



Reverse Engineering (REV3)

## **UE 02 – Statische Analyse – Protokoll**

Jakob Mayr

WS 2023/2024

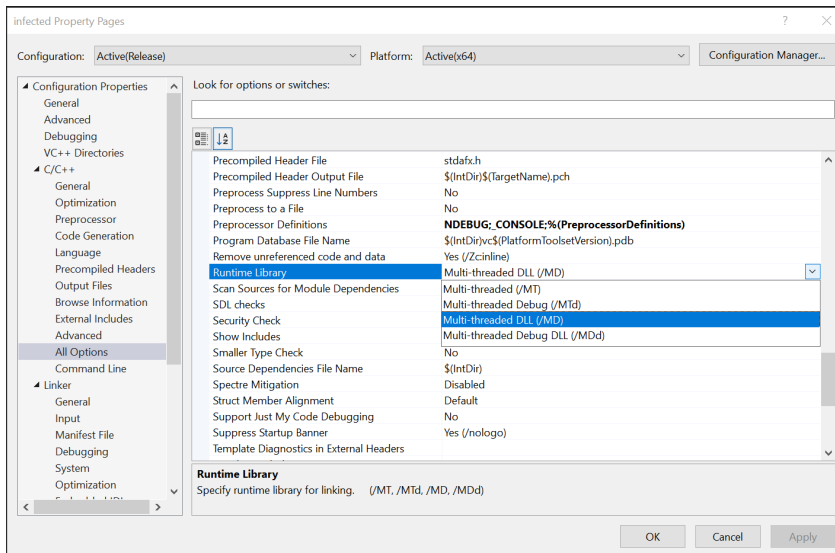
### **1 Einleitung**

...

## 2 Aufgabe 1 - Statische Analyse Windows

### 2.1 create file

```
1  #include <stdio.h>
2
3  int main() {
4      printf("infected");
5      return 0;
6  }
7
```



```
PS C:\Users\admin_sin\Desktop\rev3-s2210239021\releases> dir

Directory: C:\Users\admin_sin\Desktop\rev3-s2210239021\releases

Mode                LastWriteTime         Length Name
----                -
-a----          24.10.2023   16:15           10752 infected-md.exe
-a----          24.10.2023   16:16           14336 infected-MDd.exe
-a----          24.10.2023   16:10          139264 infected-mt.exe
-a----          24.10.2023   16:14          376832 infected-mtd.exe

PS C:\Users\admin_sin\Desktop\rev3-s2210239021\releases>
```

## 2.2 dumpbin

```
PS C:\Users\admin_sin\Desktop\rev3-s2210239021\releases> dumpbin.exe .\infected-mt.exe
Microsoft (R) COFF/PE Dumper Version 14.36.32535.0
Copyright (C) Microsoft Corporation. All rights reserved.

Dump of file .\infected-mt.exe

File Type: EXECUTABLE IMAGE

Summary

2000 .data
2000 .pdata
8000 .rdata
1000 .reloc
1000 .rsrc
15000 .text
1000 .RDATA
PS C:\Users\admin_sin\Desktop\rev3-s2210239021\releases>
```

(a) dumpbin mt-file

```
PS C:\Users\admin_sin\Desktop\rev3-s2210239021\releases> dumpbin.exe .\infected-mtd.exe
Microsoft (R) COFF/PE Dumper Version 14.36.32535.0
Copyright (C) Microsoft Corporation. All rights reserved.

Dump of file .\infected-mtd.exe

File Type: EXECUTABLE IMAGE

Summary

3000 .data
4000 .pdata
15000 .rdata
1000 .reloc
1000 .rsrc
43000 .text
1000 .RDATA
PS C:\Users\admin_sin\Desktop\rev3-s2210239021\releases>
```

(b) dumpbin mtd-file

```
PS C:\Users\admin_sin\Desktop\rev3-s2210239021\releases> dumpbin.exe .\infected-md.exe
Microsoft (R) COFF/PE Dumper Version 14.36.32535.0
Copyright (C) Microsoft Corporation. All rights reserved.

Dump of file .\infected-md.exe

File Type: EXECUTABLE IMAGE

Summary

1000 .data
1000 .pdata
1000 .rdata
1000 .reloc
1000 .rsrc
1000 .text
PS C:\Users\admin_sin\Desktop\rev3-s2210239021\releases>
```

(c) dumpbin md-file

```
PS C:\Users\admin_sin\Desktop\rev3-s2210239021\releases> dumpbin.exe .\infected-MDd.exe
Microsoft (R) COFF/PE Dumper Version 14.36.32535.0
Copyright (C) Microsoft Corporation. All rights reserved.

Dump of file .\infected-MDd.exe

File Type: EXECUTABLE IMAGE

Summary

1000 .data
1000 .pdata
1000 .rdata
1000 .reloc
1000 .rsrc
2000 .text
PS C:\Users\admin_sin\Desktop\rev3-s2210239021\releases>
```

(d) dumpbin mdd-file

Figure 1: All infected.exe files analysed with dumpbin

```

C:\Users\admin\Desktop\rev3>.\output-strings-mt.txt
! This program cannot be run in DOS mode.
C:\Users\admin\Desktop\rev3>.\\2210239021\infected_
.exe&cmd
.rdata$VolTmd
.rdata$Sz2zdbg
    _specific_handler
    _current_exception
    _current_exception_context
VCRTIME160.dll
    _crt_init_func
    _stdio_common_vfprintf
_seh_filter_exe
_set_app_type
    _getenv_matherr
_configure_narrow_argv
_initialize_narrow_environment
_get_initial_narrow_environment
    inittrue_s
    _set_fmde
..._p_argc
..._p_argv
_register_thread_local_exe_atexit_callback
21 _configthreadlocal
22 _set_new_mode
23 _p_command
24 _initialize_onexit_table
27 register_onexit_function
    _crt_atexit
api-ms-win-crt-stdio-l1-0-0.dll
api-ms-win-crt-runtime-l1-0-0.dll
api-ms-win-crt-math-l1-0-0.dll
api-ms-win-crt-localize-l1-0-0.dll
api-ms-win-crt-heap-l1-0-0.dll
RTLCaptureContext
RTLlookupFunctionEntry
SetUnhandledExceptionFilter
GetCurrentProcess
TerminateProcess
UnhandledExceptionFilter
SetUnhandledExceptionFilter
GetCurrentProcess
GetCurrentThreadID
IsProcessorFeaturePresent
QueryPerformanceCounter
GetCurrentProcessID
GetCurrentThreadId
GetModuleHandleW
GetSystemTimeAsFileTime
InitializeListHead
IdDebuggerPresent
GetModuleHandleA
KERNEL32.dll
<xml version='1.0' encoding='UTF-8' standalone='yes'
  <assembly xmlns='urn:schemas-microsoft-com:asm.v1'
    <trustInfo xmlns='urn:schemas-microsoft-com:asm.v3'
      <security>
        <requestedPrivileges>
          <requestedExecutionLevel level='asInvoker' u
            </requestedPrivileges>
        </security>
      </trustInfo>
    </assembly>
  </assembly>
  LSP Inactive -> 2 | text | 207/16 | Bst/20

```

## 3 2. Aufgabe - Statische Analyse Linux

### 3.1 create file

Gleicher code wie zuvor:

```
1  #include <stdio.h>
2
3  int main() {
4      printf("infected");
5      return = 0;
6  }
7
```

Kompilieren und auflisten der Executables:

```
mendacium fedora ./REV3 > UE02 > rev3-s2210239021 > linux
→ gcc -std=c99 -Wall -pedantic infected.c -o infected.out time:1ms
mendacium fedora ./REV3 > UE02 > rev3-s2210239021 > linux
→ gcc -std=c99 -Wall -pedantic infected.c -ggdb -o infected-ggdb.out
mendacium fedora ./REV3 > UE02 > rev3-s2210239021 > linux
→ gcc -std=c99 -Wall -pedantic infected.c -static -o infected-static.out
mendacium fedora ./REV3 > UE02 > rev3-s2210239021 > linux
→ gcc -std=c99 -Wall -pedantic infected.c -static -ggdb -o infected-static-ggdb.out
mendacium fedora ./REV3 > UE02 > rev3-s2210239021 > linux
→ time:80ms
```

```
mendacium fedora ./REV3 > UE02 > rev3-s2210239021 > linux
→ la time:1ms
total 1.6M
-rw-r--r-- 1 mendacium mendacium 69 Oct 24 16:54 infected.c
-rwxr-xr-x 1 mendacium mendacium 18K Oct 24 16:58 infected-ggdb.out*
-rwxr-xr-x 1 mendacium mendacium 17K Oct 24 16:55 infected.out*
-rwxr-xr-x 1 mendacium mendacium 777K Oct 24 17:01 infected-static-ggdb.out*
-rwxr-xr-x 1 mendacium mendacium 776K Oct 24 17:00 infected-static.out*
mendacium fedora ./REV3 > UE02 > rev3-s2210239021 > linux
→ time:1ms
```

## References

- [1] *The Official Radare2 Book*, [Online; abgerufen im Oktober 2023], <https://book.rada.re/>.