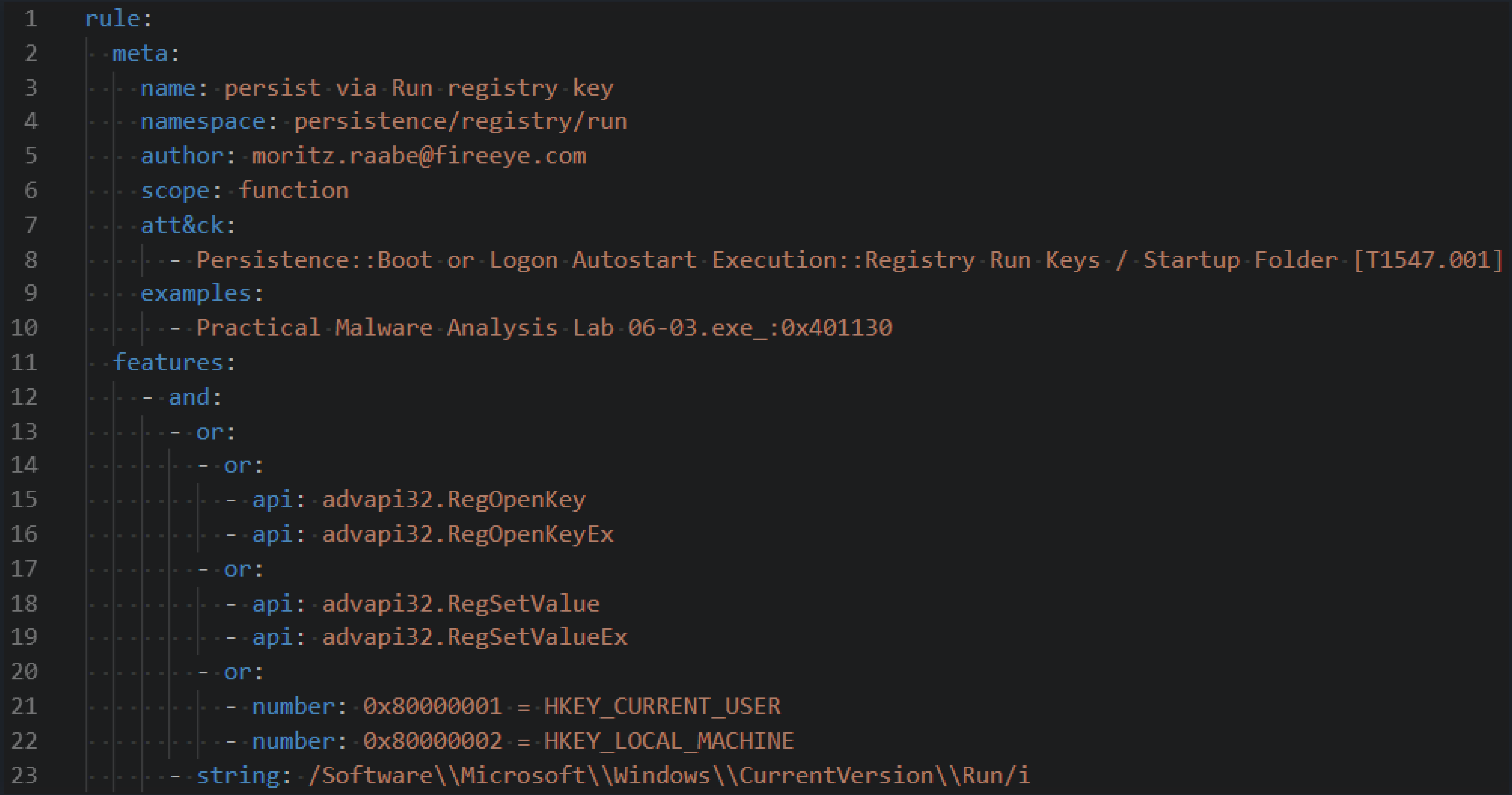
NOT

COUNT

=

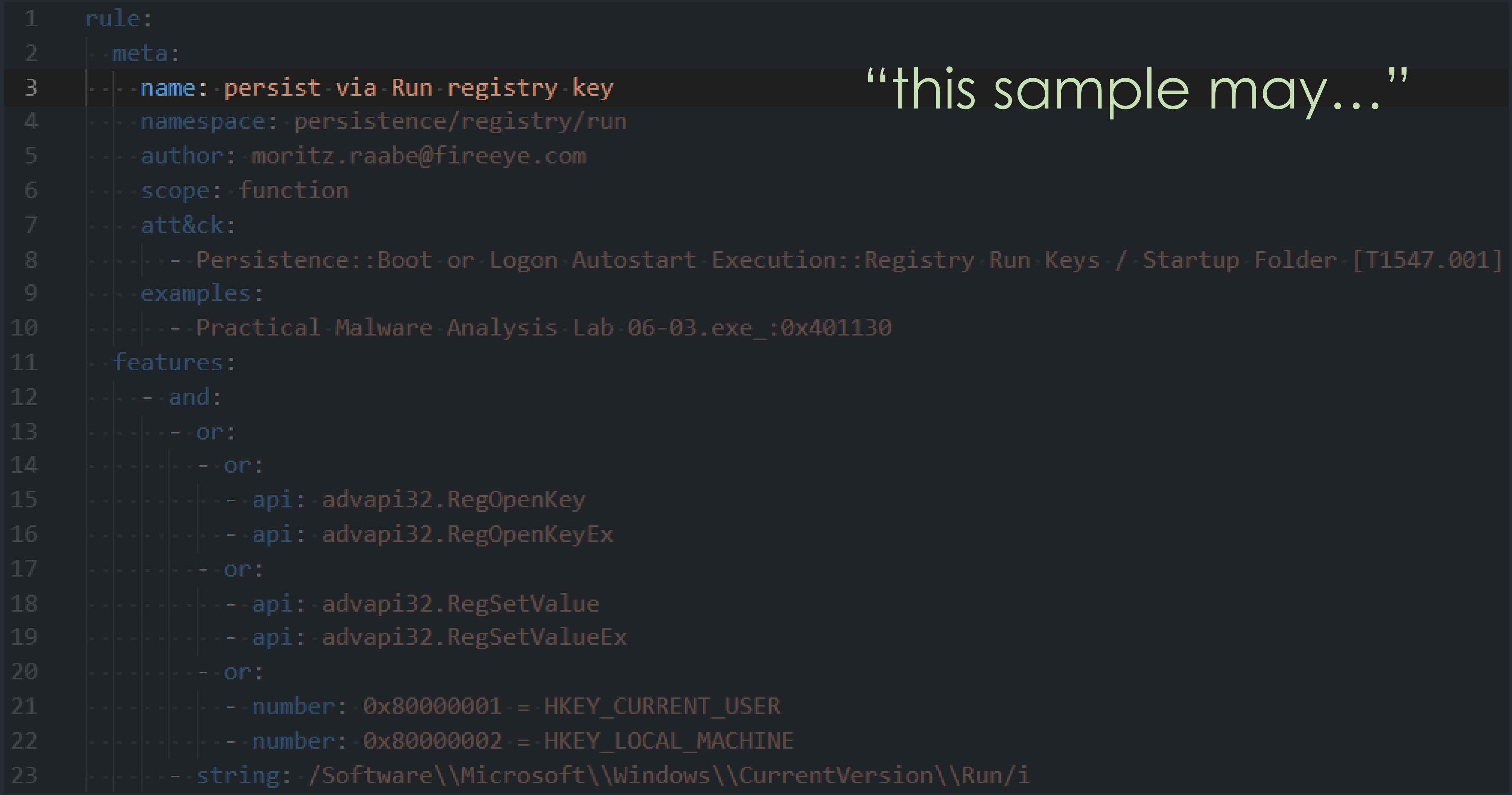
Program Capabilities

Persist via registry Run key



```yaml
rule:
  meta:
    name: persist via Run registry key
    namespace: persistence/registry/run
    author: moritz.raabe@fireeye.com
    scope: function
    att&ck:
      - Persistence::Boot or Logon Autostart Execution::Registry Run Keys / Startup Folder [T1547.001]
    examples:
      - Practical Malware Analysis Lab 06-03.exe_:0x401130
  features:
    - and:
      - or:
        - or:
          - api: advapi32.RegOpenKey
          - api: advapi32.RegOpenKeyEx
        - or:
          - api: advapi32.RegSetValue
          - api: advapi32.RegSetValueEx
        - or:
          - number: 0x80000001 = HKEY_CURRENT_USER
          - number: 0x80000002 = HKEY_LOCAL_MACHINE
      - string: /Software\\Microsoft\\Windows\\CurrentVersion\\Run/i
```

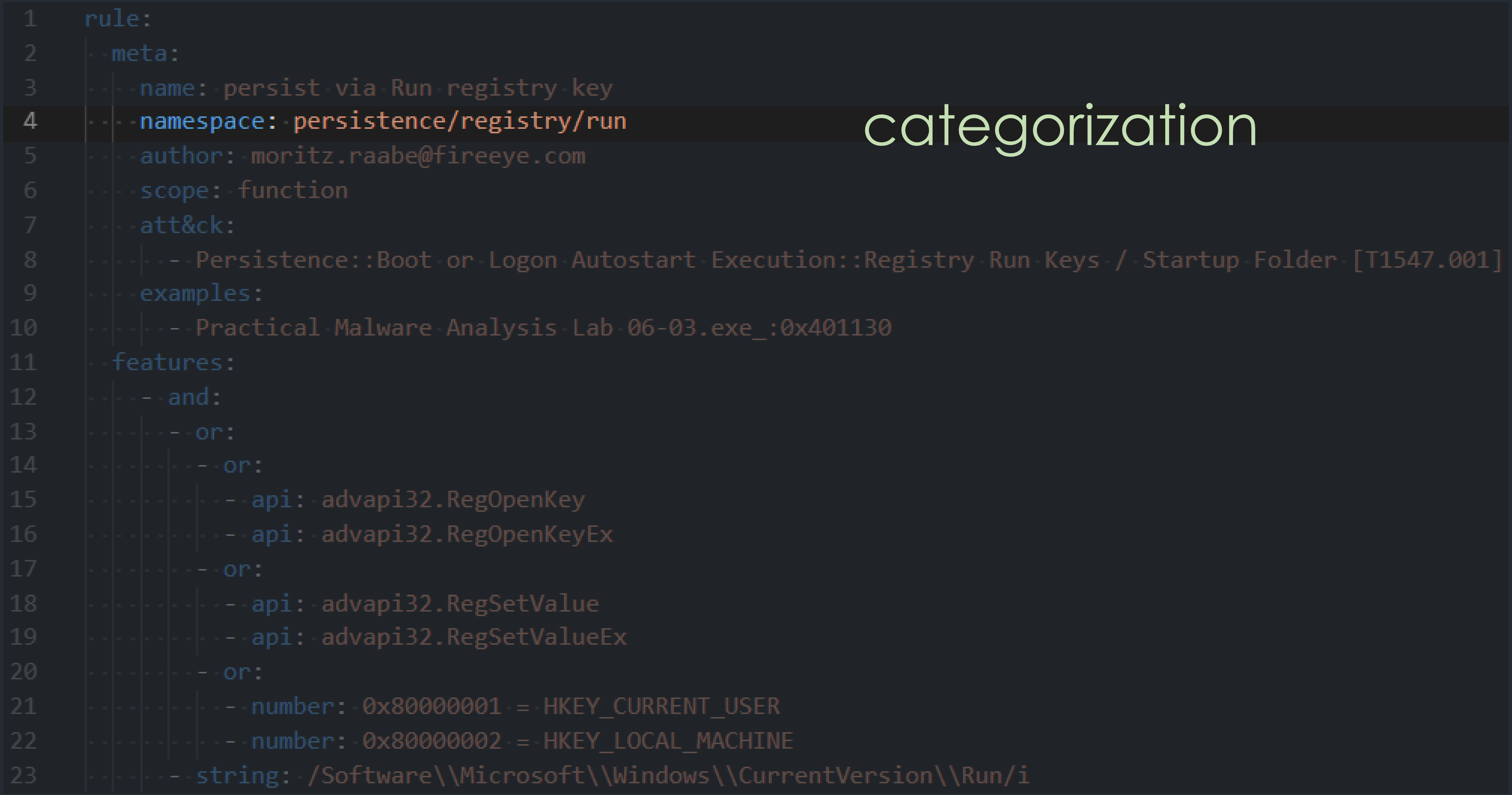
Persist via registry Run key



“this sample may…”

```
rule:
  meta:
    name: persist via Run registry key
    namespace: persistence/registry/run
    author: moritz.raabe@fireeye.com
    scope: function
    att&ck:
      - Persistence::Boot or Logon Autostart Execution::Registry Run Keys / Startup Folder [T1547.001]
    examples:
      - Practical Malware Analysis Lab 06-03.exe_:0x401130
  features:
    - and:
      - or:
        - or:
          - api: advapi32.RegOpenKey
          - api: advapi32.RegOpenKeyEx
        - or:
          - api: advapi32.RegSetValue
          - api: advapi32.RegSetValueEx
        - or:
          - number: 0x80000001 = HKEY_CURRENT_USER
          - number: 0x80000002 = HKEY_LOCAL_MACHINE
      - string: /Software\\Microsoft\\Windows\\CurrentVersion\\Run/i
```

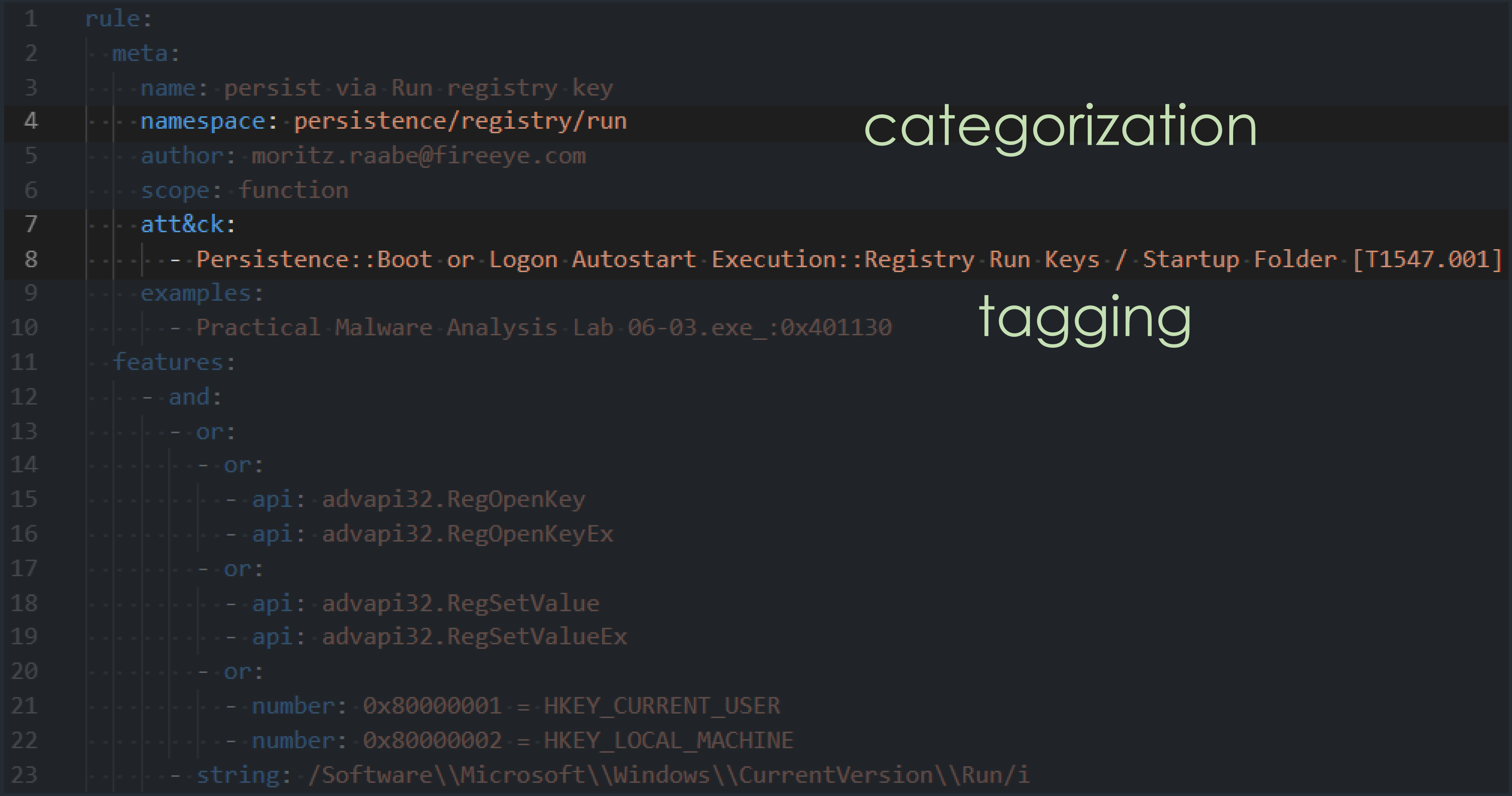
Persist via registry Run key



```
rule:
  meta:
    name: persist via Run registry key
    namespace: persistence/registry/run
    author: moritz.raabe@fireeye.com
    scope: function
    att&ck:
      - Persistence::Boot or Logon Autostart Execution::Registry Run Keys / Startup Folder [T1547.001]
    examples:
      - Practical Malware Analysis Lab 06-03.exe_:0x401130
  features:
    - and:
      - or:
        - or:
          - api: advapi32.RegOpenKey
          - api: advapi32.RegOpenKeyEx
        - or:
          - api: advapi32.RegSetValue
          - api: advapi32.RegSetValueEx
        - or:
          - number: 0x80000001 = HKEY_CURRENT_USER
          - number: 0x80000002 = HKEY_LOCAL_MACHINE
      - string: /Software\\Microsoft\\Windows\\CurrentVersion\\Run/i
```

categorization

Persist via registry Run key

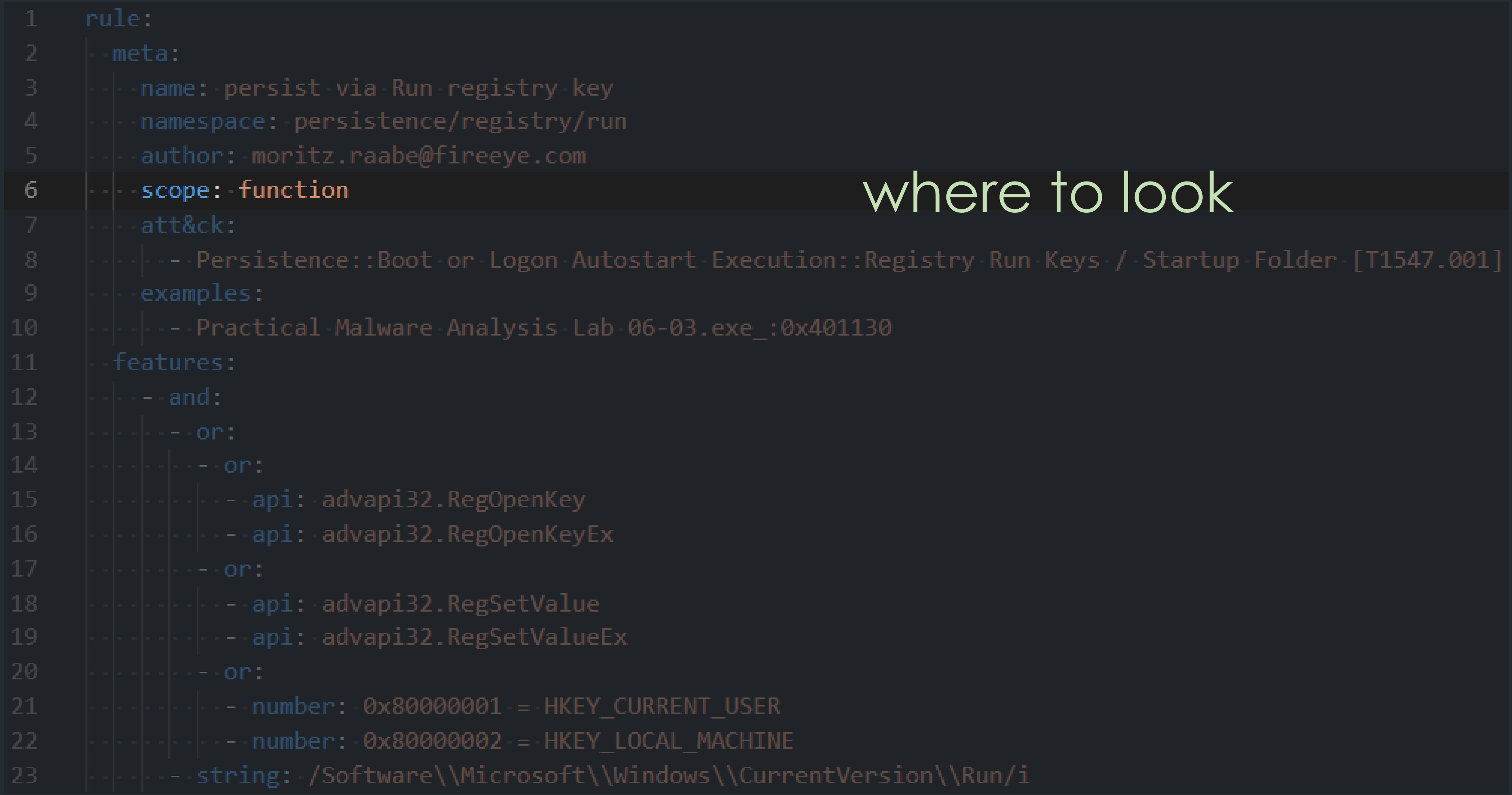


```
rule:
  meta:
    name: persist via Run registry key
    namespace: persistence/registry/run
    author: moritz.raabe@fireeye.com
    scope: function
    att&ck:
      - Persistence::Boot or Logon Autostart Execution::Registry Run Keys / Startup Folder [T1547.001]
    examples:
      - Practical Malware Analysis Lab 06-03.exe_:0x401130
  features:
    - and:
      - or:
        - or:
          - api: advapi32.RegOpenKey
          - api: advapi32.RegOpenKeyEx
        - or:
          - api: advapi32.RegSetValue
          - api: advapi32.RegSetValueEx
        - or:
          - number: 0x80000001 = HKEY_CURRENT_USER
          - number: 0x80000002 = HKEY_LOCAL_MACHINE
      - string: /Software\\Microsoft\\Windows\\CurrentVersion\\Run/i
```

categorization

tagging

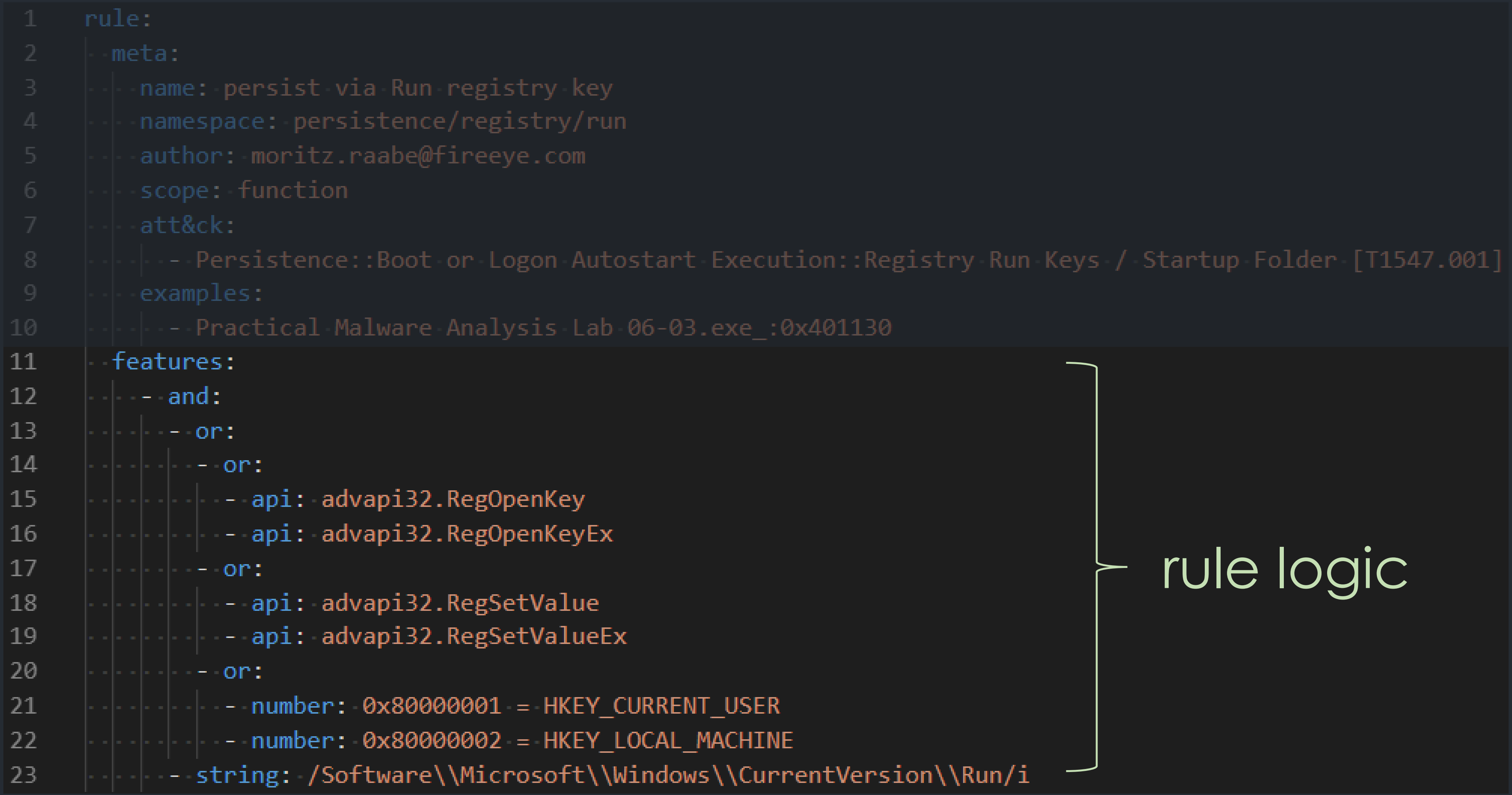
Persist via registry Run key



```
rule:
  meta:
    name: persist via Run registry key
    namespace: persistence/registry/run
    author: moritz.raabe@fireeye.com
    scope: function
    att&ck:
      - Persistence::Boot or Logon Autostart Execution::Registry Run Keys / Startup Folder [T1547.001]
    examples:
      - Practical Malware Analysis Lab 06-03.exe_:0x401130
  features:
    - and:
      - or:
        - or:
          - api: advapi32.RegOpenKey
          - api: advapi32.RegOpenKeyEx
        - or:
          - api: advapi32.RegSetValue
          - api: advapi32.RegSetValueEx
        - or:
          - number: 0x80000001 = HKEY_CURRENT_USER
          - number: 0x80000002 = HKEY_LOCAL_MACHINE
      - string: /Software\\Microsoft\\Windows\\CurrentVersion\\Run/i
```

where to look

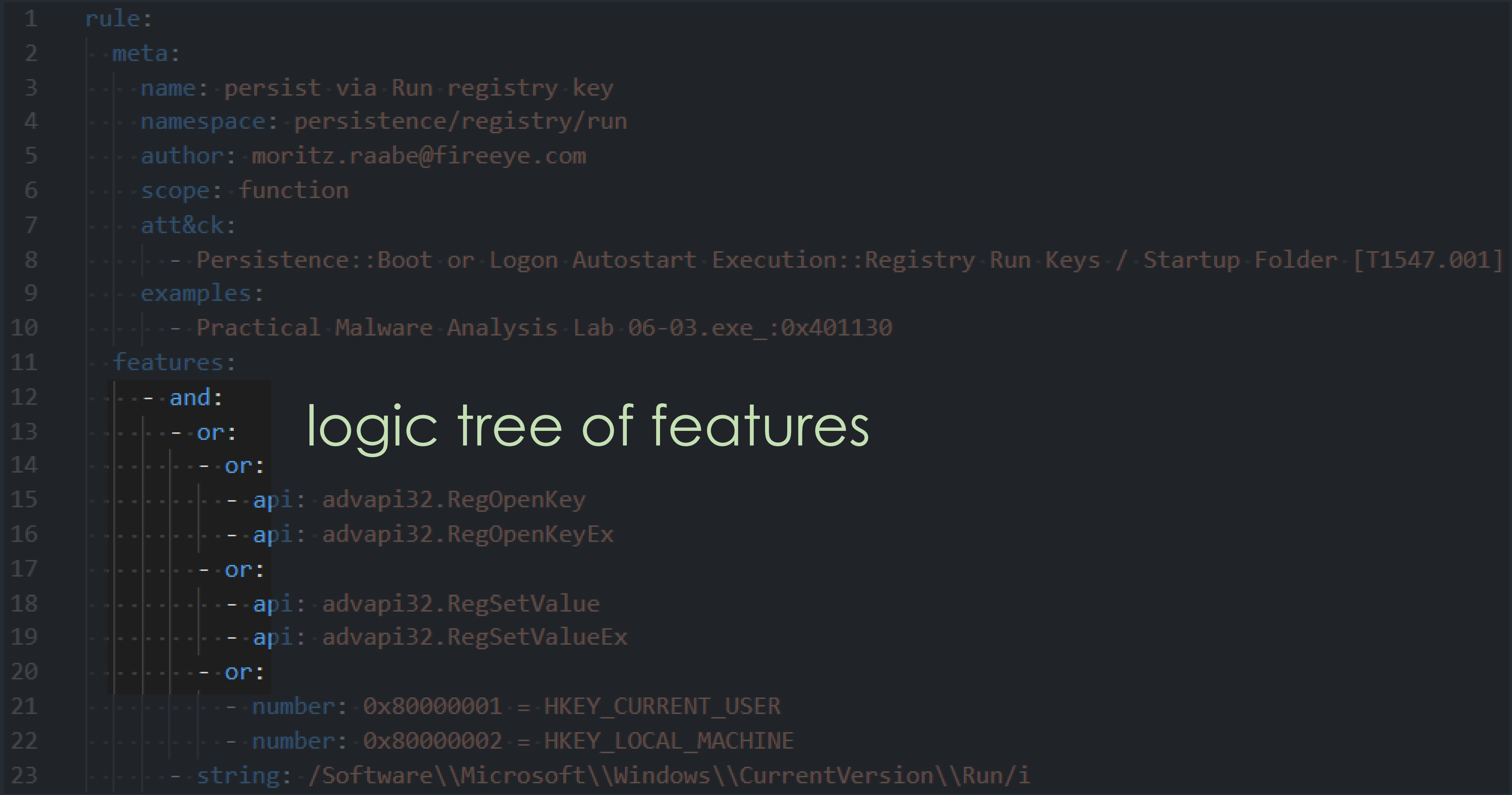
Persist via registry Run key



```
rule:
  meta:
    name: persist via Run registry key
    namespace: persistence/registry/run
    author: moritz.raabe@fireeye.com
    scope: function
    att&ck:
      - Persistence::Boot or Logon Autostart Execution::Registry Run Keys / Startup Folder [T1547.001]
    examples:
      - Practical Malware Analysis Lab 06-03.exe_:0x401130
  features:
    - and:
      - or:
        - or:
          - api: advapi32.RegOpenKey
          - api: advapi32.RegOpenKeyEx
        - or:
          - api: advapi32.RegSetValue
          - api: advapi32.RegSetValueEx
        - or:
          - number: 0x80000001 = HKEY_CURRENT_USER
          - number: 0x80000002 = HKEY_LOCAL_MACHINE
      - string: /Software\\Microsoft\\Windows\\CurrentVersion\\Run/i
```

rule logic

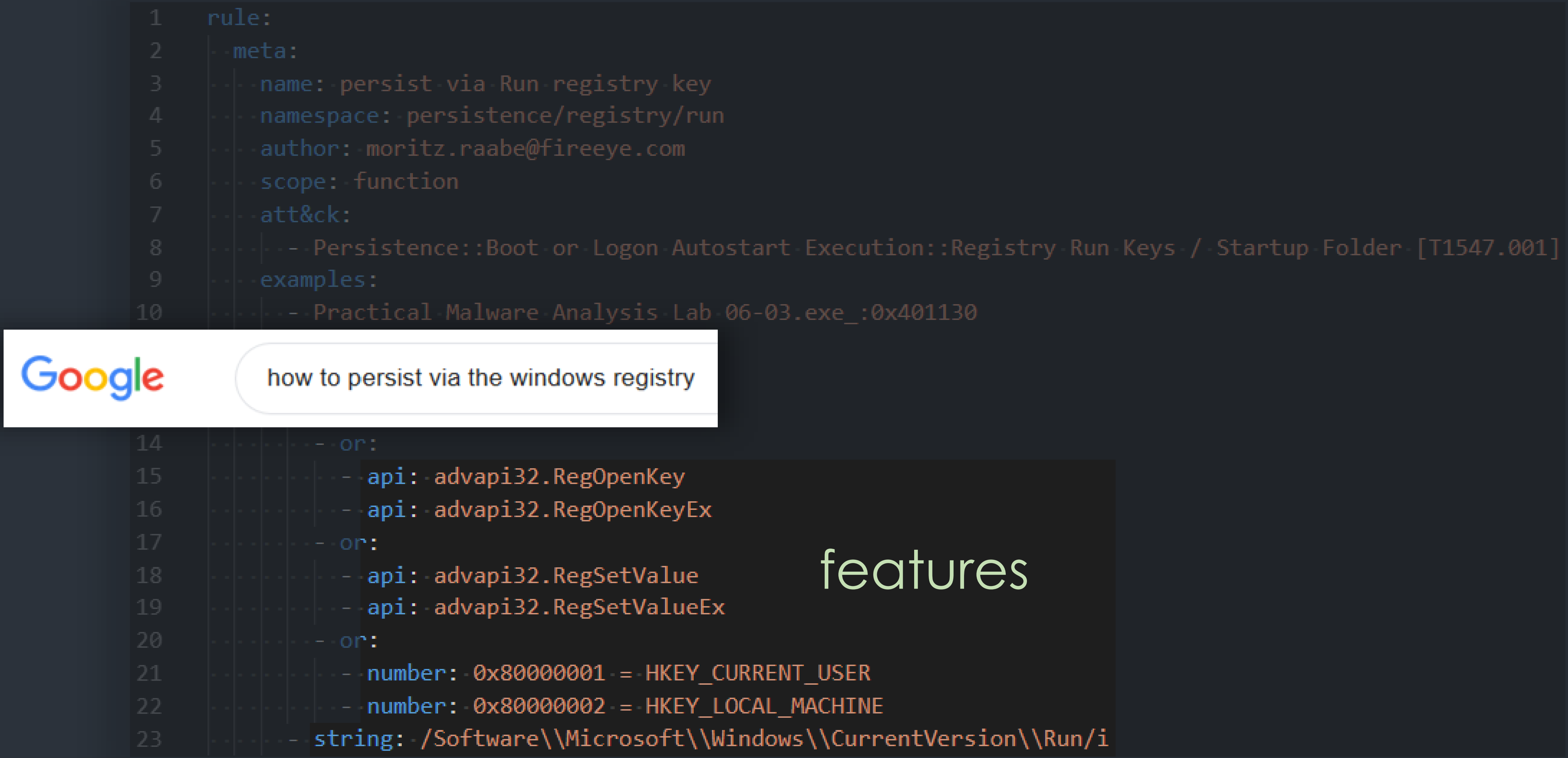
Persist via registry Run key



```
rule:
  meta:
    name: persist via Run registry key
    namespace: persistence/registry/run
    author: moritz.raabe@fireeye.com
    scope: function
    att&ck:
      - Persistence::Boot or Logon Autostart Execution::Registry Run Keys / Startup Folder [T1547.001]
    examples:
      - Practical Malware Analysis Lab 06-03.exe_:0x401130
  features:
    - and:
      - or:
        - or:
          - api: advapi32.RegOpenKey
          - api: advapi32.RegOpenKeyEx
        - or:
          - api: advapi32.RegSetValue
          - api: advapi32.RegSetValueEx
        - or:
          - number: 0x80000001 = HKEY_CURRENT_USER
          - number: 0x80000002 = HKEY_LOCAL_MACHINE
      - string: /Software\\Microsoft\\Windows\\CurrentVersion\\Run/i
```

logic tree of features

Persist via registry Run key



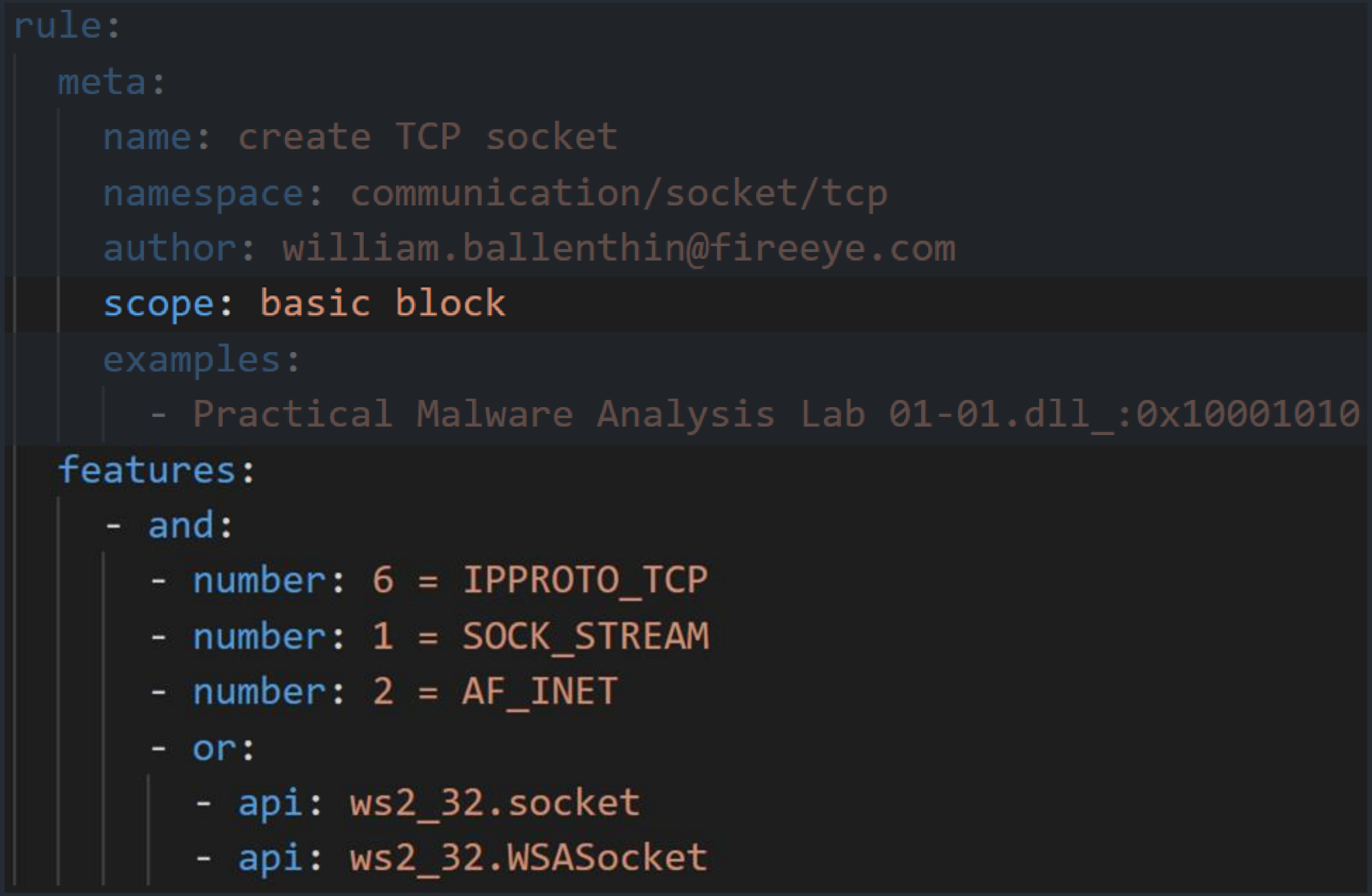
```
rule:
  meta:
    name: persist via Run registry key
    namespace: persistence/registry/run
    author: moritz.raabe@fireeye.com
    scope: function
    att&ck:
      - Persistence::Boot or Logon Autostart Execution::Registry Run Keys / Startup Folder [T1547.001]
    examples:
      - Practical Malware Analysis Lab 06-03.exe_:0x401130
```

how to persist via the windows registry

```
        - or:
          - api: advapi32.RegOpenKey
          - api: advapi32.RegOpenKeyEx
        - or:
          - api: advapi32.RegSetValue
          - api: advapi32.RegSetValueEx
        - or:
          - number: 0x80000001 = HKEY_CURRENT_USER
          - number: 0x80000002 = HKEY_LOCAL_MACHINE
      - string: /Software\\Microsoft\\Windows\\CurrentVersion\\Run/i
```

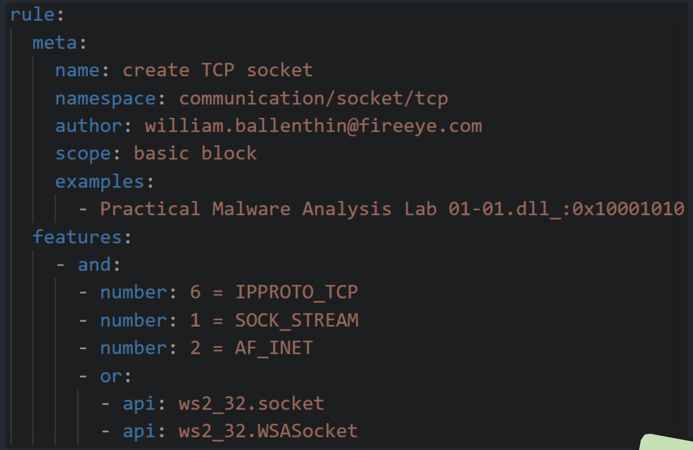
features

Create TCP socket



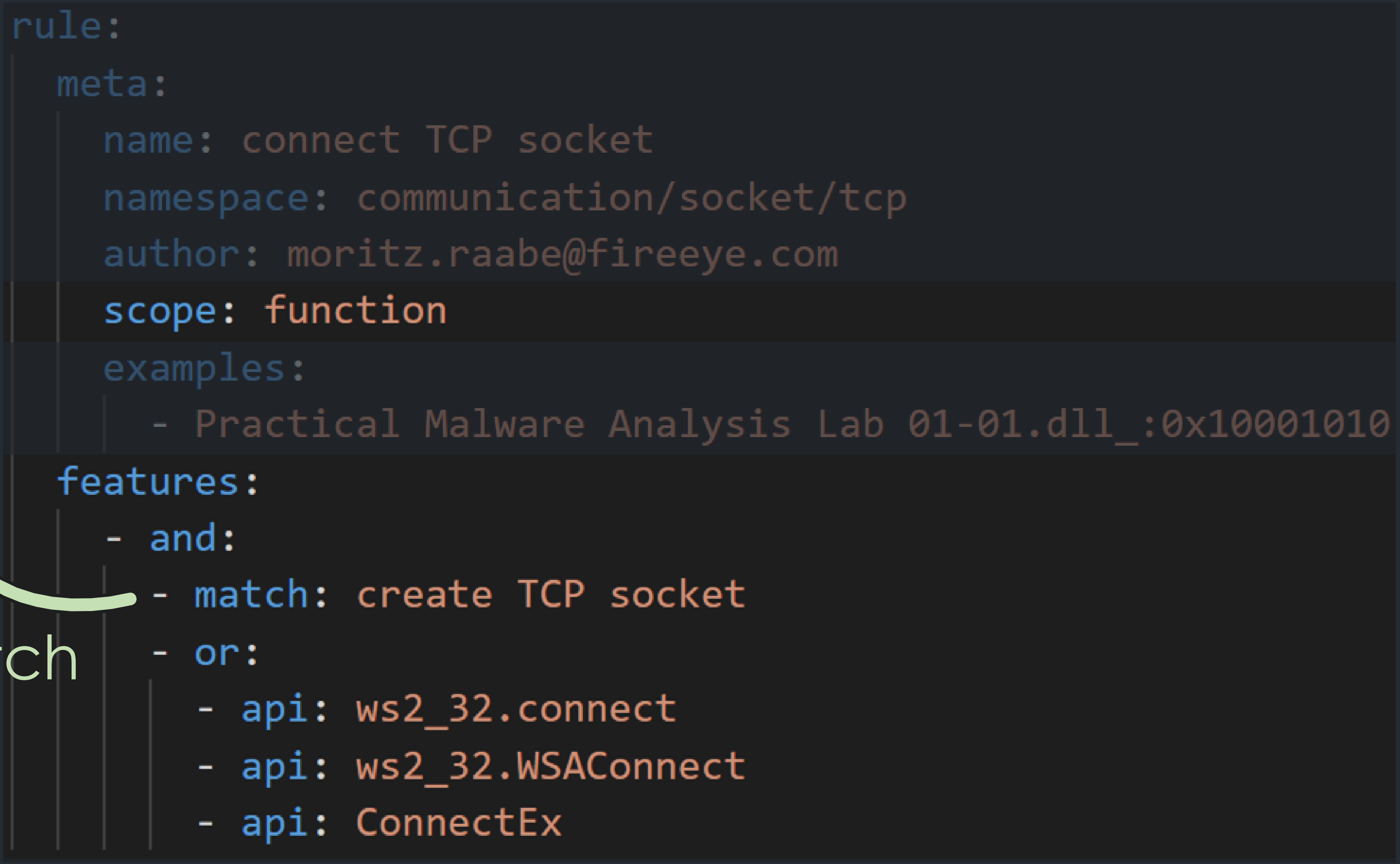
```
rule:
  meta:
    name: create TCP socket
    namespace: communication/socket/tcp
    author: william.ballenthin@fireeye.com
    scope: basic block
    examples:
      - Practical Malware Analysis Lab 01-01.dll_:0x10001010
  features:
    - and:
      - number: 6 = IPPROTO_TCP
      - number: 1 = SOCK_STREAM
      - number: 2 = AF_INET
      - or:
        - api: ws2_32.socket
        - api: ws2_32.WSASocket
```

Connect TCP socket



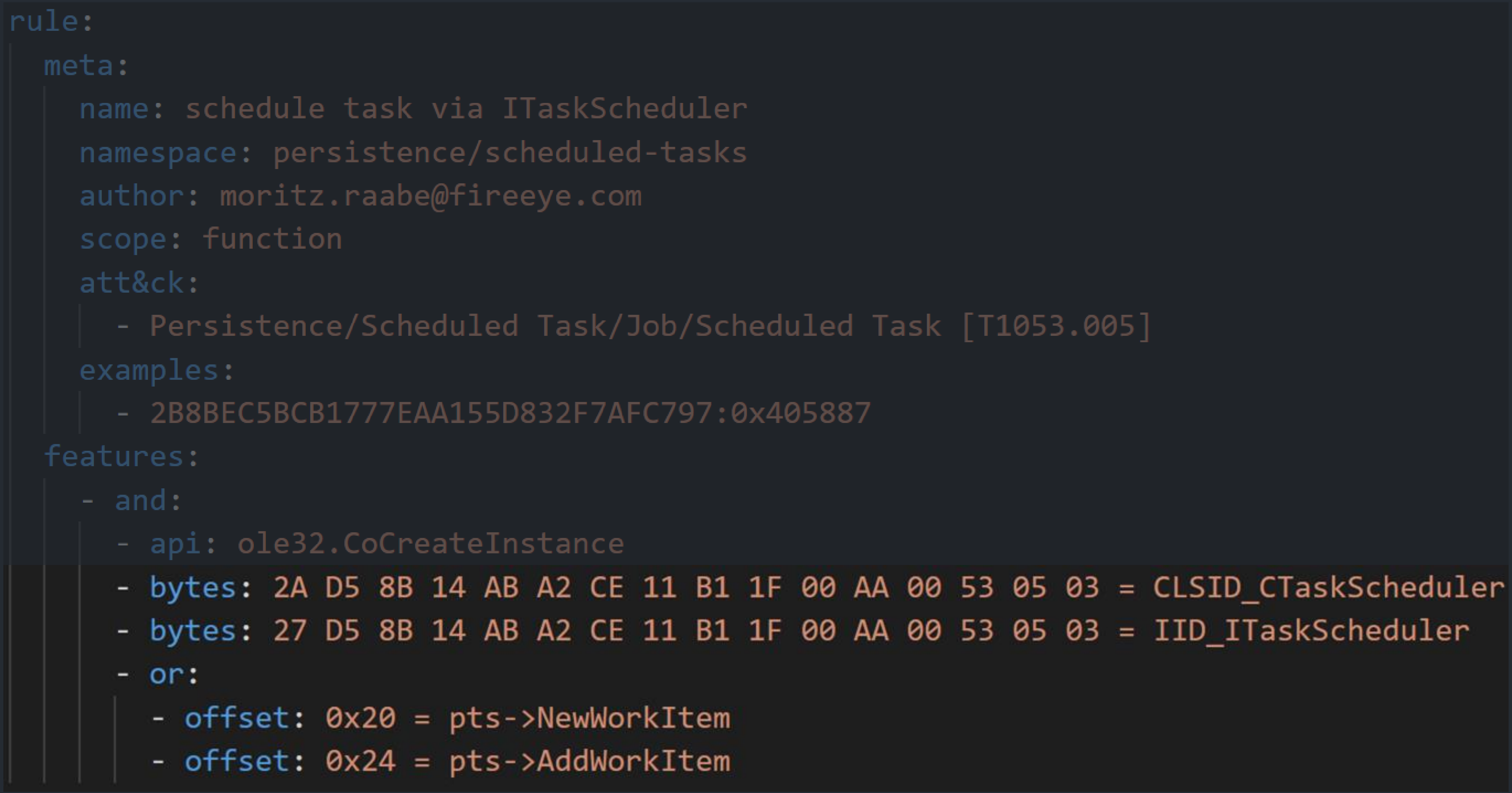
```
rule:
  meta:
    name: create TCP socket
    namespace: communication/socket/tcp
    author: william.ballenthin@fireeye.com
    scope: basic block
    examples:
      - Practical Malware Analysis Lab 01-01.dll_:0x10001010
  features:
    - and:
      - number: 6 = IPPROTO_TCP
      - number: 1 = SOCK_STREAM
      - number: 2 = AF_INET
      - or:
        - api: ws2_32.socket
        - api: ws2_32.WSASocket
```

previous rule match



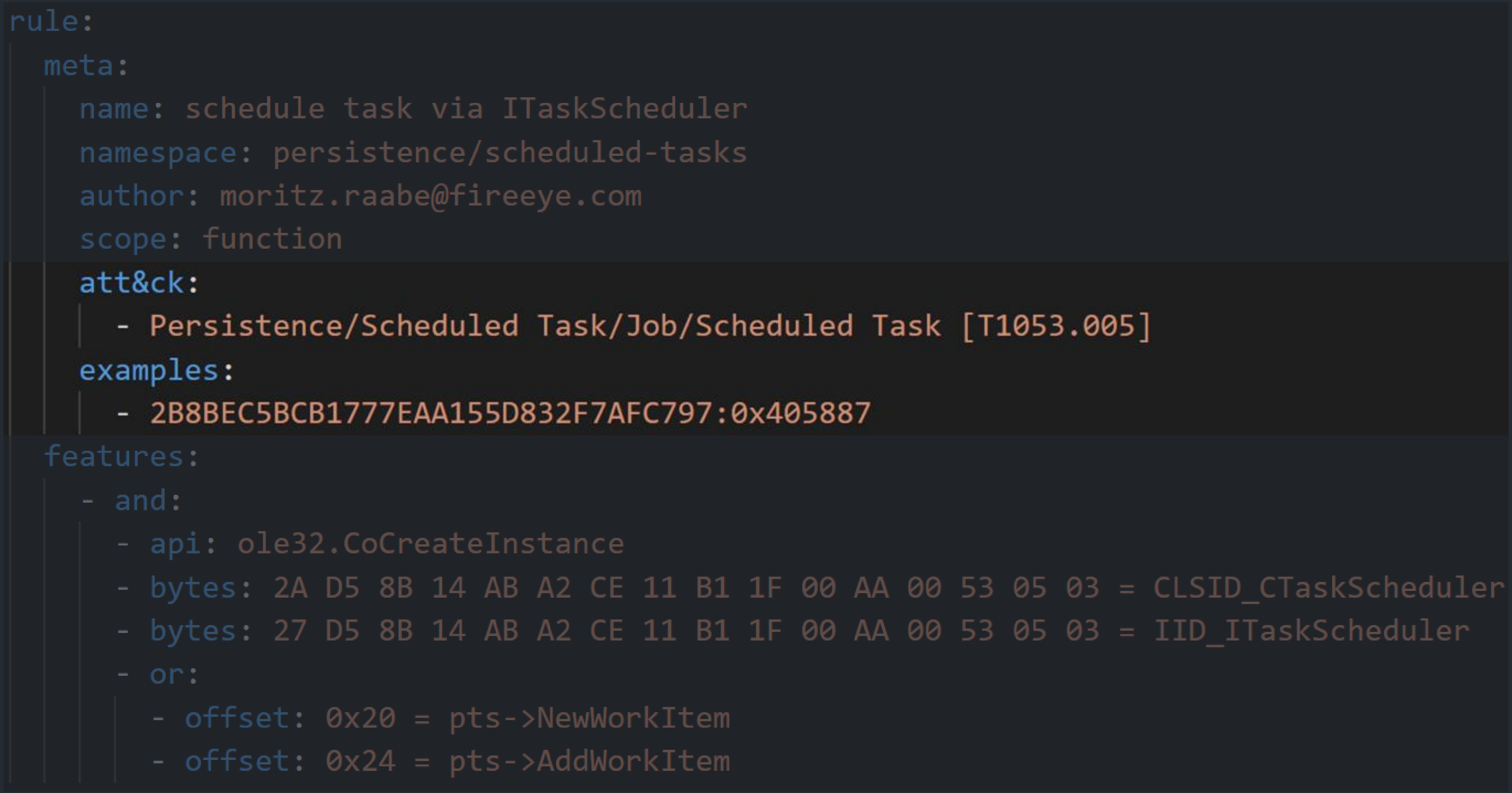
```
rule:
  meta:
    name: connect TCP socket
    namespace: communication/socket/tcp
    author: moritz.raabe@fireeye.com
    scope: function
    examples:
      - Practical Malware Analysis Lab 01-01.dll_:0x10001010
  features:
    - and:
      - match: create TCP socket
      - or:
        - api: ws2_32.connect
        - api: ws2_32.WSAConnect
        - api: ConnectEx
```

Schedule task via ITaskScheduler (COM)



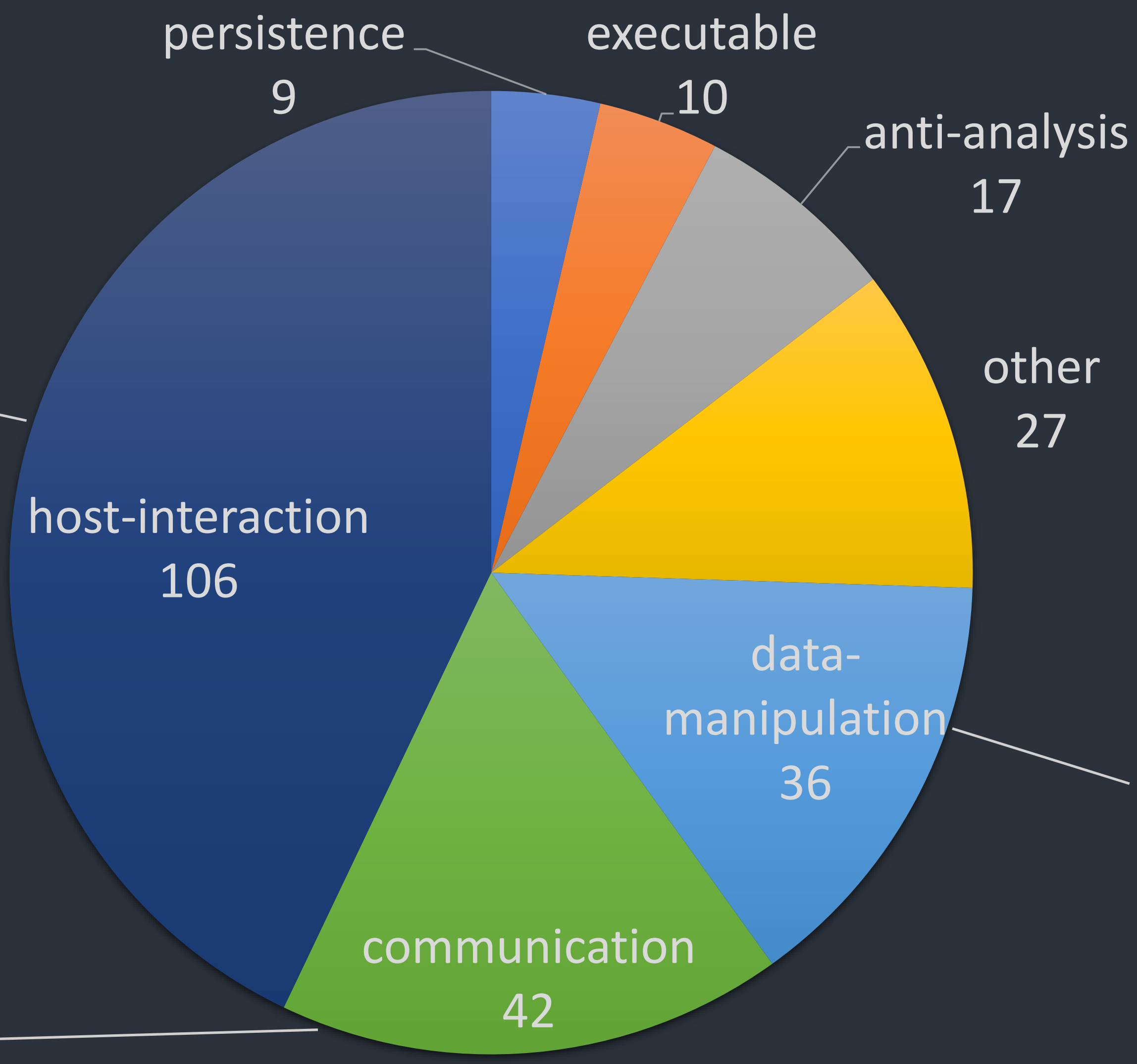
```
rule:
  meta:
    name: schedule task via ITaskScheduler
    namespace: persistence/scheduled-tasks
    author: moritz.raabe@fireeye.com
    scope: function
    att&ck:
      - Persistence/Scheduled Task/Job/Scheduled Task [T1053.005]
    examples:
      - 2B8BEC5BCB1777EAA155D832F7AFC797:0x405887
  features:
    - and:
      - api: ole32.CoCreateInstance
      - bytes: 2A D5 8B 14 AB A2 CE 11 B1 1F 00 AA 00 53 05 03 = CLSID_CTaskScheduler
      - bytes: 27 D5 8B 14 AB A2 CE 11 B1 1F 00 AA 00 53 05 03 = IID_ITaskScheduler
      - or:
        - offset: 0x20 = pts->NewWorkItem
        - offset: 0x24 = pts->AddWorkItem
```

Schedule task via ITaskScheduler (COM)



```
rule:
  meta:
    name: schedule task via ITaskScheduler
    namespace: persistence/scheduled-tasks
    author: moritz.raabe@fireeye.com
    scope: function
    att&ck:
      - Persistence/Scheduled Task/Job/Scheduled Task [T1053.005]
    examples:
      - 2B8BEC5BCB1777EAA155D832F7AFC797:0x405887
  features:
    - and:
      - api: ole32.CoCreateInstance
      - bytes: 2A D5 8B 14 AB A2 CE 11 B1 1F 00 AA 00 53 05 03 = CLSID_CTaskScheduler
      - bytes: 27 D5 8B 14 AB A2 CE 11 B1 1F 00 AA 00 53 05 03 = IID_ITaskScheduler
      - or:
        - offset: 0x20 = pts->NewWorkItem
        - offset: 0x24 = pts->AddWorkItem
```

~260 rules – by namespace



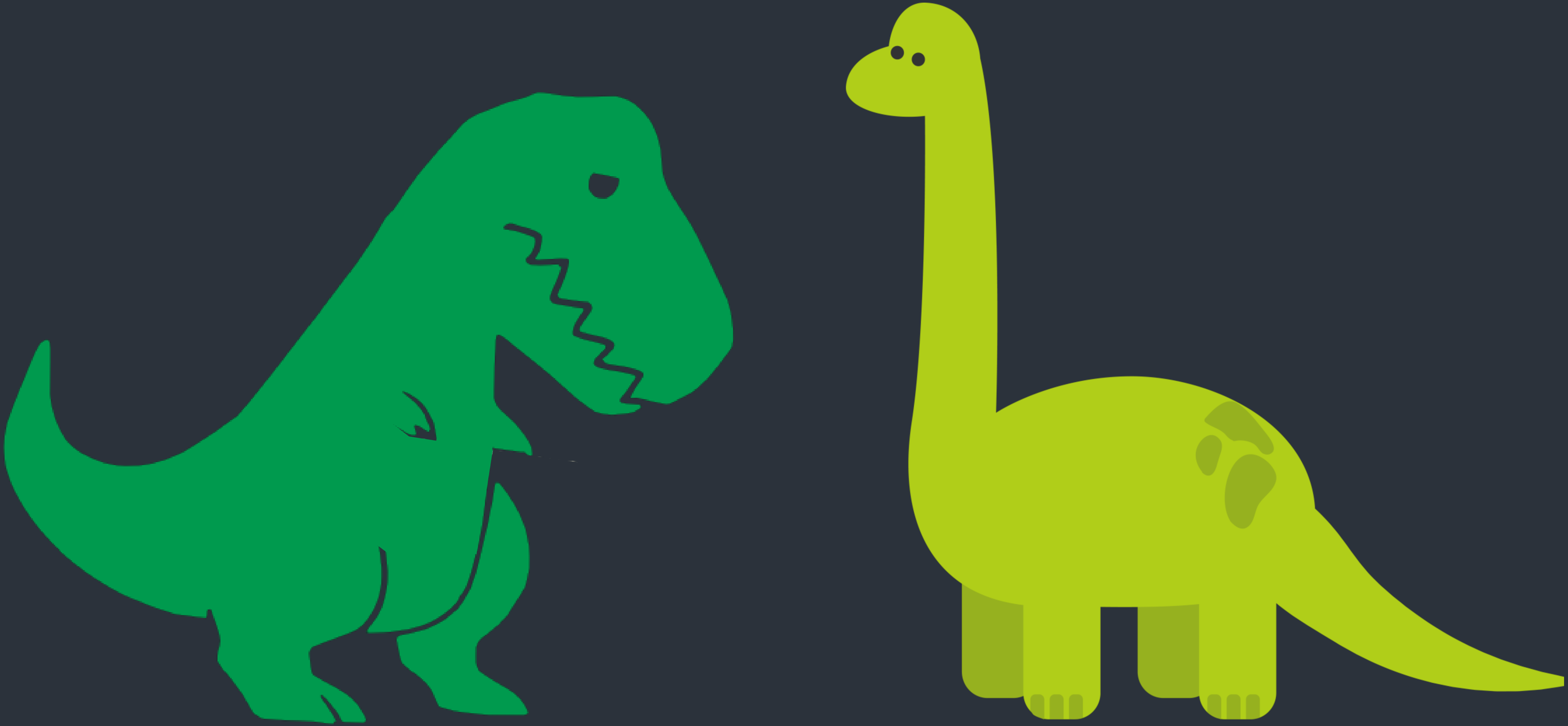
file-system
registry
process
service

compression
encoding
encryption
hashing

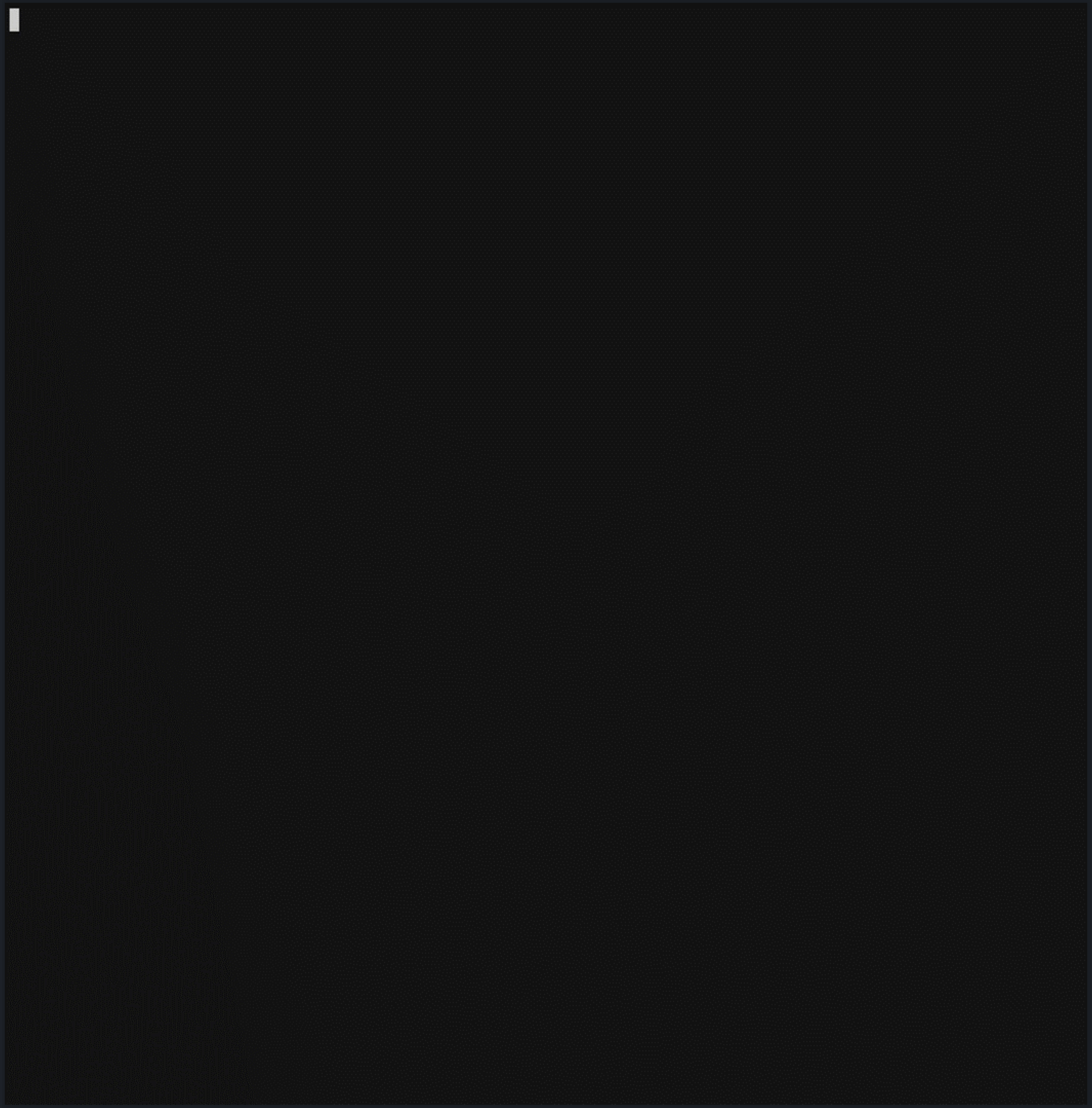
ftp
http
tcp

FLARE

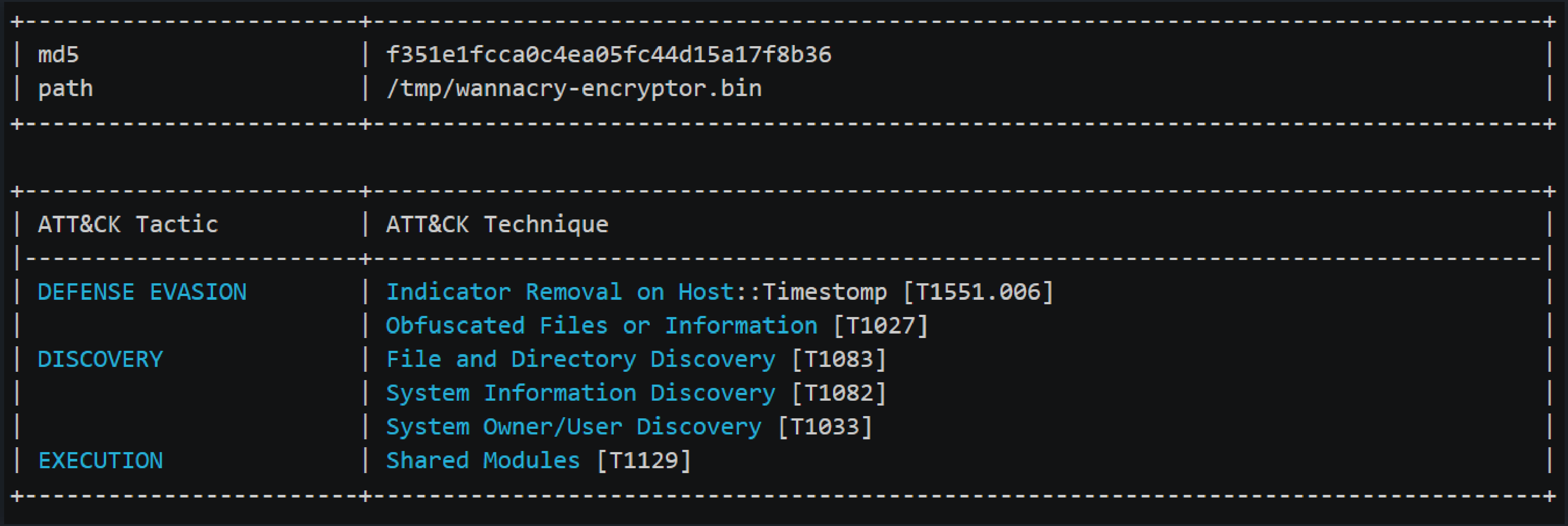
CAPA vs Wannacry encryptor



encryptor

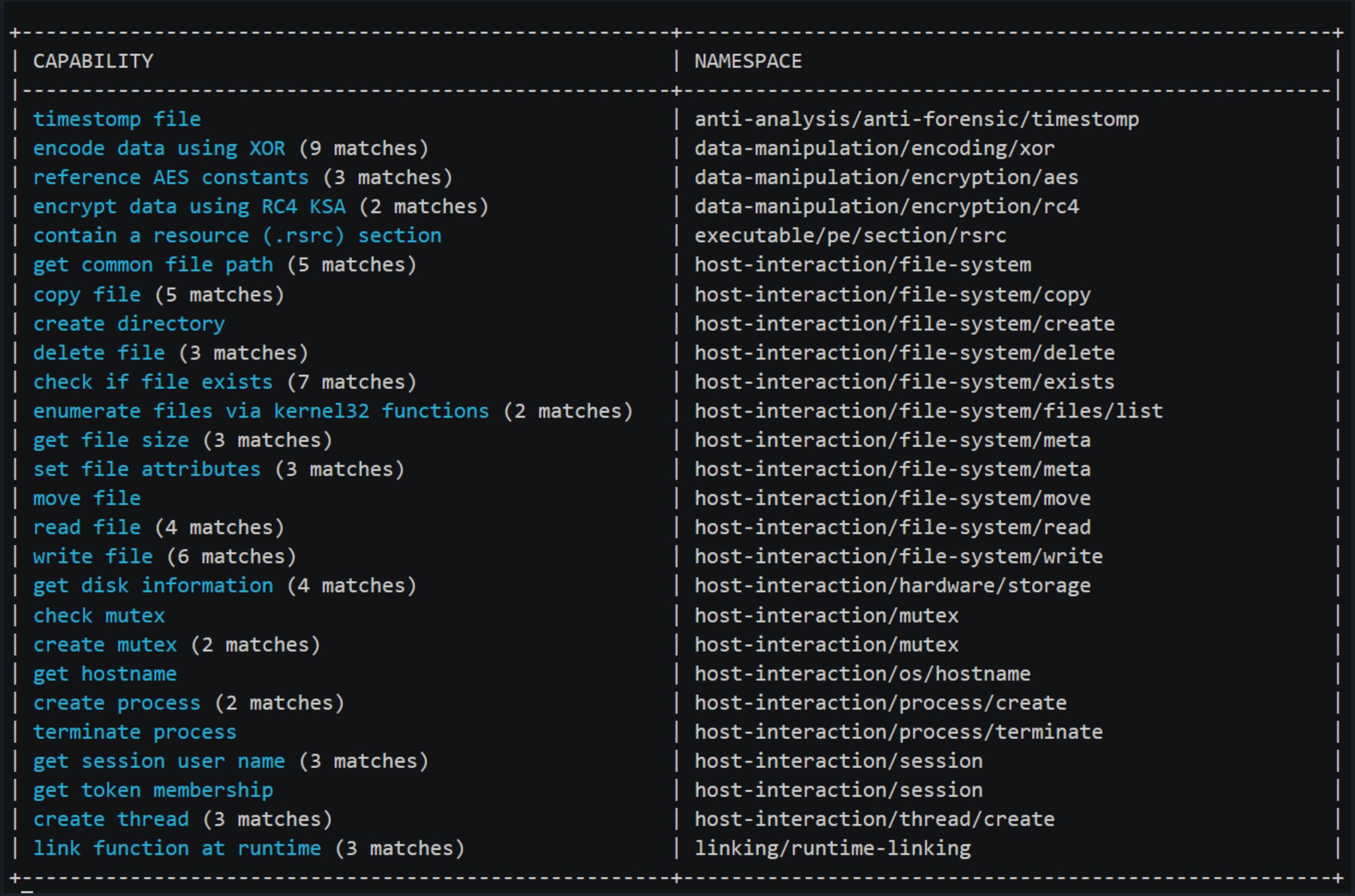


encryptor



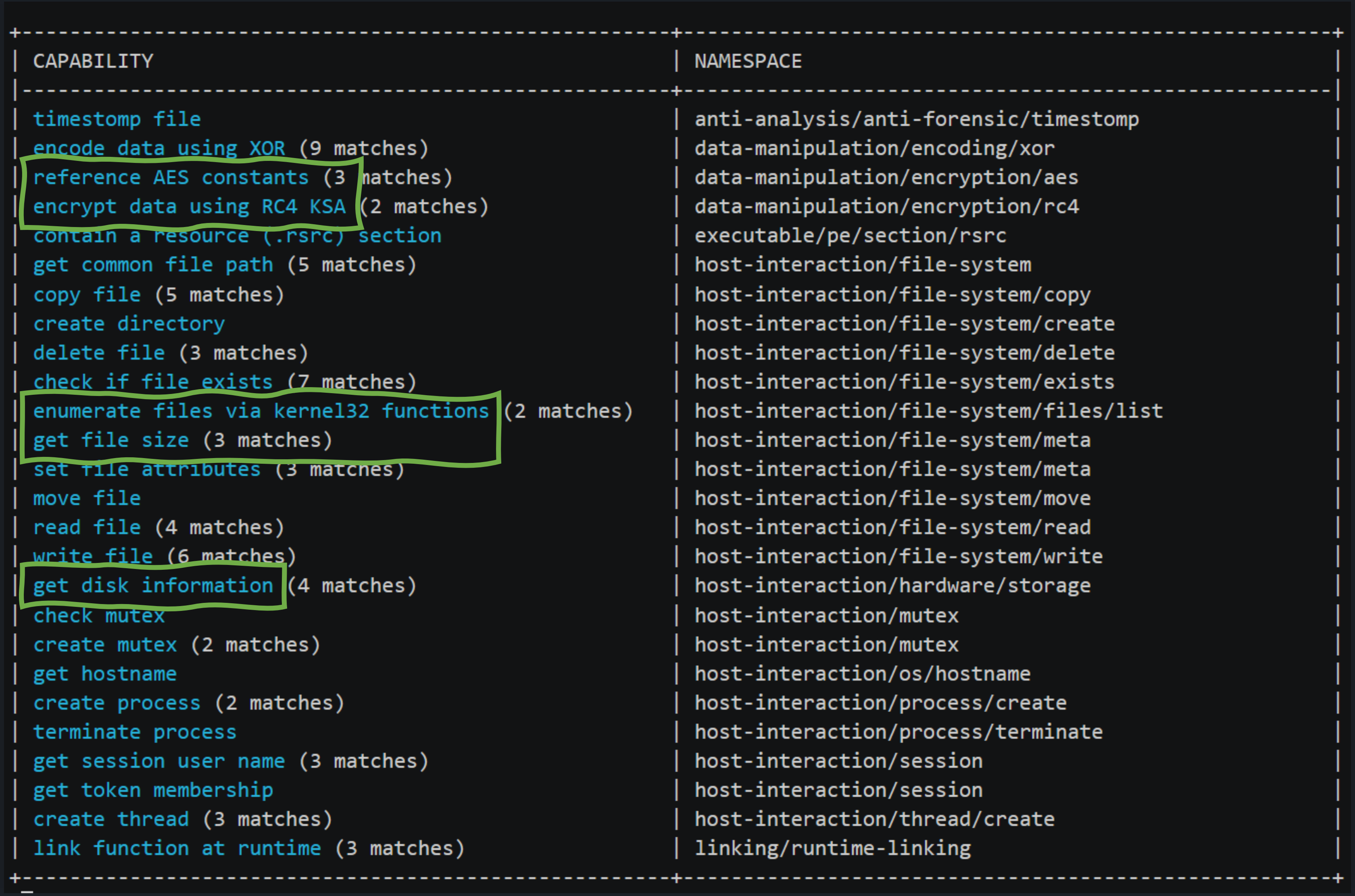
```
+------------------------+------------------------------------------------------------------------------------+
| md5                    | f351e1fcca0c4ea05fc44d15a17f8b36                                                   |
| path                   | /tmp/wannacry-encryptor.bin                                                        |
+------------------------+------------------------------------------------------------------------------------+


+------------------------+------------------------------------------------------------------------------------+
| ATT&CK Tactic          | ATT&CK Technique                                                                   |
|------------------------+------------------------------------------------------------------------------------|
| DEFENSE EVASION        | Indicator Removal on Host::Timestomp [T1551.006]                                   |
|                        | Obfuscated Files or Information [T1027]                                            |
| DISCOVERY              | File and Directory Discovery [T1083]                                               |
|                        | System Information Discovery [T1082]                                               |
|                        | System Owner/User Discovery [T1033]                                                |
| EXECUTION              | Shared Modules [T1129]                                                             |
+------------------------+------------------------------------------------------------------------------------+
```

encryptor



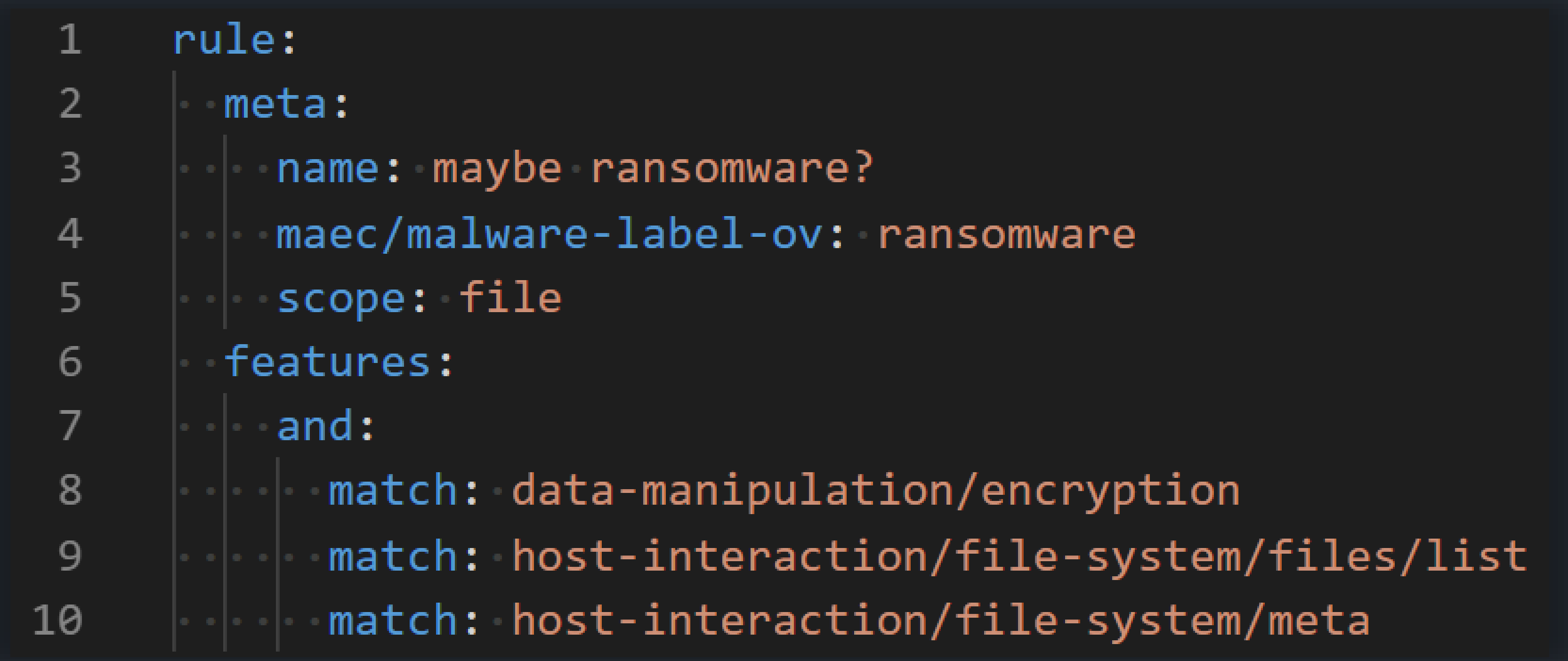
```
+------------------------------------------------------+------------------------------------------------------+
| CAPABILITY                                           | NAMESPACE                                            |
|------------------------------------------------------+------------------------------------------------------|
| timestomp file                                       | anti-analysis/anti-forensic/timestomp                |
| encode data using XOR (9 matches)                    | data-manipulation/encoding/xor                       |
| reference AES constants (3 matches)                  | data-manipulation/encryption/aes                     |
| encrypt data using RC4 KSA (2 matches)               | data-manipulation/encryption/rc4                     |
| contain a resource (.rsrc) section                   | executable/pe/section/rsrc                           |
| get common file path (5 matches)                     | host-interaction/file-system                         |
| copy file (5 matches)                                | host-interaction/file-system/copy                    |
| create directory                                     | host-interaction/file-system/create                  |
| delete file (3 matches)                              | host-interaction/file-system/delete                  |
| check if file exists (7 matches)                     | host-interaction/file-system/exists                  |
| enumerate files via kernel32 functions (2 matches)   | host-interaction/file-system/files/list              |
| get file size (3 matches)                            | host-interaction/file-system/meta                    |
| set file attributes (3 matches)                      | host-interaction/file-system/meta                    |
| move file                                            | host-interaction/file-system/move                    |
| read file (4 matches)                                | host-interaction/file-system/read                    |
| write file (6 matches)                               | host-interaction/file-system/write                   |
| get disk information (4 matches)                     | host-interaction/hardware/storage                    |
| check mutex                                          | host-interaction/mutex                               |
| create mutex (2 matches)                             | host-interaction/mutex                               |
| get hostname                                         | host-interaction/os/hostname                         |
| create process (2 matches)                           | host-interaction/process/create                      |
| terminate process                                    | host-interaction/process/terminate                   |
| get session user name (3 matches)                    | host-interaction/session                             |
| get token membership                                 | host-interaction/session                             |
| create thread (3 matches)                            | host-interaction/thread/create                       |
| link function at runtime (3 matches)                 | linking/runtime-linking                              |
+------------------------------------------------------+------------------------------------------------------+
```

encryptor



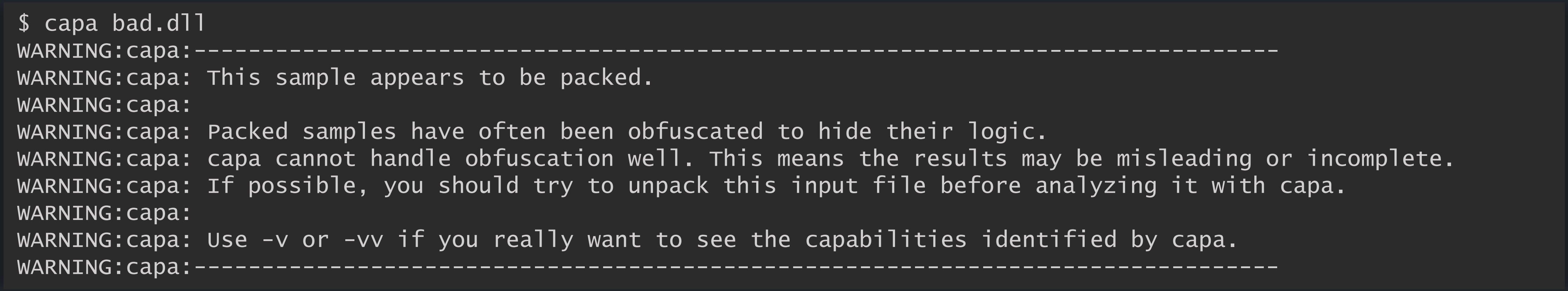
```
+------------------------------------------------------+------------------------------------------------------+
| CAPABILITY                                           | NAMESPACE                                            |
|------------------------------------------------------+------------------------------------------------------|
| timestomp file                                       | anti-analysis/anti-forensic/timestomp                |
| encode data using XOR (9 matches)                    | data-manipulation/encoding/xor                       |
| reference AES constants (3 matches)                  | data-manipulation/encryption/aes                     |
| encrypt data using RC4 KSA (2 matches)               | data-manipulation/encryption/rc4                     |
| contain a resource (.rsrc) section                   | executable/pe/section/rsrc                           |
| get common file path (5 matches)                     | host-interaction/file-system                         |
| copy file (5 matches)                                | host-interaction/file-system/copy                    |
| create directory                                     | host-interaction/file-system/create                  |
| delete file (3 matches)                              | host-interaction/file-system/delete                  |
| check if file exists (7 matches)                     | host-interaction/file-system/exists                  |
| enumerate files via kernel32 functions (2 matches)   | host-interaction/file-system/files/list              |
| get file size (3 matches)                            | host-interaction/file-system/meta                    |
| set file attributes (3 matches)                      | host-interaction/file-system/meta                    |
| move file                                            | host-interaction/file-system/move                    |
| read file (4 matches)                                | host-interaction/file-system/read                    |
| write file (6 matches)                               | host-interaction/file-system/write                   |
| get disk information (4 matches)                     | host-interaction/hardware/storage                    |
| check mutex                                          | host-interaction/mutex                               |
| create mutex (2 matches)                             | host-interaction/mutex                               |
| get hostname                                         | host-interaction/os/hostname                         |
| create process (2 matches)                           | host-interaction/process/create                      |
| terminate process                                    | host-interaction/process/terminate                   |
| get session user name (3 matches)                    | host-interaction/session                             |
| get token membership                                 | host-interaction/session                             |
| create thread (3 matches)                            | host-interaction/thread/create                       |
| link function at runtime (3 matches)                 | linking/runtime-linking                              |
+------------------------------------------------------+------------------------------------------------------+
```

encryptor

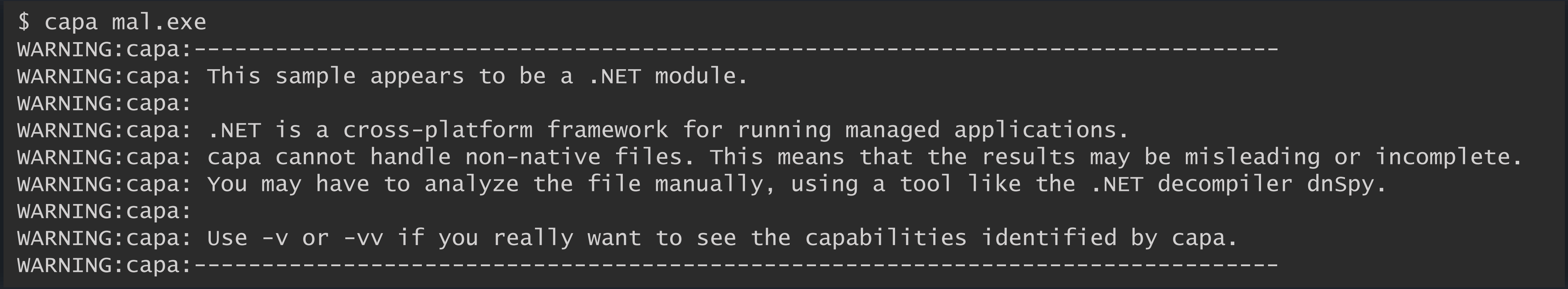


```
rule:
  meta:
    name: maybe ransomware?
    maec/malware-label-ov: ransomware
    scope: file
  features:
    and:
      match: data-manipulation/encryption
      match: host-interaction/file-system/files/list
      match: host-interaction/file-system/meta
```

when things break…

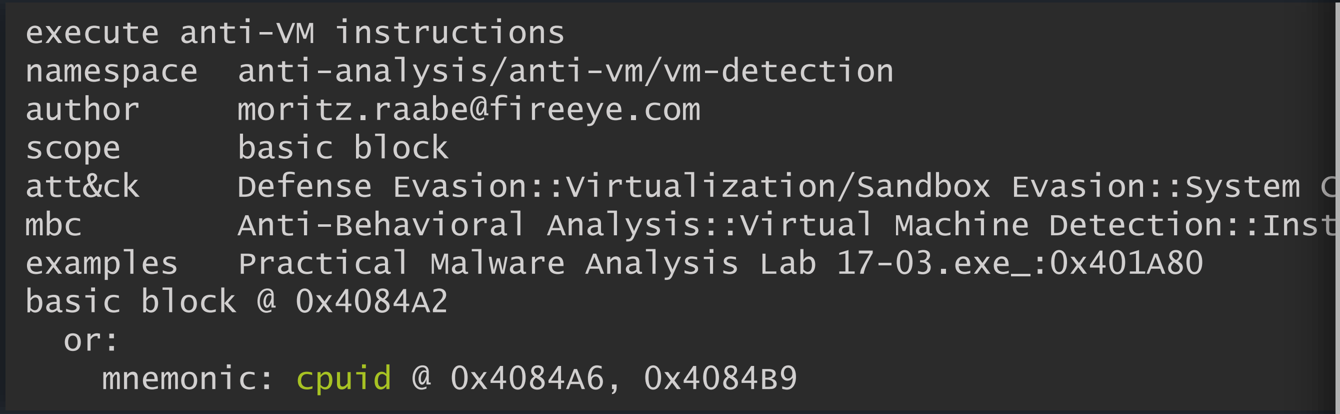


```
$ capa bad.dll
WARNING:capa:--------------------------------------------------------------------------------
WARNING:capa: This sample appears to be packed.
WARNING:capa:
WARNING:capa: Packed samples have often been obfuscated to hide their logic.
WARNING:capa: capa cannot handle obfuscation well. This means the results may be misleading or incomplete.
WARNING:capa: If possible, you should try to unpack this input file before analyzing it with capa.
WARNING:capa:
WARNING:capa: Use -v or -vv if you really want to see the capabilities identified by capa.
WARNING:capa:--------------------------------------------------------------------------------
```



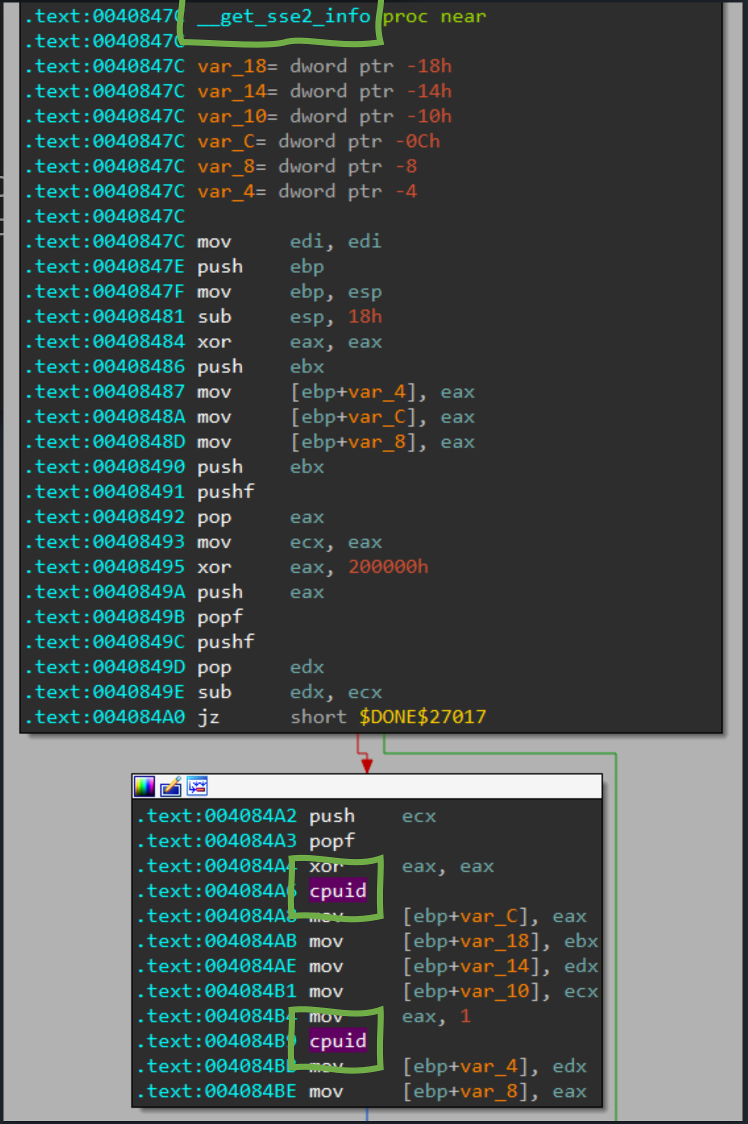
```
$ capa mal.exe
WARNING:capa:--------------------------------------------------------------------------------
WARNING:capa: This sample appears to be a .NET module.
WARNING:capa:
WARNING:capa: .NET is a cross-platform framework for running managed applications.
WARNING:capa: capa cannot handle non-native files. This means that the results may be misleading or incomplete.
WARNING:capa: You may have to analyze the file manually, using a tool like the .NET decompiler dnSpy.
WARNING:capa:
WARNING:capa: Use -v or -vv if you really want to see the capabilities identified by capa.
WARNING:capa:--------------------------------------------------------------------------------
```

capa can be TOO good



```
execute anti-VM instructions
namespace  anti-analysis/anti-vm/vm-detection
author     moritz.raabe@fireeye.com
scope      basic block
att&ck     Defense Evasion::Virtualization/Sandbox Evasion::System C
mbc        Anti-Behavioral Analysis::Virtual Machine Detection::Inst
examples   Practical Malware Analysis Lab 17-03.exe_:0x401A80
basic block @ 0x4084A2
  or:
    mnemonic: cpuid @ 0x4084A6, 0x4084B9
```

“__get_sse2_info”



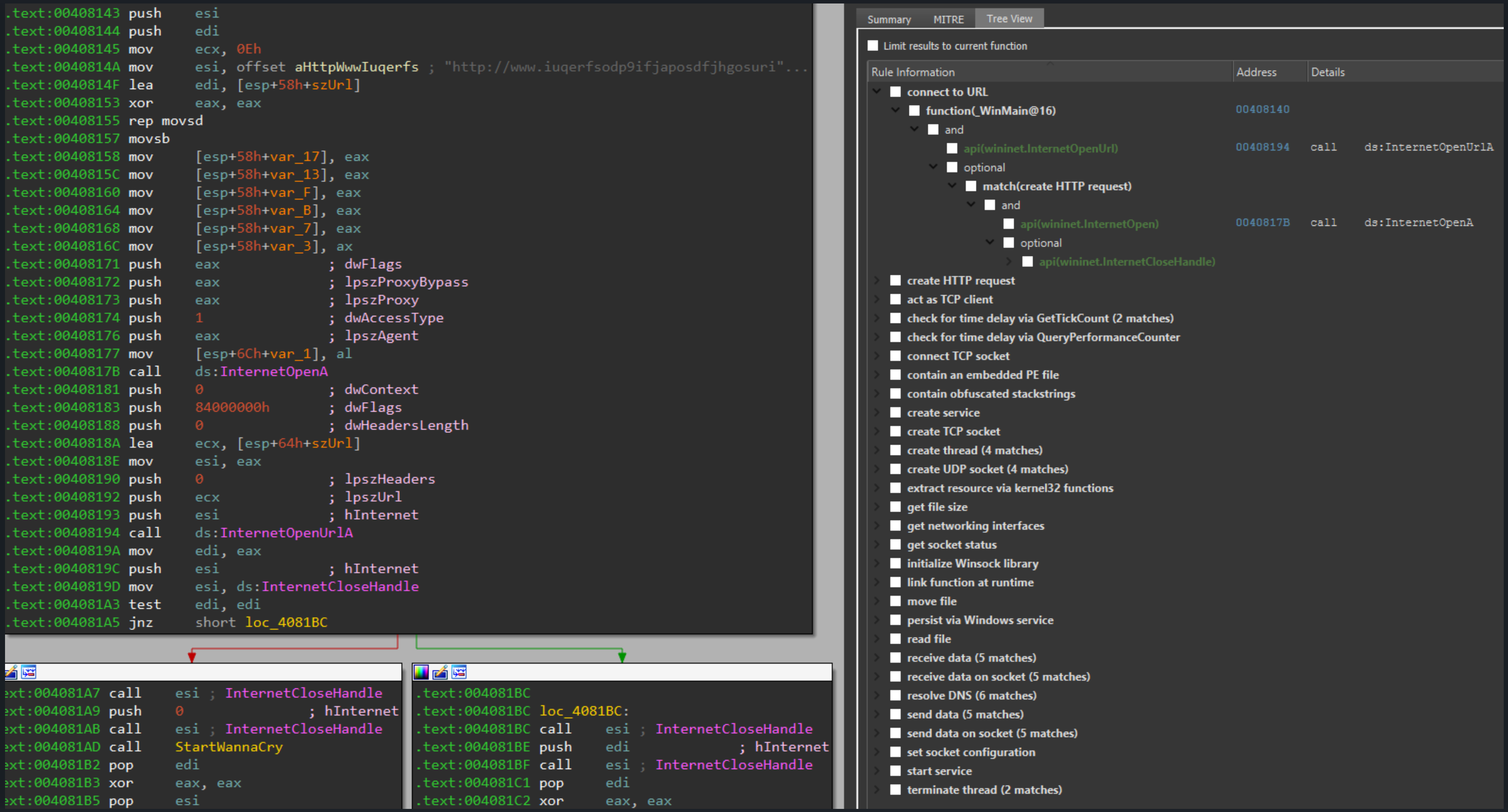
```
.text:0040847C __get_sse2_info proc near
.text:0040847C
.text:0040847C var_18= dword ptr -18h
.text:0040847C var_14= dword ptr -14h
.text:0040847C var_10= dword ptr -10h
.text:0040847C var_C= dword ptr -0Ch
.text:0040847C var_8= dword ptr -8
.text:0040847C var_4= dword ptr -4
.text:0040847C
.text:0040847C mov     edi, edi
.text:0040847E push    ebp
.text:0040847F mov     ebp, esp
.text:00408481 sub     esp, 18h
.text:00408484 xor     eax, eax
.text:00408486 push    ebx
.text:00408487 mov     [ebp+var_4], eax
.text:0040848A mov     [ebp+var_C], eax
.text:0040848D mov     [ebp+var_8], eax
.text:00408490 push    ebx
.text:00408491 pushf
.text:00408492 pop     eax
.text:00408493 mov     ecx, eax
.text:00408495 xor     eax, 200000h
.text:0040849A push    eax
.text:0040849B popf
.text:0040849C pushf
.text:0040849D pop     edx
.text:0040849E sub     edx, ecx
.text:004084A0 jz      short $DONE$27017
```

```
.text:004084A2 push    ecx
.text:004084A3 popf
.text:004084A4 xor     eax, eax
.text:004084A6 cpuid
.text:004084A8 mov     [ebp+var_C], eax
.text:004084AB mov     [ebp+var_18], ebx
.text:004084AE mov     [ebp+var_14], edx
.text:004084B1 mov     [ebp+var_10], ecx
.text:004084B4 mov     eax, 1
.text:004084B9 cpuid
.text:004084BB mov     [ebp+var_4], edx
.text:004084BE mov     [ebp+var_8], eax
```

future work

- code analysis engines
  - operate on sandbox data or API traces
  - add Python 3 support
- integration
  - easy to markup via standardized JSON output
- “bubble up” capabilities
  - confusion when a capability is split across multiple functions

IDA Pro integration



```
.text:00408143 push    esi
.text:00408144 push    edi
.text:00408145 mov     ecx, 0Eh
.text:0040814A mov     esi, offset aHttpWwwIuqerfs ; "http://www.iuqerfsodp9ifjaposdfjhgosuri"...
.text:0040814F lea     edi, [esp+58h+szUrl]
.text:00408153 xor     eax, eax
.text:00408155 rep movsd
.text:00408157 movsb
.text:00408158 mov     [esp+58h+var_17], eax
.text:0040815C mov     [esp+58h+var_13], eax
.text:00408160 mov     [esp+58h+var_F], eax
.text:00408164 mov     [esp+58h+var_B], eax
.text:00408168 mov     [esp+58h+var_7], eax
.text:0040816C mov     [esp+58h+var_3], ax
.text:00408171 push    eax             ; dwFlags
.text:00408172 push    eax             ; lpszProxyBypass
.text:00408173 push    eax             ; lpszProxy
.text:00408174 push    1               ; dwAccessType
.text:00408176 push    eax             ; lpszAgent
.text:00408177 mov     [esp+6Ch+var_1], al
.text:0040817B call    ds:InternetOpenA
.text:00408181 push    0               ; dwContext
.text:00408183 push    84000000h       ; dwFlags
.text:00408188 push    0               ; dwHeadersLength
.text:0040818A lea     ecx, [esp+64h+szUrl]
.text:0040818E mov     esi, eax
.text:00408190 push    0               ; lpszHeaders
.text:00408192 push    ecx             ; lpszUrl
.text:00408193 push    esi             ; hInternet
.text:00408194 call    ds:InternetOpenUrlA
.text:0040819A mov     edi, eax
.text:0040819C push    esi             ; hInternet
.text:0040819D mov     esi, ds:InternetCloseHandle
.text:004081A3 test    edi, edi
.text:004081A5 jnz     short loc_4081BC
```

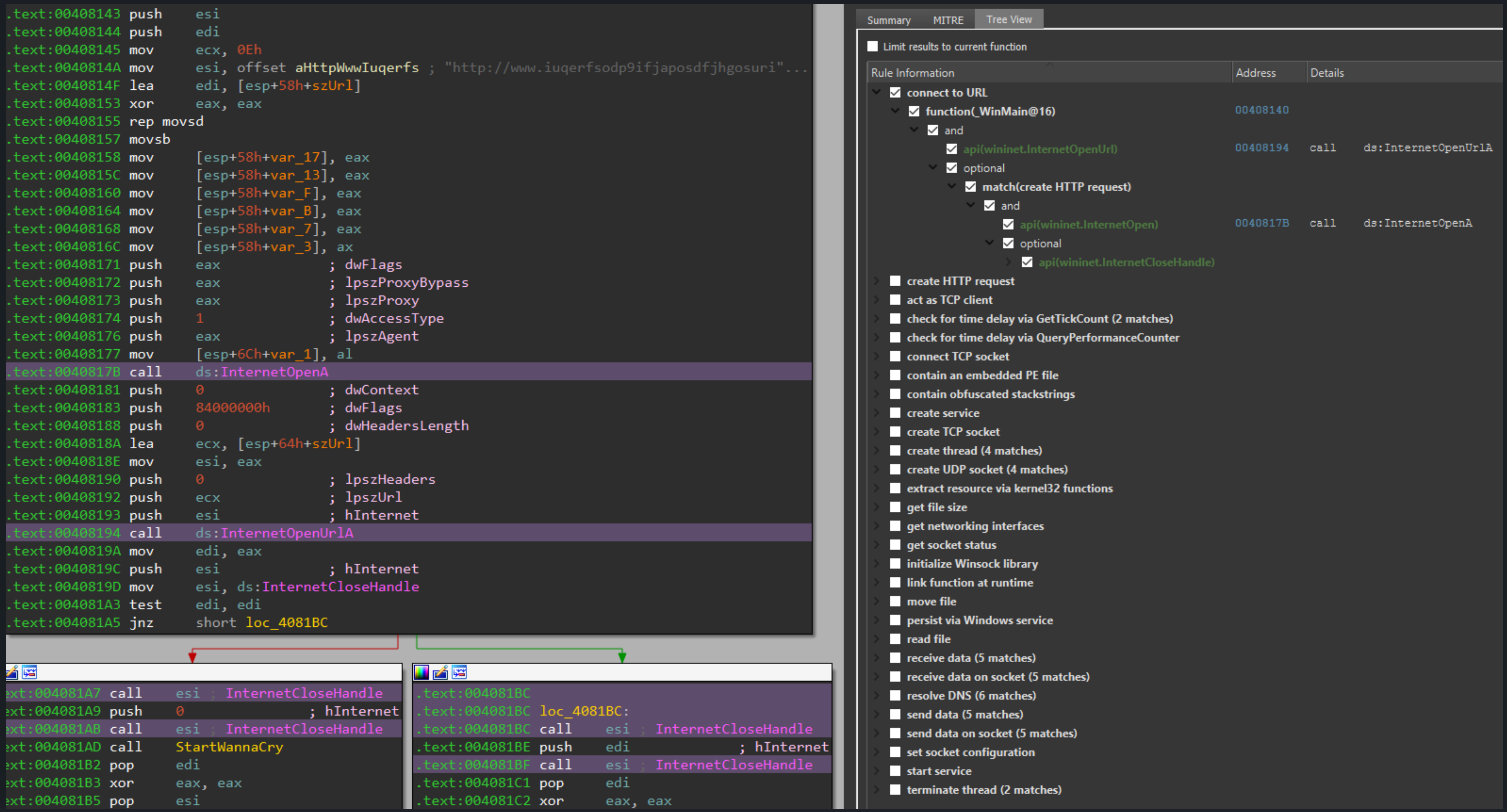
```
xt:004081A7 call    esi ; InternetCloseHandle
xt:004081A9 push    0               ; hInternet
xt:004081AB call    esi ; InternetCloseHandle
xt:004081AD call    StartWannaCry
xt:004081B2 pop     edi
xt:004081B3 xor     eax, eax
xt:004081B5 pop     esi
```

```
.text:004081BC
.text:004081BC loc_4081BC:
.text:004081BC call    esi ; InternetCloseHandle
.text:004081BE push    edi             ; hInternet
.text:004081BF call    esi ; InternetCloseHandle
.text:004081C1 pop     edi
.text:004081C2 xor     eax, eax
```

□ Limit results to current function

```
Rule Information                                     Address    Details
⌄ □ connect to URL
  ⌄ □ function(_WinMain@16)                          00408140
    ⌄ □ and
        □ api(wininet.InternetOpenUrl)               00408194   call    ds:InternetOpenUrlA
      ⌄ □ optional
        ⌄ □ match(create HTTP request)
          ⌄ □ and
              □ api(wininet.InternetOpen)            0040817B   call    ds:InternetOpenA
            ⌄ □ optional
              › □ api(wininet.InternetCloseHandle)
› □ create HTTP request
› □ act as TCP client
› □ check for time delay via GetTickCount (2 matches)
› □ check for time delay via QueryPerformanceCounter
› □ connect TCP socket
› □ contain an embedded PE file
› □ contain obfuscated stackstrings
› □ create service
› □ create TCP socket
› □ create thread (4 matches)
› □ create UDP socket (4 matches)
› □ extract resource via kernel32 functions
› □ get file size
› □ get networking interfaces
› □ get socket status
› □ initialize Winsock library
› □ link function at runtime
› □ move file
› □ persist via Windows service
› □ read file
› □ receive data (5 matches)
› □ receive data on socket (5 matches)
› □ resolve DNS (6 matches)
› □ send data (5 matches)
› □ send data on socket (5 matches)
› □ set socket configuration
› □ start service
› □ terminate thread (2 matches)
```

IDA Pro integration



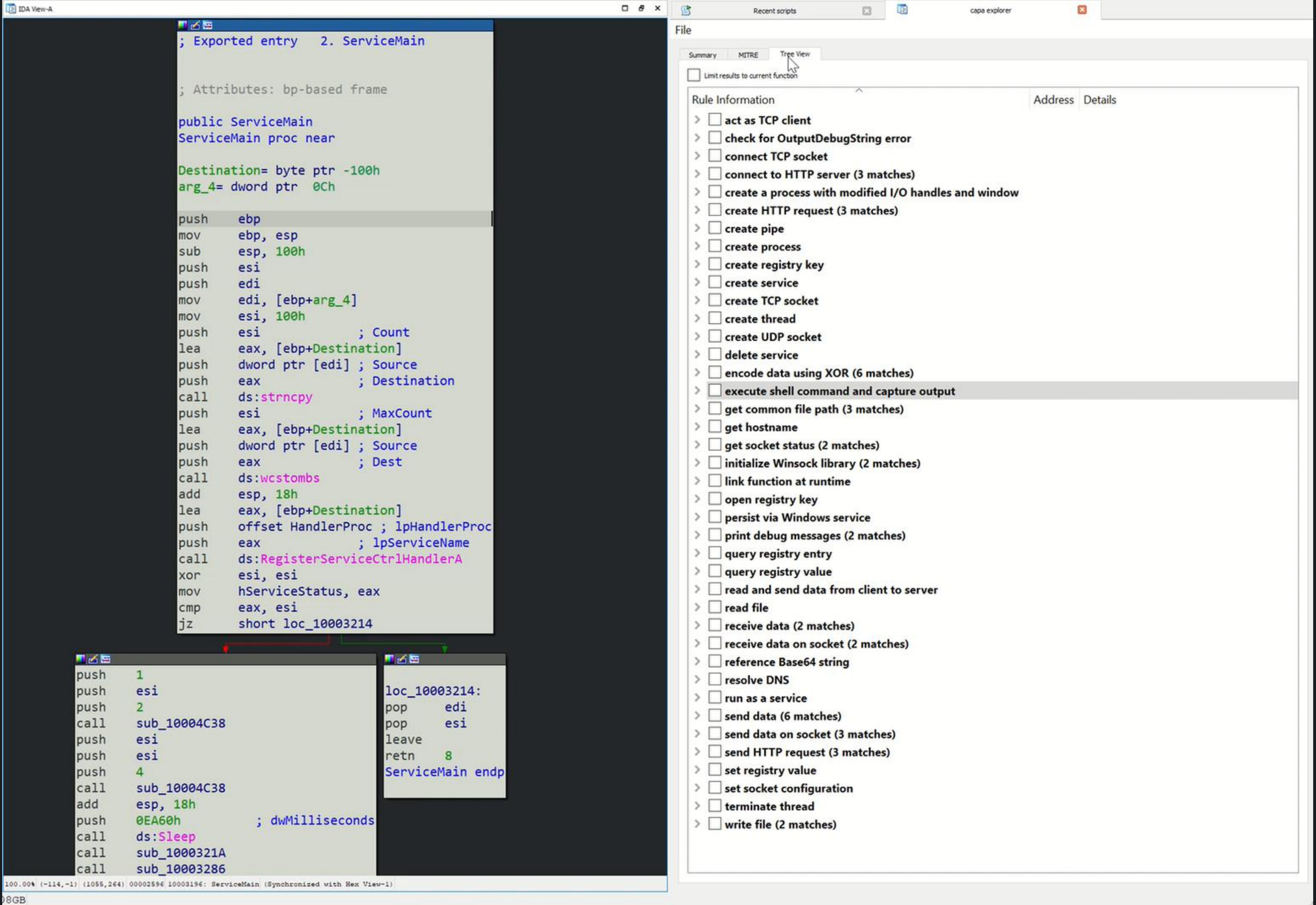
```
.text:00408143 push    esi
.text:00408144 push    edi
.text:00408145 mov     ecx, 0Eh
.text:0040814A mov     esi, offset aHttpWwwIuqerfs ; "http://www.iuqerfsodp9ifjaposdfjhgosuri"...
.text:0040814F lea     edi, [esp+58h+szUrl]
.text:00408153 xor     eax, eax
.text:00408155 rep movsd
.text:00408157 movsb
.text:00408158 mov     [esp+58h+var_17], eax
.text:0040815C mov     [esp+58h+var_13], eax
.text:00408160 mov     [esp+58h+var_F], eax
.text:00408164 mov     [esp+58h+var_B], eax
.text:00408168 mov     [esp+58h+var_7], eax
.text:0040816C mov     [esp+58h+var_3], ax
.text:00408171 push    eax             ; dwFlags
.text:00408172 push    eax             ; lpszProxyBypass
.text:00408173 push    eax             ; lpszProxy
.text:00408174 push    1               ; dwAccessType
.text:00408176 push    eax             ; lpszAgent
.text:00408177 mov     [esp+6Ch+var_1], al
.text:0040817B call    ds:InternetOpenA
.text:00408181 push    0               ; dwContext
.text:00408183 push    84000000h       ; dwFlags
.text:00408188 push    0               ; dwHeadersLength
.text:0040818A lea     ecx, [esp+64h+szUrl]
.text:0040818E mov     esi, eax
.text:00408190 push    0               ; lpszHeaders
.text:00408192 push    ecx             ; lpszUrl
.text:00408193 push    esi             ; hInternet
.text:00408194 call    ds:InternetOpenUrlA
.text:0040819A mov     edi, eax
.text:0040819C push    esi             ; hInternet
.text:0040819D mov     esi, ds:InternetCloseHandle
.text:004081A3 test    edi, edi
.text:004081A5 jnz     short loc_4081BC
```

```
xt:004081A7 call    esi ; InternetCloseHandle
xt:004081A9 push    0                ; hInternet
xt:004081AB call    esi ; InternetCloseHandle
xt:004081AD call    StartWannaCry
xt:004081B2 pop     edi
xt:004081B3 xor     eax, eax
xt:004081B5 pop     esi
```

```
.text:004081BC
.text:004081BC loc_4081BC:
.text:004081BC call    esi ; InternetCloseHandle
.text:004081BE push    edi                ; hInternet
.text:004081BF call    esi ; InternetCloseHandle
.text:004081C1 pop     edi
.text:004081C2 xor     eax, eax
```

☐ Limit results to current function

Rule Information	Address	Details
☑ connect to URL		
☑ function(_WinMain@16)	00408140	
☑ and		
☑ api(wininet.InternetOpenUrl)	00408194	call ds:InternetOpenUrlA
☑ optional		
☑ match(create HTTP request)		
☑ and		
☑ api(wininet.InternetOpen)	0040817B	call ds:InternetOpenA
☑ optional		
☑ api(wininet.InternetCloseHandle)		
☐ create HTTP request		
☐ act as TCP client		
☐ check for time delay via GetTickCount (2 matches)		
☐ check for time delay via QueryPerformanceCounter		
☐ connect TCP socket		
☐ contain an embedded PE file		
☐ contain obfuscated stackstrings		
☐ create service		
☐ create TCP socket		
☐ create thread (4 matches)		
☐ create UDP socket (4 matches)		
☐ extract resource via kernel32 functions		
☐ get file size		
☐ get networking interfaces		
☐ get socket status		
☐ initialize Winsock library		
☐ link function at runtime		
☐ move file		
☐ persist via Windows service		
☐ read file		
☐ receive data (5 matches)		
☐ receive data on socket (5 matches)		
☐ resolve DNS (6 matches)		
☐ send data (5 matches)		
☐ send data on socket (5 matches)		
☐ set socket configuration		
☐ start service		
☐ terminate thread (2 matches)		



```
; Exported entry   2. ServiceMain


; Attributes: bp-based frame

public ServiceMain
ServiceMain proc near

Destination= byte ptr -100h
arg_4= dword ptr  0Ch

push    ebp
mov     ebp, esp
sub     esp, 100h
push    esi
push    edi
mov     edi, [ebp+arg_4]
mov     esi, 100h
push    esi             ; Count
lea     eax, [ebp+Destination]
push    dword ptr [edi] ; Source
push    eax             ; Destination
call    ds:strncpy
push    esi             ; MaxCount
lea     eax, [ebp+Destination]
push    dword ptr [edi] ; Source
push    eax             ; Dest
call    ds:wcstombs
add     esp, 18h
lea     eax, [ebp+Destination]
push    offset HandlerProc ; lpHandlerProc
push    eax             ; lpServiceName
call    ds:RegisterServiceCtrlHandlerA
xor     esi, esi
mov     hServiceStatus, eax
cmp     eax, esi
jz      short loc_10003214
```

```
push    1
push    esi
push    2
call    sub_10004C38
push    esi
push    esi
push    4
call    sub_10004C38
add     esp, 18h
push    0EA60h          ; dwMilliseconds
call    ds:Sleep
call    sub_1000321A
call    sub_10003286
```

```
loc_10003214:
pop     edi
pop     esi
leave
retn    8
ServiceMain endp
```

```
100.00% (-114,-1) (1055,264) 00002596 10003196: ServiceMain (Synchronized with Hex View-1)
```

08GB

□ Limit results to current function

Rule Information	Address	Details
□ act as TCP client		
□ check for OutputDebugString error		
□ connect TCP socket		
□ connect to HTTP server (3 matches)		
□ create a process with modified I/O handles and window		
□ create HTTP request (3 matches)		
□ create pipe		
□ create process		
□ create registry key		
□ create service		
□ create TCP socket		
□ create thread		
□ create UDP socket		
□ delete service		
□ encode data using XOR (6 matches)		
□ execute shell command and capture output		
□ get common file path (3 matches)		
□ get hostname		
□ get socket status (2 matches)		
□ initialize Winsock library (2 matches)		
□ link function at runtime		
□ open registry key		
□ persist via Windows service		
□ print debug messages (2 matches)		
□ query registry entry		
□ query registry value		
□ read and send data from client to server		
□ read file		
□ receive data (2 matches)		
□ receive data on socket (2 matches)		
□ reference Base64 string		
□ resolve DNS		
□ run as a service		
□ send data (6 matches)		
□ send data on socket (3 matches)		
□ send HTTP request (3 matches)		
□ set registry value		
□ set socket configuration		
□ terminate thread		
□ write file (2 matches)		

get capa

github.com/fireeye/capa

standalone executables, no installation

FLARE-VM & REMnux
soon

share expertise

CAPA

github.com/fireeye/capa-rules

as you find cool malware behaviors,
share your rules!

rules 261

CAPA analyzes a program and identifies things the program could do.

CAPA uses rules, written by experts, to recognize these capabilities.

this can be you!

CAPA

github.com/fireeye/capa

Willi Ballenthin
williballenthin

Moritz Raabe
m_r_tz

Contributors:
Ana Maria Martinez Gomez
Mike Hunhoff
Blaine Stancill
Matt Williams
and rest of FLARE
(~200 years experience)