The University of Texas at San Antonio™

ISCS 3523-003 Intrusion Detection and Incident Response

Lab #03 Hunting in Memory
The SimSpace Cyber Range

Student:

Dillen Dela Cruz, odv464

Prepared for Intrusion Detection and Incident Response
02/30/2024
Professor: Shawn Zumwalt

Contents

To access the volatility tool for analyzing the Kobayashi file, I initially launched the Volatility application, which opened a command prompt in the desktop directory of the admin user account. To navigate to the specific directory containing the file I need to examine, which is located on the Administrator's desktop, I simply dragged and dropped the file into the command prompt. Then, I removed the file name and used the "cd" command to change the directory accordingly (figure 1). With this setup, I am now prepared to execute volatility commands on the file. Throughout the lab, I'll follow a specific command format, "volatility -f <filename> <volatility command>". The "-f" flag in the command indicates that I intend to analyze a file. Leaving out the "-f" flag will result in a "volatility.debug" error, which will ask you to specify either a location ("-l") or a filename ("-f") (figure 2).

To start my investigation, I utilized the **"imageinfo"** command to find out the operating system utilized by the victim. The output revealed that the victim's system was running both Windows XP SP2 and SP3, operating on the x86 (32-bit) architecture (figure 3). In the world of Windows operating systems, "SP" stands for "Service Pack," which encompasses a collection of updates, fixes, and enhancements distributed by Microsoft. These service packs are periodically released to address known issues, enhance system stability, and introduce new features (Fisher). The output **"winxpsp3x86 (instantiated with winxps2x86)"** implies that although the system is recognized as Windows XP SP3 (Service Pack 3), it is being managed as if it were a Windows XP SP2 system to ensure compatibility. Essentially, Volatility could be treating it as if it were a SP2 system for analysis purposes. In addition to the start of examination, examining the file properties on the Windows machine (as shown in figure 4), it's evident that the RAM included in the analysis amounts to either 536,870,912 bytes or 512 megabytes (MB).

I began by executing the "pslist" command to display all currently running processes. Upon reviewing the output, several suspicious programs caught my attention. These include "hxdef100.exe", "posionivy.exe", "iroffer.exe", "bircd.exe", "cryptcat.exe", "nc.exe", and "winvnc4.exe" (see figure 5). In a previous laboratory exercise, it was established that "posionivy.exe" is a form of malware that should not be present in the system32 directory or actively running, as it is associated with other malicious software such as Breut and Darkmoon, as documented by MITRE. Furthermore, "hxdef100.exe" is identified as a rootkit capable of granting full control to hackers once installed and executed on the targeted system, evading detection even by system administrators. This rootkit provides a range of customizable features, enabling users to conceal critical information such as file keys, process details, system services, drivers, registry keys, open ports, and create a false impression of available disk space (Alibaba Cloud). Similar to "hxdef100.exe", "iroffer.exe" presents a backdoor vulnerability and may be deployed by attackers for malicious purposes, enabling unauthorized access to the compromised computer and potential theft of sensitive information, including passwords and personal data (Process Library). Multiple instances of "iroffer.exe" could indicate attempts by malware to propagate throughout the system, launch attacks on other systems, or exfiltrate data. "bircd.exe", also recognized as "beware ircd", functions as an IRC server for both Windows and Linux systems, facilitating communication with clients via open ports. Moving on to "nc.exe" and "cryptcat.exe", these programs are renowned network tools used for establishing communication channels between hosts. While essential for forensic investigations, enabling reliable TCP connections to bridge between the target system and the forensic workstation, they also possess encryption capabilities to ensure data confidentiality. However, if exploited maliciously, these tools can facilitate various harmful activities, such as establishing covert communication channels for data exfiltration or remote access to compromised systems. Lastly, "winvnc4.exe" denotes a VNC (Virtual Network Computing) server, enabling remote access and control of a computer's desktop or graphical user interface (GUI) over a network connection. Similar to the networking tools mentioned earlier, VNC also opens ports for communication. Notably, the remaining processes observed during the analysis appeared legitimate, either serving specific program functionalities or contributing to the Windows system, with file locations aligning with expected norms based on external research.

When examining the file locations of the running processes, I utilized the "dlllist" tool, which not only enumerates all active DLLs in memory but also provides their corresponding file paths. Among the suspicious processes, "hxddef100.exe" and "cryptcat.exe" were found in the same directory, listed under "C:\hxdefrootkit" (figure 6). Both Netcat and VNC were situated in "C:\inetpub\ftproot" (figure 7). The processes "iroffer" and "birdcd" were discovered under the filename "C:\hidden". Notably, "posionivy" was located in "C:\WINDOWS\System32", a location inappropriate for an executable file within the Windows system directory. Upon further analysis of the DLLs associated with these processes, significant insights into their functionalities were revealed. For instance, examining the details of "nc.exe" unveiled its command line: "C:\inetpub\ftproot\nc.exe -L -p 6666 -e cmd.exe", indicating its utilization for establishing a listener on port 6666, thereby granting remote access via a command prompt. Similarly, "Cryptcat" exhibited a similar behavior with its command line: "C:\hxdefrootkit\cryptcat.exe" -L -p 666 -e cmd.exe", indicating its operation on port 666 with the "-e" command to maintain an open command prompt. Connecting to these ports would provide immediate access to the command prompt of the current user. Another notable discovery was the presence of "cmd.exe" with the command line: "C:\WINDOWS\system32\cmd.exe /K C:\ftproot\lock.bat" (figure 10). The "/k" option instructs cmd.exe to execute the "lock.bat" batch file and retain the Command Prompt window open afterward. Given that "lock.bat" resides in the "C:\ftproot" directory, where Netcat and VNC are also located, raises suspicion. The purpose of "lock.bat" remains speculative, however, considering its name, it could potentially involve securing files or folders, executing security-related commands, or implementing measures to enhance system security. These hypotheses are derived from the term "lock," as external research failed to provide definitive insights into the function of this file.

Expanding on the analysis of running processes, I proceeded to investigate for any concealed ones using the "psxview -R" command, designed to uncover hidden processes within memory images (O'reilly). By employing the "-R" option, the output was filtered to exclusively display these concealed processes. In examining the columns from left to right, everything appeared ordinary until reaching the "deskthrd" column, where two processes, namely "lsass.exe" and "svchost.exe", were flagged as "False". This anomaly raised suspicion, particularly considering that both are critical system processes, as evidenced by their parent processes (refer to figure 5). The designation of "False" implies potential manipulation or tampering.

To delve deeper, I searched the DLLs associated with each process individually, quickly identifying a duplication of the "comctl32.dll" (refer to figure 12-13). One instance was located in the System32 directory, consistent with the expected placement of system DLLs, while the other was sourced from the WinSxS directory. According to Microsoft standards, "comctl32.dll" is intended to reside within the System32 directory (Microsoft). This discrepancy in DLL location likely contributes to the false designation of both "lsass" and "svchost". Both "lsass.exe" (Local

Security Authority Subsystem Service) and "svchost.exe" (Service Host) are critical system processes within Windows operating systems. They fulfill crucial roles in system security, authentication, and service hosting. Due to their critical nature, they frequently attract the attention of attackers seeking to compromise system security or perpetrate malicious activities.

After looking at the processes, I proceeded to examine their origins, focusing on the processes that initiated them. As depicted in figure 14, the initial entries reveal that "services.exe" initiated "hxdef100.exe", subsequently launching "cryptcat.exe" and "bircd.exe". Similarly, "explorer.exe" initiated "posionivy.exe". Notably, "iroffer.exe" appeared to be a standalone process initiating its variants, while "winvn4.exe" and "nc.exe" were also standalone processes. What raised concern was the fact that our previously identified suspicious files were initiated by legitimate processes, "services.exe" and "explorer.exe".Upon closer inspection of "services.exe", the DLLs listed in its associated processes appeared legitimate and did not raise any red flags. However, examining the command output of "malfind" for "services.exe" revealed a page executed with read and write privileges identified as Hacker.Defender, potentially linked to the HXD rootkit (figure 15). The presence of HXD within the memory space of "services.exe" suggests that the rootkit has been injected or loaded into the address space of the "services.exe" process. This manipulation enables the rootkit to execute within the context of a legitimate Windows process, heightening its stealth and evasiveness. Consequently, it was able to start up "cryptcat" and "bircd". Similarly, "explorer.exe" exhibited signs of manipulation or compromise, with Hacker Defender also detected within its memory space (figure 16). This finding suggests that "explorer.exe" may have been compromised to execute the HXD rootkit. Additionally, the presence of the "comctl32" DLL from two different locations, namely system32 and WinSxS (refer to figure 17), raises suspicions. These factors could explain how "poisonivy.exe" was executed, either through the rootkit's actions or via arbitrary code execution from the DLL.

From what I looked at when it comes to the processes I have seen that all the processes were started at the same time, October 30, 2018 at 8:46 pm. In addition, the hxdef100 rootkit has infected all the running processes as seen from the output of the command “malfind” which shows that Hacker.Defender has been executed with read and write privileges. The output was also followed by kernel32.dll which suggests that the Hacker Defender rootkit may have injected its code into the kernel32.dll file. Hacker.Defender is a type of rootkit known for its ability to hide processes, files, and registry keys, as well as provide remote access to an attacker. Injecting its code into kernel32.dll allows the rootkit to execute within the context of a critical system library, making it more difficult to detect and remove.

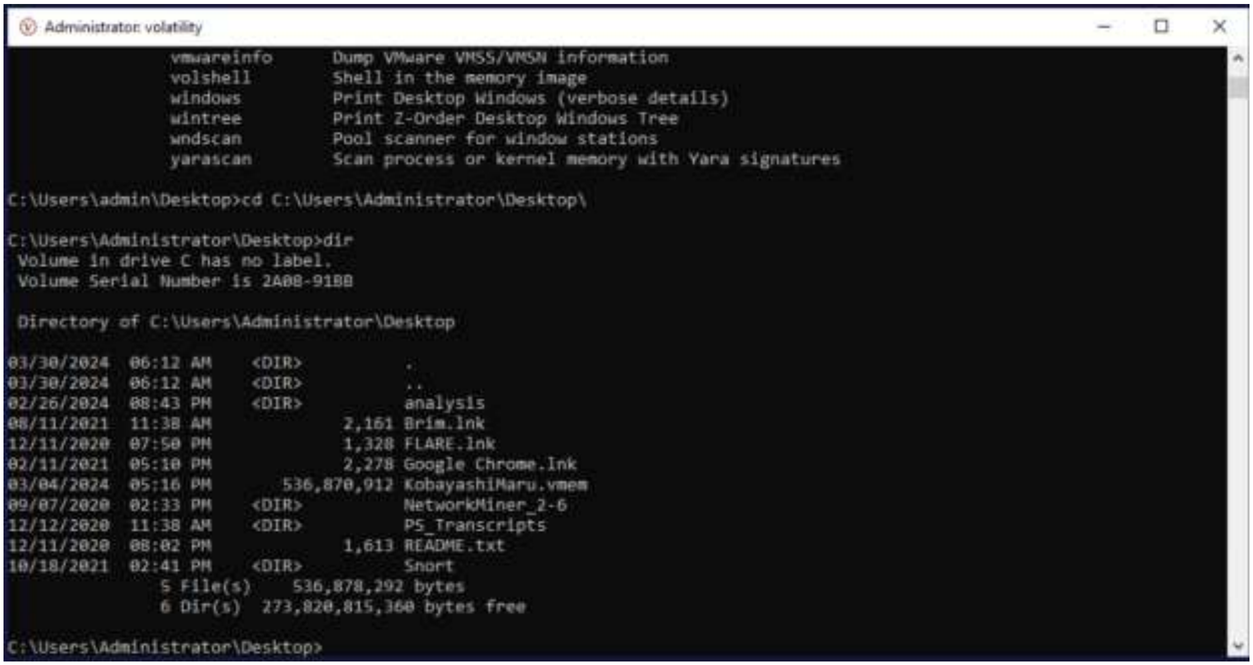
After attempting various commands like "connections", "sockets", "sockscan", and "netscan" which showed blank outputs, I resorted to using "connscan" to identify open ports. This tool not only detects active connections but also uncovers artifacts from terminated connections. From the output, I observed two distinct addresses associated with "poisonivy.exe", "iroffer.exe", and "bircd.exe" (figure 18). "poisonivy.exe" appeared to be establishing a connection with the remote address 192.168.5.98 through port 3460. However, what raised suspicion were the connections initiated by "iroffer.exe" and "bircd.exe" to the loopback address in the Internet Protocol version 4 (IPv4) addressing scheme. The loopback address is reserved for local communication within the same device. External research revealed that establishing a connection to a loopback device over a compromised local machine could enable the extraction of sensitive data, such as passwords (Ubuntu Forums). It's noteworthy that the scans primarily displayed closed connections, suggesting that these connections had been terminated. However, upon cross-referencing with the processes list, it became apparent that only "iroffer.exe" had initiated and exited, indicating that the connection to the loopback should have been the only one terminated. This discrepancy leads me to believe that the other two connections could be concealed, potentially serving the purpose of extracting data or establishing a backdoor connection to a remote site.

The cyber attacker carried out a targeted assault, exploiting weaknesses in the victim's system to gain unauthorized access. They utilized a range of malicious tools, including hxdef100.exe, poisonivy.exe, iroffer.exe, bircd.exe, cryptcat.exe, nc.exe, and winvnc4.exe, each serving a specific purpose in their malicious activities. These tools allowed the attacker to cover their tracks, create backdoors for remote access, and manipulate system functions to their advantage. Through the use of rootkits and other evasion techniques, they managed to avoid detection and maintain control over the compromised system.

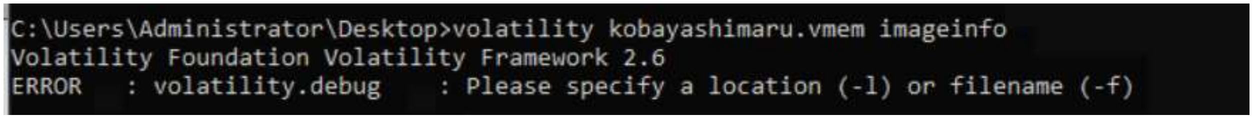
Moreover, the attacker used advanced tactics to manipulate critical system processes like lsass.exe and svchost.exe. By injecting malicious code into these processes and falsifying their characteristics, they obscured their actions and gained unauthorized access to important system components. This manipulation of system processes enabled the attacker to bypass traditional security measures and operate discreetly within the victim's environment. Additionally, their efforts to establish suspicious connections, particularly targeting remote and loopback addresses via poisonivy.exe, iroffer.exe, and bircd.exe, indicate a focused attempt to extract sensitive data or establish hidden communication channels for further malicious activities.

Taking a closer look, it's clear that the attacker's strategies went beyond simply exploiting vulnerabilities. They demonstrated a deep understanding of system architecture and employed sophisticated methods to infiltrate and manipulate critical components. This high level of sophistication suggests a well-equipped and highly skilled threat actor, possibly operating with specific objectives in mind. Furthermore, their deliberate targeting of system processes and establishment of covert communication channels underscores a strategic approach aimed at long-term persistence and data theft.

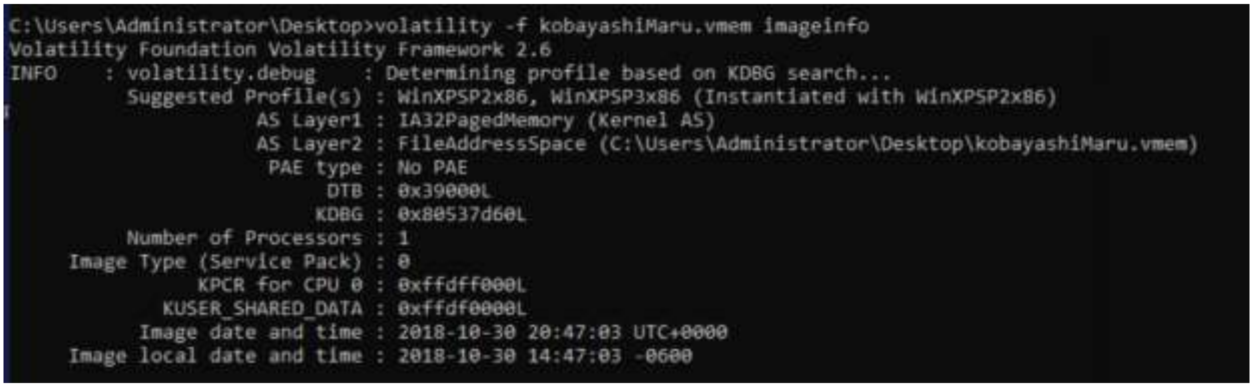
Images

1. 

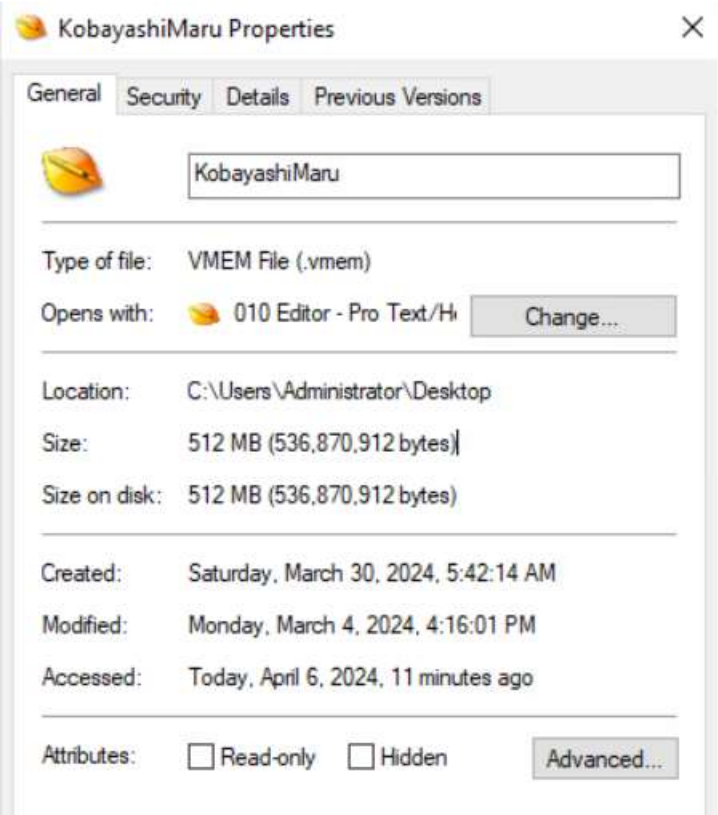
```
                vmwareinfo      Dump VMware VMSS/VMSN information
                volshell        Shell in the memory image
                windows         Print Desktop Windows (verbose details)
                wintree         Print Z-Order Desktop Windows Tree
                wndscan         Pool scanner for window stations
                yarascan        Scan process or kernel memory with Yara signatures

C:\Users\admin\Desktop>cd C:\Users\Administrator\Desktop\

C:\Users\Administrator\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 2A08-9188

 Directory of C:\Users\Administrator\Desktop

03/30/2024  06:12 AM    <DIR>          .
03/30/2024  06:12 AM    <DIR>          ..
02/26/2024  08:43 PM    <DIR>          analysis
08/11/2021  11:38 AM             2,161 Brim.lnk
12/11/2020  07:50 PM             1,328 FLARE.lnk
02/11/2021  05:10 PM             2,278 Google Chrome.lnk
03/04/2024  05:16 PM       536,870,912 KobayashiMaru.vmem
09/07/2020  02:33 PM    <DIR>          NetworkMiner_2-6
12/12/2020  11:38 AM    <DIR>          PS_Transcripts
12/11/2020  08:02 PM             1,613 README.txt
10/18/2021  02:41 PM    <DIR>          Snort
               5 File(s)    536,878,292 bytes
               6 Dir(s)  273,820,815,360 bytes free

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

2. 

```
C:\Users\Administrator\Desktop>volatility kobayashimaru.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
ERROR   : volatility.debug    : Please specify a location (-l) or filename (-f)
```

3. 

```
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
                           DTB : 0x39000L
                          KDBG : 0x80537d60L
          Number of Processors : 1
     Image Type (Service Pack) : 0
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2018-10-30 20:47:03 UTC+0000
     Image local date and time : 2018-10-30 14:47:03 -0600
```

4. 

KobayashiMaru

Type of file: VMEM File (.vmem)

Opens with: 010 Editor - Pro Text/H

Location: C:\Users\Administrator\Desktop

Size: 512 MB (536,870,912 bytes)

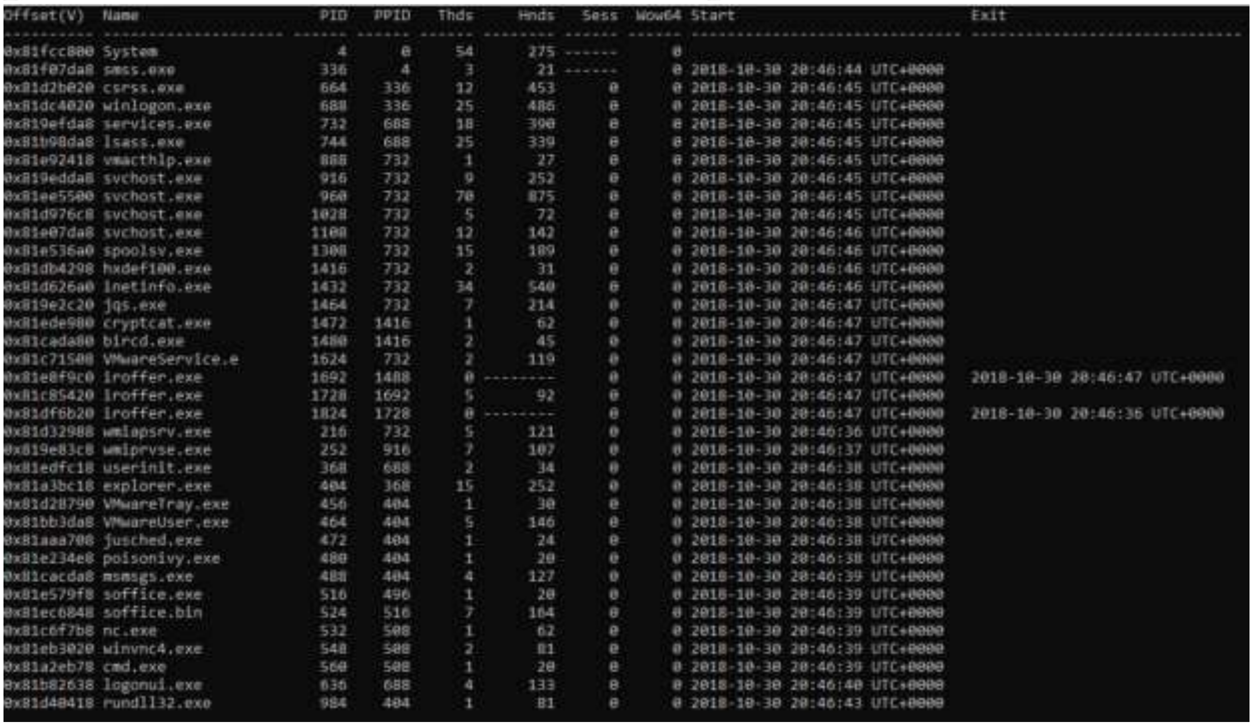
Size on disk: 512 MB (536,870,912 bytes)

Created: Saturday, March 30, 2024, 5:42:14 AM

Modified: Monday, March 4, 2024, 4:16:01 PM

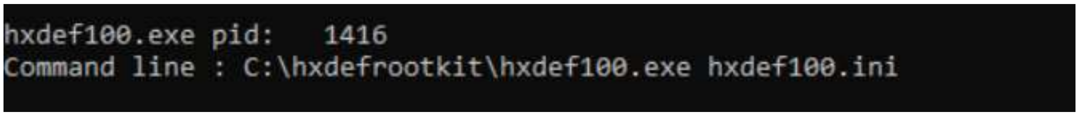
Accessed: Today, April 6, 2024, 11 minutes ago

Attributes: ☐ Read-only ☐ Hidden

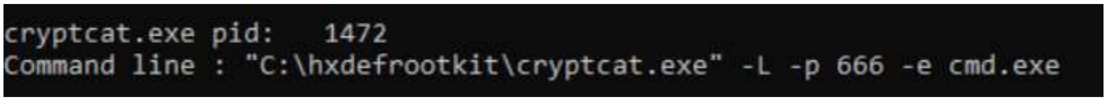
5. 

```
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
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            1300    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
0x81c71500 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      104      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
0x81b82638 logonui.exe             636    688      4      133      0      0 2018-10-30 20:46:40 UTC+0000
0x81d40418 rundll32.exe            984    404      1       81      0      0 2018-10-30 20:46:43 UTC+0000
```

6.

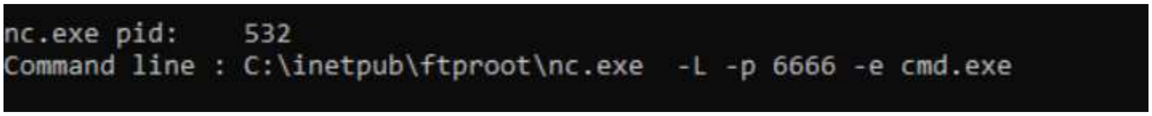


```
hxdef100.exe pid:   1416
Command line : C:\hxdefrootkit\hxdef100.exe hxdef100.ini
```

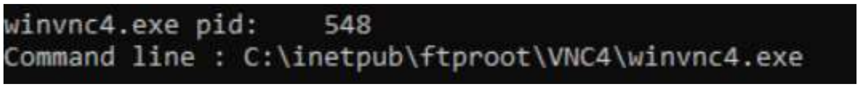


```
cryptcat.exe pid:   1472
Command line : "C:\hxdefrootkit\cryptcat.exe" -L -p 666 -e cmd.exe
```

7.

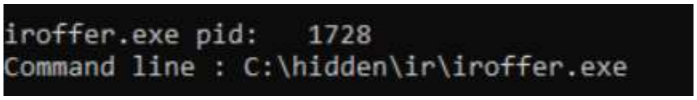


```
nc.exe pid:    532
Command line : C:\inetpub\ftproot\nc.exe  -L -p 6666 -e cmd.exe
```

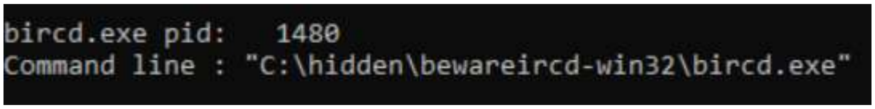


```
winvnc4.exe pid:    548
Command line : C:\inetpub\ftproot\VNC4\winvnc4.exe
```

8.

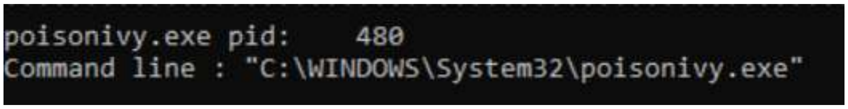


```
iroffer.exe pid:   1728
Command line : C:\hidden\ir\iroffer.exe
```



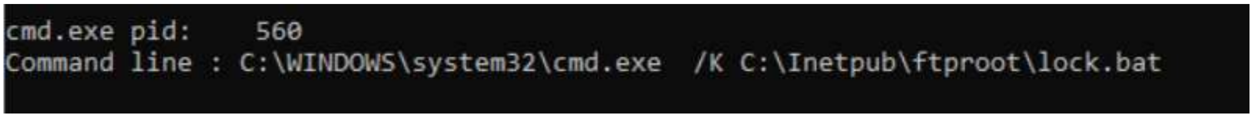
```
bircd.exe pid:   1480
Command line : "C:\hidden\bewareircd-win32\bircd.exe"
```

9.



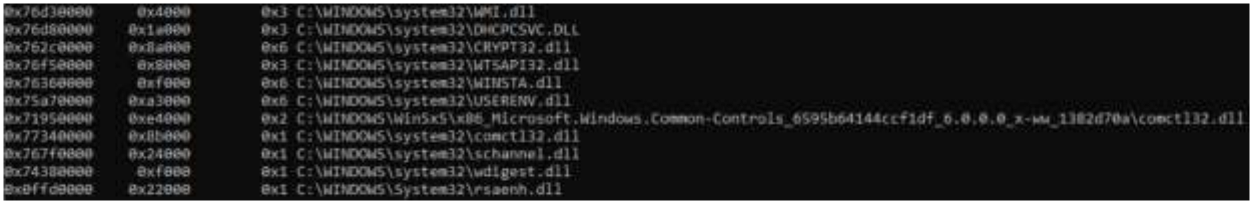
```
poisonivy.exe pid:    480
Command line : "C:\WINDOWS\System32\poisonivy.exe"
```

10.



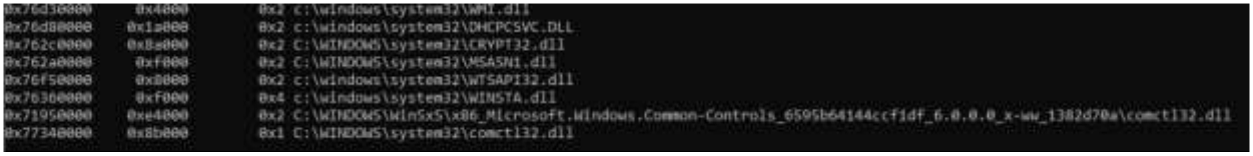
```
cmd.exe pid:    560
Command line : C:\WINDOWS\system32\cmd.exe  /K C:\Inetpub\ftproot\lock.bat
```

11.



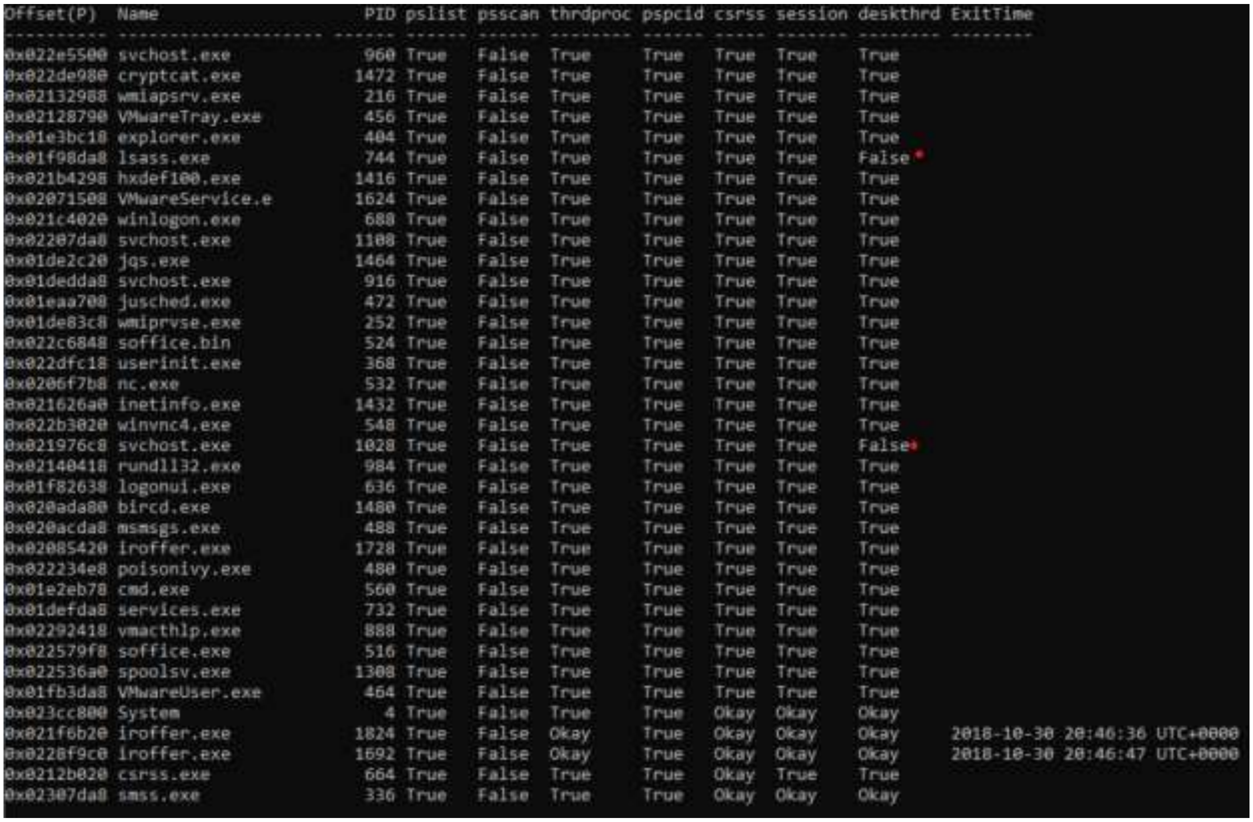
```
0x76d30000     0x4000        0x3 C:\WINDOWS\system32\WMI.dll
0x76d80000    0x1a000        0x3 C:\WINDOWS\system32\DHCPCSVC.DLL
0x762c0000    0x8a000        0x6 C:\WINDOWS\system32\CRYPT32.dll
0x76f50000     0x8000        0x3 C:\WINDOWS\system32\WTSAPI32.dll
0x76360000     0xf000        0x6 C:\WINDOWS\system32\WINSTA.dll
0x75a70000    0xa3000        0x6 C:\WINDOWS\system32\USERENV.dll
0x71950000    0xe4000        0x2 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.0.0_x-ww_1382d70a\comctl32.dll
0x77340000    0x8b000        0x1 C:\WINDOWS\system32\comctl32.dll
0x767f0000    0x24000        0x1 C:\WINDOWS\system32\schannel.dll
0x74380000     0xf000        0x1 C:\WINDOWS\system32\wdigest.dll
0x0ffd0000    0x22000        0x1 C:\WINDOWS\System32\rsaenh.dll
```

12.



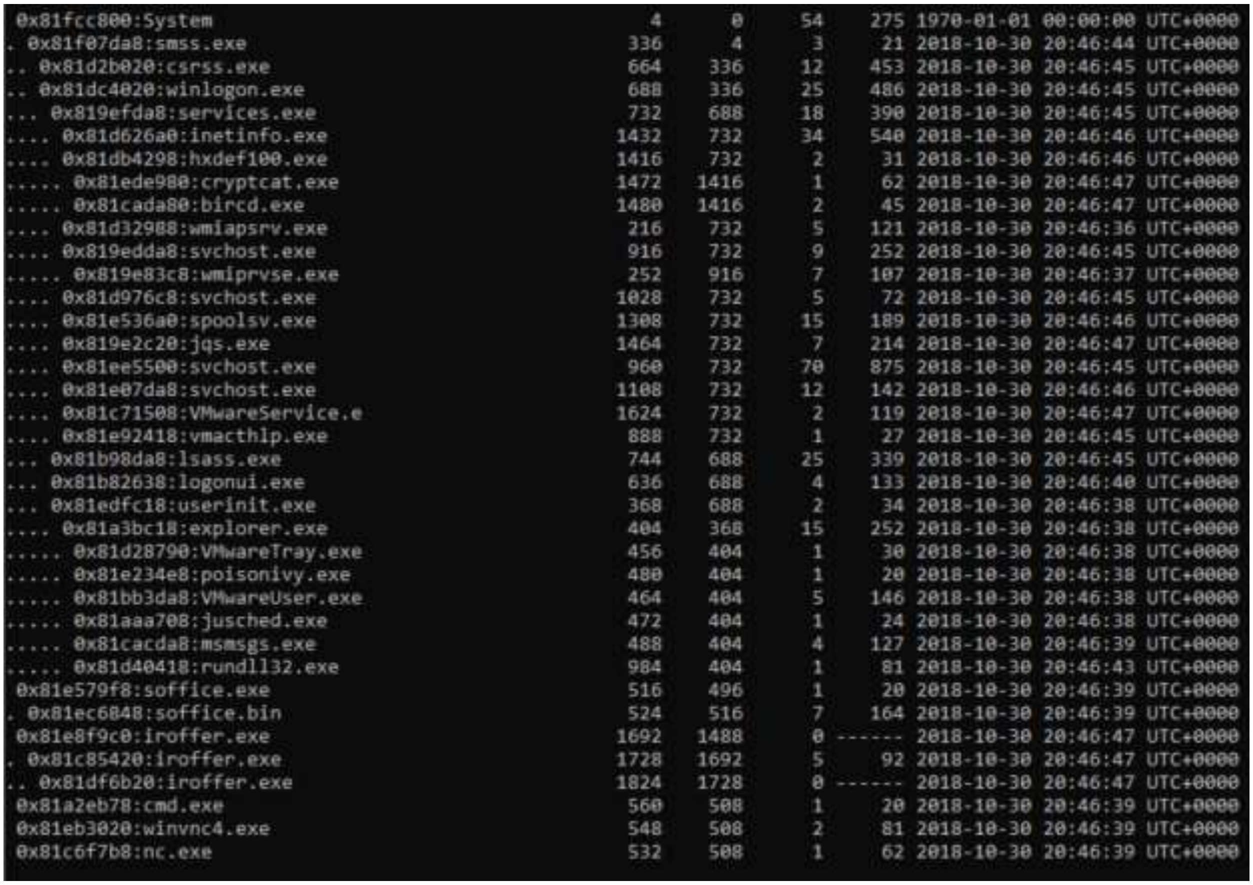
```
0x76d30000     0x4000        0x2 c:\windows\system32\WMI.dll
0x76d80000    0x1a000        0x2 c:\windows\system32\DHCPCSVC.DLL
0x762c0000    0x8a000        0x2 C:\WINDOWS\system32\CRYPT32.dll
0x762a0000     0xf000        0x2 C:\WINDOWS\system32\MSASN1.dll
0x76f50000     0x8000        0x2 c:\windows\system32\WTSAPI32.dll
0x76360000     0xf000        0x4 c:\windows\system32\WINSTA.dll
0x71950000    0xe4000        0x2 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.0.0_x-ww_1382d70a\comctl32.dll
0x77340000    0x8b000        0x1 C:\WINDOWS\system32\comctl32.dll
```

13.

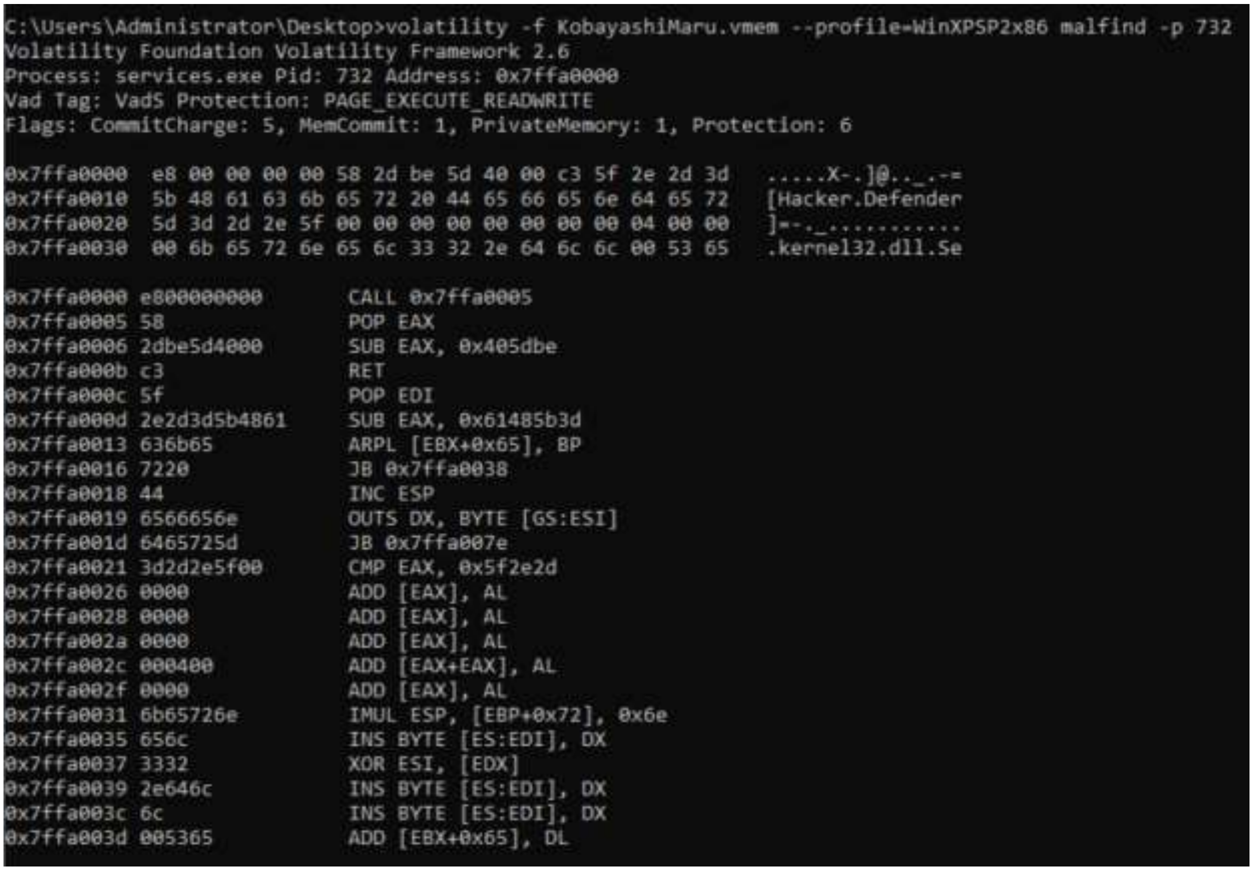


```
Offset(P)  Name                    PID pslist psscan thrdproc pspcid csrss session deskthrd ExitTime
---------- -------------------- ------ ------ ------ -------- ------ ----- ------- -------- --------
0x022e5500 svchost.exe             960 True   False  True     True   True  True    True
0x022de980 cryptcat.exe           1472 True   False  True     True   True  True    True
0x02132988 wmiapsrv.exe            216 True   False  True     True   True  True    True
0x02128790 VMwareTray.exe          456 True   False  True     True   True  True    True
0x01e3bc18 explorer.exe            404 True   False  True     True   True  True    True
0x01f98da8 lsass.exe               744 True   False  True     True   True  True    False*
0x021b4298 hxdef100.exe           1416 True   False  True     True   True  True    True
0x02071508 VMwareService.e        1624 True   False  True     True   True  True    True
0x021c4020 winlogon.exe            688 True   False  True     True   True  True    True
0x02207da8 svchost.exe            1108 True   False  True     True   True  True    True
0x01de2c20 jqs.exe                1464 True   False  True     True   True  True    True
0x01dedda8 svchost.exe             916 True   False  True     True   True  True    True
0x01eaa708 jusched.exe             472 True   False  True     True   True  True    True
0x01de83c8 wmiprvse.exe            252 True   False  True     True   True  True    True
0x022c6848 soffice.bin             524 True   False  True     True   True  True    True
0x022dfc18 userinit.exe            368 True   False  True     True   True  True    True
0x0206f7b8 nc.exe                  532 True   False  True     True   True  True    True
0x021626a0 inetinfo.exe           1432 True   False  True     True   True  True    True
0x022b3020 winvnc4.exe             548 True   False  True     True   True  True    True
0x021976c8 svchost.exe            1028 True   False  True     True   True  True    False*
0x02140418 rundll32.exe            984 True   False  True     True   True  True    True
0x01f82638 logonui.exe             636 True   False  True     True   True  True    True
0x020ada80 bircd.exe              1480 True   False  True     True   True  True    True
0x020acda8 msmsgs.exe              488 True   False  True     True   True  True    True
0x02085420 iroffer.exe            1728 True   False  True     True   True  True    True
0x022234e8 poisonivy.exe           480 True   False  True     True   True  True    True
0x01e2eb78 cmd.exe                 560 True   False  True     True   True  True    True
0x01defda8 services.exe            732 True   False  True     True   True  True    True
0x02292418 vmacthlp.exe            888 True   False  True     True   True  True    True
0x022579f8 soffice.exe             516 True   False  True     True   True  True    True
0x022536a0 spoolsv.exe            1308 True   False  True     True   True  True    True
0x01fb3da8 VMwareUser.exe          464 True   False  True     True   True  True    True
0x023cc800 System                    4 True   False  True     True   Okay  Okay    Okay
0x021f6b20 iroffer.exe            1824 True   False  Okay     True   Okay  Okay    Okay     2018-10-30 20:46:36 UTC+0000
0x0228f9c0 iroffer.exe            1692 True   False  Okay     True   Okay  Okay    Okay     2018-10-30 20:46:47 UTC+0000
0x0212b020 csrss.exe               664 True   False  True     True   Okay  True    True
0x02307da8 smss.exe                336 True   False  True     True   Okay  Okay    Okay
```

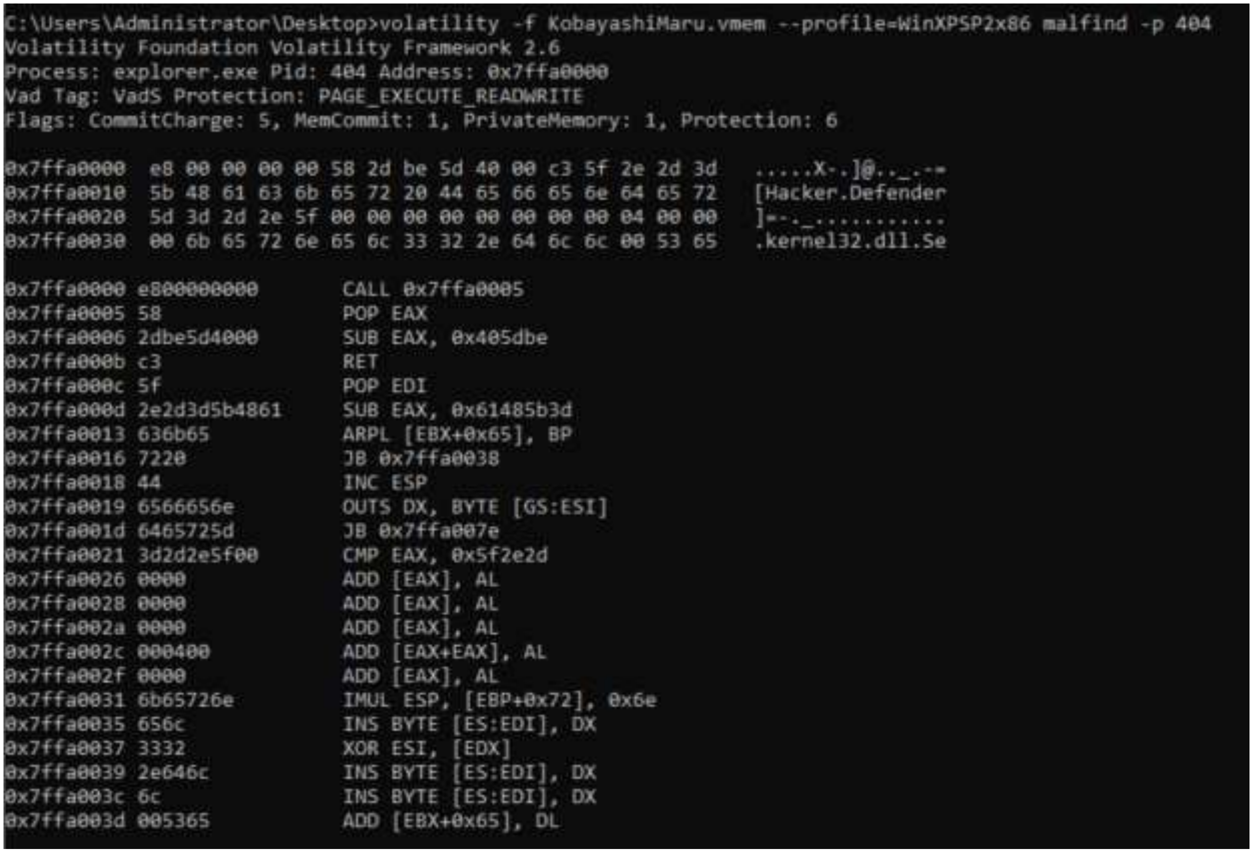
14.



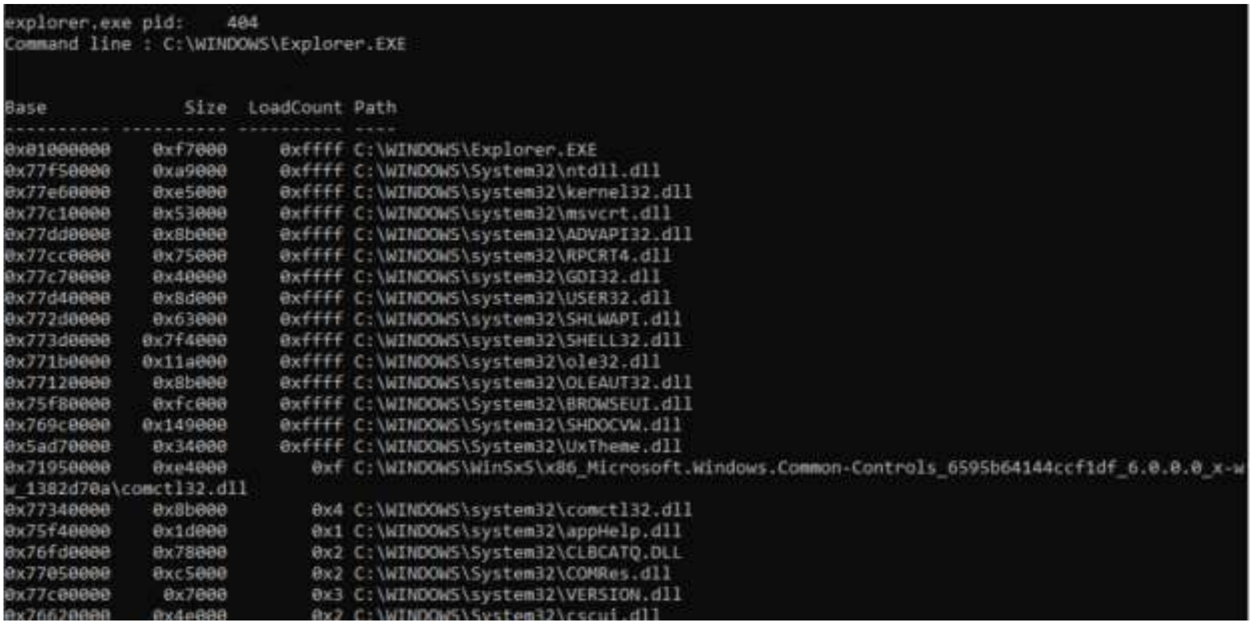
```
 0x81fcc800:System                                      4      0     54    275 1970-01-01 00:00:00 UTC+0000
. 0x81f07da8:smss.exe                                 336      4      3     21 2018-10-30 20:46:44 UTC+0000
.. 0x81d2b020:csrss.exe                               664    336     12    453 2018-10-30 20:46:45 UTC+0000
.. 0x81dc4020:winlogon.exe                            688    336     25    486 2018-10-30 20:46:45 UTC+0000
... 0x819efda8:services.exe                           732    688     18    390 2018-10-30 20:46:45 UTC+0000
.... 0x81d626a0:inetinfo.exe                         1432    732     34    540 2018-10-30 20:46:46 UTC+0000
.... 0x81db4298:hxdef100.exe                         1416    732      2     31 2018-10-30 20:46:46 UTC+0000
..... 0x81ede980:cryptcat.exe                        1472   1416      1     62 2018-10-30 20:46:47 UTC+0000
..... 0x81cada80:bircd.exe                           1480   1416      2     45 2018-10-30 20:46:47 UTC+0000
.... 0x81d32988:wmiapsrv.exe                          216    732      5    121 2018-10-30 20:46:36 UTC+0000
.... 0x819edda8:svchost.exe                           916    732      9    252 2018-10-30 20:46:45 UTC+0000
..... 0x819e83c8:wmiprvse.exe                         252    916      7    107 2018-10-30 20:46:37 UTC+0000
.... 0x81d976c8:svchost.exe                          1028    732      5     72 2018-10-30 20:46:45 UTC+0000
.... 0x81e536a0:spoolsv.exe                          1308    732     15    189 2018-10-30 20:46:46 UTC+0000
.... 0x819e2c20:jqs.exe                              1464    732      7    214 2018-10-30 20:46:47 UTC+0000
.... 0x81ee5500:svchost.exe                           960    732     70    875 2018-10-30 20:46:45 UTC+0000
.... 0x81e07da8:svchost.exe                          1108    732     12    142 2018-10-30 20:46:46 UTC+0000
.... 0x81c71508:VMwareService.e                      1624    732      2    119 2018-10-30 20:46:47 UTC+0000
.... 0x81e92418:vmacthlp.exe                          888    732      1     27 2018-10-30 20:46:45 UTC+0000
... 0x81b98da8:lsass.exe                              744    688     25    339 2018-10-30 20:46:45 UTC+0000
... 0x81b82638:logonui.exe                            636    688      4    133 2018-10-30 20:46:40 UTC+0000
... 0x81edfc18:userinit.exe                           368    688      2     34 2018-10-30 20:46:38 UTC+0000
.... 0x81a3bc18:explorer.exe                          404    368     15    252 2018-10-30 20:46:38 UTC+0000
..... 0x81d28790:VMwareTray.exe                       456    404      1     30 2018-10-30 20:46:38 UTC+0000
..... 0x81e234e8:poisonivy.exe                        480    404      1     20 2018-10-30 20:46:38 UTC+0000
..... 0x81bb3da8:VMwareUser.exe                       464    404      5    146 2018-10-30 20:46:38 UTC+0000
..... 0x81aaa708:jusched.exe                          472    404      1     24 2018-10-30 20:46:38 UTC+0000
..... 0x81cacda8:msmsgs.exe                           488    404      4    127 2018-10-30 20:46:39 UTC+0000
..... 0x81d40418:rundll32.exe                         984    404      1     81 2018-10-30 20:46:43 UTC+0000
 0x81e579f8:soffice.exe                               516    496      1     20 2018-10-30 20:46:39 UTC+0000
. 0x81ec6848:soffice.bin                              524    516      7    164 2018-10-30 20:46:39 UTC+0000
 0x81e8f9c0:iroffer.exe                              1692   1488      0 ------ 2018-10-30 20:46:47 UTC+0000
. 0x81c85420:iroffer.exe                             1728   1692      5     92 2018-10-30 20:46:47 UTC+0000
.. 0x81df6b20:iroffer.exe                            1824   1728      0 ------ 2018-10-30 20:46:47 UTC+0000
 0x81a2eb78:cmd.exe                                   560    508      1     20 2018-10-30 20:46:39 UTC+0000
 0x81eb3020:winvnc4.exe                               548    508      2     81 2018-10-30 20:46:39 UTC+0000
 0x81c6f7b8:nc.exe                                    532    508      1     62 2018-10-30 20:46:39 UTC+0000
```

15. 

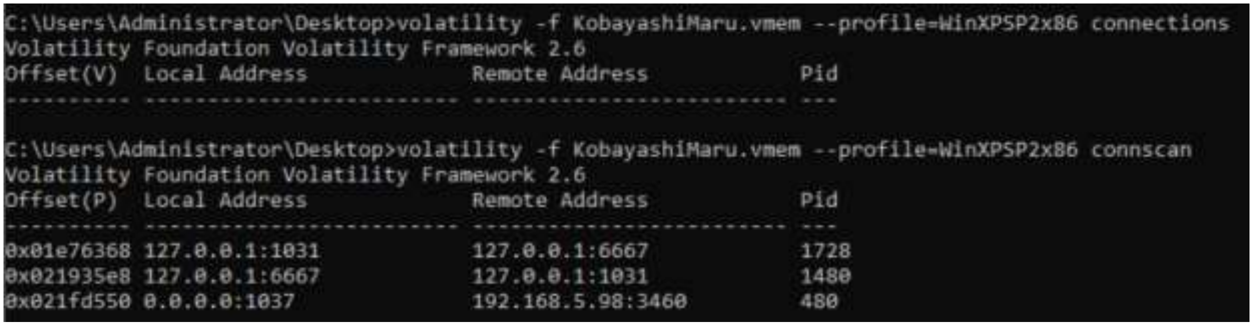
```
C:\Users\Administrator\Desktop>volatility -f KobayashiMaru.vmem --profile=WinXPSP2x86 malfind -p 732
Volatility Foundation Volatility Framework 2.6
Process: services.exe Pid: 732 Address: 0x7ffa0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 5, MemCommit: 1, PrivateMemory: 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
```

16. 

```
C:\Users\Administrator\Desktop>volatility -f KobayashiMaru.vmem --profile=WinXPSP2x86 malfind -p 404
Volatility Foundation Volatility Framework 2.6
Process: explorer.exe Pid: 404 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
```

17. 

```
explorer.exe pid:    404
Command line : C:\WINDOWS\Explorer.EXE


Base             Size  LoadCount Path
---------- ---------- ---------- ----
0x01000000    0xf7000     0xffff C:\WINDOWS\Explorer.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
0x77dd0000    0x8b000     0xffff C:\WINDOWS\system32\ADVAPI32.dll
0x77cc0000    0x75000     0xffff C:\WINDOWS\system32\RPCRT4.dll
0x77c70000    0x40000     0xffff C:\WINDOWS\system32\GDI32.dll
0x77d40000    0x8d000     0xffff C:\WINDOWS\system32\USER32.dll
0x772d0000    0x63000     0xffff C:\WINDOWS\system32\SHLWAPI.dll
0x773d0000   0x7f4000     0xffff C:\WINDOWS\system32\SHELL32.dll
0x771b0000   0x11a000     0xffff C:\WINDOWS\system32\ole32.dll
0x77120000    0x8b000     0xffff C:\WINDOWS\system32\OLEAUT32.dll
0x75f80000    0xfc000     0xffff C:\WINDOWS\System32\BROWSEUI.dll
0x769c0000   0x149000     0xffff C:\WINDOWS\System32\SHDOCVW.dll
0x5ad70000    0x34000     0xffff C:\WINDOWS\System32\UxTheme.dll
0x71950000    0xe4000        0xf C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.0.0_x-w
w_1382d70a\comctl32.dll
0x77340000    0x8b000        0x4 C:\WINDOWS\system32\comctl32.dll
0x75f40000    0x1d000        0x1 C:\WINDOWS\system32\appHelp.dll
0x76fd0000    0x78000        0x2 C:\WINDOWS\System32\CLBCATQ.DLL
0x77050000    0xc5000        0x2 C:\WINDOWS\System32\COMRes.dll
0x77c00000     0x7000        0x3 C:\WINDOWS\system32\VERSION.dll
0x76620000    0x4e000        0x2 C:\WINDOWS\System32\cscui.dll
```

18. 

```
C:\Users\Administrator\Desktop>volatility -f KobayashiMaru.vmem --profile=WinXPSP2x86 connections
Volatility Foundation Volatility Framework 2.6
Offset(V)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---

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
```

Citations:

Computer Hope. “What is SP?” *Computer Hope*, 13 March 2021, https://www.computerhope.com/jargon/s/sp.htm. Accessed 4 April 2024.

EaseUS. “Three Ways to Lock a Folder in Windows 7 Without Sofware.” *EaseUS*, https://toolbox.easeus.com/file-lock-tips/lock-a-folder-in-windows-7-without-sofware.html. Accessed 6 April 2024.

Fisher, Tim. “What Is a Service Pack?” *Lifewire*, 9 February 2023, https://www.lifewire.com/what-is-a-service-pack-2626010. Accessed 4 April 2024.

Microsoft. *Learn*, https://learn.microsoft.com/en-us/answers/questions/1031264/what-is-the-latest-version-of-windows-os-file-comc. Accessed 7 April 2024.

O'reilly. *Wikipedia*, https://www.oreilly.com/library/view/digital-forensics-with/9781788625005/4d0403d3-9cba-4a16-bbe4-0a3df437044c.xhtml. Accessed 7 April 2024.

Process Library. “iroffer.exe - What is iroffer.exe?” *Process Library*, https://www.processlibrary.com/en/directory/files/iroffer/23813/. Accessed 6 April 2024.

Ubuntu Forums. “Ubuntu Forums.” *Ubuntu Forums*, 14 September 2012, https://ubuntuforums.org/showthread.php?t=2057377. Accessed 7 April 2024.