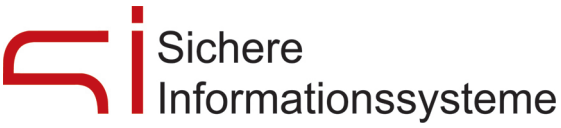


Reverse Engineering (REV3)

UE 02 – Statische Analyse – Protokoll

Jakob Mayr

WS 2023/2024

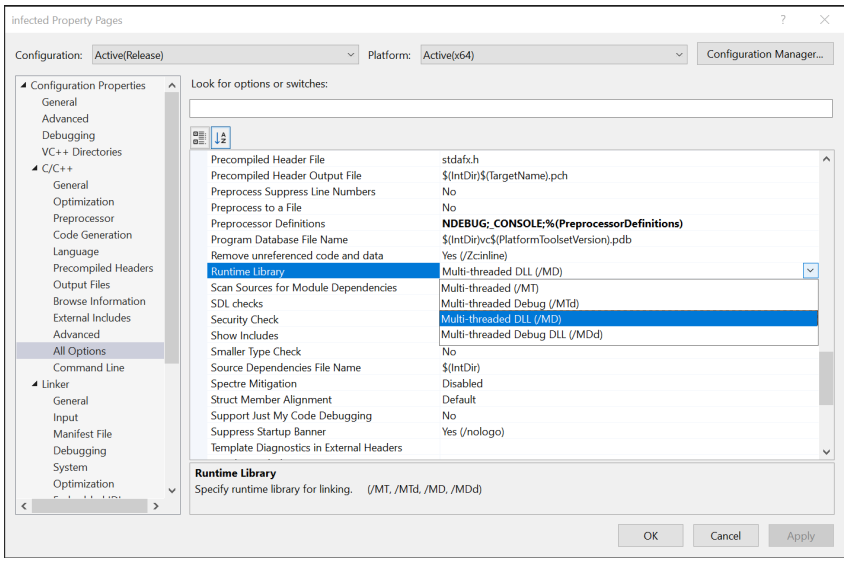
1 Einleitung

...

2 Aufgabe 1 - Statische Analyse Windows

2.1 create file

```c
#include <stdio.h>

int main() {
  printf("infected");
  return = 0;
}

```




```
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
        B000 .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

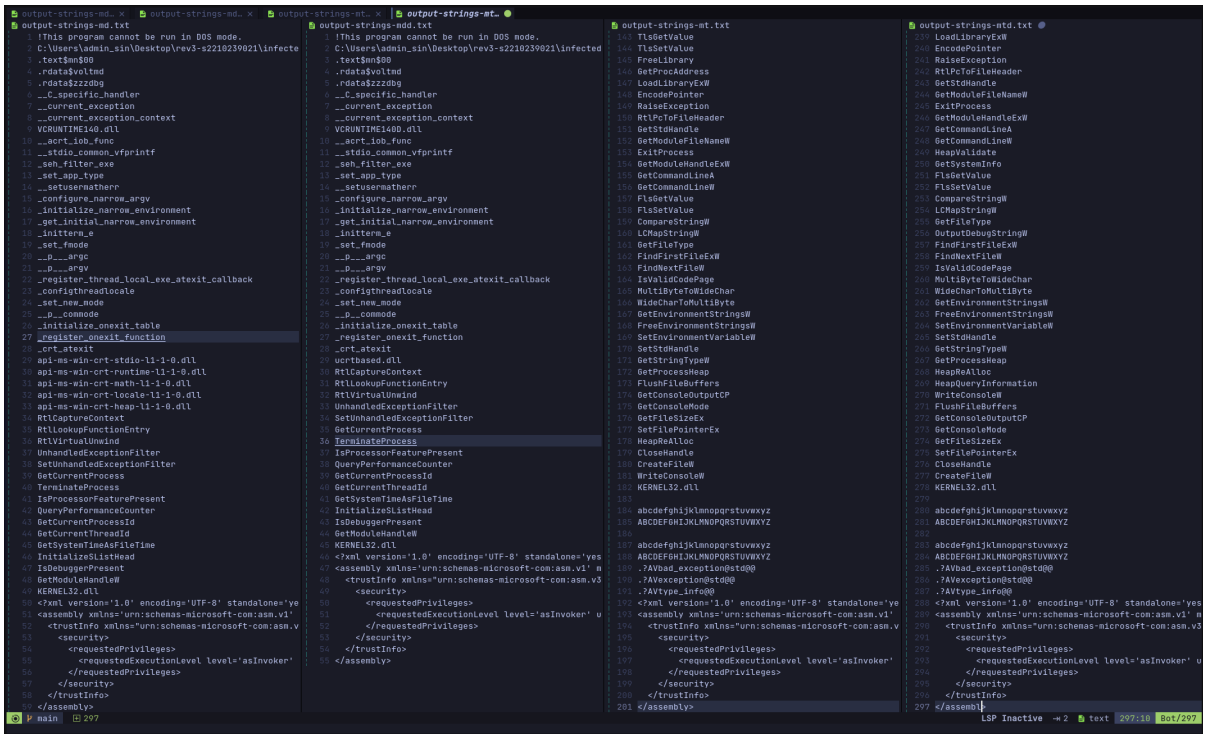
```
PS C:\Users\admin_sin\Desktop\rev3-s2210239021\releases> dumpbin.exe .\infected-MDd.exe
Microsoft (R) COFF/PE Dumper Version 14.36.32535.0
Copyright (C) Microsoft Corporation.  All rights reserved.


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

2.3 strings


output-strings-md.txt
output-strings-mdd.txt
output-strings-mt.txt
output-strings-mtd.txt


output-strings-md.txt
output-strings-mdd.txt
output-strings-mt.txt
output-strings-mtd.txt

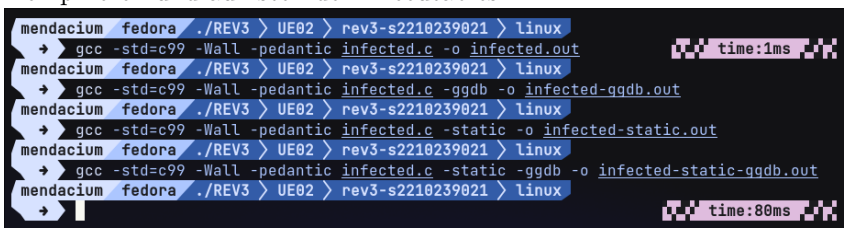
3 2. Aufgabe - Statische Analyse Linux

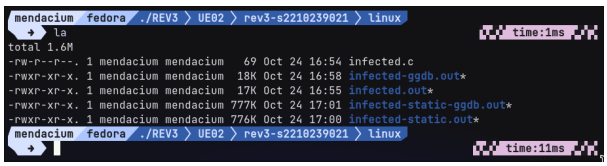
3.1 create file

Gleicher code wie zuvor:

```c
#include <stdio.h>

int main() {
  printf("infected");
  return = 0;
}

```

Kompilieren und auflisten der Executables:





References

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