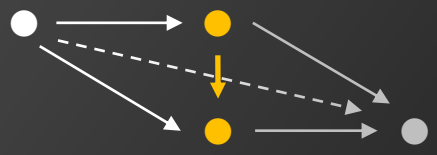
Part 2 Draft

Windows API

for Software Diagnostics

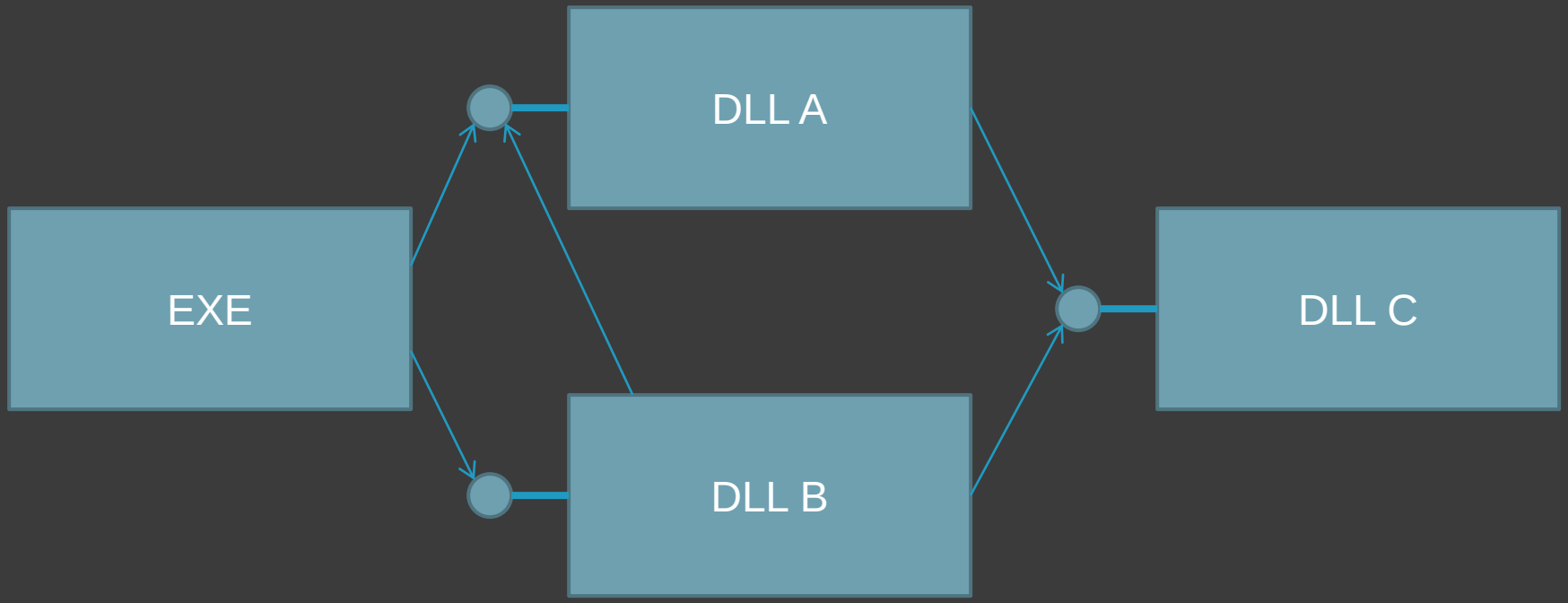
Accelerated

With Category Theory in View



Dmitry Vostokov
Software Diagnostics Services

Modules

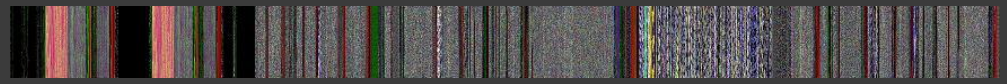


WinDbg Commands

```
0:000> lm

0:000> x mpattern!_imp_fpattern

0:000> x *!fpattern

0:000> dps module!_imp_name L1
```

Modules and Analysis Patterns

- Module memory analysis patterns
  - Module Collection
  - Coupled Modules
  - Duplicated Module



- Namespace malware analysis pattern

Exercise W2

- **Goal:** Explore modules and their dependencies
- **Memory Analysis Patterns:** Module Collection; Coupled Modules
- **Malware Analysis Patterns:** Namespace
- \AWAPI-Dumps\Exercise-W2.pdf

API Usage

- Module usage (static analysis)
  - Hidden Module
- Function usage (dynamic analysis)

WinDbg Commands

```
0:000> .imgscan

0:000> bm mpattern!fpattern
```

Exercise W3

- **Goal:** Find usage of specific Windows API functions
- **Debugging Implementation Patterns:** Code Breakpoint; Breakpoint Action
- \AWAPI-Dumps\Exercise-W3.pdf

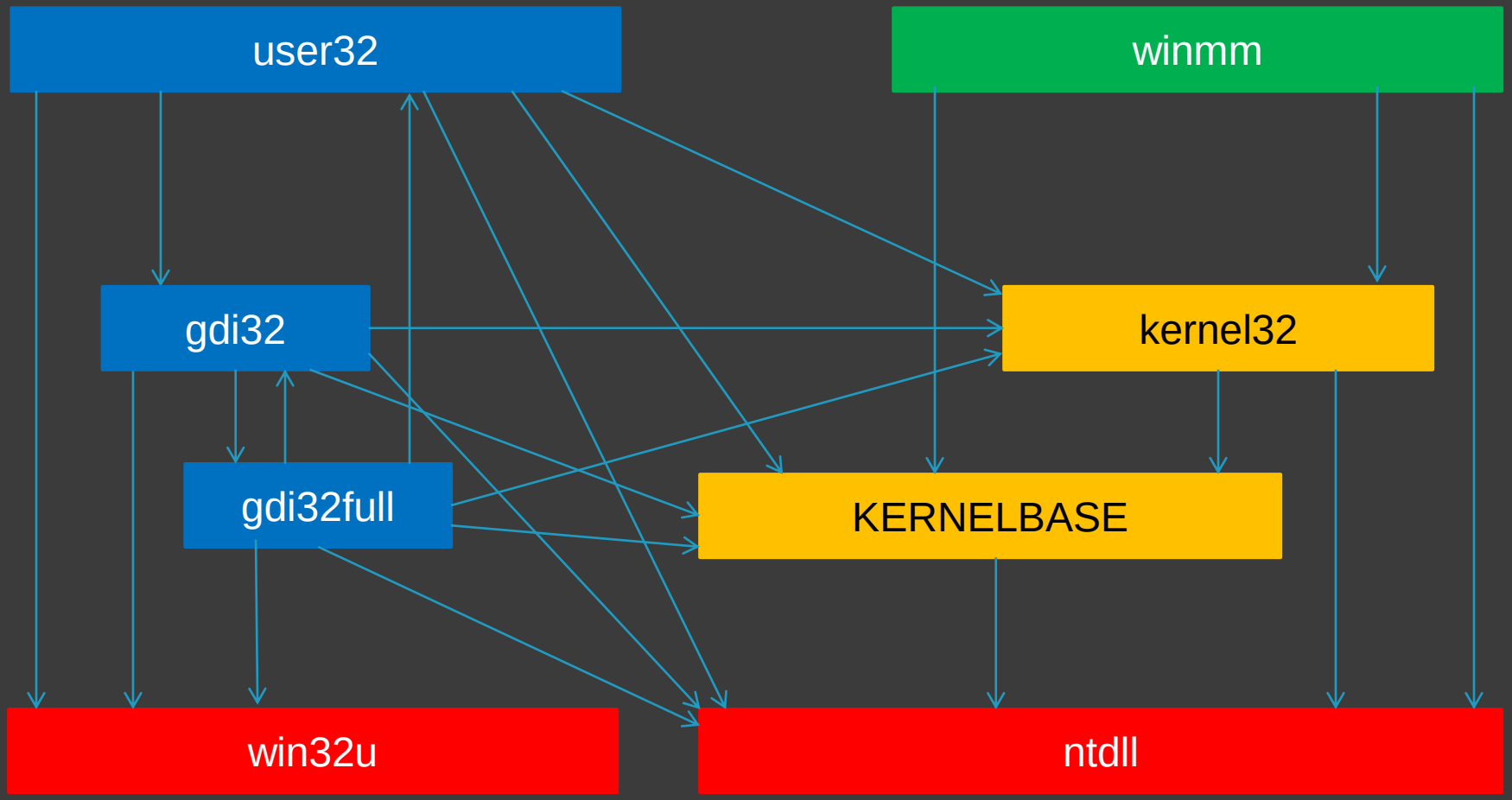
API Sequences (Prescriptive)

- CreateThread, …, CloseHandle
- RegisterClass, CreateWindowEx
- GetMessage, TranslateMessage, DispatchMessage
- BeginPaint, …, EndPaint
- GetDC, …, ReleaseDC

API Sequences (Descriptive)

- Horizontal
  - Code disassembly
  - Traces and logs (Thread of Activity analysis pattern)
- Vertical
  - Stack trace
  - Traces and logs (Fiber Bundle analysis pattern)

API Layers



API Internals

- Memory analysis patterns:
  - Hooked Functions (User Space)
  - Module patterns
    - Hooked Modules
- Malware analysis patterns:
  - Patched Code

WinDbg Commands

```
0:000> .chkimg

0:000> !for_each_module

0:000> u fname

0:000> uf /c fname
```

Exercise W4

- **Goal:** Explore API layers and internals of specific API functions
- **ADDR Patterns:** Function Skeleton; Call Path
- \AWAPI-Dumps\Exercise-W4.pdf

Delay-loaded API

- Documentation
- Example:

```
pub func   00007ffc`e85b6d30    0 winmm!_imp_load_waveInOpen (__imp_load_waveInOpen)
pub global 00007ffc`e85db3c0    0 winmm!_imp_waveInOpen = <no type information>
```

API Sets

- Documentation

```
contract_name => module.dll
```

- Example of API contract:

```
api_ms_win_mm_mme_l1_1_0 => winmmbase.dll
```

Exercise W5

- **Goal:** Explore the delay-loaded API and API sets.
- **Debugging Implementation Patterns:** Code Breakpoint
- **ADDR Patterns:** Call Path
- \AWAPI-Dumps\Exercise-W5.pdf