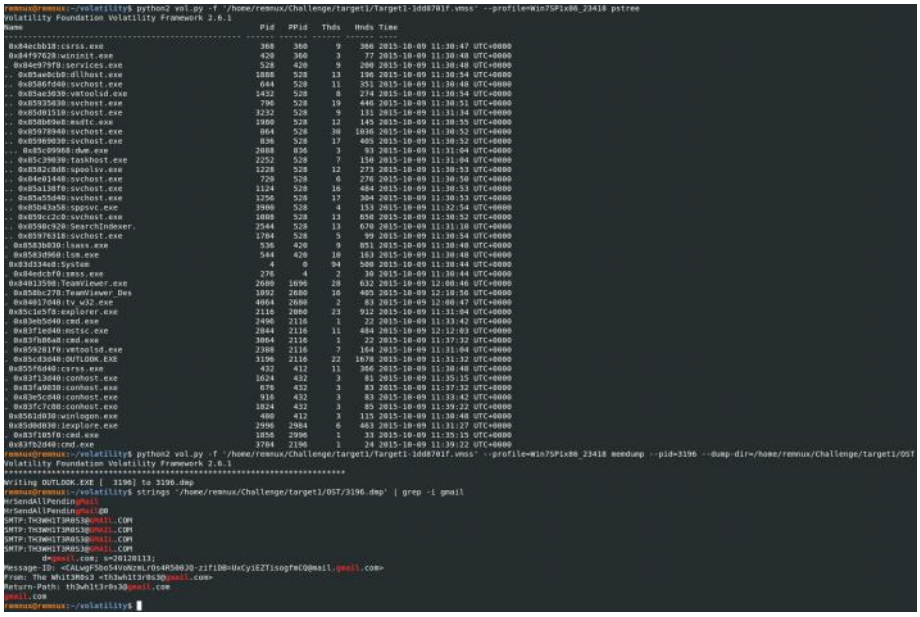
MrRobot Lab Challenge

Scenario:

An employee reported that his machine started to act strangely after receiving a suspicious email for a security update. The incident response team captured a couple of memory dumps from the suspected machines for further inspection. Analyze the dumps and help the SOC analysts team figure out what happened!

Task 1:
Machine:Target1 What email address tricked the front desk employee into installing a security update?

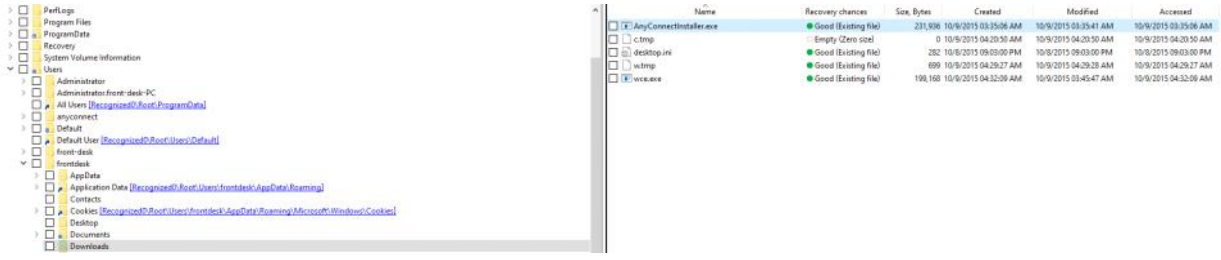
I used volatility2 with the pstree plugin, then I found the PID of Outlook.exe and dumped the process memory and used strings on it



Answer: th3wh1t3r0s3@gmail.com

Task 2:
Machine:Target1 What is the filename that was delivered in the email?

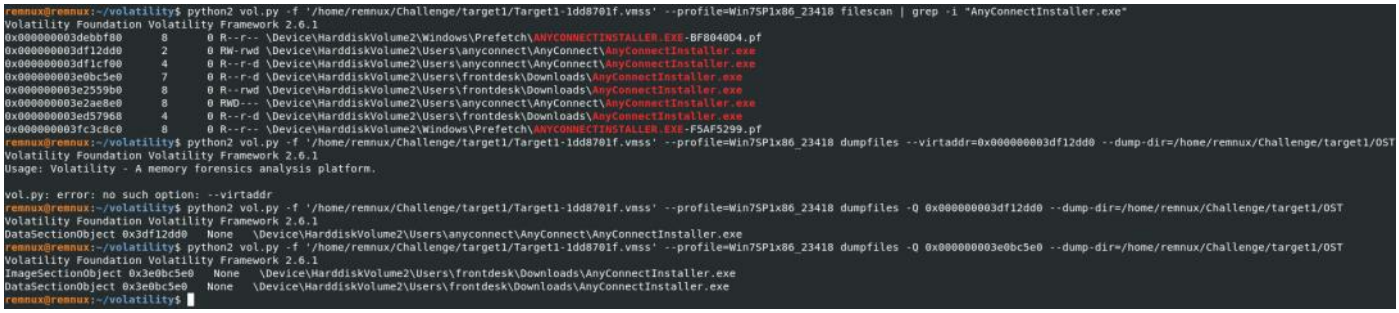
I opened the Target1 memory dump with R-Studio and navigate the users directories and I found inside the Downloads folder a known remote tool

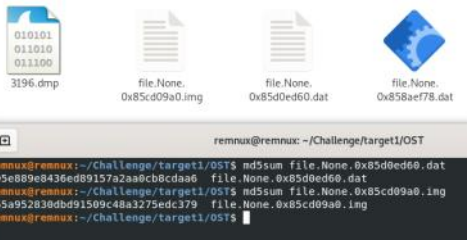


Answer: AnyConnectInstaller.exe

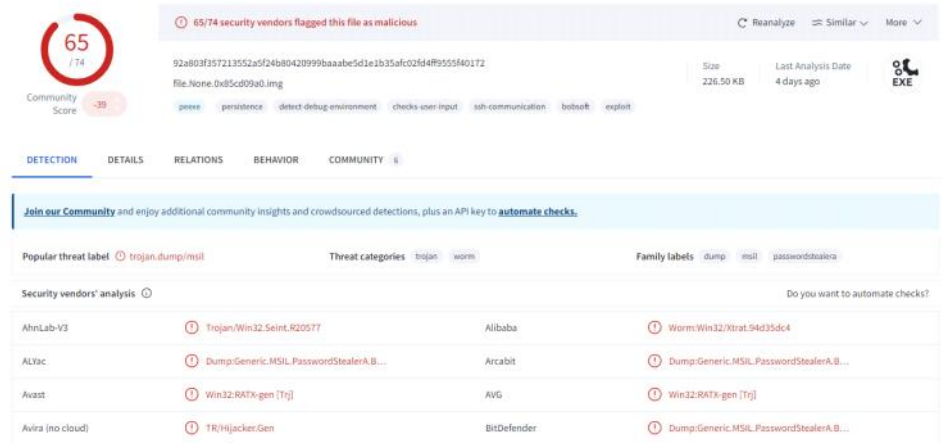
Task 3:
Machine:Target1 What is the name of the rat's family used by the attacker?

I tried to retrieve the file from R-Studio but the file hash was clean. So I used filescan plugin and searched for the file and found several files with the same name in different path's so I dumped the files and checked their MD5.

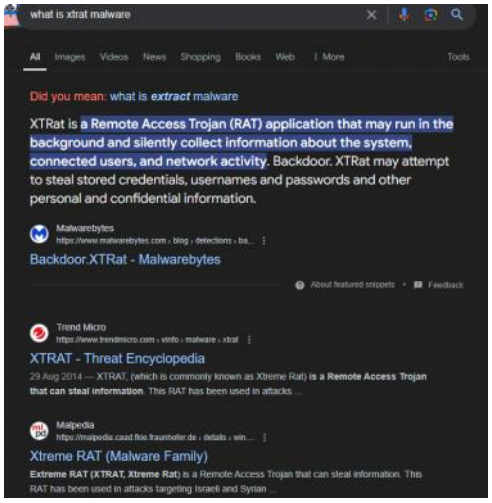




MD5 - 165a952830dbd91509c48a3275edc379



I noticed a lot of "RATX-gen" and "Xtrat" so I checked it on Google



Answer: XtremeRAT

Task 4:
Machine:Target1 The malware appears to be leveraging process injection. What is the PID of the process that is injected?

I used the pslist and investigated with handles plugin several PID's until I noticed several suspicious things on the process "iexplorer.exe"
First I saw the Downloads path of the user so it was look suspicious

```
remnux@remnux:~/volatility$ python2 vol.py -f '/home/remnux/Challenge/target1/Target1-1dd8701f.vmss' --profile=Win7SP1x86_23418 handles --pid=2996
Volatility Foundation Volatility Framework 2.6.1
Offset(V)     Pid     Handle     Access Type            Details
---------- ------ ---------- ---------- ---------------- -------
0x879c4e50   2996        0x4        0x3 Directory        KnownDlls
0x85d12c38   2996        0x8   0x100020 File             \Device\HarddiskVolume2\Users\frontdesk\Downloads
```

Then I saw a file "fsociety0.dat" this one was familiar to me from the MR.Robot series and the name of the Challenge is MrRobot so I thought it could be associated with it so I noted this down

```
0x85d11700   2996      0x150   0x1f0001 Mutant            fsociety0.dat
0x85d0d978   2996      0x154   0x1fffff Thread            TID 3000 PID 2996
```

Then I saw some Mutex activity related to TeamViewer

```
0x98e5f478   2996      0x5b0    0xf0007 Section           TeamViewerHooks7_SharedMemory
0x83fc4450   2996      0x5b4   0x1f0001 Mutant            TeamViewerHooks_LogBuffer
0x84016860   2996      0x5b8   0x1f0001 Mutant            TeamViewerHooks_Mutex4
0x84009200   2996      0x5bc   0x1f0001 Mutant            TeamViewerHooks_Mutex1
0x859c8698   2996      0x5c0   0x1f0003 Event             TeamViewerHooks_Command_w32
0x8402ca90   2996      0x5c4   0x1f0001 Mutant            TeamViewerHooks_Mutex5
0x859c86e8   2996      0x5c8   0x1f0003 Event             TeamViewerHooks_RetCommandDesktop
0x84019af0   2996      0x5cc   0x1f0003 Event             TeamViewerHooks_RetCommandAck
0x84019aa0   2996      0x5d0   0x1f0003 Event             TeamViewerHooks_RetCommandGUI
0x84015b98   2996      0x5d4   0x1f0001 Mutant            TeamViewerHooks_DynamicMemMutex
0x84015b38   2996      0x5d8   0x1f0001 Mutant            TeamViewerHooks_DirectXBufferMutex
```

So I assumed the answer for this task was the iexplorer.exe PID

Answer: 2996

Task 5:
Machine:Target1 What is the unique value the malware is using to maintain persistence after reboot?

First I used filescan and grepped for startup folder but found nothing.
Then I tried to use filescan and searched for the registry hive to dumped them but it didn't work also.
Then I tried to do hivedump but it's also didn't work why I tried to open it with Registry Explorer.
I asked ChatGPT and he told me to use the printkey plugin

To find the run registry key for persistence using Volatility, you'll want to use the `printkey` plugin with the appropriate registry hive. In Windows, persistence mechanisms are often found in registry keys under `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` or `HKLM\Software\Microsoft\Windows\CurrentVersion\Run`.

Based on your `hivelist`, you have several registry hives available:

1. `ntuser.dat` for the user's profile.
2. `UsrClass.dat` for user-specific settings.
3. `SYSTEM` for system settings.
4. `SOFTWARE` for installed software.

The `SOFTWARE` hive is likely where you'll find the `Run` key. You should use `printkey` to examine the `Run` key under `HKLM\Software\Microsoft\Windows\CurrentVersion\Run` and `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`.

Then I used the printkey with the command
python2 vol.py -f '/home/remnux/Challenge/target1/Target1-1dd8701f.vmss' --profile=Win7SP1x86_23418 printkey -K Software\\Microsoft\\Windows\\CurrentVersion\\Run

```
remnux@remnux:~/volatility$ python2 vol.py -f '/home/remnux/Challenge/target1/Target1-1dd8701f.vmss' --profile=Win7SP1x86_23418 printkey -K  Software\\Microsoft\\Windows\\CurrentVersion\\Run
Volatility Foundation Volatility Framework 2.6.1
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
Key name: Run (S)
Last updated: 2009-07-14 04:34:14 UTC+0000

Subkeys:

Values:
REG_EXPAND_SZ Sidebar         : (S) %ProgramFiles%\Windows Sidebar\Sidebar.exe /autoRun
----------------------------
Registry: \??\C:\Users\frontdesk\ntuser.dat
Key name: Run (S)
Last updated: 2015-10-09 10:36:11 UTC+0000

Subkeys:

Values:
REG_EXPAND_SZ MrRobot         : (S) c:\users\anyconnect\AnyConnect\AnyConnectInstaller.exe
```

Then I saw the AnyConnectInstaller.exe file with the value name.

Answer: MrRobot

Task 6:
Machine:Target1 Malware often uses a unique value or name to ensure that only one copy runs on the system. What is the unique name the malware is using?

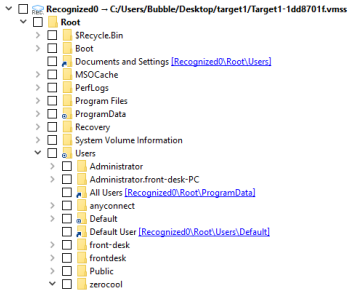
This one took me a while, I thought the process was TeamViewer and I tried to dumped them and checked the MD5 but it was wrong.
Then I checked the Task 4 again which I already saved pictures from the handles plugin and found the "fsociety0.dat" so I assumed this is the file and it was correct

```
0x85d11700   2996      0x150   0x1f0001 Mutant            fsociety0.dat
0x85d0d978   2996      0x154   0x1fffff Thread            TID 3000 PID 2996
```

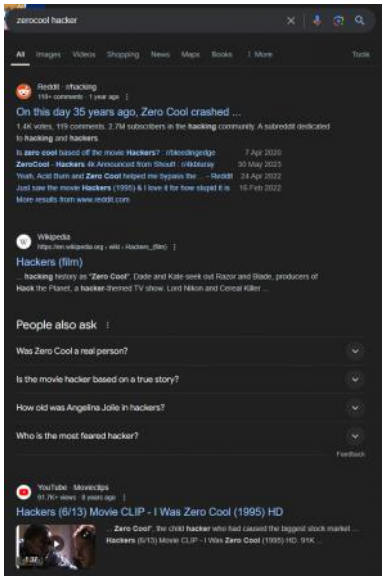
Answer: fsociety0.dat

Task 7:
Machine:Target1 It appears that a notorious hacker compromised this box before our current attackers. Name the movie he or she is from.

I searched the Users with R-Studio and saw some known name "zerocool"



Then I checked this name on Google



Answer: hackers

Task 8:
Machine:Target1 What is the NTLM password hash for the administrator account?

I used the hashdump plugin

```
remnux@remnux:~/volatility$ python2 vol.py -f '/home/remnux/Challenge/target1/Target1-1dd8701f.vmss' --profile=Win7SP1x86_23418 hashdump
Volatility Foundation Volatility Framework 2.6.1
Administrator:500:aad3b435b51404eeaad3b435b51404ee:79402b7671c317877b8b954b3311fa82:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
front-desk:1000:aad3b435b51404eeaad3b435b51404ee:2ae4c526659523d58350e4d70107fc11:::
```

Answer: 79402b7671c317877b8b954b3311fa82

Task 9:
Machine:Target1 The attackers appear to have moved over some tools to the compromised front desk host. How many tools did the attacker move?

I used the consoles plugin and saw several files and tools

```
CommandHistory: 0x2d90d0 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 5 LastAdded: 4 LastDisplayed: 4
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
Cmd #0 at 0x2cfe88: cd ..
Cmd #1 at 0x2cfea0: cd Temp
Cmd #2 at 0x2d6de0: dir
Cmd #3 at 0x2d67f0: wce.exe -w
Cmd #4 at 0x2bbc10: wce.exe -w > w.tmp
----
Screen 0x2bfea0 X:80 Y:300
Dump:
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>cd ..

C:\Windows>cd Temp

C:\Windows\Temp>
C:\Windows\Temp>dir
 Volume in drive C has no label.
 Volume Serial Number is FE0F-F423

 Directory of C:\Windows\Temp

10/09/2015  07:29 AM    <DIR>          .
10/09/2015  07:29 AM    <DIR>          ..
10/09/2015  01:27 AM                 0 DMIE58D.tmp
10/09/2015  06:57 AM            50,176 getlsasrvaddr.exe
10/09/2015  02:02 AM             7,572 MpCmdRun.log
10/09/2015  12:07 AM             4,636 MpSigStub.log
10/09/2015  03:37 AM    <DIR>          MPTelemetrySubmit
10/09/2015  06:45 AM            36,864 nbtscan.exe
10/09/2015  06:44 AM           503,800 Rar.exe
10/09/2015  01:28 AM           180,224 TS_A16D.tmp
10/09/2015  01:28 AM           196,608 TS_A3BF.tmp
10/09/2015  01:28 AM           376,832 TS_A42D.tmp
10/09/2015  01:28 AM           114,688 TS_A528.tmp
10/09/2015  01:28 AM           425,984 TS_A5C5.tmp
10/09/2015  01:28 AM           131,072 TS_A887.tmp
10/09/2015  01:28 AM           655,360 TS_A911.tmp
10/09/2015  01:28 AM           114,688 TS_AA79.tmp
10/09/2015  01:28 AM           180,224 TS_AF79.tmp
10/08/2015  11:43 PM    <DIR>          vmware-SYSTEM
10/09/2015  07:34 AM               333 w.tmp
10/09/2015  06:45 AM           199,168 wce.exe
              17 File(s)      3,178,229 bytes
               4 Dir(s)  22,603,194,368 bytes free

C:\Windows\Temp>wce.exe -w
WCE v1.42beta (Windows Credentials Editor) - (c) 2010-2013 Amplia Security - by
Hernan Ochoa (hernan@ampliasecurity.com)
Use -h for help.


Administrator\front-desk-PC:flagadmin@1234
frontdesk\ALLSAFECYBERSEC:THzV7mpz
FRONT-DESK-PC$\ALLSAFECYBERSEC:o0&77qj:^zctL2T]ljn3<niK2Kbqi`(:LeBoO7zE>'d8<>J"P
K;\*5IS@Oxg:rC:P:z Y!%fUiIX0y_J& uNUTJ?%:Y;qJY,xq/:)%5^f&zDK.)F%H;V?.^Z

C:\Windows\Temp>wce.exe -w > w.tmp

C:\Windows\Temp>
```

Answer: 3

Task 10:
Machine:Target1 What is the password for the front desk local administrator account?

Same like task 9, the password is at the bottom of the consoles plugin

```
Administrator\front-desk-PC:flagadmin@1234
frontdesk\ALLSAFECYBERSEC:THzV7mpz
FRONT-DESK-PC$\ALLSAFECYBERSEC:o0&77qj:^zctL2T]ljn3<niK2Kbqi`(:LeBoO7zE>'d8<>J"P
K;\*5IS@Oxg:rC:P:z Y!%fUiIX0y_J& uNUTJ?%:Y;qJY,xq/:)%5^f&zDK.)F%H;V?.^Z

C:\Windows\Temp>wce.exe -w > w.tmp
```

Answer: flagadmin@1234

Task 11:
Machine:Target1 What is the std create data timestamp for the nbtscan.exe tool?

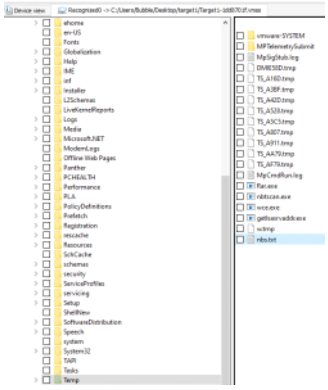
I used the mftparser plugin with grep of the filename

```
remnux@remnux:~/volatility$ python2 vol.py -f '/home/remnux/Challenge/target1/Target1-1dd8701f.vmss' --profile=Win7SP1x86_23418 mftparser | grep -i nbtscan
Volatility Foundation Volatility Framework 2.6.1
2015-10-09 10:45:12 UTC+0000 2015-10-09 10:45:12 UTC+0000   2015-10-09 10:45:12 UTC+0000   2015-10-09 10:45:12 UTC+0000   Windows\Temp\nbtscan.exe
2015-10-09 10:47:07 UTC+0000 2015-10-09 10:47:07 UTC+0000   2015-10-09 10:47:07 UTC+0000   2015-10-09 10:47:07 UTC+0000   Windows\Prefetch\NBTSCAN.EXE-44BD0B89.pf
```

Answer: 2015-10-09 10:45:12 UTC

Task 12:
Machine:Target1 The attackers appear to have stored the output from the nbtscan.exe tool in a text file on a disk called nbs.txt. What is the IP address of the first machine in that file?

I retrieved the file "nbs.txt" with R-Studio from the Temp folder



```
10.1.1.2        ALLSAFECYBERSEC\AD01            SHARING DC
10.1.1.3        ALLSAFECYBERSEC\EX01            SHARING
10.1.1.20       ALLSAFECYBERSEC\FRONT-DESK-PC   SHARING
10.1.1.21       ALLSAFECYBERSEC\GIDEON-PC       SHARING
```

Answer: 10.1.1.2

Task 13:
Machine:Target1 What is the full IP address and the port was the attacker's malware using?

I used the netscan plugin and checked for the iexplorer.exe file

```
0x3e0eedf8          TCPv4    10.1.1.20:49205                 180.76.254.120:22    ESTABLISHED      2996     iexplore.exe
```

Answer: 180.76.254.120:22

Task 14:
Machine:Target1 It appears the attacker also installed legit remote administration software. What is the name of the running process?

Saw it several times already, the pslist plugin will show it

```
0x84013598 TeamViewer.exe          2680   1696     28      632      1      0 2015-10-09 12:08:46 UTC+0000
0x84017d40 tv_w32.exe              4064   2680      2       83      1      0 2015-10-09 12:08:47 UTC+0000
0x858bc278 TeamViewer_Des          1092   2680     16      405      1      0 2015-10-09 12:10:56 UTC+0000
```

Answer: teamviewer.exe

Task 15:
Machine:Target1 It appears the attackers also used a built-in remote access method. What IP address did they connect to?

I used netscan and saw he mstsc process

```
0x3fb7a560          TCPv4    10.1.1.20:49301                 10.1.1.21:3389       ESTABLISHED      2844     mstsc.exe
```

Answer: 10.1.1.20

Task 16:
Machine:Target2 It appears the attacker moved latterly from the front desk machine to the security admins (Gideon) machine and dumped the passwords. What is Gideon's password?

First I used the hashdump and tried to crack the password with crackstation and also with John The Ripper and HashCat with no success.
Then I dumped the mstsc process and used handles and strings and found nothing.
After that I used the console plugin again after found the last password there and once again I saw the attacker used wce.exe

> Windows Credentials Editor (WCE) is a security tool that allows to list Windows logon sessions and add, change, list and delete associated credentials (e.g.: LM/NT hashes, Kerberos tickets and cleartext passwords). The tool allows users to: - Perform Pass-the-Hash on Windows.

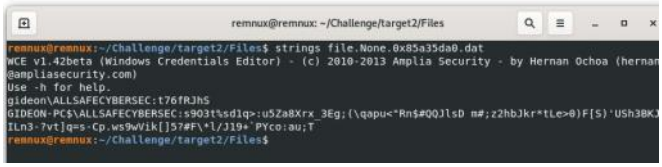
```
CommandHistory: 0xe9198 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 18 LastAdded: 17 LastDisplayed: 17
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
Cmd #0 at 0xe6030: cd C:\Users
Cmd #1 at 0xe6ea8: dir
Cmd #2 at 0xee3d0: wce.exe -w > gideon/w.tmp
Cmd #3 at 0xe0170: who ami
Cmd #4 at 0xe0188: whoami
Cmd #5 at 0xea3c8: net use z: \\10.1.1.2\c$
Cmd #6 at 0xe01b8: cd z:
Cmd #7 at 0xe6ed8: dir
Cmd #8 at 0xe6070: cd gideon
Cmd #9 at 0xe6ef8: dir
Cmd #10 at 0xe6f08: z:
Cmd #11 at 0xe6f18: dir
Cmd #12 at 0xf2418: copy c:\users\gideon\rar.exe z:\crownjewels
Cmd #13 at 0xe0cb8: cd crownjewels
Cmd #14 at 0xe6f28: dir
Cmd #15 at 0xe6f38: rar
Cmd #16 at 0xf2478: rar crownjewlez.rar *.txt -hp123qwe!@#
Cmd #17 at 0xf24d0: rar a -hp123!@#qwe crownjewlez.rar *.txt
```

I saw the user used the wce.exe and saved it as w.tmp so I used filescan and then dumped it

```
remnux@remnux:~/volatility$ python2 vol.py -f '/home/remnux/Challenge/target2/target2-6186fe9f.vmss' --profile=Win7SP1x86_23418 filescan | grep -i w.tmp
Volatility Foundation Volatility Framework 2.6.1
0x000000003fcf2798      8      0 -W-r-- \Device\HarddiskVolume2\Users\gideon\w.tmp
remnux@remnux:~/volatility$ python2 vol.py -f '/home/remnux/Challenge/target2/target2-6186fe9f.vmss' --profile=Win7SP1x86_23418 dumpfiles -Q 0x000000003fcf2798 -D '/home/remnux/Challenge/target2/Files'
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x3fcf2798   None   \Device\HarddiskVolume2\Users\gideon\w.tmp
```

Then I used strings on it

file.None.
0x85a35da0.dat



Answer: t76fRJhS

Task 17:
Machine:Target2 Once the attacker gained access to "Gideon," they pivoted to the AllSafeCyberSec domain controller to steal files. It appears they were successful. What password did they use?

Same like task 16, I saw it on the consoles plugin

```
Cmd #12 at 0xf2418: copy c:\users\gideon\rar.exe z:\crownjewels
Cmd #13 at 0xe0cb8: cd crownjewels
Cmd #14 at 0xe6f28: dir
Cmd #15 at 0xe6f38: rar
Cmd #16 at 0xf2478: rar crownjewlez.rar *.txt -hp123qwe!@#
Cmd #17 at 0xf24d0: rar a -hp123!@#qwe crownjewlez.rar *.txt
```

Answer: 123qwe!@#

Task 18:
Machine:Target2 What was the name of the RAR file created by the attackers?

Same as previous task

```
Cmd #12 at 0xf2418: copy c:\users\gideon\rar.exe z:\crownjewels
Cmd #13 at 0xe0cb8: cd crownjewels
Cmd #14 at 0xe6f28: dir
Cmd #15 at 0xe6f38: rar
Cmd #16 at 0xf2478: rar crownjewlez.rar *.txt -hp123qwe!@#
Cmd #17 at 0xf24d0: rar a -hp123!@#qwe crownjewlez.rar *.txt
```

Answer: crownjewlez.rar

Task 19:
Machine:Target2 How many files did the attacker add to the RAR archive?

This task took me forever to complete
First I tried somehow to view the contents inside the Z: folder with R-Studio.
Then I tried to search for the crownjewels directory
I tried to use handles and I dump all the cmd process memories and used strings but nothing was found.
I did a lot of more things I can't even remember.

Then I checked the commands again and observed that the $process initiating everything was conhost.exe with PID of 3048

```
CommandProcess: conhost.exe Pid: 3048
CommandHistory: 0xe9198 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 18 LastAdded: 17 LastDisplayed: 17
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
Cmd #0 @ 0xe6030: cd C:\Users
Cmd #1 @ 0xe6ea8: dir
Cmd #2 @ 0xee3d0: wce.exe -w > gideon/w.tmp
Cmd #3 @ 0xe0170: who ami
Cmd #4 @ 0xe0188: whoami
Cmd #5 @ 0xea3c8: net use z: \\10.1.1.2\c$
Cmd #6 @ 0xe01b8: cd z:
Cmd #7 @ 0xe6ed8: dir
Cmd #8 @ 0xe6070: cd gideon
Cmd #9 @ 0xe6ef8: dir
Cmd #10 @ 0xe6f08: z:
Cmd #11 @ 0xe6f18: dir
Cmd #12 @ 0xf2418: copy c:\users\gideon\rar.exe z:\crownjewels
Cmd #13 @ 0xe0cb8: cd crownjewels
Cmd #14 @ 0xe6f28: dir
Cmd #15 @ 0xe6f38: rar
Cmd #16 @ 0xf2478: rar crownjewlez.rar *.txt -hp123qwe!@#
Cmd #17 @ 0xf24d0: rar a -hp123!@#qwe crownjewlez.rar *.txt
Cmd #36 @ 0xb00c4: ??
                   ???
```

I dumped the process and used strings on it but still didn't found nothing.

My last way before watching the walkthrough was to used strings on the target2 memory dump file and used grep for crownjewel.
Then I noticed some suspicious filename "SecretSauce2.txt" and also the command with the password - hp123qwe!@# and at the bottom more files with the name of SecretSauce.
In general from the output there was 3 files SecretSauce1.txt 2 and 3 so I assumed the answer will be 3

Answer: 3

Task 20:
Machine:Target2 The attacker appears to have created a scheduled task on Gideon's machine. What is the name of the file associated with the scheduled task?

First I tried to use the printkey on the 2 registry known path's but it didn't worked.
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks

Then I tried to view the Tasks directory in System32 but nothing found.

So I used the filescan and grepped for taskscheduler and dumped the files

```
remnux@remnux:~/volatility$ python2 vol.py -f '/home/remnux/Challenge/target2/target2-6186fe9f.vmss' --profile=Win7SP1x86_23418 filescan | grep -i taskscheduler
Volatility Foundation Volatility Framework 2.6.1
0x000000003e00d270      1      1 RW-r-- \Device\HarddiskVolume2\Windows\System32\winevt\Logs\Microsoft-Windows-TaskScheduler%4Operational.evtx
^C
remnux@remnux:~/volatility$ ^C
remnux@remnux:~/volatility$ python2 vol.py -f '/home/remnux/Challenge/target2/target2-6186fe9f.vmss' --profile=Win7SP1x86_23418 dumpfiles -Q 0x000000003e00d270 -D '/home/remnux/Challenge/target2'
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x3e00d270   None   \Device\HarddiskVolume2\Windows\System32\winevt\Logs\Microsoft-Windows-TaskScheduler%4Operational.evtx
SharedCacheMap 0x3e00d270   None   \Device\HarddiskVolume2\Windows\System32\winevt\Logs\Microsoft-Windows-TaskScheduler%4Operational.evtx
```

I changed the extensions to evtx from dat and tried to open it with Log Explorer but its was not worked so I used strings and analyzed it until I saw suspicious file

```
Microsoft-Windows-TaskScheduler
Microsoft-Windows-TaskScheduler/Operational
\At1
ALLSAFECYBERSEC\GIDEON-PC$
O=cO
gr&
O=cO
Microsoft-Windows-TaskScheduler
Microsoft-Windows-TaskScheduler/Operational
\At1
c:\users\gideon\1.bat
O=cO
gr&
O=cO
Microsoft-Windows-TaskScheduler
Microsoft-Windows-TaskScheduler/Operational
\At1
C:\Windows\SYSTEM32\cmd.exe
```

Answer: 1.bat

Task 21:
Machine:POS What is the malware CNC's server?

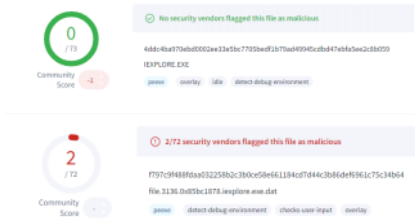
I used the netscan plugin and noticed the iexplorer.exe process with an external IP

```
0x3e135df8         TCPv4    10.1.1.10:58751                54.84.237.92:80      CLOSE_WAIT      3208     iexplore.exe
```

Answer: 54.84.237.92

Task 22:
Machine:POS What is the common name of the malware used to infect the POS system?

Because the iexplore.exe was the process that initiated the C2 IP from task 21 I used pstree and noticed there is 2 processes with the same name and path but with different PID 3208 and 3136.
I dumped both files and checked the MDS hash on Virus Total, one file is clean and the other reported only 2 times with no details.



I tried to use strings on the files but nothing was found.
Then I also tried to dump the memory of the processes and used strings and saw the C2 IP and and a weird filename called "allsafe_protector.exe", after I checked the next tasks this file was the answer for the next task 23.

```
!This program cannot be run in DOS mode.
Rich
.text
.data
.idata
@.rsrc
@.reloc
allsafe_protector.exe
svchost.exe
iexplore.exe
explorer.exe
System
smss.exe
csrss.exe
winlogon.exe
lsass.exe
spoolsv.exe
ship.exe
wuauclt.exe
ABCDEFGHIKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
SeDebugPrivilege
NtQueryInformationProcess
NTDLL.DLL
54.84.237.92
gateway.php
GetNativeSystemInfo
kernel32.dll
```

After analyzing the strings I did not find anything but I was sure this file is the one I need.

I tried to do more several things even from R-Studio and dumped the file also from filescan and not only from PID but nothing worked.

Then I used the malfind plugin and its was showing the iexplore.exe process again but it doesn't had too much details

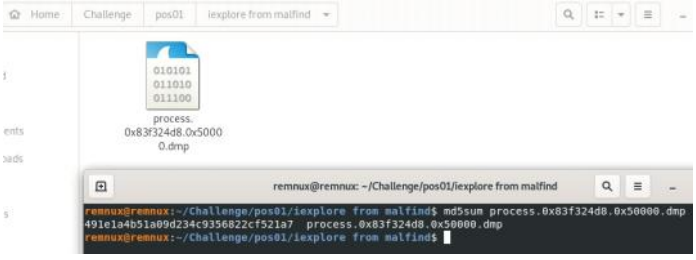
```
Process: iexplore.exe Pid: 3208 Address: 0x50000
Vad Tag: Vad5 Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 11, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x0000000000050000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00   MZ..............
0x0000000000050010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ........@.......
0x0000000000050020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x0000000000050030  00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00   ................

0x0000000000050000 4d              DEC EBP
0x0000000000050001 5a              POP EDX
0x0000000000050002 90              NOP
0x0000000000050003 0003            ADD [EBX], AL
0x0000000000050005 0000            ADD [EAX], AL
0x0000000000050007 000400          ADD [EAX+EAX], AL
0x000000000005000a 0000            ADD [EAX], AL
0x000000000005000c ff              DB 0xff
0x000000000005000d ff00            INC DWORD [EAX]
0x000000000005000f 00b000000000    ADD [EAX+0x0], DH
0x0000000000050015 0000            ADD [EAX], AL
0x0000000000050017 004000          ADD [EAX+0x0], AL
0x000000000005001a 0000            ADD [EAX], AL
0x000000000005001c 0000            ADD [EAX], AL
0x000000000005001e 0000            ADD [EAX], AL
0x0000000000050020 0000            ADD [EAX], AL
0x0000000000050022 0000            ADD [EAX], AL
0x0000000000050024 0000            ADD [EAX], AL
0x0000000000050026 0000            ADD [EAX], AL
0x0000000000050028 0000            ADD [EAX], AL
0x000000000005002a 0000            ADD [EAX], AL
0x000000000005002c 0000            ADD [EAX], AL
0x000000000005002e 0000            ADD [EAX], AL
0x0000000000050030 0000            ADD [EAX], AL
0x0000000000050032 0000            ADD [EAX], AL
0x0000000000050034 0000            ADD [EAX], AL
0x0000000000050036 0000            ADD [EAX], AL
0x0000000000050038 0000            ADD [EAX], AL
0x000000000005003a 0000            ADD [EAX], AL
0x000000000005003c d800            FADD DWORD [EAX]
0x000000000005003e 0000            ADD [EAX], AL

Process: iexplore.exe Pid: 3136 Address: 0x50000
Vad Tag: Vad5 Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 11, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x0000000000050000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00   MZ..............
0x0000000000050010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ........@.......
0x0000000000050020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x0000000000050030  00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00   ................
```

Then I checked the malfind -h to see if there is something I can use with this process and I noticed that there is an options to dump the process so I dumped it once again

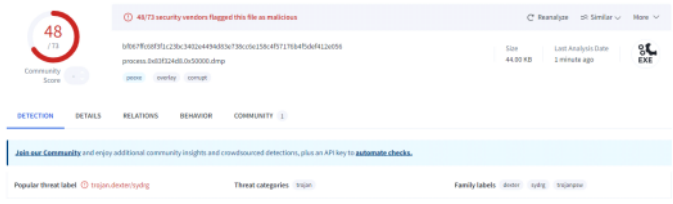
```
                      EPROCESS offset (hex) in the physical address space
-p PID, --pid=PID     Operate on these Process IDs (comma-separated)
-n NAME, --name=NAME  Operate on these process names (regex)
-D DUMP_DIR, --dump-dir=DUMP_DIR
                      Directory in which to dump the VAD files
```

```
remnux@remnux:~/volatility$ python2 vol.py -f '/home/remnux/Challenge/pos01/POS-01-c4e8f706.vmss' --profile=Win7SP1x86_23418 malfind -p 3208 -D '/home/remnux/Challenge/pos01/iexplore from malfind'
Volatility Foundation Volatility Framework 2.6.1
Process: iexplore.exe Pid: 3208 Address: 0x50000
Vad Tag: Vad5 Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 11, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x0000000000050000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00   MZ..............
0x0000000000050010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ........@.......
0x0000000000050020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x0000000000050030  00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00   ................

0x0000000000050000 4d              DEC EBP
0x0000000000050001 5a              POP EDX
0x0000000000050002 90              NOP
0x0000000000050003 0003            ADD [EBX], AL
0x0000000000050005 0000            ADD [EAX], AL
0x0000000000050007 000400          ADD [EAX+EAX], AL
0x000000000005000a 0000            ADD [EAX], AL
0x000000000005000c ff              DB 0xff
0x000000000005000d ff00            INC DWORD [EAX]
0x000000000005000f 00b000000000    ADD [EAX+0x0], DH
0x0000000000050015 0000            ADD [EAX], AL
0x0000000000050017 004000          ADD [EAX+0x0], AL
0x000000000005001a 0000            ADD [EAX], AL
0x000000000005001c 0000            ADD [EAX], AL
0x000000000005001e 0000            ADD [EAX], AL
0x0000000000050020 0000            ADD [EAX], AL
0x0000000000050022 0000            ADD [EAX], AL
0x0000000000050024 0000            ADD [EAX], AL
0x0000000000050026 0000            ADD [EAX], AL
0x0000000000050028 0000            ADD [EAX], AL
0x000000000005002a 0000            ADD [EAX], AL
0x000000000005002c 0000            ADD [EAX], AL
0x000000000005002e 0000            ADD [EAX], AL
0x0000000000050030 0000            ADD [EAX], AL
0x0000000000050032 0000            ADD [EAX], AL
0x0000000000050034 0000            ADD [EAX], AL
0x0000000000050036 0000            ADD [EAX], AL
0x0000000000050038 0000            ADD [EAX], AL
0x000000000005003a 0000            ADD [EAX], AL
0x000000000005003c d800            FADD DWORD [EAX]
0x000000000005003e 0000            ADD [EAX], AL
```

Then I checked the MD5 of the process



I checked the MD5 on Virus Total and suddenly this hash was highly reported



The popular threat label flagged this malware as "dexter"

Answer: dexter

Task 23:
Machine:POS In the POS malware whitelist. What application was specific to Allsafecybersec?

I found the answer while searching the answer for task 22

!This program cannot be run in DOS mode.
Rich
.text
.data
.idata
@.rsrc
@.reloc
allsafe_protector.exe
svchost.exe
iexplore.exe
explorer.exe
System
smss.exe
csrss.exe
winlogon.exe
lsass.exe
spoolsv.exe
alg.exe
wuauclt.exe
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
SeDebugPrivilege
NtQueryInformationProcess
NTDLL.DLL
54.84.237.92
gateway.php
GetNativeSystemInfo
kernel32.dll

Answer: allsafe_protector.exe

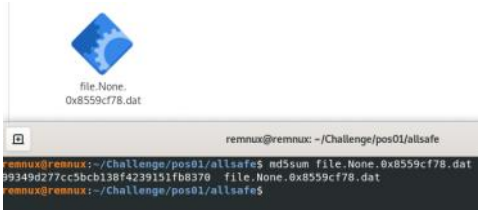
Task 24:
Machine:POS What is the name of the file the malware was initially launched from?

Took me some time to complete this task.
I was searching the folders in the Administrator user with R-Studio and noticed that on his Desktop
there is several files that's start with "Allsafe"

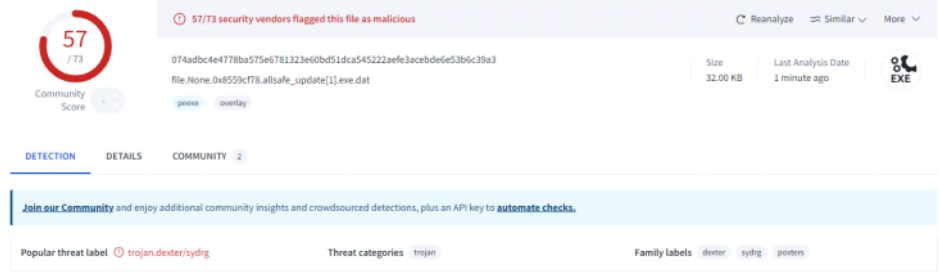
I retrieved the files and view the contents but nothing was found there.

The question for the previous task 23 was also started with allsafe and by looking at the answer format
it was also looked like the start of the file allsafe.
I used the filescan and grepped for allsafe and found some exe file starting with allsafe name so I
dumped it and took his MD5 hash - 99349d277cc5bcb138f4239151fb8370

```
remnux@remnux:~/volatility$ python2 vol.py -f '/home/remnux/Challenge/pos01/POS-01-c4e8f786.vmss' --profile=Win7SP1x86_23418 filescan | grep -i allsafe
Volatility Foundation Volatility Framework 2.6.1
0x000000003e03ea40      1      1 RW-r-- \Device\HarddiskVolume2\Users\Administrator\Desktop\AllSafeCustomerData.csv
0x000000003e5f9f80      1      1 RW-r-- \Device\HarddiskVolume2\Users\Administrator\Desktop\AllSafeCustomerData.txt
0x000000003e6f9bc0     14      6 RW-r-- \Device\HarddiskVolume2\Users\pos\AppData\Local\Microsoft\Outlook\pos@allsafecybersec.com.ost
0x000000003e7ab038      8      0 -W-rwd \Device\HarddiskVolume2\Users\pos\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\NEQ2CLDX\allsafe_update[1].exe
0x000000003ecf1280      6      1 RW-rw- \Device\HarddiskVolume2\Users\pos\AppData\Local\Microsoft\Outlook\~pos@allsafecybersec.com.ost.tmp
0x000000003fc9ff80      5      0 RW-r-- \Device\HarddiskVolume2\Users\pos\AppData\Local\Microsoft\Outlook\pos@allsafecybersec.com.ost
0x000000003fd56038      1      1 R--rw- \Device\HarddiskVolume2\Users\Administrator\Desktop\AllSafeCustomerData.txt
0x000000003fd8cc30      8      0 RW-rw- \Device\HarddiskVolume2\Users\Administrator\Desktop\AllSafeCustomerData.csv
0x000000003fda7ee8      8      0 RW-r-- \Device\HarddiskVolume2\Users\Administrator\Desktop\AllSafeCusto
0x000000003fdd7f80      2      1 R--rw- \Device\HarddiskVolume2\Users\Administrator\Desktop\AllSafeCustomerData.txt
remnux@remnux:~/volatility$ python2 vol.py -f '/home/remnux/Challenge/pos01/POS-01-c4e8f786.vmss' --profile=Win7SP1x86_23418 dumpfiles -Q 0x000000003e7ab038 -D '/home/remnux/Challenge/pos01/allsafe'
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x3e7ab038   None   \Device\HarddiskVolume2\Users\pos\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\NEQ2CLDX\allsafe_update[1].exe
```



The file was highly reported and also known as "dexter"



So I assumed the answer is the exe filename

Answer: allsafe_update.exe