

# ROOT-ME - Command & Control niveau 3

On cherche dans le dump mémoire un programme malveillant, le mot de passe est le hash du chemien absolu vers l'executable.

## Lister les processus

J'utilise Volatility et la commande suivante:

```
> volatility -f ch2.dmp --profile=Win7SP1x86_23418 pstree
```

.. 0x9542a030:TPAutoConnSvc.	1612	560	9	135	2013-01-12	16:39:23	UTC+0000
... 0x87ae2880:TPAutoConnect.	2568	1612	5	146	2013-01-12	16:40:28	UTC+0000
.. 0x88cded40:sppsvc.exe	1872	560	4	143	2013-01-12	16:39:02	UTC+0000
.. 0x8a102748:svchost.exe	1748	560	18	310	2013-01-12	16:38:58	UTC+0000
.. 0x8a0f9c40:spoolsv.exe	1712	560	14	338	2013-01-12	16:38:58	UTC+0000
.. 0x9541c7e0:wlmcs.exe	336	560	4	45	2013-01-12	16:39:21	UTC+0000
.. 0x8a1f5030:VMUpgradeHelpe	448	560	4	89	2013-01-12	16:39:21	UTC+0000
... 0x892ced40:winlogon.exe	500	448	3	111	2013-01-12	16:38:14	UTC+0000
... 0x88d03a00:csrss.exe	468	448	10	471	2013-01-12	16:38:14	UTC+0000
... 0x87c595b0:conhost.exe	3228	468	2	54	2013-01-12	16:44:50	UTC+0000
... 0x87a9c288:conhost.exe	2600	468	1	35	2013-01-12	16:40:28	UTC+0000
... 0x954826b0:conhost.exe	2168	468	2	49	2013-01-12	16:55:50	UTC+0000
.. 0x87bd35b8:wmpnetwk.exe	3176	560	9	240	2013-01-12	16:40:48	UTC+0000
.. 0x87ac0620:taskhost.exe	2352	560	8	149	2013-01-12	16:40:24	UTC+0000
.. 0x897b5c20:svchost.exe	764	560	7	263	2013-01-12	16:38:23	UTC+0000
.. 0x8962f7e8:lsm.exe	584	456	10	142	2013-01-12	16:38:16	UTC+0000
.. 0x896427b8:lsass.exe	576	456	6	566	2013-01-12	16:38:16	UTC+0000
.. 0x8929fd40:csrss.exe	404	396	9	469	2013-01-12	16:38:14	UTC+0000
.. 0x87978b78:System	4	0	103	3257	2013-01-12	16:38:09	UTC+0000
.. 0x88c3ed40:smss.exe	308	4	2	29	2013-01-12	16:38:09	UTC+0000
.. 0x87ac6030:explorer.exe	2548	2484	24	766	2013-01-12	16:40:27	UTC+0000
.. 0x87b6b030:iexplore.exe	2772	2548	2	74	2013-01-12	16:40:34	UTC+0000
.. 0x89898030:cmd.exe	1616	2772	2	101	2013-01-12	16:55:49	UTC+0000
.. 0x95495c18:taskmgr.exe	1232	2548	6	116	2013-01-12	16:42:29	UTC+0000
.. 0x87bf7030:cmd.exe	3152	2548	1	23	2013-01-12	16:44:50	UTC+0000
.. 0x87cbfd40:winpmem-1.3.1.	3144	3152	1	23	2013-01-12	16:59:17	UTC+0000
.. 0x898fe8c0:StikyNot.exe	2744	2548	8	135	2013-01-12	16:40:32	UTC+0000
.. 0x87b784b0:AvastUI.exe	2720	2548	14	220	2013-01-12	16:40:31	UTC+0000
.. 0x87b82438:VMwareTray.exe	2660	2548	5	80	2013-01-12	16:40:29	UTC+0000
.. 0x87c6a2a0:swriter.exe	3452	2548	1	19	2013-01-12	16:41:01	UTC+0000
.. 0x87ba4030:soffice.exe	3512	3452	1	28	2013-01-12	16:41:03	UTC+0000
... 0x87b8ca58:soffice.bin	3564	3512	12	400	2013-01-12	16:41:05	UTC+0000
.. 0x9549f678:iexplore.exe	1136	2548	18	454	2013-01-12	16:57:44	UTC+0000
.. 0x87d4d338:iexplore.exe	3044	1136	37	937	2013-01-12	16:57:46	UTC+0000
.. 0x87aa9220:VMwareUser.exe	2676	2548	8	190	2013-01-12	16:40:30	UTC+0000
.. 0x95483d18:soffice.bin	3556	3544	0	-----	2013-01-12	16:41:05	UTC+0000

On remarque sur la figure précédente qu'il y a 2 processus iexplore.exe d'ouvert c'est l'executable d'Internet Explorer en général, mais on remarque également que l'un d'entre eux execute un processus cmd.exe relatif à l'execution d'un terminal sous Windows.

.. 0x87b6b030:iexplore.exe	2772	2548	2	74	2013-01-12	16:40:34	UTC+0000
.. 0x89898030:cmd.exe	1616	2772	2	101	2013-01-12	16:55:49	UTC+0000

Je vais regarder sur le pid 2772 le chemin absolu le fichier lancé grâce à la commande cmdline.

```
.../IUT/SAE-ROOTME/ch3
> volatility -f ch2.dmp --profile=Win7SP1x86_23418 cmdline -p 2772
Volatility Foundation Volatility Framework 2.6
*****
iexplore.exe pid: 2772
Command line : "C:\Users\John Doe\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\iexplore.exe"
```

Je compare avec le chemin de l'autre processus iexplore.exe (PID 1136)

```
.../IUT/SAE-ROOTME/ch3
> volatility -f ch2.dmp --profile=Win7SP1x86_23418 cmdline -p 1136
Volatility Foundation Volatility Framework 2.6
*****
iexplore.exe pid: 1136
Command line : "C:\Program Files\Internet Explorer\iexplore.exe"
```

Ce fichier semble être le vrai internet explorer installé dans le répertoire usuel des programmes windows.

On peut également regarder l'historique des commandes utilisés avec le modules consoles de Volatility:

```
*****
ConsoleProcess: conhost.exe Pid: 2168
Console: 0x1081c0 CommandHistorySize: 50
HistoryBufferCount: 3 HistoryBufferMax: 4
OriginalTitle: %SystemRoot%\system32\cmd.exe
Title: C:\Windows\system32\cmd.exe
AttachedProcess: cmd.exe Pid: 1616 Handle: 0x64
----
CommandHistory: 0x427a60 Application: tcprelay.exe Flags:
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x0
----
CommandHistory: 0x427890 Application: whoami.exe Flags:
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x0
----
CommandHistory: 0x427700 Application: cmd.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x64
----
Screen 0x416348 X:80 Y:300
Dump:
```

On remarque que le processus cmd.exe au PID 1616 qui est exécuté par le processus 2772 ouvre un programme tcprelay.exe qui est sûrement suspicieux au point de peut-être ouvrir une backdoor ?

Le programme malveillant est donc celui au PID 2772 se trouvant ici: `C:\Users\John Doe\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\iexplore.exe`

# MD5 Hash Generator

Use this generator to create an MD5 hash of a string:

C:\Users\John Doe\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\iexplore.exe

Generate →

Your String	C:\Users\John Doe\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\iexplore.exe	
MD5 Hash	49979149632639432397b3a1df8cb43d	Copy

On récupérer le hash du chemin Absolu du fichier. Le mot de passe du challenge est donc 49979149632639432397b3a1df8cb43d.