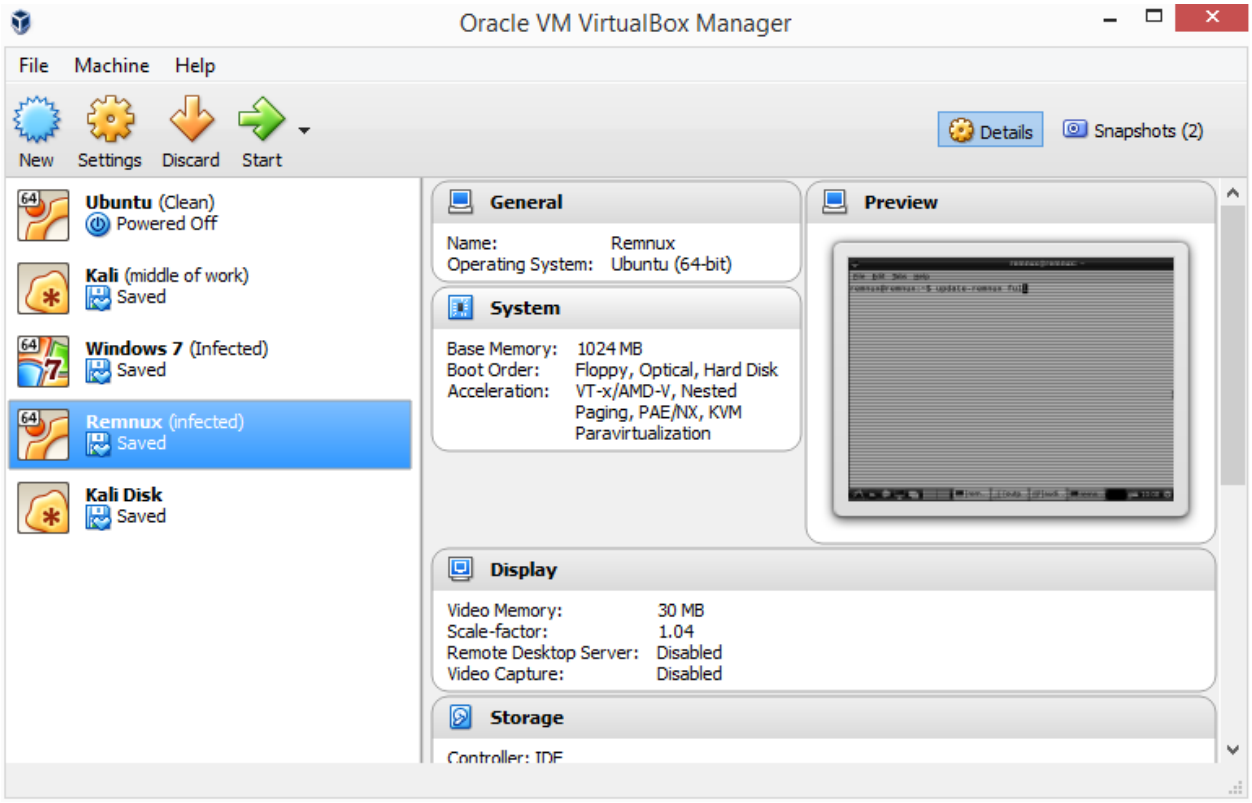
Malware Analysis/Reverse Engineering Tools and Techniques

Background:

Setup:

Open Remnux inside of Virtual Box.

If you do not have the Remnux Virtual Machine setup refer to the environment setup sheets for instructions.



Learning objectives:

1. Apply common tools to examine malware
2. Examine static properties of malware
3. Performing code analysis of executables
4. Reversing malicious code
5. Using memory forensics for analysis

Static Analysis

Profile the file

First fingerprint the files so you know if they change during analysis

Tools:

```
remnux@remnux:~/Desktop$ pehash wcry.exe
file:                   wcry.exe
md5:                    db349b97c37d22f5ea1d1841e3c89eb4
sha1:                   e889544aff85ffaf8b0d0da705105dee7c97fe26
```

```
ssdeep:
98304:wDqPoBhz1aRxcSUDk36SAEdhvxWa9P593R8yAVp2g3R:wDqPe1Cxcxk3ZAEUadzR8yc4gB

header:                 IMAGE_DOS_HEADER
md5:                    5084c5d5cfe99932e67450023c068941
sha1:                   856558429bb575486a46a92ba2684eaab8578cef
ssdeep:                 3:WlWUqt/vllPln:idqH

header:                 IMAGE_COFF_HEADER
md5:                    ba2507c4d04aae88857b753ac54e5111
sha1:                   9d6abdee74212ebd896620608862654ee73a287d
ssdeep:                 3:OE//akn:t/Sk

header:                 IMAGE_OPTIONAL_HEADER
md5:                    42745911ea567b1ff4ab7ec4f9faa277
sha1:                   f7914ae89d21dc68182ea30b8d35453b841ff15b
ssdeep:                 3:3/H3/l7lHlflt/99lhtllrllTl9/ll/ldt1l9tllH:3/F

section:                .text
md5:                    c7613102e2ecec5dcefc144f83189153
sha1:                   79c2158426a696ba552e9d0092008ada753dc3e1
ssdeep:
768:mkgNaOty1IYyvldx9f2uoZw6jThDkyWq+/uDbu2iX17qUD1:mkJOty1IYyvlVaThD9WhuG2u17q

section:                .rdata
md5:                    d8037d744b539326c06e897625751cc9
sha1:                   8c528f41cd4533228264ee639fad17e5be8bf817
ssdeep:
48:liQSFw8mkkiQSFwBXX2cjqB+Cn+2LxA0+efPtboyl14:lR+w8mkkR+wx2cjqQC3GNefPtboyn

section:                .data
md5:                    22a8598dc29cad7078c291e94612ce26
sha1:                   26a45092c8e8e59cb26e39d75f64ae7eb5ad5196
ssdeep:
3072:3ILEVTCW5DgSglPcTcMXaDfldx0dFJtkoeV0XXg6:3IYVTH5DgSg8ajldktM0XXr

section:                .rsrc
md5:                    12e1bd7375d82cca3a51ca48fe22d1a9
sha1:                   4c33b2b6715cc1b982e158401a06fcb156c409a3
ssdeep:
98304:pqPoBhz1aRxcSUDk36SAEdhvxWa9P593R8yAVp2g3R:pqPe1Cxcxk3ZAEUadzR8yc4gB
```

Search for information in the binary using pestr tool or the strings command line command

```
remnux@remnux:~/Desktop$ pestr wcry.exe
...lots of gibber…
...strings of note:
b.wnry
c.wnry
1AgG
msg/m_bulgarian.wnry
"t=)
msg/m_chinese (simplified).wnry
```

"t=.|Vbq-
msg/m_chinese (traditional).wnry
"t=.
msg/m_croatian.wnry
msg/m_czech.wnry
msg/m_danish.wnry
msg/m_dutch.wnry
msg/m_english.wnry
"t=m
msg/m_filipino.wnry
"t=?
msg/m_finnish.wnry
"t=-
msg/m_french.wnry
msg/m_german.wnry
&XZR%
msg/m_greek.wnry
"t=x
msg/m_indonesian.wnry
"t=j%
msg/m_italian.wnry
"t=x-
msg/m_japanese.wnry
msg/m_korean.wnry
msg/m_latvian.wnry
msg/m_norwegian.wnry
msg/m_polish.wnry
msg/m_portuguese.wnry
"t=@W
msg/m_romanian.wnry
msg/m_russian.wnry
"t=3M
msg/m_slovak.wnry
msg/m_spanish.wnry
msg/m_swedish.wnry
msg/m_turkish.wnry
msg/m_vietnamese.wnry
r.wnry
Jcg4k_
s.wnry
t.wnry
*($:{
taskdl.exe
taskse.exe
lN$D
u.wnry
VS_VERSION_INFO
StringFileInfo
040904B0
CompanyName
Microsoft Corporation
FileDescription
DiskPart
FileVersion
6.1.7601.17514 (win7sp1_rtm.101119-1850)
InternalName
diskpart.exe
LegalCopyright

Microsoft Corporation. All rights reserved.
OriginalFilename
diskpart.exe
ProductName
Microsoft
Windows
Operating System
ProductVersion
6.1.7601.17514
VarFileInfo
Translation
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
<trustInfo xmlns="urn:schemas-microsoft-com:asm.v2">
<security>
<requestedPrivileges>
<requestedExecutionLevel level="asInvoker" />
</requestedPrivileges>
</security>
</trustInfo>
<dependency>
<dependentAssembly>
<assemblyIdentity
type="win32"
name="Microsoft.Windows.Common-Controls"
version="6.0.0.0"
processorArchitecture="*"
publicKeyToken="6595b64144ccf1df"
language="*"
/>
</dependentAssembly>
</dependency>
<compatibility xmlns="urn:schemas-microsoft-com:compatibility.v1">
<application>
<!-- Windows 10 -->
<supportedOS Id="{8e0f7a12-bfb3-4fe8-b9a5-48fd50a15a9a}"/>
<!-- Windows 8.1 -->
<supportedOS Id="{1f676c76-80e1-4239-95bb-83d0f6d0da78}"/>
<!-- Windows Vista -->
<supportedOS Id="{e2011457-1546-43c5-a5fe-008deee3d3f0}"/>
<!-- Windows 7 -->
<supportedOS Id="{35138b9a-5d96-4fbd-8e2d-a2440225f93a}"/>
<!-- Windows 8 -->
<supportedOS Id="{4a2f28e3-53b9-4441-ba9c-d69d4a4a6e38}"/>
</application>
</compatibility>
</assembly>
PPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGX
XPADDINGPADDINGXXPADDING
VS_VERSION_INFO
StringFileInfo
040904B0
CompanyName
Microsoft Corporation
FileDescription
Microsoft
Disk Defragmenter
FileVersion
6.1.7601.17514 (win7sp1_rtm.101119-1850)

```
InternalName
lhdfrgui.exe
LegalCopyright
 Microsoft Corporation. All rights reserved.
OriginalFilename
lhdfrgui.exe
ProductName
Microsoft
 Windows
 Operating System
ProductVersion
6.1.7601.17514
VarFileInfo
Translation
```

From our PE string search we see that there are more files inside of the wcry.exe file. We can unpack those, but first let's continue with wcry.exe and see what else we can learn.

Analyze the Win 32 PE (portable executable)

```
remnux@remnux:~/Desktop$ readpe --imports  wcry.exe

Imported functions

KERNEL32.dll
                        WaitForSingleObject
                        InterlockedIncrement
                        GetCurrentThreadId
                        GetCurrentThread
                        ReadFile
                        GetFileSize
                        CreateFileA
                        MoveFileExA
                        SizeofResource
                        TerminateThread
                        LoadResource
                        FindResourceA
                        GetProcAddress
                        GetModuleHandleW
                        ExitProcess
                        GetModuleFileNameA
                        LocalFree
                        LocalAlloc
                        CloseHandle
                        InterlockedDecrement
                        EnterCriticalSection
                        LeaveCriticalSection
                        InitializeCriticalSection
                        GlobalAlloc
                        GlobalFree
                        QueryPerformanceFrequency
                        QueryPerformanceCounter
                        GetTickCount
                        LockResource
                        Sleep
```

	GetStartupInfoA
	GetModuleHandleA
ADVAPI32.dll	
	StartServiceCtrlDispatcherA
	RegisterServiceCtrlHandlerA
	ChangeServiceConfig2A
	SetServiceStatus
	OpenSCManagerA
	CreateServiceA
	CloseServiceHandle
	StartServiceA
	CryptGenRandom
	CryptAcquireContextA
	OpenServiceA
WS2_32.dll	
	3
	16
	19
	8
	14
	115
	12
	10
	18
	9
	23
	4
	11
MSVCP60.dll	
	??1_Lockit@std@@QAE@XZ
	??0_Lockit@std@@QAE@XZ
iphlpapi.dll	
	GetAdaptersInfo
	GetPerAdapterInfo
WININET.dll	
	InternetOpenA
	InternetOpenUrlA
	InternetCloseHandle
MSVCRT.dll	
	__set_app_type
	_stricmp
	__p__fmode
	__p__commode
	_except_handler3
	__setusermatherr
	_initterm
	__getmainargs
	_acmdln
	_adjust_fdiv
	_controlfp
	exit
	_XcptFilter

```
_exit
_onexit
__dllonexit
free
??2@YAPAXI@Z
_ftol
sprintf
_endthreadex
strncpy
rand
_beginthreadex
__CxxFrameHandler
srand
time
__p___argc
```

We can extract the files we saw from the strings search earlier by using the foremost tool in Remnux.
It extracts files and adds them to a folder called “output” by default.

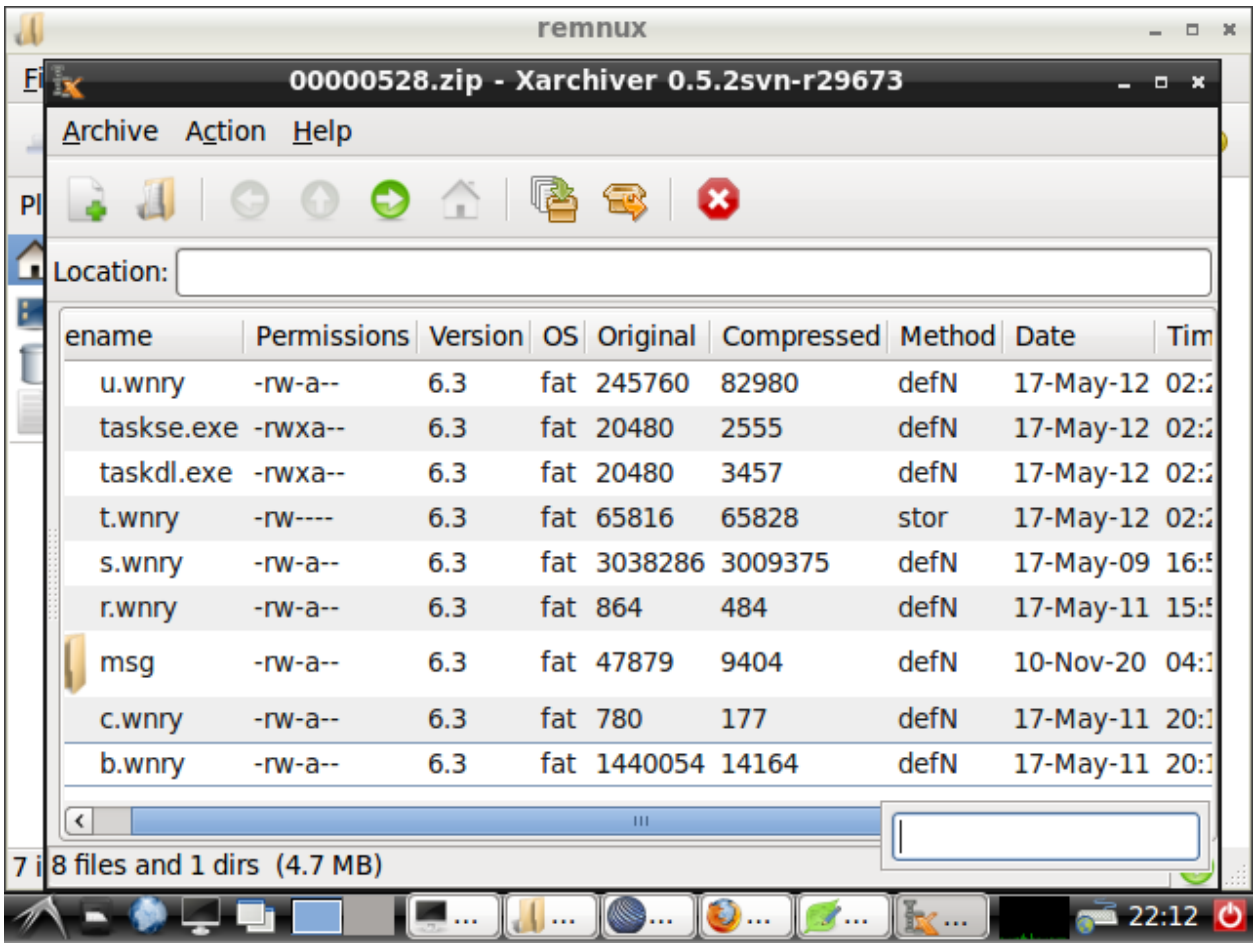
```
remnux@remnux:~/Desktop$ foremost  wcry.exe
Foremost started at Sun Aug  6 22:05:15 2017
Invocation: foremost wcry.exe
Output directory: /home/remnux/Desktop/output
Configuration file: /etc/foremost.conf
------------------------------------------------------------------
File: wcry.exe
Start: Sun Aug  6 22:05:15 2017
Length: 3 MB (3723264 bytes)

Num      Name (bs=512)          Size      File Offset         Comment

0:       00000528.zip           3 MB            270740
1:       00000000.exe           3 MB            0          11/20/2010 09:03:08
Finish: Sun Aug  6 22:05:15 2017

2 FILES EXTRACTED

zip:= 1
exe:= 1
------------------------------------------------------------------
```



Notice that again there are executables that we can dig deeper into.