DIGITAL FORENSICS

La *memory forensics*, ossia le indagini sul contenuto della memoria RAM di un dispositivo digitale come un computer, rappresentano una materia abbastanza complessa, infatti occorre conoscere molto bene come funzionano i processi ed il sistema operativo, al fine di comprendere cosa è in esecuzione e quali file sono coinvolti.

In quest'articolo si tratterà un piccolo esempio di "*malware hunting*" (caccia al malware) per illustrare come con degli strumenti open source ed online, si può trovare il software maligno che infesta un computer, chiaramente è un percorso semplice per fini descrittivi e didattici, dato che scovare i malware e le loro varie declinazioni spesso è molto più complicato.

di Nanni Bassetti UN ESEMPIO PRATICO DI MEMORY FORENSICS CON L'OPEN SOURCE



Nanni BASSETTI è laureato in Scienze dell'Informazione, libero professionista specializzato in digital forensics, fondatore di CFI (Computer Forensics Italy) e project manager di CAINE Linux/GNU Live distro per indagini informatiche. Docente, relatore in parecchi corsi ed eventi, autore di molti articoli tecnici e di un paio di libri.

1. Introduzione

Di seguito vengono descritti i passaggi operativi che occorre effettuare per il "*malware hunting*", iniziando con il download del file immagine di una RAM che appartiene ad un computer compromesso da un noto malware, in questo caso si tratta del "vecchio" SpyEye:

https://code.google.com/archive/p/volatility/wikis/SampleMemoryImages.wiki

ATTENZIONE i file contengono veramente il malware, quindi operate in ambiente di test a vostro rischio.

Il file in questione è: **spyeye.vmem (512Mb).** Il percorso operativo sarà così composto:

- 1. Cerchiamo le connessioni in esecuzione.
- 2. Cerchiamo i processi che le creano.
- 3. Cerchiamo il malware iniettato nel processo.
- 4. Estraiamo il malware.
- 5. Lo controlliamo su https://virustotal.com/.
- 6. Estraiamo le stringhe contenute nel malware al fine di cercare la chiave di registro che lo manda in esecuzione.
- 7. Analizziamo la chiave di registro per trovare qual'è il file eseguibile e dov'è allocato nel computer.

I programmi utilizzati saranno:

- ✤ OS CAINE 8.0
- * Volatility Framework 2.5
- ✤ VirusTotal.com
- * Strings

2. Procedura operativa

PASSO 1: Cerchiamo le connessioni in esecuzione

volatility -f spyeye.vmem connscan

🗌 root@caine: /media/w	in/test (as superu	ser)			_ = ×
File Edit View Search	n Terminal Help				
root@caine:/media/w [:] Volatility Foundatio	in/test# volati on Volatility R	ility -f spyey Framework 2.5	e.vmem conn	iscan	-
Offset(P) Local Address		Remote Add	lress	Pid	
0x01eacc00 192.168.	16.129:1039	65.55.	:443	1068	
0x01fd3170 192.168.3	16.129:1040	207.46.	: 80	1068	
		Figura 1			

Troviamo la connessione all'indirizzo IP 65.55.xxx.xxx sulla porta 443 ID del Processo: 1068 (figura 1). Troviamo la connessione all'indirizzo IP 207.46.xxx.xxx sulla porta 80 ID del Processo: 1068 (figura 1).

PASSO 2: Cerchiamo i processi che le creano

volatility -f spyeye.vmem pslist

🗖 root@caine: /media/win/test (as supe	ruser) 📲	10					- = ×
File Edit View Search Terminal H	elp						
root@caine:/media/win/test# vol Volatility Foundation Volatilit	atility · y Framewo	-f spyeye ork 2.5	e.vmem p	oslist g	гер 1068		-
0x822a0758 svchost.exe -11-11 22:02:17 UTC+0000	1068	704	58	1256	Θ	0	2010
0x8236d7a0 wuauclt.exe -11-11 22:03:33 UTC+0000	536	1068	4	107	Θ	0	2010
0x82389020 wscntfy.exe -11-11 22:03:56 UTC+0000	2772	1068	2	29	Θ	Θ	2010
	Fig	jura 2					

Scopriamo che il processo è: 0x822a0758 svchost.exe 1068 (figura 2).

SVCHOST è un esecutore di servizi, per dirla in maniera semplice ed è normale che sia in esecuzione.

PASSO 3: Cerchiamo il malware iniettato nel processo sospetto

volatility -f spyeye.vmem malfind -p 1068



Figura 3

Il -p 1068 serve per indicare il processo numerato come 1068 ossia SVCHOST (figura 3).

Notiamo che il plugin malfind di Volatility trova all'indirizzo 0xea50000 un file eseguibile, perchè inizia con "MZ", la tipica sequenza di caratteri con la quale iniziano tutti i file EXE.

Inoltre notiamo che la VADS PROTECTION è PAGE_EXECUTE_READWRITE, ossia il Virtual Address Descriptor, che rappresenta ciascun file presente in memoria e sul disco, è eseguibile (EXECUTE).

Abbiamo chiesto a Volatility di estrarre il nodo VAD che inizia all'indirizzo 0xea50000 e salvarlo nella directory /home/caine/ dump, il software l'ha nominato automaticamente in **svchost.exe.22a0758.0x0ea50000-0x0ea7dfff.dmp** (figura 4).

DIGITAL FORENSICS



PASSO 5: Controlliamo il file su VirusTotal.com

Carichiamo il file **svchost.exe.22a0758.0x0ea50000-0x0ea7dfff.dmp** su **VirusTotal.com**, un grande meta-motore di ricerca che invia il file a vari scanner antivirus ed otteniamo il riconoscimento del tipo di malware (figura 5).

PASSO 6: Estraiamo le stringhe contenute nel malware al fine di cercare la chiave di registro che lo manda in esecuzione strings svchost.exe.22a0758.0x0ea50000-0x0ea7dfff.dmp > strings.txt

Osservando le stringhe estratte possiamo trovare molte informazioni, come il nome del file eseguibile e la chiave di registro di Windows che lo manda *in running* (figura 6).

PASSO 7: Individuiamo il file

volatility -f spyeye.vmem printkey -K "SOFTWARE\
MICROSOFT\WINDOWS\CURRENTVERSION\RUN"
Volatility Foundation Volatility Framework 2.5
Legend: (S) = Stable (V) = Volatile

REG_SZ cleansweep.exe : (S) C:\cleansweep.exe\
cleansweep.exe

Abbiamo scovato il "cattivone"! Si trova in C:\cleansweep.exe\ cleansweep.exe e così possiamo andarlo a prendere e cancellarlo o analizzarlo, ecc.

3. Conclusioni

È sempre emozionante usare gli strumenti a "basso livello", ossia senza troppi automatismi ed interfacce grafiche, perché sembra proprio di scavare nelle informazioni digitali e capire meglio come sono organizzate, ma ricordiamo che il presente articolo è utile solo per dare un esempio veloce e comprensibile di come si possa fare della "memory" e "malware forensics", che forse sono le branche più ostiche di tutta la digital forensics, poiché comportano conoscenze veramente approfondite dei sistemi, delle reti, del reverse engineering anche in Assembly, pertanto a chi vuole approcciare questi temi, non ci resta che augurare buona caccia!

<pre>strings_asci.txt (/home/caine/dump) - Pluma (as superuser) *** File Edit View Search Tools Documents Help Strings_asci.txt * Strings_asci.tx</pre>								
<pre>File Edit View Search Tools Documents Help File Edit Clear Search Tools Documents Help File Edit Tools Documents File Edit Tools Documents File Edit Tools Documents File Edit Tools Tools Documents File Edit Edit Tools Documents File Edit Edit Edit Edit Edit File Edit Edit Edit Edit Edit Edit Edit Edit</pre>	strings_ascii.txt (/home/caine/dump) - Pluma (as superuser)							
Image: Open v Factor in the second	File Edit View Search Tools Documents Help							
<pre>strings_ascil.txt ** 994 LocalFree 995 InterlockedIncrement 996 lstrcmpW 997 PostMessageA 998 GetCursorPos 999 IsWindowUnicode 1000 GetWindowLongA 1001 IsWindow 1002 SetWindowLongA 1003 GetClientRect 1004 CoTaskMemAlloc 1005 _wcsnicmp 1006 SE9063A019482A8D172568655C83D0C2 1007 [A::8 1008 GOTMARE/MICROSOFT/WINDOWS/CURRENTVERSION/RUM 1019 System 1010 smss.exe 1016 ''UU 1017 Cleansweepud.exe 1016 ''UU 1022 S;uD 1023 z?auY 1024 D?\$? 1025 S;uC 1025 S;uC 1025 S;uC 1025 S;uC 1026 Z;uC 1027 ::3g</pre>	🗄 🛅 Open 🔻 🐺 Save 📲 🗠 Undo 🖙 🐰 📮 🛍							
994 LocalFree 995 InterlockedIncrement 996 IstrcmpW 997 PostMessageA 998 GetCursorPos 999 IsWindowUnicode 1000 GetWindowLongA 1001 IsWindow 1002 SetWindowLongA 1003 GetClientRect 1004 CoTasKMemAlloc 1005 _wcsnicmp 1006 SE9D63A019482A8D172568655C83D0C2 1007 [A::8 1008 SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN 1009 System 1010 smss.exe 1011 csrss.exe 1011 csrss.exe 1012 NtOpenProcess 1013 config.dat 1014 config.dat 1015 cleansweep.exe 1015 cleansweep.exe 1018 MV5 1019 HMX8 1020 72d; 1021 7/L[1022 S;uD 1023 z?aUY 1024 D?S? 1025 U>C{ 1025 CE 1025 U>C{ 1026 ZcXC1 1027 .:3q Figura 6	🖹 strings ascii.txt 🕷							
994 LocalFree 995 InterlockedIncrement 996 StrcmpW 997 PostMessageA 998 GetCursorPos 999 IsWindowLongA 1001 IsWindow 1002 SetWindowLongA 1003 GetClientRect 1004 CoTaskMemAlloc 1005 _wcsnicmp 1006 SE9D63A019482A8D172568655C83D0C2 1007 [A::8 1008 SOFTWARELMICROSOFT\WINDOWS\CURRENTVERSION\RUN 1009 System 1010 smss.exe 1012 orfig.bin 1013 config.bin 1014 config.dat 1015 cleansweepupd.exe 1018 KU'9 1019 HMXB 1020 72d; 1021 7/L[1022 S;uD 1023 z7aUY 1024 D?S? 1025 U>C{ 1025 U>C{ 1026 zCKc1 1027 .:3g Figura 6								
<pre>996 lstrompW 997 PostMessageA 998 GetCursorPos 999 IsWindowUnicode 1000 GetWindowLongA 1001 IsWindowUnicode 1000 GetWindowLongA 1003 GetClientRect 1004 CoTaskMemAlloc 1005 wcsnicmp 1006 SE9D63A019482A8D172568655C83D0C2 1007 [A::8 1008 SOFTWARELVIICROSOFT/WINDOWS/CURRENTVERSION/RUN 1009 System 1010 Smss.exe 1012 NtOpenProcess 1013 config.bin 1015 cleansweepupd.exe 1016 ''UU 1017 cleansweepupd.exe 1018 kU'9 1019 HMXB 1020 72d; 1021 7/L[1022 S;uD 1023 z?aUY 1024 D?5? 1025 Loc{ 1026 zcKc1 1027 .:3g </pre>	994 LocalFree							
Job Cast Charge 997 Post MessageA 998 GetCursorPos 999 IsWindowUnicode 1000 GetWindowLongA 1001 IsWindowUnicode 1002 SetWindowLongA 1003 GetClientRect 1004 CoTaskMemAlloc 1005 Secontemp 1006 SE9D63A019482A8D172568655C83D0C2 1007 JA::8 1008 SOFTMEINICROSOFT\WINDOWS\CURRENTVERSION\RUN 1009 System 1010 smss.exe 1011 csrss.exe 1012 NtOpenProcess 1013 config.bin 1014 config.dat 1015 cleansweep.exe 1018 kU'9 1019 HMXB 1020 72d; 1021 7/L[1022 sjuD 1023 z?aUY 1024 D75? 1025 clexcl1 1027 .:30	995 InterlockedIncrement							
998 GetCursorPos 999 IswindowUnicode 1006 GetWindowLongA 1001 IsWindow 1003 GetClientRect 1004 CoTaskMemAlloc 1005 _wcsnicmp 1006 SE9063A019482A8D172568655C83D0C2 1007 [A::8 1008 SOFTMARE/MICROSOFT/WINDOWS/CURRENTVERSION/RUN 1019 System 1010 Smss.exe 1011 Csrss.exe 1011 Csrss.exe 1012 NtOpenProcess 1013 config.bin 1014 config.dat 1015 cleansweep.exe 1016 ''UU 1017 cleansweepupd.exe 1018 kU'9 1019 HMXB 1020 72d; 1021 ?/L[1022 S;UD 1022 S;UD 1023 z?aUY 1024 D?S? 1025 U>c{ 1026 zcxc1 1027 .:3g <i>Figura 6</i>	997 PostMessageA							
999 ISWindowUnicode 1000 GetWindowLongA 1001 ISWindow 1002 SetWindowLongA 1003 GetClientRect 1004 CoTasKMemAlloc 1005 _wcsnicmp 1006 SE9D63A019482A8D172568655C83D0C2 1007 [A::8 1008 SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN 1009 System 1010 smss.exe 1011 csrss.exe 1011 csrss.exe 1012 NtOpenProcess 1013 config.dat 1014 config.dat 1015 cleansweep.exe 1018 (''UU 1017 cleansweepupd.exe 1018 HV'8 1020 72d; 1021 7/L[1022 S;uD 1023 z?aUY 1024 D?S? 1025 U>C{ 1025 U>C{ 1026 zcKc1 1027 .:3q Figura 6	998 GetCursorPos							
1000 GetWindowLongA 1001 ISWindow 1002 SetWindowLongA 1003 GetClientRect 1004 CoTaskMemAlloc 1005 _wcsnicmp 1006 SE9D63A019482A8D172568655C83D0C2 1007 [A::8 1008 SOFTWARELVICROSOFT/WINDOWS/CURRENTVERSION/RUN 1009 System 1010 Smss.exe 1011 Csrss.exe 1012 NtOpenProcess 1013 config.bin 1015 cleansweep.exe 1016 ''UU 1017 cleansweep.upd.exe 1018 KU'9 1019 HMXB 1020 72d; 1021 7/L[1022 S;uD 1023 z?aUY 1024 D?S? 1025 U>c{ 1025 U>c{ 1026 zcKc1 1027 .:3g Figura 6	999 IsWindowUnicode							
1001 IsWindow 1002 SetWindowLongA 1003 GetClientRect 1004 CoTasKMemAlloc 1005 wcsntcmp 1006 SE9D63A019482A8D172568655C83D0C2 1007 JA::8 1008 SOFTWARELVICROSOFT\WINDOWS\CURRENTVERSION\RUN 1009 System 1010 smss.exe 1011 csrss.exe 1012 NtOpenProcess 1013 config.bin 1015 cleansweep.exe 1016 ''UU 1017 cleansweep.upd.exe 1018 kU'9 1019 HMXB 1020 72d; 1021 7/L[1022 S;uD 1023 z;aUY 1024 D?S? 1025 U>c{ 1026 zcxc1 1027 .:3g Figura 6	1000 GetWindowLongA							
1003 GetClientRect 1003 GetClientRect 1004 CoTaskwemAlloc 1005 _wcsnicmp 1005 SEOBG3A019482A8D172568655C83D0C2 1007 [A::8 1008 SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN 1009 System 1010 Smss.exe 1011 csrs.exe 1011 csrs.exe 1012 NtOpenProcess 1013 config.bin 1014 config.dat 1015 cleansweep.exe 1016 ''UU 1017 cleansweepupd.exe 1018 kU'9 1019 HMXB 1020 72d; 1021 ?/L[1022 S;UD 1023 z?aUY 1024 D?S? 1025 U>c{ 1026 zc%c1 1027 .:3g Figura 6	1001 IsWindow							
1004 COT askMemAlloc 1005 WCSNICmp 1006 SE9D63A019482A8D172568655C83D0C2 1007 [A::8 1008 SOFTWARE/MICROSOFT/WINDOWS/CURRENTVERSION/RUN 1009 System 1010 smss.exe 1011 csrss.exe 1011 csrss.exe 1012 NtOpenProcess 1013 config.dat 1015 cleansweep.exe 1016 'UU 1017 cleansweep.exe 1018 KU'9 1019 HWXB 1020 ?Zd; 1021 ?/L[1022 S;UD 1023 z?aUY 1024 D?S? 1025 U>c[1026 zc%C1 1027 .:3g Figura 6	1002 SetWindowLongA							
1005 _wcsnicmp 1006 SE9D63A019482A8D172568655C83D0C2 1007 [A:: 8 1008 SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN 1009 System 1010 smss.@xe 1011 csrss.@xe 1012 config.dat 1015 cleansweep.@xe 1016 ''UU 1017 cleansweep.@xe 1016 ''UU 1019 HMXB 1020 72d; 1021 7/L[1022 S;UD 1023 z?aUY 1024 D?S? 1025 U>c{ 1026 zc%c1 1027 .:3q Figura 6	1004 CoTaskMemAlloc							
1006 5E9D63A019482A8D172568655C83D0C2 1007 [A::8 1008 5OFTWARE(VICROSOFT/WINDOWS/CURRENTVERSION/RUN 1009 System 1010 Smss.exe 1011 csrss.exe 1012 NtOpenProcess 1013 config.bin 1015 cleansweep.exe 1016 ''UU 1017 cleansweepupd.exe 1018 kU'9 1019 HMXB 1020 72d; 1021 7/L[1022 S;UD 1023 z?aUY 1024 D?S? 1025 U>c{ 1026 zcKc1 1027 .:3g Figura 6	1005 wcsnicmp							
1007 A::8 1008 SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN 1009 System 1010 Smss.exe 1011 csrss.exe 1011 csrss.exe 1012 NtOpenProcess 1013 config.bin 1014 config.dat 1015 cleansweep.exe 1016 '''UU 1017 cleansweepupd.exe 1018 kU'9 1019 HMXB 1020 72d; 1021 ?/L[1022 S;UU 1022 S;UU 1023 z?aUY 1024 D?S? 1025 U>c{ 1026 zc%c1 1027 .:3g Figura 6	1006 5E9D63A019482A8D172568655C83D0C2							
1008 SOFTWARE VAIC ROSOFT V WINDOWS CURRENT VERSION (RUN 1009 System 1010 smss. exe 1011 csrss. exe 1012 NtOpenProcess 1013 config.dat 1014 config.dat 1015 cleansweep.exe 1016 'UU 1017 cleansweepupd.exe 1018 kU'9 1019 HMXB 1020 ?Zd; 1021 ?/L[1022 S; UD 1023 z?aUY 1024 D?S? 1025 U>c[1026 zc%C1 1027 .:3q Figura 6	1007 A::8							
1000 System 1010 system 1011 csrss.exe 1011 csrss.exe 1012 conss.exe 1014 config.dat 1015 cleansweep.exe 1016 ''UU 1017 cleansweepupd.exe 1018 MU'9 1019 HMXB 1020 ?Zd; 1021 Z?aUY 1022 S; UD 1023 Z?aUY 1024 D?S? 1025 U>c{ 1026 zcxc1 1027 .:3q	1008 SOFTWARE MICROSOFT WINDOWS CURRENTVERSION RUN							
1010 SHS3.Ext 1011 CSTS.Ext 1012 CSTS.Ext 1013 Config.bin 1014 Config.dat 1015 Cleansweep.ext 1016 'UU 1017 Cleansweep.ext 1018 KU'9 1019 HMXB 1020 72d; 1021 7/L[1022 S; UD 1023 Z?AUY 1026 Z:K1 1027 .:3q	1009 System							
1012 NtOpenProcess 1013 config.bin 1014 config.dat 1015 cleansweep.exe 1016 ''UU 1017 cleansweepupd.exe 1018 kU'9 1019 HMXB 1020 72d; 1021 7/L[1022 5;UU 1023 z?aUY 1024 D?\$? 1025 U>c{ 1026 zc%c1 1027 .:3q Figura 6	1010 SHSS.exe							
1013 config.bin 1014 config.dat 1015 cleansweep.exe 1016 ''UU 1017 cleansweepupd.exe 1018 kU'9 1019 HMXB 1020 72d; 1021 7/L[1022 5;UD 1023 z?aUY 1024 D?S? 1025 U>c{ 1025 U>c{ 1025 cxC1 1027 .:3q Figura 6	1012 NtOpenProcess							
1014 config.dat 1015 cleansweep.exe 1016 ''UU 1017 cleansweepupd.exe 1018 kU'9 1019 HMXB 1020 ?Zd; 1021 ?/L[1022 S;UD 1023 z?aUY 1024 D?S? 1025 U>C{ 1025 CC{ 1026 cc%C1 1027 .:3q Figura 6	1013 config.bin							
1015 cleansweep.exe 1016 ''UU 1017 cleansweepupd.exe 1018 kU'9 1019 HMXB 1020 7Zd; 1021 7/L[1022 S;UD 1023 Z;AUY 1024 D?S? 1025 U>c{ 1026 Z;KC1 1027 .:3q Figura 6	1014 config.dat							
1016 100 1017 cleansweepupd. exe 1018 kU'9 1019 HMXB 1020 7Zd; 1021 7/L[1022 5;uD 1023 z?aUY 1024 D?5? 1025 U>c{ 1026 zc≪c1 1027 .:3q Figura 6	1015 cleansweep.exe							
1017 Cteansweepupu. Exe 1018 kU'9 1019 HMX8 1020 7Zd; 1021 7/L[1022 S;uD 1024 D?S? 1025 U>c{ 1026 zc%c1 1027 .:3q Figura 6								
1019 HMXB 1020 72d; 1021 7/L[1022 5;UD 1023 2?aUY 1024 D?S? 1025 U>c{ 1026 zc%C1 1027 .:3q Figura 6	1017 cteansweepupu.exe							
1020 ?Zd; 1021 ?/L[1022 S;UD 1023 Z?aUY 1024 D?S? 1025 U>C{ 1026 Zc%C1 1027 .:3q Figura 6	1019 HMXB							
1021 ?/L[1022 S; UD 1023 2?aUY 1024 D?S? 1025 U>c{ 1026 zc%c1 1027 .:3q Figura 6	1020 ?Zd;							
1022 S;UD 1023 z?aUY 1024 D?S? 1025 U>c{ 1026 zc%c1 1027 .:3q Figura 6	1021 ?/L[
1023 27004 1024 D7\$7 1025 U>c{ 1026 zc%c1 1027 .:3q Figura 6	1022 S; UD							
1025 U>C{ 1026 zc%C1 1027 .:3q Figura 6	1025 2:001							
1026 zcxč1 1027 .:3q Figura 6	1025 U>c{							
1027 . : 39 Figura 6	1026 zc%C1							
Figura 6	1027.:3q							
Figura 6								
Figura 6								
Figura 6	Figura 6							
	Figura 6							

BIBLIOGRAFIA

- The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory Michael Hale Ligh, Andrew Case, Jamie Levy, AAron Walters - 2014 WILEY
- http://trickandtipsforpc.blogspot.it/2015/07/malware-memory-forensics-introduction.html
- http://securityxploded.com/malware-memory-forensics.php
- http://www.behindthefirewalls.com/2013/07/zeus-trojan-memory-forensics-with.html. ©