CYBERUS
TECHNOLOGY

Automated System Call Interpretation

Markus Partheymüller, Cyberus Technology GmbH

BSides Luxembourg, October 2018

Introduction

Introduction

- Software developer

Introduction

- Software developer
- OS/virtualization background

Introduction

- Software developer
- OS/virtualization background
- TU Dresden

Introduction

- Software developer
- OS/virtualization background
- TU Dresden
  - NOVA microhypervisor

Introduction

- Software developer
- OS/virtualization background
- TU Dresden
  - NOVA microhypervisor
- Worked for Intel and FireEye

Introduction

- Software developer
- OS/virtualization background
- TU Dresden
  - NOVA microhypervisor
- Worked for Intel and FireEye
  - VM technology in security-related scenarios (endpoint protection, malware analysis)

Introduction

- Software developer
- OS/virtualization background
- TU Dresden
  - NOVA microhypervisor
- Worked for Intel and FireEye
  - VM technology in security-related scenarios (endpoint protection, malware analysis)
- Co-Founder of Cyberus

Introduction

- Software developer
- OS/virtualization background
- TU Dresden
  - NOVA microhypervisor
- Worked for Intel and FireEye
  - VM technology in security-related scenarios (endpoint protection, malware analysis)
- Co-Founder of Cyberus
  - Product platform featuring NOVA

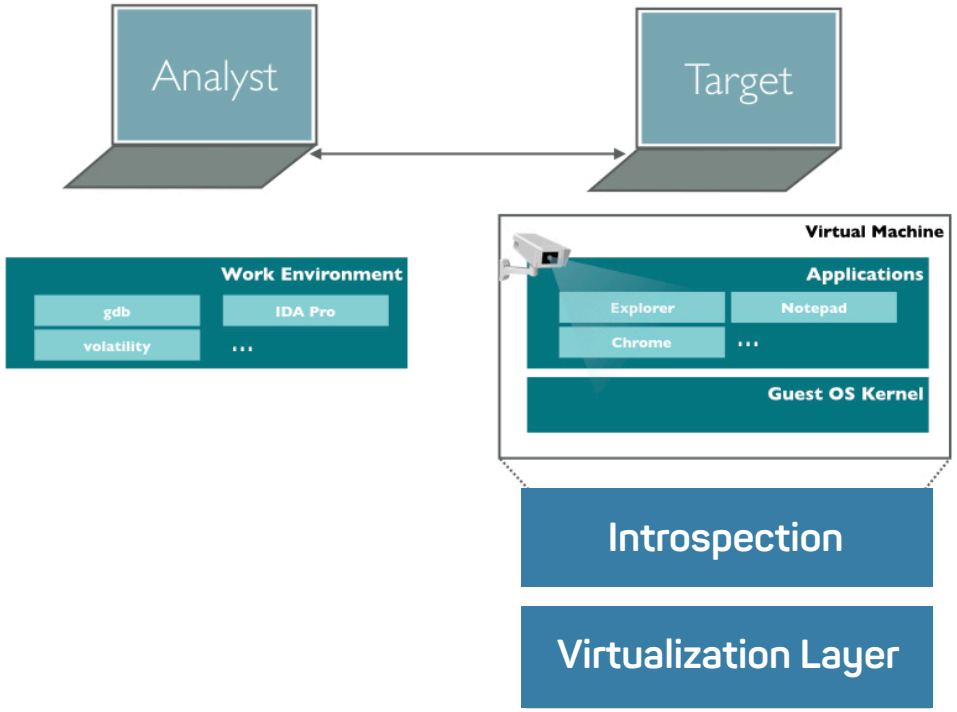
Motivation

Motivation

- Tycho Malware Analysis Platform

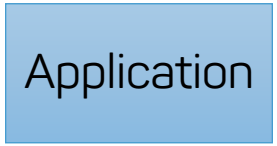
Motivation

- Tycho Malware Analysis Platform

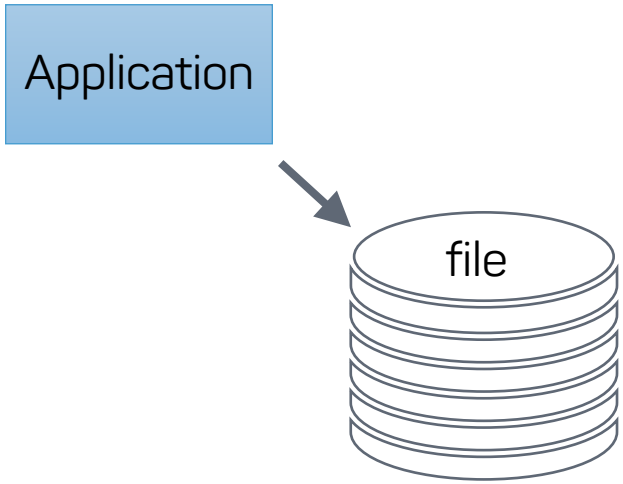


Application behavior

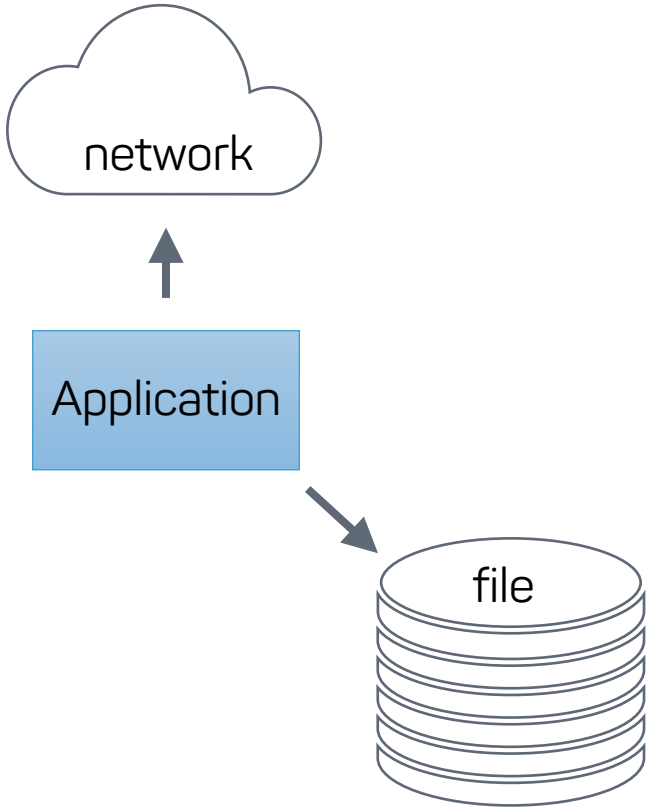
Application behavior



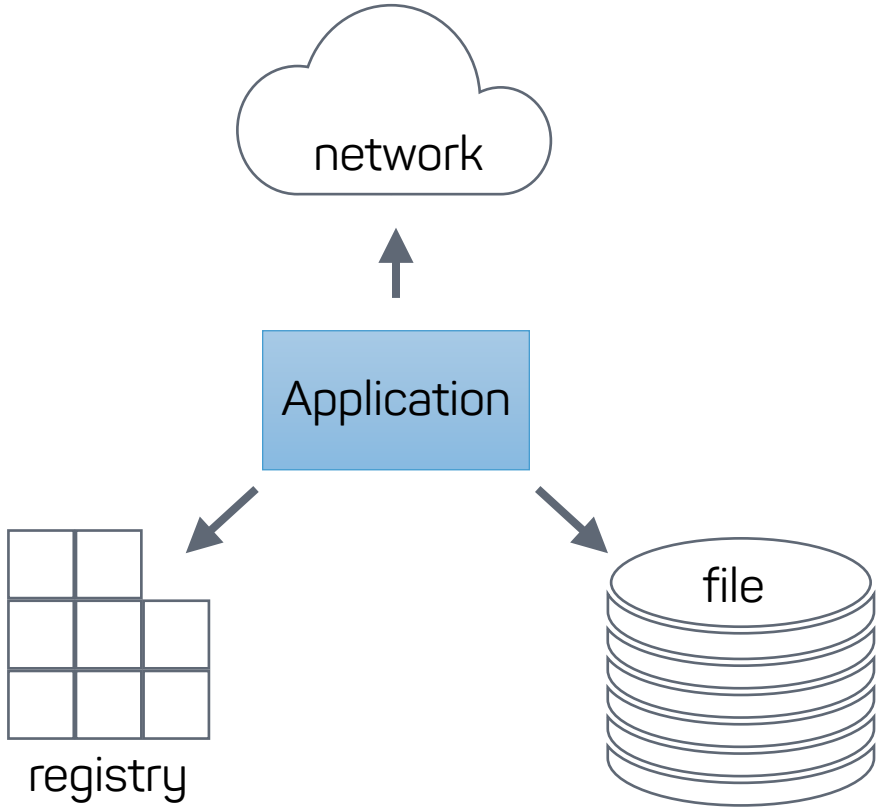
Application behavior



Application behavior



Application behavior



System calls

System calls

- Interface between kernel and user application

System calls

- Interface between kernel and user application
- Service requests

System calls

- Interface between kernel and user application
- Service requests
    - File access

System calls

- Interface between kernel and user application
- Service requests
  - File access
  - Network access

System calls

- Interface between kernel and user application
- Service requests
  - File access
  - Network access
  - Registry modifications

System calls

- Interface between kernel and user application
- Service requests
  - File access
  - Network access
  - Registry modifications
  - Memory requests

System calls

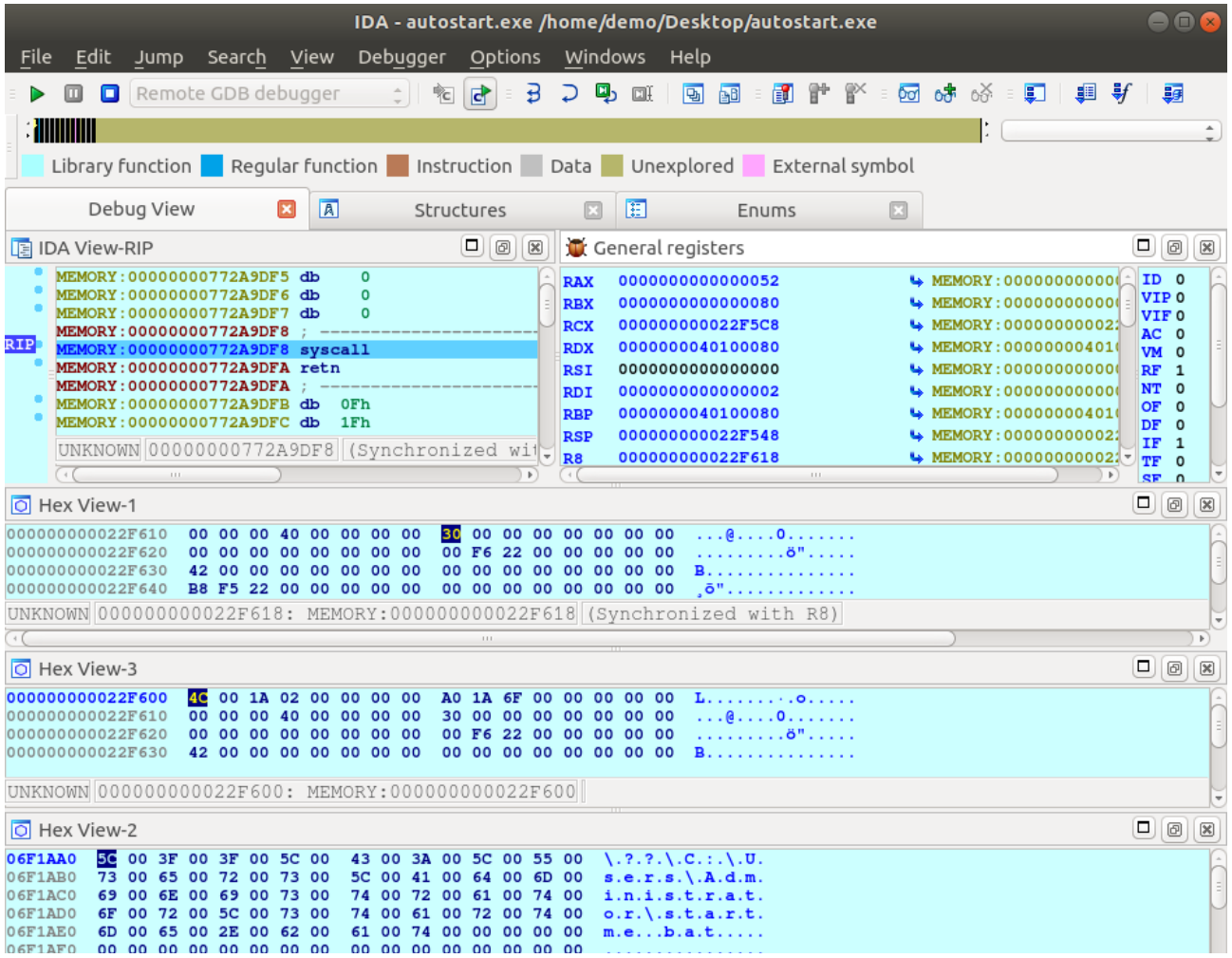
- Interface between kernel and user application
- Service requests
  - File access
  - Network access
  - Registry modifications
  - Memory requests
  - Process/Thread control

System calls

- Interface between kernel and user application
- Service requests
  - File access
  - Network access
  - Registry modifications
  - Memory requests
  - Process/Thread control
  - ...

System call: Example

System call: Example



System call: Example

→ObjectAttributes	OBJECT_ATTRIBUTES*	0x22F618
RootDirectory	VOID*	0x0
ObjectName	UNICODE_STRING*	0x22F600
Buffer	USHORT*	0x751AA0
\??\C:\Users\Administrator\startme.bat		
Length	USHORT	0x4C
MaximumLength	USHORT	0x21A
SecurityQualityOfService	VOID*	0x22F5B8
SecurityDescriptor	VOID*	0x0
Length	ULONG	0x30
Attributes	ULONG	0x42

Feeling the pain

Interpreting a system call

How to interpret a system call on Windows

How to interpret a system call on Windows

- System call number and result: RAX

How to interpret a system call on Windows

- System call number and result: RAX
- Microsoft calling convention: first four parameters in RCX, RDX, R8, R9

How to interpret a system call on Windows

- System call number and result: RAX
- Microsoft calling convention: first four parameters in RCX, RDX, R8, R9
- SYSCALL instruction needs RCX internally -> swap with R10

How to interpret a system call on Windows

- System call number and result: RAX
- Microsoft calling convention: first four parameters in RCX, RDX, R8, R9
- SYSCALL instruction needs RCX internally -> swap with R10
- Additional parameters on stack

What do we need to know?

- Windows version (e.g., Windows 7 SP1)
- Architectural state (registers)
- Memory dumps

Example

Example

syscall no.	rax	0x52
	rbx	0x80
	rcx	0x22f3d8
param 1	rdx	0x40100080
	rdi	0x2
	rsi	0x0
	rbp	0x40100080
	rsp	0x22f358
param 2	r8	0x22f428
param 3	r9	0x22f3e8
param 0	r10	0x22f3d8
	r11	0x731a88
	r12	0x5
	r13	0x0
	r14	0x0
	r15	0x731a80
	rip	0x777e9df8

Example

syscall no.	rax	0x52
	rbx	0x80
	rcx	0x22f3d8
param 1	rdx	0x40100080
	rdi	0x2
	rsi	0x0
	rbp	0x40100080
	rsp	0x22f358
param 2	r8	0x22f428
param 3	r9	0x22f3e8
param 0	r10	0x22f3d8
	r11	0x731a88
	r12	0x5
	r13	0x0
	r14	0x0
	r15	0x731a80
	rip	0x777e9df8

result	rax	0x0
	rbx	0x80
	rcx	0x777e9dfa
	rdx	0x0
	rdi	0x2
	rsi	0x0
	rbp	0x40100080
	rsp	0x22f358
	r8	0x22f358
	r9	0x40100080
	r10	0x0
	r11	0x10202
	r12	0x5
	r13	0x0
	r14	0x0
	r15	0x731a80
	rip	0x777e9dfa

Example

syscall no.	rax	0x52
	rbx	0x80
	rcx	0x22f3d8
param 1	rdx	0x40100080
	rdi	0x2
	rsi	0x0
	rbp	0x40100080
	rsp	0x22f358
param 2	r8	0x22f428
param 3	r9	0x22f3e8
param 0	r10	0x22f3d8
	r11	0x731a88
	r12	0x5
	r13	0x0
	r14	0x0
	r15	0x731a80
	rip	0x777e9df8

result	rax	0x0
	rbx	0x80
	rcx	0x777e9dfa
	rdx	0x0
	rdi	0x2
	rsi	0x0
	rbp	0x40100080
	rsp	0x22f358
	r8	0x22f358
	r9	0x40100080
	r10	0x0
	r11	0x10202
	r12	0x5
	r13	0x0
	r14	0x0
	r15	0x731a80
	rip	0x777e9dfa

The internet knows things

The internet knows things

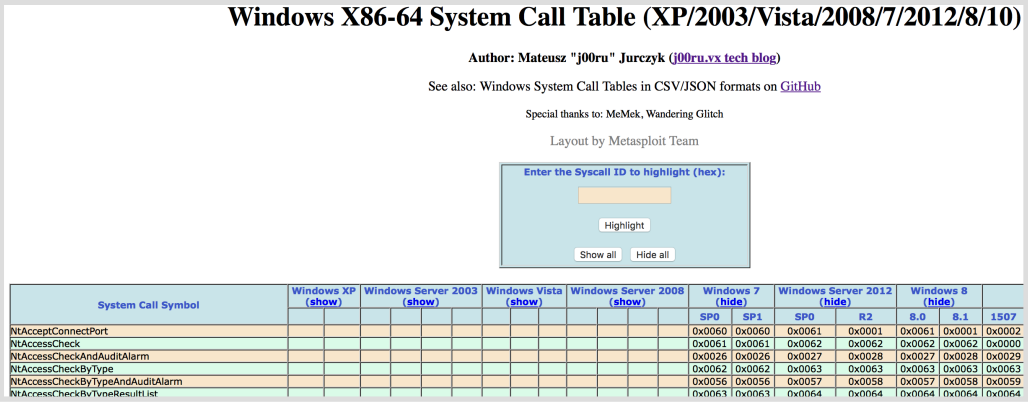
- MSDN (incomplete, sometimes difficult to parse)

The internet knows things

- MSDN (incomplete, sometimes difficult to parse)
- Third-party websites

The internet knows things

- MSDN (incomplete, sometimes difficult to parse)
- Third-party websites



Windows X86-64 System Call Table (XP/2003/Vista/2008/7/2012/8/10)

Author: Mateusz "j00ru" Jurczyk (j00ru.vx tech blog)

See also: Windows System Call Tables in CSV/JSON formats on GitHub

Special thanks to: MeMek, Wandering Glitch

Layout by Metasploit Team

Enter the Syscall ID to highlight (hex):

Highlight

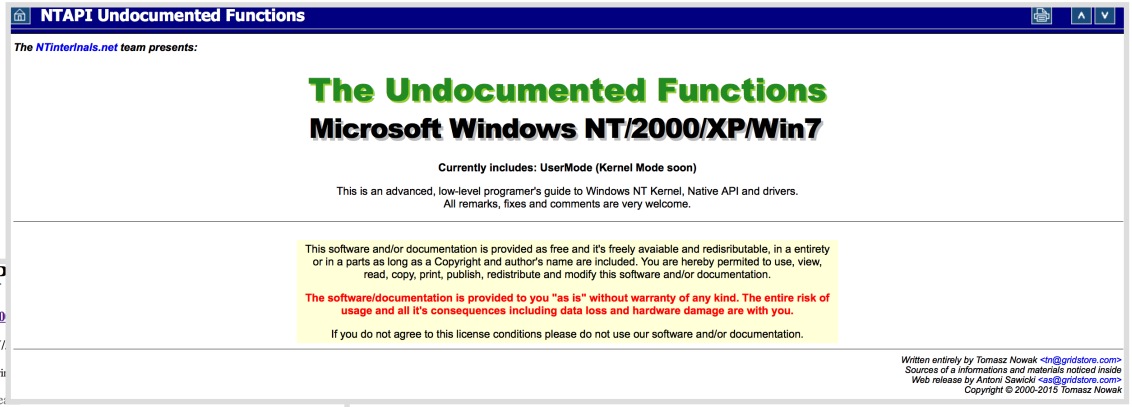
Show all | Hide all

System Call Symbol	Windows XP (show)		Windows Server 2003 (show)			Windows Vista (show)			Windows Server 2008 (show)				Windows 7 (hide)		Windows Server 2012 (hide)		Windows 8 (hide)		
													SP0	SP1	SP0	R2	8.0	8.1	1507
NtAcceptConnectPort													0x0060	0x0060	0x0061	0x0001	0x0061	0x0001	0x0002
NtAccessCheck													0x0061	0x0061	0x0062	0x0062	0x0062	0x0062	0x0000
NtAccessCheckAndAuditAlarm													0x0026	0x0026	0x0027	0x0028	0x0027	0x0028	0x0029
NtAccessCheckByType													0x0062	0x0062	0x0063	0x0063	0x0063	0x0063	0x0063
NtAccessCheckByTypeAndAuditAlarm													0x0056	0x0056	0x0057	0x0058	0x0057	0x0058	0x0059
NtAccessCheckByTypeResultList													0x0063	0x0063	0x0064	0x0064	0x0064	0x0064	0x0064

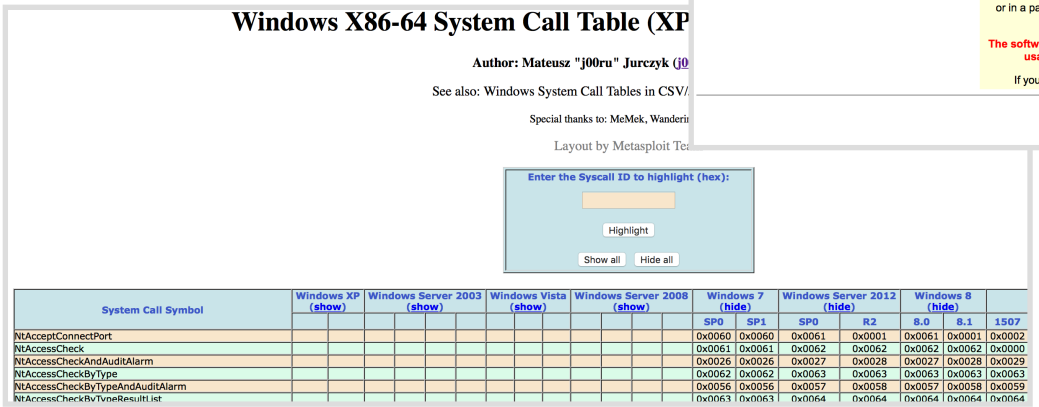
https://j00ru.vexillium.org/syscalls/nt/64/

The internet knows things

- MSDN (incomplete, sometimes difficult to parse)
- Third-party websites



https://undocumented.ntinternals.net



https://j00ru.vexillium.org/syscalls/nt/64/

First assessment

```
NtCreateFile(


  OUT PHANDLE              FileHandle,
  IN ACCESS_MASK           DesiredAccess,
  IN POBJECT_ATTRIBUTES    ObjectAttributes,
  OUT PIO_STATUS_BLOCK     IoStatusBlock,
  IN PLARGE_INTEGER        AllocationSize OPTIONAL,
  IN ULONG                 FileAttributes,
  IN ULONG                 ShareAccess,
  IN ULONG                 CreateDisposition,
  IN ULONG                 CreateOptions,
  IN PVOID                 EaBuffer OPTIONAL,
  IN ULONG                 EaLength );
```

rax	0x52
r10	0x22f3d8
rdx	0x40100080
r8	0x22f428
r9	0x22f3e8

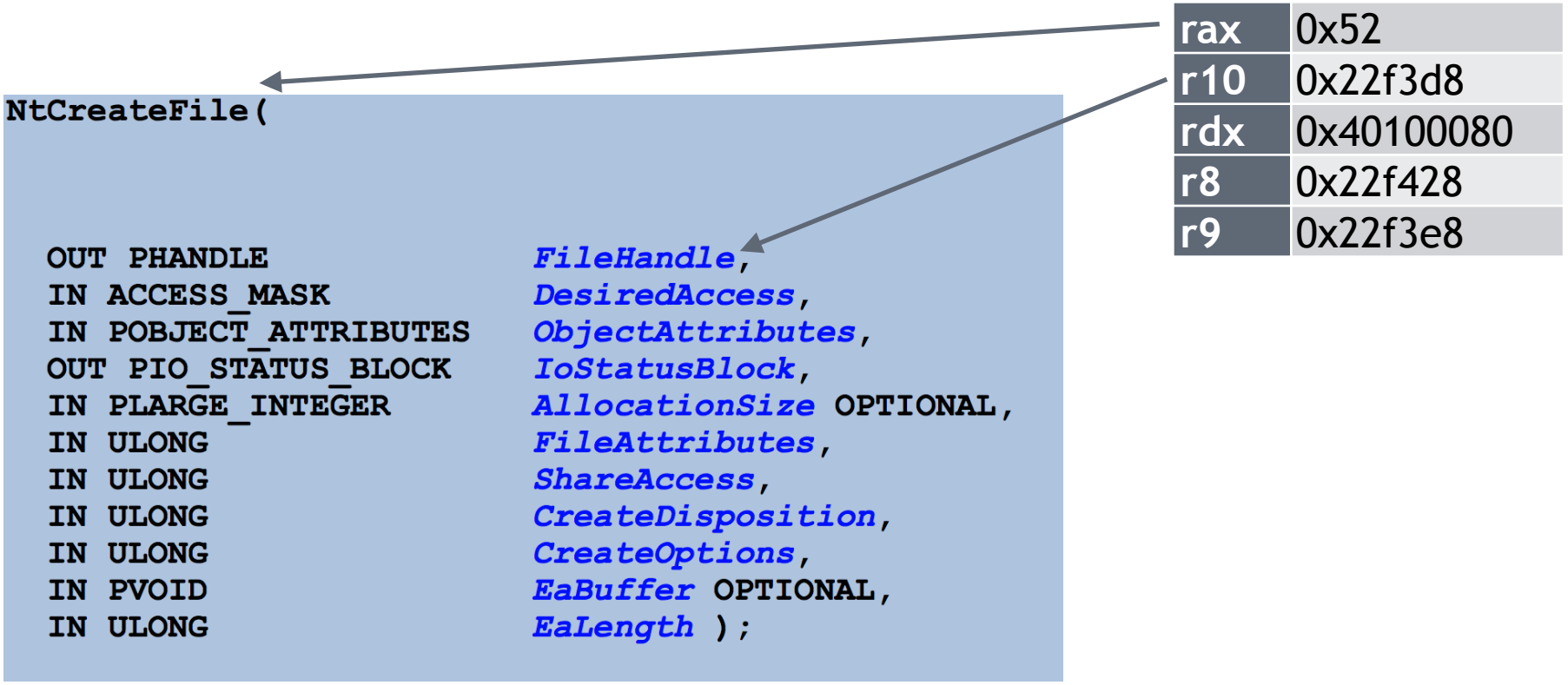
First assessment

rax	0x52
r10	0x22f3d8
rdx	0x40100080
r8	0x22f428
r9	0x22f3e8

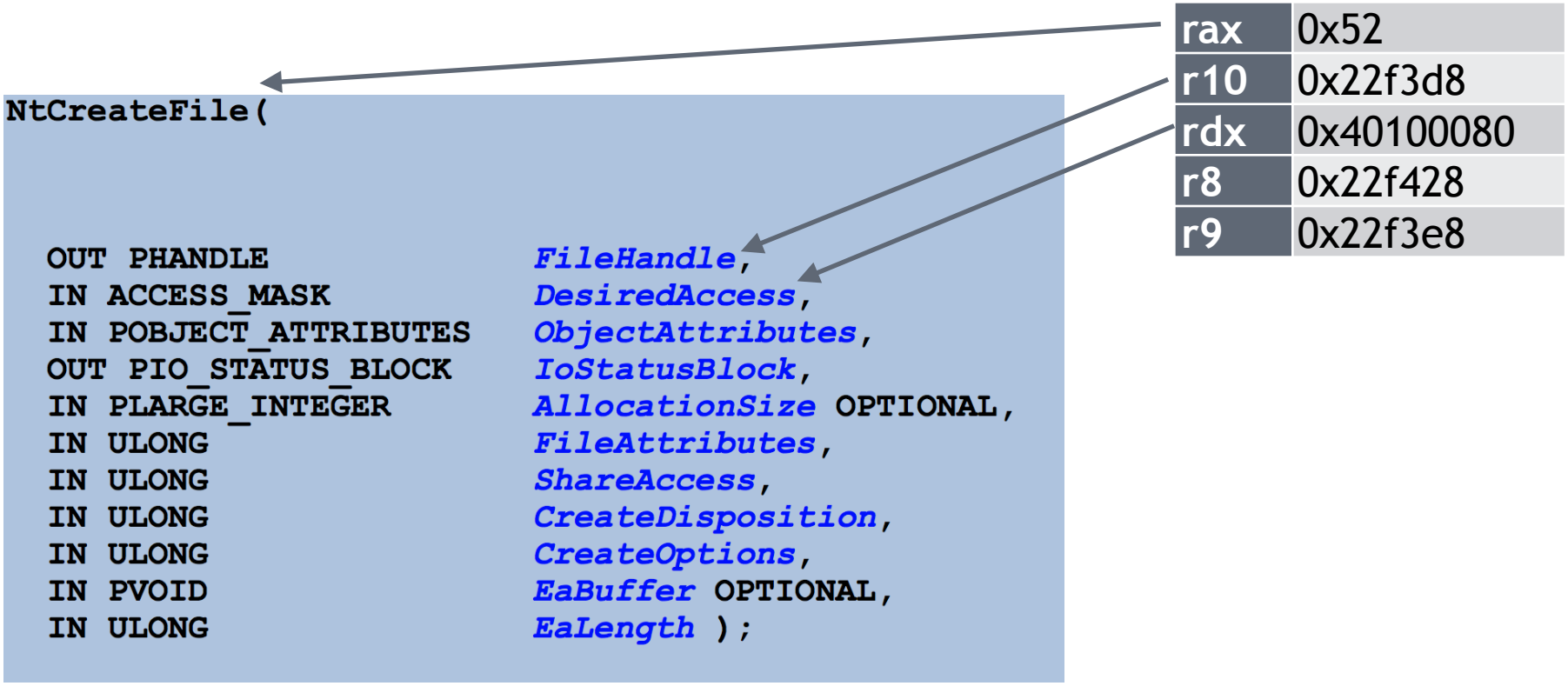
```
NtCreateFile(


  OUT PHANDLE              FileHandle,
  IN ACCESS_MASK           DesiredAccess,
  IN POBJECT_ATTRIBUTES    ObjectAttributes,
  OUT PIO_STATUS_BLOCK     IoStatusBlock,
  IN PLARGE_INTEGER        AllocationSize OPTIONAL,
  IN ULONG                 FileAttributes,
  IN ULONG                 ShareAccess,
  IN ULONG                 CreateDisposition,
  IN ULONG                 CreateOptions,
  IN PVOID                 EaBuffer OPTIONAL,
  IN ULONG                 EaLength );
```

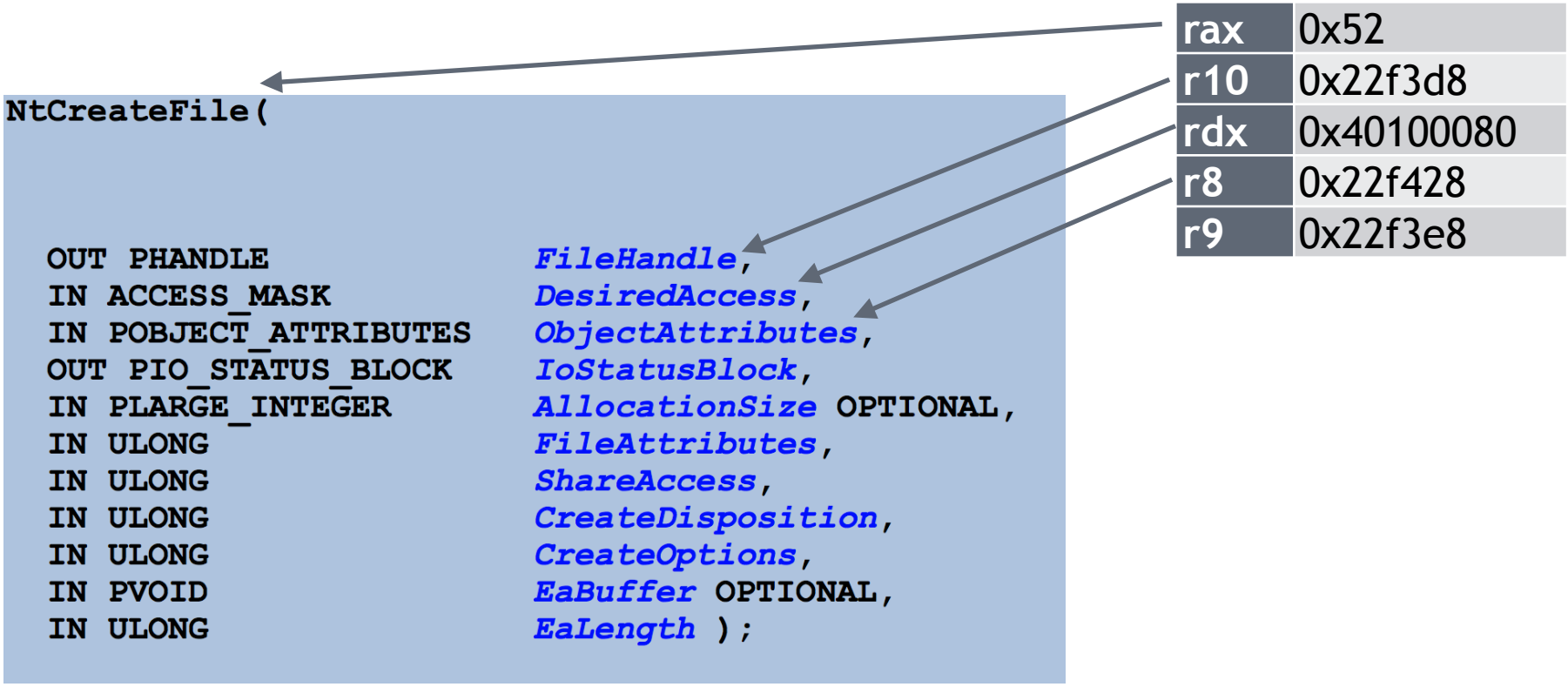
First assessment



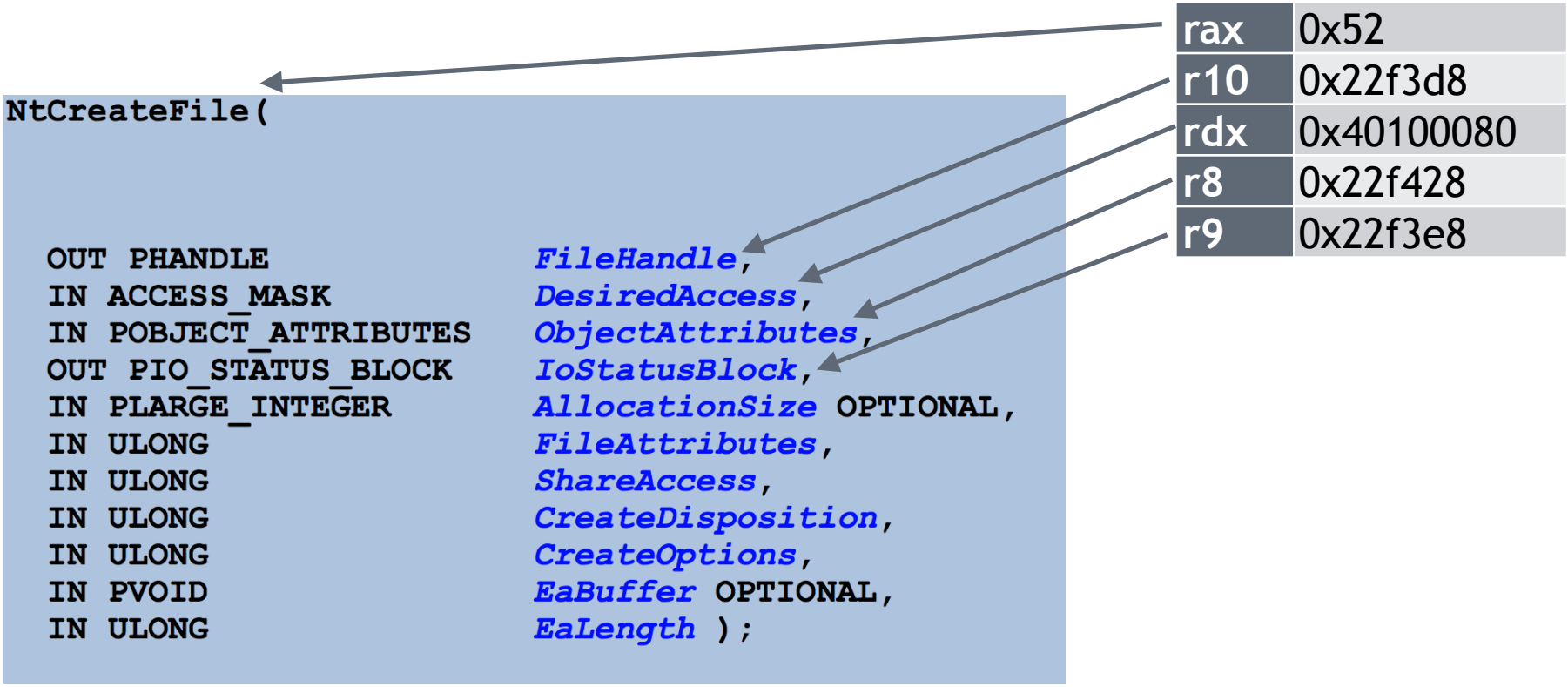
First assessment



First assessment



First assessment



Follow the pointers

Follow the pointers

- POBJECT_ATTRIBUTES is a pointer to a data structure

Follow the pointers

- POBJECT_ATTRIBUTES is a pointer to a data structure
- Read from memory dump

Follow the pointers

- POBJECT_ATTRIBUTES is a pointer to a data structure
- Read from memory dump
- Struct layout?

Follow the pointers

- POBJECT_ATTRIBUTES is a pointer to a data structure
- Read from memory dump
- Struct layout?
    - Website does not provide this info.. :(

Follow the pointers

- POBJECT_ATTRIBUTES is a pointer to a data structure
- Read from memory dump
- Struct layout?
  - Website does not provide this info.. :(
- Symbol files (ntkrnlmp.pdb) contain type information

Follow the pointers

```
0x13a7 : Length = 162, Leaf = 0x1203 LF_FIELDLIST
        list[0] = LF_MEMBER, public, type = T_ULONG(0022), offset = 0
                member name = 'Length'
        list[1] = LF_MEMBER, public, type = T_64PVOID(0603), offset = 8
                member name = 'RootDirectory'
        list[2] = LF_MEMBER, public, type = 0x10D2, offset = 16
                member name = 'ObjectName'
        list[3] = LF_MEMBER, public, type = T_ULONG(0022), offset = 24
                member name = 'Attributes'
        list[4] = LF_MEMBER, public, type = T_64PVOID(0603), offset = 32
                member name = 'SecurityDescriptor'
        list[5] = LF_MEMBER, public, type = T_64PVOID(0603), offset = 40
                member name = 'SecurityQualityOfService'

0x10d3 : Length = 66, Leaf = 0x1203 LF_FIELDLIST
        list[0] = LF_MEMBER, public, type = T_USHORT(0021), offset = 0
                member name = 'Length'
        list[1] = LF_MEMBER, public, type = T_USHORT(0021), offset = 2
                member name = 'MaximumLength'
        list[2] = LF_MEMBER, public, type = T_64PUSHORT(0621), offset = 8
                member name = 'Buffer'
```

Memory dump

Memory dump

0x22f428: OBJECT_ATTRIBUTES

```
0022f420  00 00 00 40 00 00 00 00  30 00 00 00 00 00 00 00  |...@....0.......|
0022f430  00 00 00 00 00 00 00 00  10 f4 22 00 00 00 00 00  |..........".....|
0022f440  42 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |B...............|
0022f450  c8 f3 22 00 00 00 00 00  00 00 00 00 00 00 00 00  |..”.............|
```

Memory dump

0x22f428: OBJECT_ATTRIBUTES

```
0022f420  00 00 00 40 00 00 00 00  30 00 00 00 00 00 00 00  |...@....0.......|
0022f430  00 00 00 00 00 00 00 00  10 f4 22 00 00 00 00 00  |..........".....|
0022f440  42 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |B...............|
0022f450  c8 f3 22 00 00 00 00 00  00 00 00 00 00 00 00 00  |..”.............|
```

0x22f410: UNICODE_STRING

```
0022f410  4c 00 1a 02 00 00 00 00  80 1a 2d 00 00 00 00 00  |L.........-.....|
```

Memory dump

↓ 0x22f428: OBJECT_ATTRIBUTES

```
0022f420  00 00 00 40 00 00 00 00  30 00 00 00 00 00 00 00  |...@....0.......|
0022f430  00 00 00 00 00 00 00 00  10 f4 22 00 00 00 00 00  |..........".....|
0022f440  42 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |B...............|
0022f450  c8 f3 22 00 00 00 00 00  00 00 00 00 00 00 00 00  |..".............|
```

↓ 0x22f410: UNICODE_STRING

```
0022f410  4c 00 1a 02 00 00 00 00  80 1a 2d 00 00 00 00 00  |L.........-.....|
```

↓ 0x2d1a80: T_64PUSHORT (aka UTF-16 string)

```
002d1a80  5c 00 3f 00 3f 00 5c 00  43 00 3a 00 5c 00 55 00  |\.?.?.\.C.:.\.U.|
002d1a90  73 00 65 00 72 00 73 00  5c 00 41 00 64 00 6d 00  |s.e.r.s.\.A.d.m.|
002d1aa0  69 00 6e 00 69 00 73 00  74 00 72 00 61 00 74 00  |i.n.i.s.t.r.a.t.|
002d1ab0  6f 00 72 00 5c 00 73 00  74 00 61 00 72 00 74 00  |o.r.\.s.t.a.r.t.|
002d1ac0  6d 00 65 00 2e 00 62 00  61 00 74 00 00 00 00 00  |m.e...b.a.t.....|
```

Decoding the memory

Decoding the memory

- Cumbersome process:

Decoding the memory

- Cumbersome process:
  - Find memory location

Decoding the memory

- Cumbersome process:
  - Find memory location
  - Decode structure

Decoding the memory

- Cumbersome process:
  - Find memory location
  - Decode structure
  - Follow pointers

Decoding the memory

- Cumbersome process:
  - Find memory location
  - Decode structure
  - Follow pointers
  - Repeat

Decoding the memory

- Cumbersome process:
  - Find memory location
  - Decode structure
  - Follow pointers
  - Repeat
- Tailored to specific situation

Decoding the memory

- Cumbersome process:
  - Find memory location
  - Decode structure
  - Follow pointers
  - Repeat
- Tailored to specific situation
- Generic script needs machine-readable knowledge base!

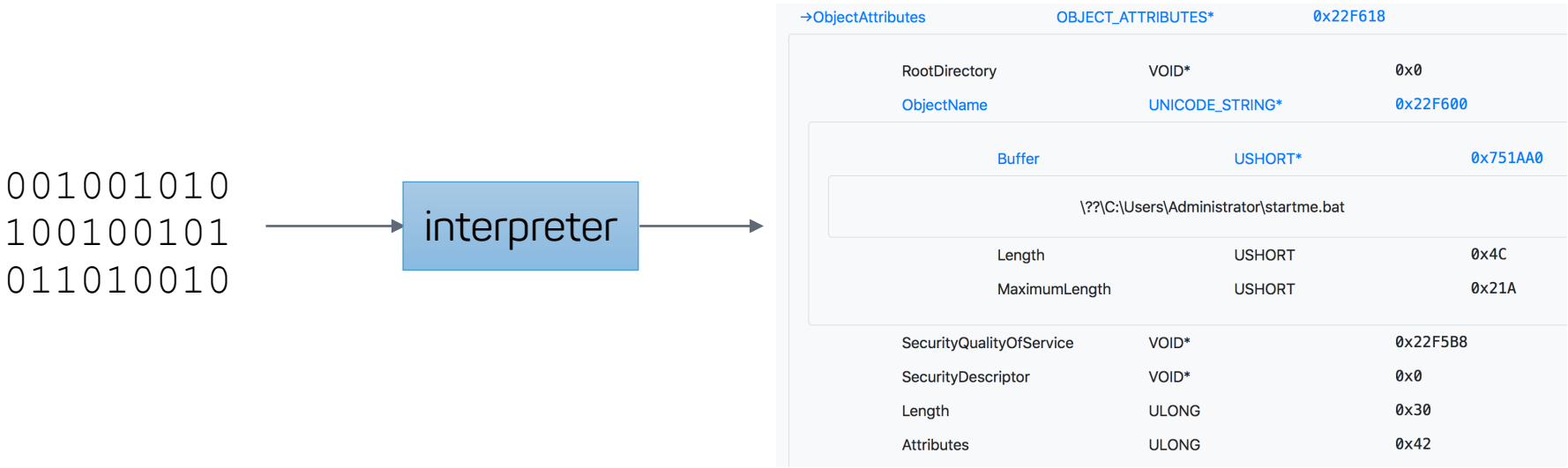
Semantic interpretation

Semantic interpretation

```
001001010
100100101
011010010
```

Semantic interpretation

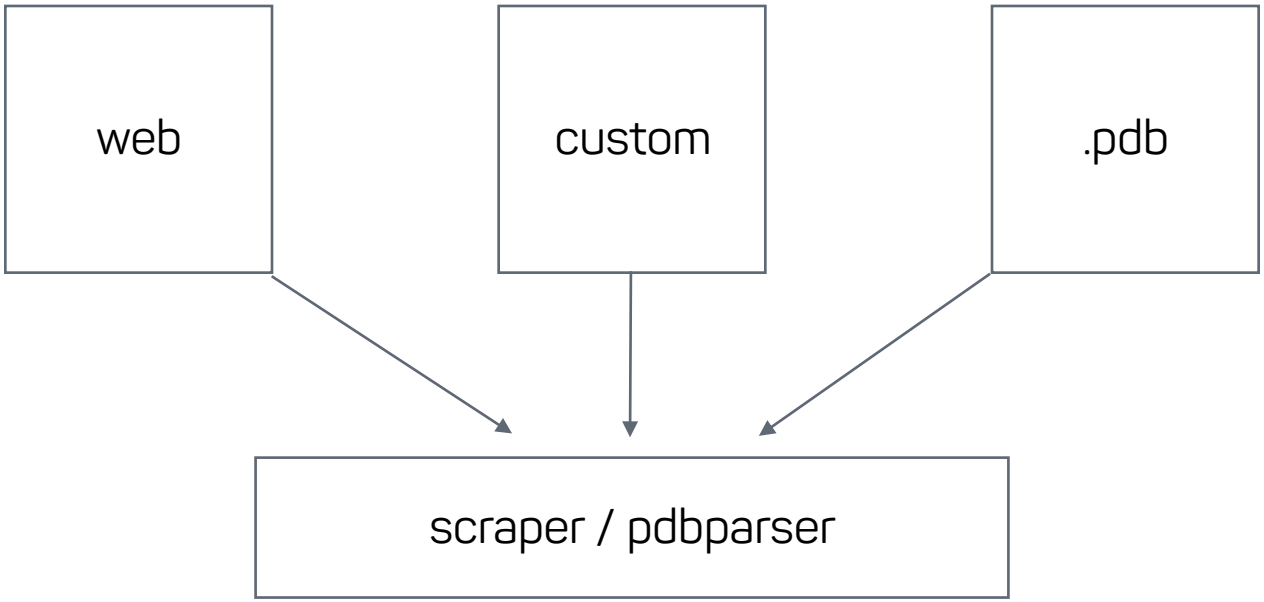
Semantic interpretation

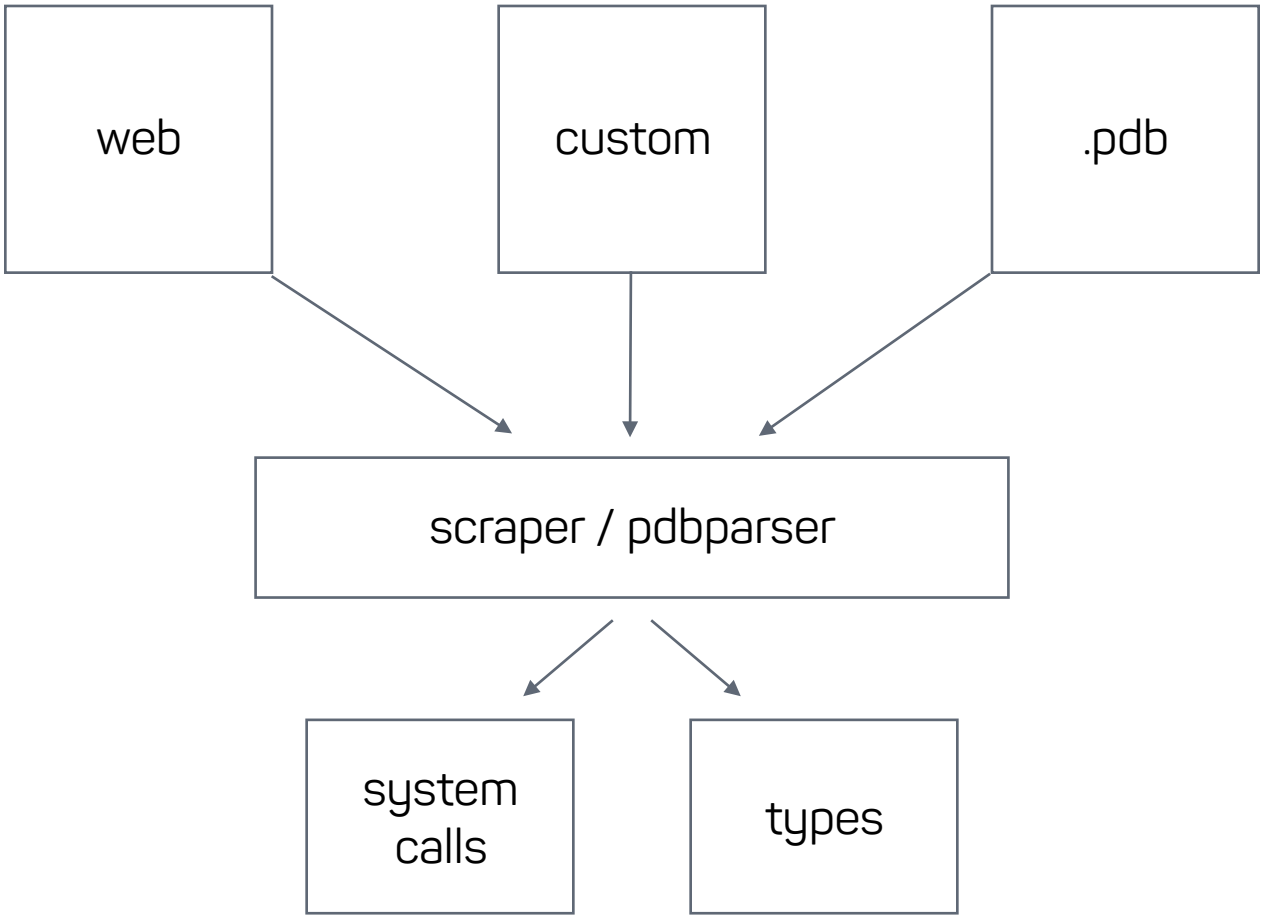


OS internals scraping toolkit

Taking it all in


web
custom
.pdb


web
custom
.pdb
scraper / pdbparser


web
custom
.pdb
scraper / pdbparser
system calls
types

Current sources

Current sources

- https://j00ru.vexillium.org (system call list)

Current sources

- https://j00ru.vexillium.org (system call list)
- https://undocumented.ntinternals.net (signature definitions)

Current sources

- https://j00ru.vexillium.org (system call list)
- https://undocumented.ntinternals.net (signature definitions)
- http://msdl.microsoft.com/download/symbols (type definitions)

Output format: System call list

- CSV

System Call Name	Windows 10 1607	Windows 7 SP0	…
…			
NtCreateFile	85	82	…
…			

Output format: System call signatures

- JSON

```
...
"NtCreateFile": [
    [
        [ "OUT", "PHANDLE" ],
        "FileHandle"
    ],
    [
        [ "IN", "ACCESS_MASK" ],
        "DesiredAccess"
    ],
    [
        [ "IN", "POBJECT_ATTRIBUTES" ],
        "ObjectAttributes"
    ],
    ...
],
...
```

Output format: Type definitions

- JSON

```
"OBJECT_ATTRIBUTES": [
  "0x30",
  [
    [ "Length",                    "0x0",  "T_ULONG"          ],
    [ "RootDirectory",             "0x8",  "T_64PVOID"        ],
    [ "ObjectName",                "0x10", "UNICODE_STRING*" ],
    [ "Attributes",                "0x18", "T_ULONG"          ],
    [ "SecurityDescriptor",        "0x20", "T_64PVOID"        ],
    [ "SecurityQualityOfService", "0x28", "T_64PVOID"        ]
  ]
],
```

Run the script!

https://cyberus-technology.de/bsides/syscall.zip

Run the script!

https://cyberus-technology.de/bsides/syscall.zip

```
$ ./syscall.py states.json before.dmp after.dmp
```

Run the script!

https://cyberus-technology.de/bsides/syscall.zip

```
$ ./syscall.py states.json before.dmp after.dmp
SYSTEM CALL NtCreateFile START
```

Run the script!

https://cyberus-technology.de/bsides/syscall.zip

```
$ ./syscall.py states.json before.dmp after.dmp
SYSTEM CALL NtCreateFile START
PARAM1: IN ACCESS_MASK DesiredAccess: 0x40100080
```

Run the script!

https://cyberus-technology.de/bsides/syscall.zip

```
$ ./syscall.py states.json before.dmp after.dmp
SYSTEM CALL NtCreateFile START
PARAM1: IN ACCESS_MASK DesiredAccess: 0x40100080
PARAM2: IN POBJECT_ATTRIBUTES ObjectAttributes: 0x22f428
```

Run the script!

https://cyberus-technology.de/bsides/syscall.zip

```
$ ./syscall.py states.json before.dmp after.dmp
SYSTEM CALL NtCreateFile START
PARAM1: IN ACCESS_MASK DesiredAccess: 0x40100080
PARAM2: IN POBJECT_ATTRIBUTES ObjectAttributes: 0x22f428
   Found pointer argument to OBJECT_ATTRIBUTES
```

Run the script!

https://cyberus-technology.de/bsides/syscall.zip

```
$ ./syscall.py states.json before.dmp after.dmp
SYSTEM CALL NtCreateFile START
PARAM1: IN ACCESS_MASK DesiredAccess: 0x40100080
PARAM2: IN POBJECT_ATTRIBUTES ObjectAttributes: 0x22f428
   Found pointer argument to OBJECT_ATTRIBUTES
   T_ULONG Length: 0x30
```

Run the script!

https://cyberus-technology.de/bsides/syscall.zip

```
$ ./syscall.py states.json before.dmp after.dmp
SYSTEM CALL NtCreateFile START
PARAM1: IN ACCESS_MASK DesiredAccess: 0x40100080
PARAM2: IN POBJECT_ATTRIBUTES ObjectAttributes: 0x22f428
   Found pointer argument to OBJECT_ATTRIBUTES
   T_ULONG Length: 0x30
   T_64PVOID RootDirectory: 0x0
```

Run the script!

https://cyberus-technology.de/bsides/syscall.zip

```
$ ./syscall.py states.json before.dmp after.dmp
SYSTEM CALL NtCreateFile START
PARAM1: IN ACCESS_MASK DesiredAccess: 0x40100080
PARAM2: IN POBJECT_ATTRIBUTES ObjectAttributes: 0x22f428
   Found pointer argument to OBJECT_ATTRIBUTES
   T_ULONG Length: 0x30
   T_64PVOID RootDirectory: 0x0
   UNICODE_STRING* ObjectName: 0x22f410
```

Run the script!

https://cyberus-technology.de/bsides/syscall.zip

```
$ ./syscall.py states.json before.dmp after.dmp
SYSTEM CALL NtCreateFile START
PARAM1: IN ACCESS_MASK DesiredAccess: 0x40100080
PARAM2: IN POBJECT_ATTRIBUTES ObjectAttributes: 0x22f428
   Found pointer argument to OBJECT_ATTRIBUTES
   T_ULONG Length: 0x30
   T_64PVOID RootDirectory: 0x0
   UNICODE_STRING* ObjectName: 0x22f410
      UTF-16 length 76: \??\C:\Users\Administrator\startme.bat
```

Run the script!

https://cyberus-technology.de/bsides/syscall.zip

```
$ ./syscall.py states.json before.dmp after.dmp
SYSTEM CALL NtCreateFile START
PARAM1: IN ACCESS_MASK DesiredAccess: 0x40100080
PARAM2: IN POBJECT_ATTRIBUTES ObjectAttributes: 0x22f428
   Found pointer argument to OBJECT_ATTRIBUTES
   T_ULONG Length: 0x30
   T_64PVOID RootDirectory: 0x0
   UNICODE_STRING* ObjectName: 0x22f410
      UTF-16 length 76: \??\C:\Users\Administrator\startme.bat
   T_ULONG Attributes: 0x42
```

Run the script!

https://cyberus-technology.de/bsides/syscall.zip

```
$ ./syscall.py states.json before.dmp after.dmp
SYSTEM CALL NtCreateFile START
PARAM1: IN ACCESS_MASK DesiredAccess: 0x40100080
PARAM2: IN POBJECT_ATTRIBUTES ObjectAttributes: 0x22f428
   Found pointer argument to OBJECT_ATTRIBUTES
   T_ULONG Length: 0x30
   T_64PVOID RootDirectory: 0x0
   UNICODE_STRING* ObjectName: 0x22f410
      UTF-16 length 76: \??\C:\Users\Administrator\startme.bat
   T_ULONG Attributes: 0x42
   T_64PVOID SecurityDescriptor: 0x0
```

Run the script!

https://cyberus-technology.de/bsides/syscall.zip

```
$ ./syscall.py states.json before.dmp after.dmp
SYSTEM CALL NtCreateFile START
PARAM1: IN ACCESS_MASK DesiredAccess: 0x40100080
PARAM2: IN POBJECT_ATTRIBUTES ObjectAttributes: 0x22f428
   Found pointer argument to OBJECT_ATTRIBUTES
   T_ULONG Length: 0x30
   T_64PVOID RootDirectory: 0x0
   UNICODE_STRING* ObjectName: 0x22f410
      UTF-16 length 76: \??\C:\Users\Administrator\startme.bat
   T_ULONG Attributes: 0x42
   T_64PVOID SecurityDescriptor: 0x0
   T_64PVOID SecurityQualityOfService: 0x22f3c8
```

Run the script!

https://cyberus-technology.de/bsides/syscall.zip

```
$ ./syscall.py states.json before.dmp after.dmp
SYSTEM CALL NtCreateFile START
PARAM1: IN ACCESS_MASK DesiredAccess: 0x40100080
PARAM2: IN POBJECT_ATTRIBUTES ObjectAttributes: 0x22f428
   Found pointer argument to OBJECT_ATTRIBUTES
   T_ULONG Length: 0x30
   T_64PVOID RootDirectory: 0x0
   UNICODE_STRING* ObjectName: 0x22f410
      UTF-16 length 76: \??\C:\Users\Administrator\startme.bat
   T_ULONG Attributes: 0x42
   T_64PVOID SecurityDescriptor: 0x0
   T_64PVOID SecurityQualityOfService: 0x22f3c8
SYSTEM CALL RESULT: 0
```

Run the script!

https://cyberus-technology.de/bsides/syscall.zip

```
$ ./syscall.py states.json before.dmp after.dmp
SYSTEM CALL NtCreateFile START
PARAM1: IN ACCESS_MASK DesiredAccess: 0x40100080
PARAM2: IN POBJECT_ATTRIBUTES ObjectAttributes: 0x22f428
   Found pointer argument to OBJECT_ATTRIBUTES
   T_ULONG Length: 0x30
   T_64PVOID RootDirectory: 0x0
   UNICODE_STRING* ObjectName: 0x22f410
      UTF-16 length 76: \??\C:\Users\Administrator\startme.bat
   T_ULONG Attributes: 0x42
   T_64PVOID SecurityDescriptor: 0x0
   T_64PVOID SecurityQualityOfService: 0x22f3c8
SYSTEM CALL RESULT: 0
PARAM0: OUT PHANDLE FileHandle: 0x22f3d8
```

Run the script!

https://cyberus-technology.de/bsides/syscall.zip

```
$ ./syscall.py states.json before.dmp after.dmp
SYSTEM CALL NtCreateFile START
PARAM1: IN ACCESS_MASK DesiredAccess: 0x40100080
PARAM2: IN POBJECT_ATTRIBUTES ObjectAttributes: 0x22f428
   Found pointer argument to OBJECT_ATTRIBUTES
   T_ULONG Length: 0x30
   T_64PVOID RootDirectory: 0x0
   UNICODE_STRING* ObjectName: 0x22f410
      UTF-16 length 76: \??\C:\Users\Administrator\startme.bat
   T_ULONG Attributes: 0x42
   T_64PVOID SecurityDescriptor: 0x0
   T_64PVOID SecurityQualityOfService: 0x22f3c8
SYSTEM CALL RESULT: 0
PARAM0: OUT PHANDLE FileHandle: 0x22f3d8
   Found pointer argument to PHANDLE: 0x34
```

Run the script!

https://cyberus-technology.de/bsides/syscall.zip

```
$ ./syscall.py states.json before.dmp after.dmp
SYSTEM CALL NtCreateFile START
PARAM1: IN ACCESS_MASK DesiredAccess: 0x40100080
PARAM2: IN POBJECT_ATTRIBUTES ObjectAttributes: 0x22f428
   Found pointer argument to OBJECT_ATTRIBUTES
   T_ULONG Length: 0x30
   T_64PVOID RootDirectory: 0x0
   UNICODE_STRING* ObjectName: 0x22f410
      UTF-16 length 76: \??\C:\Users\Administrator\startme.bat
   T_ULONG Attributes: 0x42
   T_64PVOID SecurityDescriptor: 0x0
   T_64PVOID SecurityQualityOfService: 0x22f3c8
SYSTEM CALL RESULT: 0
PARAM0: OUT PHANDLE FileHandle: 0x22f3d8
   Found pointer argument to PHANDLE: 0x34
PARAM3: OUT PIO_STATUS_BLOCK IoStatusBlock: 0x22f3e8
```

Run the script!

https://cyberus-technology.de/bsides/syscall.zip

```
$ ./syscall.py states.json before.dmp after.dmp
SYSTEM CALL NtCreateFile START
PARAM1: IN ACCESS_MASK DesiredAccess: 0x40100080
PARAM2: IN POBJECT_ATTRIBUTES ObjectAttributes: 0x22f428
   Found pointer argument to OBJECT_ATTRIBUTES
   T_ULONG Length: 0x30
   T_64PVOID RootDirectory: 0x0
   UNICODE_STRING* ObjectName: 0x22f410
      UTF-16 length 76: \??\C:\Users\Administrator\startme.bat
   T_ULONG Attributes: 0x42
   T_64PVOID SecurityDescriptor: 0x0
   T_64PVOID SecurityQualityOfService: 0x22f3c8
SYSTEM CALL RESULT: 0
PARAM0: OUT PHANDLE FileHandle: 0x22f3d8
   Found pointer argument to PHANDLE: 0x34
PARAM3: OUT PIO_STATUS_BLOCK IoStatusBlock: 0x22f3e8
   Found pointer argument to IO_STATUS_BLOCK
```

Run the script!

https://cyberus-technology.de/bsides/syscall.zip

```
$ ./syscall.py states.json before.dmp after.dmp
SYSTEM CALL NtCreateFile START
PARAM1: IN ACCESS_MASK DesiredAccess: 0x40100080
PARAM2: IN POBJECT_ATTRIBUTES ObjectAttributes: 0x22f428
   Found pointer argument to OBJECT_ATTRIBUTES
   T_ULONG Length: 0x30
   T_64PVOID RootDirectory: 0x0
   UNICODE_STRING* ObjectName: 0x22f410
      UTF-16 length 76: \??\C:\Users\Administrator\startme.bat
   T_ULONG Attributes: 0x42
   T_64PVOID SecurityDescriptor: 0x0
   T_64PVOID SecurityQualityOfService: 0x22f3c8
SYSTEM CALL RESULT: 0
PARAM0: OUT PHANDLE FileHandle: 0x22f3d8
   Found pointer argument to PHANDLE: 0x34
PARAM3: OUT PIO_STATUS_BLOCK IoStatusBlock: 0x22f3e8
   Found pointer argument to IO_STATUS_BLOCK
   T_LONG Status: 0x0
```

Run the script!

https://cyberus-technology.de/bsides/syscall.zip

```
$ ./syscall.py states.json before.dmp after.dmp
SYSTEM CALL NtCreateFile START
PARAM1: IN ACCESS_MASK DesiredAccess: 0x40100080
PARAM2: IN POBJECT_ATTRIBUTES ObjectAttributes: 0x22f428
   Found pointer argument to OBJECT_ATTRIBUTES
   T_ULONG Length: 0x30
   T_64PVOID RootDirectory: 0x0
   UNICODE_STRING* ObjectName: 0x22f410
      UTF-16 length 76: \??\C:\Users\Administrator\startme.bat
   T_ULONG Attributes: 0x42
   T_64PVOID SecurityDescriptor: 0x0
   T_64PVOID SecurityQualityOfService: 0x22f3c8
SYSTEM CALL RESULT: 0
PARAM0: OUT PHANDLE FileHandle: 0x22f3d8
   Found pointer argument to PHANDLE: 0x34
PARAM3: OUT PIO_STATUS_BLOCK IoStatusBlock: 0x22f3e8
   Found pointer argument to IO_STATUS_BLOCK
   T_LONG Status: 0x0
   T_64PVOID Pointer: 0x0
```

Run the script!

https://cyberus-technology.de/bsides/syscall.zip

```
$ ./syscall.py states.json before.dmp after.dmp
SYSTEM CALL NtCreateFile START
PARAM1: IN ACCESS_MASK DesiredAccess: 0x40100080
PARAM2: IN POBJECT_ATTRIBUTES ObjectAttributes: 0x22f428
   Found pointer argument to OBJECT_ATTRIBUTES
   T_ULONG Length: 0x30
   T_64PVOID RootDirectory: 0x0
   UNICODE_STRING* ObjectName: 0x22f410
      UTF-16 length 76: \??\C:\Users\Administrator\startme.bat
   T_ULONG Attributes: 0x42
   T_64PVOID SecurityDescriptor: 0x0
   T_64PVOID SecurityQualityOfService: 0x22f3c8
SYSTEM CALL RESULT: 0
PARAM0: OUT PHANDLE FileHandle: 0x22f3d8
   Found pointer argument to PHANDLE: 0x34
PARAM3: OUT PIO_STATUS_BLOCK IoStatusBlock: 0x22f3e8
   Found pointer argument to IO_STATUS_BLOCK
   T_LONG Status: 0x0
   T_64PVOID Pointer: 0x0
   T_UQUAD Information: 0x2
```

The Good, The Bad, The Ugly

The Good, The Bad, The Ugly

- Missing entries (e.g., NtOpenKeyEx)

The Good, The Bad, The Ugly

- Missing entries (e.g., NtOpenKeyEx)
- Inaccuracies (missing pointer indicator)

```
NtQueryMultipleValueKey(


  IN HANDLE                          KeyHandle,
  IN OUT PKEY_MULTIPLE_VALUE_INFORMATION ValuesList,
  IN ULONG                           NumberOfValues,
  OUT PVOID                          DataBuffer,
  IN OUT ULONG                       BufferLength,
  OUT PULONG                         RequiredLength OPTIONAL );
```

The Good, The Bad, The Ugly

- Missing entries (e.g., NtOpenKeyEx)
- Inaccuracies (missing pointer indicator)
- Quirk infrastructure for corrections and additions until fixed

```
NtQueryMultipleValueKey(

  IN HANDLE                          KeyHandle,
  IN OUT PKEY_MULTIPLE_VALUE_INFORMATION ValuesList,
  IN ULONG                           NumberOfValues,
  OUT PVOID                          DataBuffer,
  IN OUT ULONG                       BufferLength,
  OUT PULONG                         RequiredLength OPTIONAL );
```

Next steps

Next steps

- More sources -> more coverage, more accuracy
  - ReactOS
  - wine
  - ProcessHacker

Next steps

- More sources -> more coverage, more accuracy
  - ReactOS
  - wine
  - ProcessHacker
- Versioning / Update checker

Next steps

- More sources -> more coverage, more accuracy
  - ReactOS
  - wine
  - ProcessHacker
- Versioning / Update checker
- More operating systems (currently Windows 7 x64)

Next steps

- More sources -> more coverage, more accuracy
  - ReactOS
  - wine
  - ProcessHacker
- Versioning / Update checker
- More operating systems (currently Windows 7 x64)
- Engage with open-source community!
  https://gitlab.com/cyberus/os-generation

Next steps

- More sources -> more coverage, more accuracy
  - ReactOS
  - wine
  - ProcessHacker
- Versioning / Update checker
- More operating systems (currently Windows 7 x64)
- Engage with open-source community!
  https://gitlab.com/cyberus/os-generation
- **Wanna play?** Micro-CTF around system call interpretation at our Cyberus booth

Summary

Summary

- Interpreting low-level system calls is hard work

Summary

- Interpreting low-level system calls is hard work
- Information scattered around the internet

Summary

- Interpreting low-level system calls is hard work
- Information scattered around the internet
- Scriptability rocks!

Summary

- Interpreting low-level system calls is hard work
- Information scattered around the internet
- Scriptability rocks!
- Open-source rocks!

Summary

- Interpreting low-level system calls is hard work
- Information scattered around the internet
- Scriptability rocks!
- Open-source rocks!

Summary

- Interpreting low-level system calls is hard work
- Information scattered around the internet
- Scriptability rocks!
- Open-source rocks!

- https://gitlab.com/cyberus/os-generation

Summary

- Interpreting low-level system calls is hard work
- Information scattered around the internet
- Scriptability rocks!
- Open-source rocks!

- https://gitlab.com/cyberus/os-generation
- https://cyberus-technology.de/bsides/syscall.zip

Summary

- Interpreting low-level system calls is hard work
- Information scattered around the internet
- Scriptability rocks!
- Open-source rocks!

- https://gitlab.com/cyberus/os-generation
- https://cyberus-technology.de/bsides/syscall.zip
- Twitter: @kleeparthy, @cyberustech

References

- https://gitlab.com/cyberus/os-generation
- https://j00ru.vexillium.org
- https://undocumented.ntinternals.net
- https://blog.cyberus-technology.de
- https://cyberus-technology.de/bsides/syscall.zip