University of Texas at San Antonio

Lab Report 4

Vincent Cruz (hza026)

IS 3523-003

Juan Munoz

December 3, 2022

Table of Contents

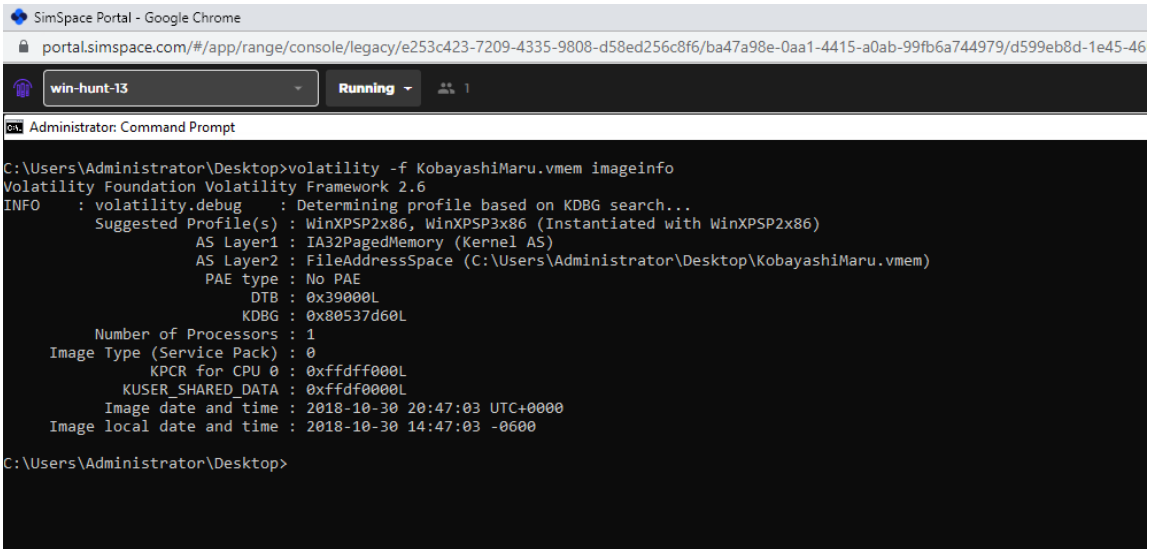
Introduction

When investigating an image of a compromised disk, most of the story can be interpreted by looking through its memory. To do this, volatility was used to gain information about the image and what processes were found running on it. The tough part is combing through all the information and creating a clear story. After interpreting the data, and what processes were running, I will be able to tell if there was any malware executed on this machine.

Findings

1. In order to find out which operating system is on the image, the command imageinfo was called to gain some knowledge about the file. Under suggested profiles, you can see the operating system is Windows XP SP2. Just as in the case of many other compromises, this computer is using an outdated software. In Image 1, you can see the table created by imageinfo.

Image 1



2. Finding out how much RAM was included in the analysis was fairly easy. All that was needed was to navigate to the directory in which the KobayashiMaru file is in using the dir command and look at how many bytes are contained in the file. In this case, 536 megabytes were contained in the memory image. Since memory is the main mode of storage, we can tell those 536 megabytes were in its RAM. The screenshot image 2 shows the command and the information given about the vmem file.

Image 2

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19042.631]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd Desktop

C:\Users\Administrator\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 2A08-91BB

 Directory of C:\Users\Administrator\Desktop

12/01/2022  04:41 PM    <DIR>          .
12/01/2022  04:41 PM    <DIR>          ..
08/11/2021  10:38 AM             2,161 Brim.lnk
12/11/2020  06:50 PM             1,328 FLARE.lnk
11/14/2022  08:58 PM    <DIR>          FTPmemoryfile
02/11/2021  04:10 PM             2,278 Google Chrome.lnk
12/01/2022  04:32 PM    <DIR>          IPE_work
11/15/2022  04:40 PM       536,870,912 KobayashiMaru.vmem
09/07/2020  01:33 PM    <DIR>          NetworkMiner_2-6
11/17/2022  05:21 PM               767 OneDrive - Shortcut.lnk
12/12/2020  10:38 AM    <DIR>          PS_Transcripts
12/11/2020  07:02 PM             1,613 README.txt
10/18/2021  01:41 PM    <DIR>          Snort
09/17/2022  11:46 AM    <DIR>          Test
               6 File(s)    536,879,059 bytes
               8 Dir(s)  273,965,617,152 bytes free

C:\Users\Administrator\Desktop>volatility -f KobayashiMaru.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:\Users\Administrator\Desktop\KobayashiMaru.vmem)
                      PAE type : No PAE
```

3. In order to gain insight on what processes were running it the time of the disk image's creation, I used command pslist with the table shown in image 3. There were definitely unusual processes running on this machine. For example, cryptcat with PID 1472, poisonivy with PID 480, iroffer with PIDs 1692 1728 and 1824, hxdef100 with PID 1416, bircd with PID 1480, cmd with PID 560, netcat with PID 532, and soffice with PID 516. Cryptcat, netcat, and iroffer are known vulnerabilities for allowing hackers to write to your computer and create backdoors. Poisonivy is a known remote access toolkit. Hxdef100 allows for trojan horse vulnerabilities. Bircd is a third-party application. Command prompt running could mean an outside user was executing code. Soffice's PPID could not be found in the table.

Image 3

```
Administrator: Command Prompt
0x81fcc800 System                    4      0     54      275 ------      0
0x81f07da8 smss.exe                336      4      3       21 ------      0 2018-10-30 20:46:44 UTC+0000
0x81d2b020 csrss.exe               664    336     12      453      0      0 2018-10-30 20:46:45 UTC+0000
0x81dc4020 winlogon.exe            688    336     25      486      0      0 2018-10-30 20:46:45 UTC+0000
0x819efda8 services.exe            732    688     18      390      0      0 2018-10-30 20:46:45 UTC+0000
0x81b98da8 lsass.exe               744    688     25      339      0      0 2018-10-30 20:46:45 UTC+0000
0x81e92418 vmacthlp.exe            888    732      1       27      0      0 2018-10-30 20:46:45 UTC+0000
0x819edda8 svchost.exe             916    732      9      252      0      0 2018-10-30 20:46:45 UTC+0000
0x81ee5500 svchost.exe             960    732     70      875      0      0 2018-10-30 20:46:45 UTC+0000
0x81d976c8 svchost.exe            1028    732      5       72      0      0 2018-10-30 20:46:45 UTC+0000
0x81e07da8 svchost.exe            1108    732     12      142      0      0 2018-10-30 20:46:46 UTC+0000
0x81e536a0 spoolsv.exe            1308    732     15      189      0      0 2018-10-30 20:46:46 UTC+0000
0x81db4298 hxdef100.exe           1416    732      2       31      0      0 2018-10-30 20:46:46 UTC+0000
0x81d626a0 inetinfo.exe           1432    732     34      540      0      0 2018-10-30 20:46:46 UTC+0000
0x819e2c20 jqs.exe                1464    732      7      214      0      0 2018-10-30 20:46:47 UTC+0000
0x81ede980 cryptcat.exe           1472   1416      1       62      0      0 2018-10-30 20:46:47 UTC+0000
0x81cada80 bircd.exe              1480   1416      2       45      0      0 2018-10-30 20:46:47 UTC+0000
0x81c71508 VMwareService.e        1624    732      2      119      0      0 2018-10-30 20:46:47 UTC+0000
0x81e8f9c0 iroffer.exe            1692   1488      0 --------      0      0 2018-10-30 20:46:47 UTC+0000   2018-10-30 20:46:47 UTC+0000
0x81c85420 iroffer.exe            1728   1692      5       92      0      0 2018-10-30 20:46:47 UTC+0000
0x81df6b20 iroffer.exe            1824   1728      0 --------      0      0 2018-10-30 20:46:47 UTC+0000   2018-10-30 20:46:36 UTC+0000
0x81d32988 wmiapsrv.exe            216    732      5      121      0      0 2018-10-30 20:46:36 UTC+0000
0x819e83c8 wmiprvse.exe            252    916      7      107      0      0 2018-10-30 20:46:37 UTC+0000
0x81edfc18 userinit.exe            368    688      2       34      0      0 2018-10-30 20:46:38 UTC+0000
0x81a3bc18 explorer.exe            404    368     15      252      0      0 2018-10-30 20:46:38 UTC+0000
0x81d28790 VMwareTray.exe          456    404      1       30      0      0 2018-10-30 20:46:38 UTC+0000
0x81bb3da8 VMwareUser.exe          464    404      5      146      0      0 2018-10-30 20:46:38 UTC+0000
0x81aaa708 jusched.exe             472    404      1       24      0      0 2018-10-30 20:46:38 UTC+0000
0x81e234e8 poisonivy.exe           480    404      1       20      0      0 2018-10-30 20:46:38 UTC+0000
0x81cacda8 msmsgs.exe              488    404      4      127      0      0 2018-10-30 20:46:39 UTC+0000
0x81e579f8 soffice.exe             516    496      1       20      0      0 2018-10-30 20:46:39 UTC+0000
0x81ec6848 soffice.bin             524    516      7      164      0      0 2018-10-30 20:46:39 UTC+0000
0x81c6f7b8 nc.exe                  532    508      1       62      0      0 2018-10-30 20:46:39 UTC+0000
0x81eb3020 winvnc4.exe             548    508      2       81      0      0 2018-10-30 20:46:39 UTC+0000
0x81a2eb78 cmd.exe                 560    508      1       20      0      0 2018-10-30 20:46:39 UTC+0000
Type here to search
```

In order to dive deeper, I executed the command malfind to scan the processes for malware. To no surprise, poisonivy returned with hacker defender as seen in image 4. The same was returned for netcat in image 5, cmd in image 6, and soffice in image 7.

Image 4

```
Administrator: Command Prompt
C:\Users\Administrator\Desktop>volatility -f KobayashiMaru.vmem --profile=WinXPSP2x86 malfind -p 480
Volatility Foundation Volatility Framework 2.6
Process: poisonivy.exe Pid: 480 Address: 0x7ffa0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 5, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x7ffa0000  e8 00 00 00 00 58 2d be 5d 40 00 c3 5f 2e 2d 3d   .....X-.]@.._.-=
0x7ffa0010  5b 48 61 63 6b 65 72 20 44 65 66 65 6e 64 65 72   [Hacker.Defender
0x7ffa0020  5d 3d 2d 2e 5f 00 00 00 00 00 00 00 00 04 00 00   ]=-._...........
0x7ffa0030  00 6b 65 72 6e 65 6c 33 32 2e 64 6c 6c 00 53 65   .kernel32.dll.Se

0x7ffa0000 e800000000       CALL 0x7ffa0005
0x7ffa0005 58               POP EAX
0x7ffa0006 2dbe5d4000       SUB EAX, 0x405dbe
0x7ffa000b c3               RET
0x7ffa000c 5f               POP EDI
0x7ffa000d 2e2d3d5b4861     SUB EAX, 0x61485b3d
0x7ffa0013 636b65           ARPL [EBX+0x65], BP
0x7ffa0016 7220             JB 0x7ffa0038
0x7ffa0018 44               INC ESP
0x7ffa0019 6566656e         OUTS DX, BYTE [GS:ESI]
0x7ffa001d 6465725d         JB 0x7ffa007e
0x7ffa0021 3d2d2e5f00       CMP EAX, 0x5f2e2d
0x7ffa0026 0000             ADD [EAX], AL
0x7ffa0028 0000             ADD [EAX], AL
0x7ffa002a 0000             ADD [EAX], AL
0x7ffa002c 000400           ADD [EAX+EAX], AL
0x7ffa002f 0000             ADD [EAX], AL
0x7ffa0031 6b65726e         IMUL ESP, [EBP+0x72], 0x6e
0x7ffa0035 656c             INS BYTE [ES:EDI], DX
0x7ffa0037 3332             XOR ESI, [EDX]
0x7ffa0039 2e646c           INS BYTE [ES:EDI], DX
0x7ffa003c 6c               INS BYTE [ES:EDI], DX
0x7ffa003d 005365           ADD [EBX+0x65], DL
```

image 5

```
Administrator: Command Prompt
C:\Users\Administrator\Desktop>volatility -f KobayashiMaru.vmem --profile=WinXPSP2x86 malfind -p 532
Volatility Foundation Volatility Framework 2.6
Process: nc.exe Pid: 532 Address: 0x7ffa0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 5, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x7ffa0000  e8 00 00 00 00 58 2d be 5d 40 00 c3 5f 2e 2d 3d   .....X-.]@.._.-=
0x7ffa0010  5b 48 61 63 6b 65 72 20 44 65 66 65 6e 64 65 72   [Hacker.Defender
0x7ffa0020  5d 3d 2d 2e 5f 00 00 00 00 00 00 00 00 04 00 00   ]=-._...........
0x7ffa0030  00 6b 65 72 6e 65 6c 33 32 2e 64 6c 6c 00 53 65   .kernel32.dll.Se

0x7ffa0000 e800000000       CALL 0x7ffa0005
0x7ffa0005 58               POP EAX
0x7ffa0006 2dbe5d4000       SUB EAX, 0x405dbe
0x7ffa000b c3               RET
0x7ffa000c 5f               POP EDI
0x7ffa000d 2e2d3d5b4861     SUB EAX, 0x61485b3d
0x7ffa0013 636b65           ARPL [EBX+0x65], BP
0x7ffa0016 7220             JB 0x7ffa0038
0x7ffa0018 44               INC ESP
0x7ffa0019 6566656e         OUTS DX, BYTE [GS:ESI]
0x7ffa001d 6465725d         JB 0x7ffa007e
0x7ffa0021 3d2d2e5f00       CMP EAX, 0x5f2e2d
0x7ffa0026 0000             ADD [EAX], AL
0x7ffa0028 0000             ADD [EAX], AL
0x7ffa002a 0000             ADD [EAX], AL
0x7ffa002c 000400           ADD [EAX+EAX], AL
0x7ffa002f 0000             ADD [EAX], AL
0x7ffa0031 6b65726e         IMUL ESP, [EBP+0x72], 0x6e
0x7ffa0035 656c             INS BYTE [ES:EDI], DX
0x7ffa0037 3332             XOR ESI, [EDX]
0x7ffa0039 2e646c           INS BYTE [ES:EDI], DX
0x7ffa003c 6c               INS BYTE [ES:EDI], DX
0x7ffa003d 005365           ADD [EBX+0x65], DL
```

Image 6

```
Administrator: Command Prompt

C:\Users\Administrator\Desktop>volatility -f KobayashiMaru.vmem --profile=WinXPSP2x86 malfind -p 560
Volatility Foundation Volatility Framework 2.6
Process: cmd.exe Pid: 560 Address: 0x7ffa0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 5, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x7ffa0000  e8 00 00 00 00 58 2d be 5d 40 00 c3 5f 2e 2d 3d   .....X-.]@.._.-=
0x7ffa0010  5b 48 61 63 6b 65 72 20 44 65 66 65 6e 64 65 72   [Hacker.Defender
0x7ffa0020  5d 3d 2d 2e 5f 00 00 00 00 00 00 00 00 04 00 00   ]=-._..........
0x7ffa0030  00 6b 65 72 6e 65 6c 33 32 2e 64 6c 6c 00 53 65   .kernel32.dll.Se

0x7ffa0000 e800000000       CALL 0x7ffa0005
0x7ffa0005 58               POP EAX
0x7ffa0006 2dbe5d4000       SUB EAX, 0x405dbe
0x7ffa000b c3               RET
0x7ffa000c 5f               POP EDI
0x7ffa000d 2e2d3d5b4861     SUB EAX, 0x61485b3d
0x7ffa0013 636b65           ARPL [EBX+0x65], BP
0x7ffa0016 7220             JB 0x7ffa0038
0x7ffa0018 44               INC ESP
0x7ffa0019 6566656e         OUTS DX, BYTE [GS:ESI]
0x7ffa001d 6465725d         JB 0x7ffa007e
0x7ffa0021 3d2d2e5f00       CMP EAX, 0x5f2e2d
0x7ffa0026 0000             ADD [EAX], AL
0x7ffa0028 0000             ADD [EAX], AL
0x7ffa002a 0000             ADD [EAX], AL
0x7ffa002c 000400           ADD [EAX+EAX], AL
0x7ffa002f 0000             ADD [EAX], AL
0x7ffa0031 6b65726e         IMUL ESP, [EBP+0x72], 0x6e
0x7ffa0035 656c             INS BYTE [ES:EDI], DX
0x7ffa0037 3332             XOR ESI, [EDX]
0x7ffa0039 2e646c           INS BYTE [ES:EDI], DX
0x7ffa003c 6c               INS BYTE [ES:EDI], DX
0x7ffa003d 005365           ADD [EBX+0x65], DL
```

Image 7

```
Administrator: Command Prompt

C:\Users\Administrator\Desktop>volatility -f KobayashiMaru.vmem --profile=WinXPSP2x86 malfind -p 516
Volatility Foundation Volatility Framework 2.6
Process: soffice.exe Pid: 516 Address: 0x7ffa0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 5, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x7ffa0000  e8 00 00 00 00 58 2d be 5d 40 00 c3 5f 2e 2d 3d   .....X-.]@.._.-=
0x7ffa0010  5b 48 61 63 6b 65 72 20 44 65 66 65 6e 64 65 72   [Hacker.Defender
0x7ffa0020  5d 3d 2d 2e 5f 00 00 00 00 00 00 00 00 04 00 00   ]=-._..........
0x7ffa0030  00 6b 65 72 6e 65 6c 33 32 2e 64 6c 6c 00 53 65   .kernel32.dll.Se

0x7ffa0000 e800000000       CALL 0x7ffa0005
0x7ffa0005 58               POP EAX
0x7ffa0006 2dbe5d4000       SUB EAX, 0x405dbe
0x7ffa000b c3               RET
0x7ffa000c 5f               POP EDI
0x7ffa000d 2e2d3d5b4861     SUB EAX, 0x61485b3d
0x7ffa0013 636b65           ARPL [EBX+0x65], BP
0x7ffa0016 7220             JB 0x7ffa0038
0x7ffa0018 44               INC ESP
0x7ffa0019 6566656e         OUTS DX, BYTE [GS:ESI]
0x7ffa001d 6465725d         JB 0x7ffa007e
0x7ffa0021 3d2d2e5f00       CMP EAX, 0x5f2e2d
0x7ffa0026 0000             ADD [EAX], AL
0x7ffa0028 0000             ADD [EAX], AL
0x7ffa002a 0000             ADD [EAX], AL
0x7ffa002c 000400           ADD [EAX+EAX], AL
0x7ffa002f 0000             ADD [EAX], AL
0x7ffa0031 6b65726e         IMUL ESP, [EBP+0x72], 0x6e
0x7ffa0035 656c             INS BYTE [ES:EDI], DX
0x7ffa0037 3332             XOR ESI, [EDX]
0x7ffa0039 2e646c           INS BYTE [ES:EDI], DX
0x7ffa003c 6c               INS BYTE [ES:EDI], DX
0x7ffa003d 005365           ADD [EBX+0x65], DL
```

4. After trying to find usernames or passwords using the command hashdump, volatility returned an error saying unable to read hashes from registry. This error can be seen in image 8. Though there were not any usernames or passwords to be found on the image, in image 9 using the command handles, poisonivy was in a directory belonging to an account named Daniel Faraday. This can be a key detail in finding out where this malware came from.

Image 8

```
win-hunt-13    Running    1
Administrator: Command Prompt

C:\Users\Administrator\Desktop>volatility -f KobayashiMaru.vmem --profile=WinXPSP2x86 hashdump
Volatility Foundation Volatility Framework 2.6
ERROR   : volatility.debug    : Unable to read hashes from registry

C:\Users\Administrator\Desktop>
```

Image 9

```
SimSpace Portal - Google Chrome
portal.simspace.com/#/app/range/console/legacy/e253c423-7209-4335-9808-d58ed256c8f6/ba47a98e-0aa1-4415-a0ab-99fb6a744979/d599eb8d-1e45-4609-a259-3ab
win-hunt-13    Running    1
Administrator: Command Prompt

C:\Users\Administrator\Desktop>volatility -f KobayashiMaru.vmem --profile=WinXPSP2x86 handles -p 480
Volatility Foundation Volatility Framework 2.6
Offset(V)     Pid     Handle     Access Type             Details
---------- ------ ---------- ---------- --------------- -------
0xe10096e0    480        0x4   0xf0003 KeyedEvent      CritSecOutOfMemoryEvent
0xe17201b8    480        0x8       0x3 Directory       KnownDlls
0x81c7ff90    480        0xc  0x100020 File            \Device\HarddiskVolume1\Documents and Settings\Daniel Faraday
0x81db8d18    480       0x10       0x1 Mutant          NlsCacheMutant
0xe149f478    480       0x14   0xf000f Directory       Windows
0xe114e1c8    480       0x18 0x21f0001 Port
0xe159a2a8    480       0x1c   0xf001f Section
0xe10dd798    480       0x20 0x20f003f Key             MACHINE
0x8193e4c8    480       0x24 0x21f0003 Event
0x81a7e4c0    480       0x28   0xf037f WindowStation   WinSta0
0x81e436d0    480       0x2c   0xf01ff Desktop         Default
0x81a7e4c0    480       0x30   0xf037f WindowStation   WinSta0
0x81c3abd0    480       0x34  0x1f0003 Event
0xe158b7d8    480       0x38   0x2000f Directory       BaseNamedObjects
0x81eaf348    480       0x3c  0x1f0001 Mutant          )!VoqA.I4
0x81a30a08    480       0x40  0x1f03ff Thread          TID 484 PID 480
0xe10b09d8    480       0x44   0xf003f Key             MACHINE\SYSTEM\CONTROLSET001\SERVICES\WINSOCK2\PARAMETERS\PROTOCOL_CATALOG9
0x81c3aba0    480       0x48  0x1f0003 Event
0xe10b0970    480       0x4c   0xf003f Key             MACHINE\SYSTEM\CONTROLSET001\SERVICES\WINSOCK2\PARAMETERS\NAMESPACE_CATALOG5
0x81f35870    480       0x54  0x1f0003 Event

C:\Users\Administrator\Desktop>_
```

5. Upon looking at the dynamically linked libraries using the dlllist command, it is clear this is not a normal box. Several of the suspicious processes can be seen being used to make changes to the box in the following images. Image 10 shows netcat being executed to connect to port 6666, a known method of creating a backdoor. Image 11 shows cryptcat connecting to port 666, known for being used for Doom, but also backdoors and trojans. Image 12 shows poisonivy in the System32 folder and being executed in command line, likely activating the RAT. In image 13, cmd is used to call lock.bat, likely to hide/lock files.

Image 10

```
Administrator: Command Prompt

C:\Users\Administrator\Desktop>volatility -f KobayashiMaru.vmem --profile=WinXPSP2x86 dlllist -p 532
Volatility Foundation Volatility Framework 2.6
************************************************************************
nc.exe pid:    532
Command line : C:\inetpub\ftproot\nc.exe  -L -p 6666 -e cmd.exe


Base             Size  LoadCount Path
---------- ---------- ---------- ----
0x00400000    0x10000     0xffff C:\inetpub\ftproot\nc.exe
0x77f50000    0xa9000     0xffff C:\WINDOWS\System32\ntdll.dll
0x77e60000    0xe5000     0xffff C:\WINDOWS\system32\kernel32.dll
0x71ab0000    0x15000     0xffff C:\WINDOWS\System32\WS2_32.dll
0x77c10000    0x53000     0xffff C:\WINDOWS\system32\msvcrt.dll
0x71aa0000     0x8000     0xffff C:\WINDOWS\System32\WS2HELP.dll
0x77dd0000    0x8b000     0xffff C:\WINDOWS\system32\ADVAPI32.dll
0x77cc0000    0x75000     0xffff C:\WINDOWS\system32\RPCRT4.dll
0x71a50000    0x3b000        0x4 C:\WINDOWS\System32\mswsock.dll
0x76f20000    0x25000        0x3 C:\WINDOWS\System32\DNSAPI.dll
0x76d60000    0x15000        0x3 C:\WINDOWS\System32\iphlpapi.dll
0x76de0000    0x26000        0x1 C:\WINDOWS\System32\netman.dll
0x76d40000    0x16000        0x1 C:\WINDOWS\System32\MPRAPI.dll
0x76e40000    0x2f000        0x1 C:\WINDOWS\System32\ACTIVEDS.dll
0x76e10000    0x24000        0x1 C:\WINDOWS\System32\adsldpc.dll
0x71c20000    0x4f000        0x6 C:\WINDOWS\System32\NETAPI32.dll
0x76f60000    0x2c000        0x2 C:\WINDOWS\system32\WLDAP32.dll
0x77d40000    0x8d000       0x28 C:\WINDOWS\system32\USER32.dll
0x77c70000    0x40000       0x16 C:\WINDOWS\system32\GDI32.dll
0x76b20000    0x15000        0x1 C:\WINDOWS\System32\ATL.DLL
0x771b0000   0x11a000        0x7 C:\WINDOWS\system32\ole32.dll
0x77120000    0x8b000        0x4 C:\WINDOWS\system32\OLEAUT32.dll
0x76e80000     0xd000        0x4 C:\WINDOWS\System32\rtutils.dll
0x71bf0000    0x11000        0x1 C:\WINDOWS\System32\SAMLIB.dll
0x76670000    0xe4000        0x1 C:\WINDOWS\System32\SETUPAPI.dll
```

Image 11

```
Administrator: Command Prompt
0x5aaf0000     0x5000        0x1 C:\WINDOWS\system32\w3ctrs.dll
0x59990000    0x18000        0x1 C:\WINDOWS\System32\wbem\wmiaprpl.dll
0x72f60000    0x1a000        0x1 C:\WINDOWS\system32\loadperf.dll
0x75290000    0x38000        0x1 C:\WINDOWS\System32\wbem\wbemcomn.dll
**************************************************************************
cryptcat.exe pid:   1472
Command line : "C:\hxdefrootkit\cryptcat.exe" -L -p 666 -e cmd.exe


Base             Size  LoadCount Path
---------- ---------- ---------- ----
0x00400000    0x18000     0xffff C:\hxdefrootkit\cryptcat.exe
0x77f50000    0xa9000     0xffff C:\WINDOWS\System32\ntdll.dll
0x77e60000    0xe5000     0xffff C:\WINDOWS\system32\kernel32.dll
0x71ab0000    0x15000     0xffff C:\WINDOWS\system32\WS2_32.dll
0x77c10000    0x53000     0xffff C:\WINDOWS\system32\msvcrt.dll
0x71aa0000     0x8000     0xffff C:\WINDOWS\system32\WS2HELP.dll
0x77dd0000    0x8b000     0xffff C:\WINDOWS\system32\ADVAPI32.dll
0x77cc0000    0x75000     0xffff C:\WINDOWS\system32\RPCRT4.dll
0x71a50000    0x3b000        0x4 C:\WINDOWS\System32\mswsock.dll
0x76f20000    0x25000        0x3 C:\WINDOWS\system32\DNSAPI.dll
0x76d60000    0x15000        0x3 C:\WINDOWS\system32\iphlpapi.dll
0x76de0000    0x26000        0x1 C:\WINDOWS\system32\netman.dll
0x76d40000    0x16000        0x1 C:\WINDOWS\system32\MPRAPI.dll
0x76e40000    0x2f000        0x1 C:\WINDOWS\system32\ACTIVEDS.dll
0x76e10000    0x24000        0x1 C:\WINDOWS\system32\adsldpc.dll
0x71c20000    0x4f000        0x6 C:\WINDOWS\system32\NETAPI32.dll
0x76f60000    0x2c000        0x2 C:\WINDOWS\system32\WLDAP32.dll
0x77d40000    0x8d000       0x28 C:\WINDOWS\system32\USER32.dll
0x77c70000    0x40000       0x16 C:\WINDOWS\system32\GDI32.dll
0x76b20000    0x15000        0x1 C:\WINDOWS\system32\ATL.DLL
0x771b0000   0x11a000        0x7 C:\WINDOWS\system32\ole32.dll
0x77120000    0x8b000        0x4 C:\WINDOWS\system32\OLEAUT32.dll
0x76e80000     0xd000        0x4 C:\WINDOWS\system32\rtutils.dll
0x71bf0000    0x11000        0x1 C:\WINDOWS\system32\SAMLIB.dll
```

Image 12

```
Administrator: Command Prompt
42c6d552127e548b11644fc14fdf99c7 *executable.480.exe

C:\Users\Administrator\Desktop>volatility -f KobayashiMaru.vmem --profile=WinXPSP2x86 dlllist -p 480
Volatility Foundation Volatility Framework 2.6
************************************************************************
poisonivy.exe pid:    480
Command line : "C:\WINDOWS\System32\poisonivy.exe"


Base             Size  LoadCount Path
---------- ---------- ---------- ----
0x00400000     0x1c00     0xffff C:\WINDOWS\System32\poisonivy.exe
0x77f50000    0xa9000     0xffff C:\WINDOWS\System32\ntdll.dll
0x77e60000    0xe5000     0xffff C:\WINDOWS\system32\kernel32.dll
0x77dd0000    0x8b000       0x1a C:\WINDOWS\system32\advapi32.dll
0x77cc0000    0x75000        0xb C:\WINDOWS\system32\RPCRT4.dll
0x77d40000    0x8d000        0x5 C:\WINDOWS\system32\user32.dll
0x77c70000    0x40000        0x4 C:\WINDOWS\system32\GDI32.dll
0x75260000    0x27000        0x1 C:\WINDOWS\System32\advpack.dll
0x771b0000   0x11a000        0x1 C:\WINDOWS\system32\ole32.dll
0x77c00000     0x7000        0x1 C:\WINDOWS\system32\VERSION.dll
0x71ab0000    0x15000        0x5 C:\WINDOWS\System32\ws2_32.dll
0x77c10000    0x53000        0x8 C:\WINDOWS\system32\msvcrt.dll
0x71aa0000     0x8000        0x7 C:\WINDOWS\System32\WS2HELP.dll
0x71a50000    0x3b000        0x2 C:\WINDOWS\system32\mswsock.dll
0x71a90000     0x8000        0x1 C:\WINDOWS\System32\wshtcpip.dll
0x76fc0000     0x5000        0x1 C:\WINDOWS\System32\rasadhlp.dll
```

Image 13

```
Administrator: Command Prompt

C:\Users\Administrator\Desktop>volatility -f KobayashiMaru.vmem --profile=WinXPSP2x86 dlllist -p 560
Volatility Foundation Volatility Framework 2.6
************************************************************************
cmd.exe pid:    560
Command line : C:\WINDOWS\system32\cmd.exe  /K C:\Inetpub\ftproot\lock.bat


Base             Size  LoadCount Path
---------- ---------- ---------- ----
0x4ad00000    0x5e000     0xffff C:\WINDOWS\system32\cmd.exe
0x77f50000    0xa9000     0xffff C:\WINDOWS\System32\ntdll.dll
0x77e60000    0xe5000     0xffff C:\WINDOWS\system32\kernel32.dll
0x77c10000    0x53000     0xffff C:\WINDOWS\system32\msvcrt.dll
0x77d40000    0x8d000     0xffff C:\WINDOWS\system32\USER32.dll
0x77c70000    0x40000     0xffff C:\WINDOWS\system32\GDI32.dll
0x77dd0000    0x8b000     0xffff C:\WINDOWS\system32\ADVAPI32.dll
0x77cc0000    0x75000     0xffff C:\WINDOWS\system32\RPCRT4.dll

C:\Users\Administrator\Desktop>_
```

6. Both netcat and cryptcat can be seen running cmd, therefore what was executed from cmd can be linked back to those processes. Also, using the command connscan, poisonivy can be seen connecting to a remote computer in image 14, illustrating this really is being used as a RAT.

Image 14

```
win-hunt-13    Running    1
Administrator: Command Prompt
0x81d40418 rundll32.exe            984    404      1       81      0      0 2018-10-30 20:46:43 UTC+0000

C:\Users\Administrator\Desktop>volatility -f KobayashiMaru.vmem --profile=WinXPSP2x86 connscan
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x01e76368 127.0.0.1:1031            127.0.0.1:6667            1728
0x021935e8 127.0.0.1:6667            127.0.0.1:1031            1480
0x021fd550 0.0.0.0:1037              192.168.5.98:3460         480

C:\Users\Administrator\Desktop>
```

7. It is worth noting that some of the files linked to the suspicious processes are in different directories than they usually are. According to windowsbulletin.com, bircd.exe should be in program files. However, in image 15 it is seen stored in a hidden folder. The same can be said for iroffer. In image 16 you can see the directory is to the hidden folder. In image 11 you can see cryptcat.exe is stored in a folder titled hxdefrootkit, making it very plain that it was meant to be used in a malicious fashion.

Image 15

```
Administrator: Command Prompt

C:\Users\Administrator\Desktop>volatility -f KobayashiMaru.vmem --profile=WinXPSP2x86 dlllist -p 1480
Volatility Foundation Volatility Framework 2.6
************************************************************************
bircd.exe pid:   1480
Command line : "C:\hidden\bewareircd-win32\bircd.exe"


Base             Size  LoadCount Path
---------- ---------- ---------- ----
0x00400000    0x95000     0xffff C:\hidden\bewareircd-win32\bircd.exe
0x77f50000    0xa9000     0xffff C:\WINDOWS\System32\ntdll.dll
0x77e60000    0xe5000     0xffff C:\WINDOWS\system32\kernel32.dll
0x77dd0000    0x8b000     0xffff C:\WINDOWS\system32\advapi32.dll
0x77cc0000    0x75000     0xffff C:\WINDOWS\system32\RPCRT4.dll
0x77120000    0x8b000     0xffff C:\WINDOWS\system32\oleaut32.dll
0x77c10000    0x53000     0xffff C:\WINDOWS\system32\MSVCRT.DLL
0x771b0000   0x11a000     0xffff C:\WINDOWS\system32\OLE32.DLL
0x77c70000    0x40000     0xffff C:\WINDOWS\system32\GDI32.dll
0x77d40000    0x8d000     0xffff C:\WINDOWS\system32\USER32.dll
0x76b40000    0x2c000     0xffff C:\WINDOWS\system32\winmm.dll
0x71ad0000     0x8000     0xffff C:\WINDOWS\system32\wsock32.dll
0x71ab0000    0x15000     0xffff C:\WINDOWS\system32\WS2_32.dll
0x71aa0000     0x8000     0xffff C:\WINDOWS\system32\WS2HELP.dll
0x5ad70000    0x34000        0x2 C:\WINDOWS\system32\uxtheme.dll
0x71a50000    0x3b000        0x3 C:\WINDOWS\system32\mswsock.dll
0x71a90000     0x8000        0x1 C:\WINDOWS\System32\wshtcpip.dll
```

Image 16

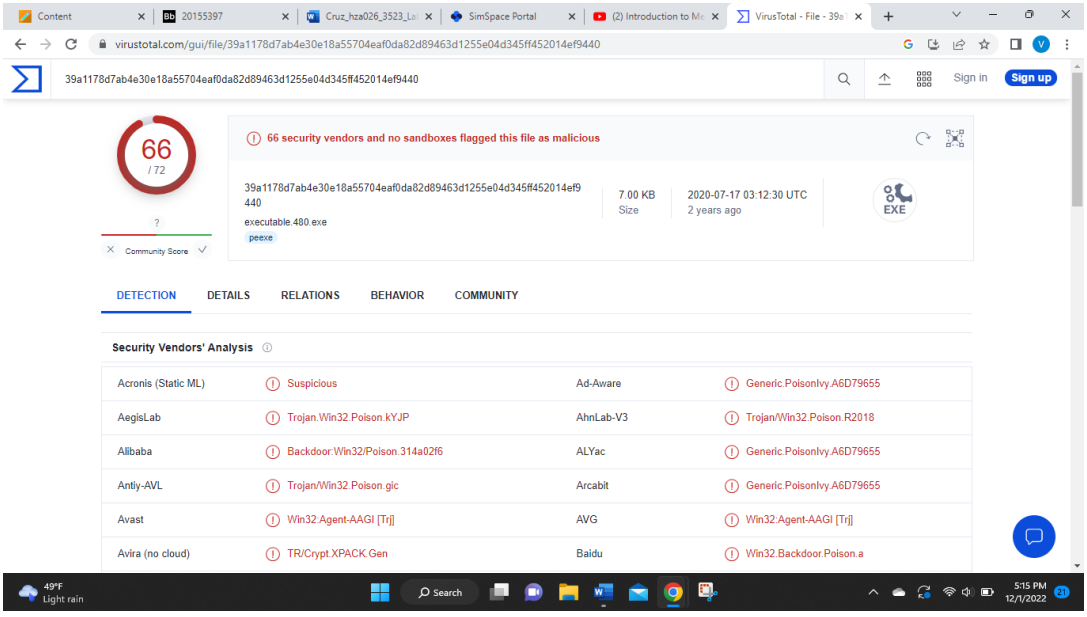
Administrator: Command Prompt

```
C:\Users\Administrator\Desktop>volatility -f KobayashiMaru.vmem --profile=WinXPSP2x86 dlllist -p 1728
Volatility Foundation Volatility Framework 2.6
************************************************************************
iroffer.exe pid:   1728
Command line : C:\hidden\ir\iroffer.exe


Base             Size  LoadCount Path
---------- ---------- ---------- ----
0x00400000    0x39000     0xffff C:\hidden\ir\iroffer.exe
0x77f50000    0xa9000     0xffff C:\WINDOWS\System32\ntdll.dll
0x77e60000    0xe5000     0xffff C:\WINDOWS\system32\kernel32.dll
0x10000000     0x7000     0xffff C:\hidden\ir\cygcrypt-0.dll
0x61000000   0x259000     0xffff C:\hidden\ir\cygwin1.dll
0x77dd0000    0x8b000     0xffff C:\WINDOWS\system32\ADVAPI32.DLL
0x77cc0000    0x75000     0xffff C:\WINDOWS\system32\RPCRT4.dll
0x71ad0000     0x8000        0x1 C:\WINDOWS\system32\wsock32.dll
0x71ab0000    0x15000       0x12 C:\WINDOWS\system32\WS2_32.dll
0x77c10000    0x53000       0x15 C:\WINDOWS\system32\msvcrt.dll
0x71aa0000     0x8000       0x15 C:\WINDOWS\system32\WS2HELP.dll
0x71a50000    0x3b000        0x3 C:\WINDOWS\system32\mswsock.dll
0x71a90000     0x8000        0x1 C:\WINDOWS\System32\wshtcpip.dll
0x76b40000    0x2c000        0x1 C:\WINDOWS\system32\winmm.dll
0x77d40000    0x8d000        0x2 C:\WINDOWS\system32\USER32.dll
0x77c70000    0x40000        0x2 C:\WINDOWS\system32\GDI32.dll
```

8. To form a conclusion from the analysis, this computer was obviously compromised with malware. Once again, Daniel Faraday's account fell victim to the poisonivy RAT. The malware was likely loaded onto the computer by the hacker after gaining access via netcat. By looking at the process list, hxdef100 then opened up for the other processes like cryptcat, iroffer, and bircd. Once this was accomplished, the hacker had free reign over Daniel's files and his computer's resources. To verify poisonivy actually contained malware, I uploaded a hash to Virus Total to reference other sources. The results can be seen in image 17.

Image 17



Works Cited

Hart, Phil, "What is bircd.exe? Is it Safe or a Virus? How to remove or fix it", https://windowsbulletin.com/files/exe/windows-software-developer/third-party-application/bircd-exe

"iroffer.exe", https://www.processlibrary.com/en/directory/files/iroffer/23813/.

"Port 666 details", https://www.speedguide.net/port.php?port=666#:~:text=Port%20666%20Details&text=Doom%20game%20(ID%20Software)%20uses,by%20numerous%20trojan%20horses%2Fbackdoors.

Spruell, Darren, "PoisonIvy", https://attack.mitre.org/software/S0012/. 31 May 2017.

VirusTotal, https://www.virustotal.com/gui/file/39a1178d7ab4e30e18a55704eaf0da82d89463d1255e04d345ff452014ef9440