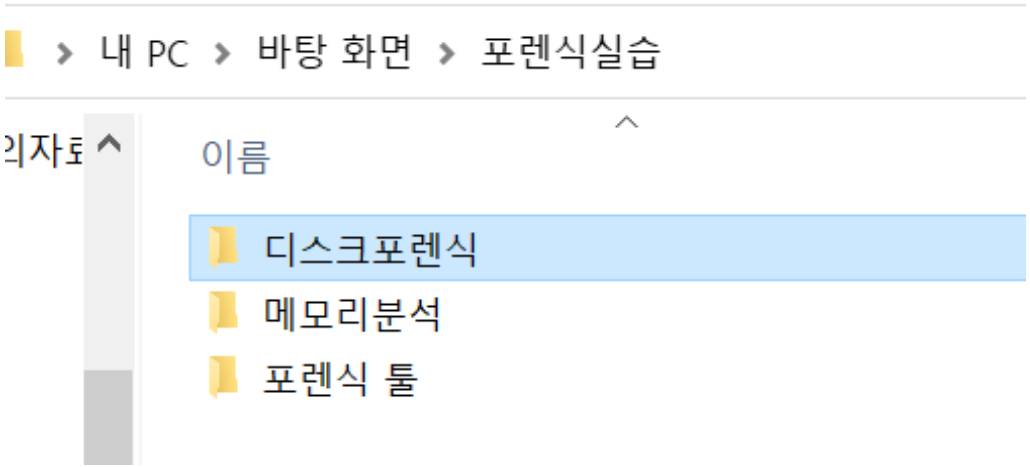
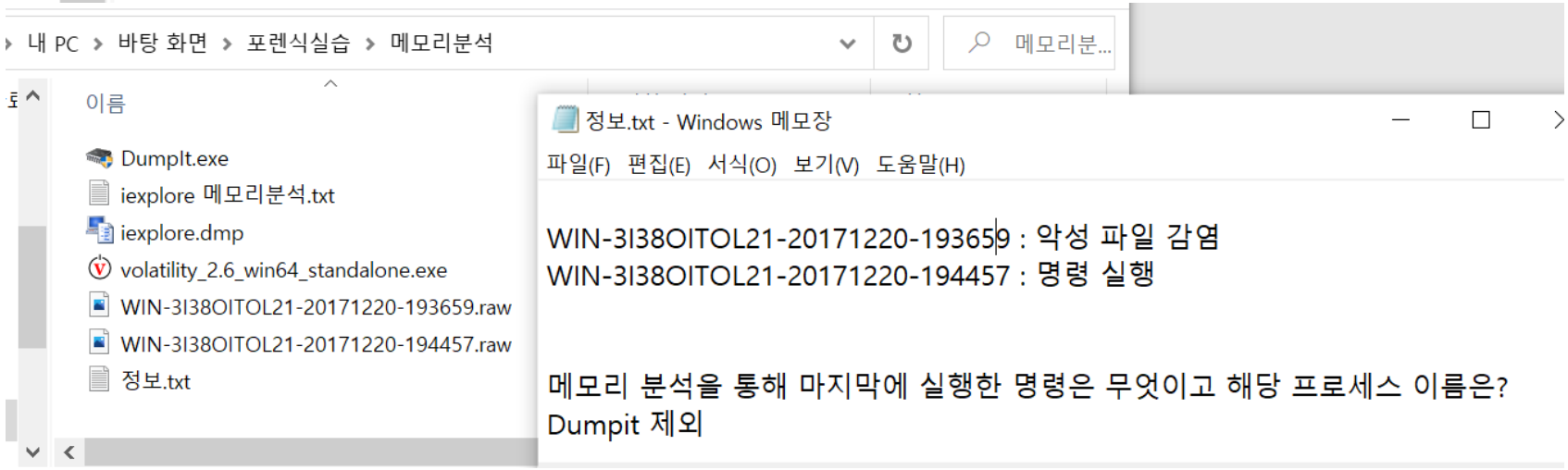
2020.05.26

메모리 포렌식

발 표 자 박 재 희


내 PC › 바탕 화면 › 포렌식실습
이름
디스크포렌식
메모리분석
포렌식 툴


내 PC › 바탕 화면 › 포렌식실습 › 메모리분석
메모리분...
이름
DumpIt.exe
iexplore 메모리분석.txt
iexplore.dmp
volatility_2.6_win64_standalone.exe
WIN-3I38OITOL21-20171220-193659.raw
WIN-3I38OITOL21-20171220-194457.raw
정보.txt
정보.txt - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)
WIN-3I38OITOL21-20171220-193659 : 악성 파일 감염
WIN-3I38OITOL21-20171220-194457 : 명령 실행
메모리 분석을 통해 마지막에 실행한 명령은 무엇이고 해당 프로세스 이름은?
Dumpit 제외

CONTENTS

01 디지털 포렌식

범죄 수사에서 적용되고 있는 과학적 증거 수집 및 분석기법의 일종

각종 디지털 데이터 및 통화 기록 등등 정보를 수집, 분석하여

범행과 관련된 증거를 확보하는 수사기법

침해사고에서 악성코드는 조직 내부의 중요 기밀 데이터를 유출하는데

포렌식 기법을 통해 피해의 시작과 범위를 조사하고 분석할 수 있다.

무결성, 진정성, 동일성, 신뢰성, 정당성

01 디지털 포렌식

멀웨어 포렌식(Malware Forensic)

- 메모리 포렌식
- 레지스트리 포렌식
- 인터넷 포렌식
- 네트워크 포렌식
- 파일 시스템 포렌식

01 디지털 포렌식

메모리 포렌식

- 휘발성이 강하다. 고유의 독특한 정보가 많이 존재하는 물리적인 램에 남아 있는 악성코드 감염과 관련된 다양한 흔적을 분석

레지스트리 포렌식

- 일반적인 악성코드는 감염된 시스템이 재부팅을 하거나 사용자가 특정 행위를 수행했을 때 악성코드가 실행되기 위해 윈도 시스템의 레지스트리에 새로운 키를 생성 및 변경한다.

01 디지털 포렌식

인터넷 포렌식

- 인터넷 활동과 관련된 애플리케이션의 행위와 흔적 분석을 통해 악성코드의 감염 경로와 감염 매개체를 파악할 수 있다

네트워크 포렌식

- 악성코드는 인터넷에 존재하는 시스템과 네트워크의 연결이 이루어짐으로써 네트워크 패킷에 기반한 분석을 통해 감염 경로와 함께 감염 시스템을 추적하고 분류할 수 있음

01 디지털 포렌식

파일 시스템 포렌식

- 전통적인 컴퓨터 포렌식 분야에서 중요하게 언급하는 기법 중 하나

시스템의 디스크 이미징을 통해 생성한 디스크 복사본을

FTK와 같은 파일 시스템 분석 소프트웨어를 통해 디스크 전체를 분석

02 메모리 포렌식

메모리 포렌식이란?

컴퓨터 하드웨어 중 주기억장치(메모리)에 존재하는 휘발성 데이터를 덤프 분석

메모리 포렌식 하는 이유

물리 메모리에 존재하는 모든 흔적을 확인할 수 있음

ex) 프로세스 정보, 네트워크 연결 정보, 윈도우 레지스터리 정보, 패스워드, 캐시정보, 클립보드 정보, 악성코드 파일 정보, 하드웨어 설정 정보 등등

02 메모리 포렌식

메모리 덤프

Tribble:

RAM 슬롯에 장착하여 메모리 덤프 수행

사전에 설치 되어 있어야 한다

Win32/64dd

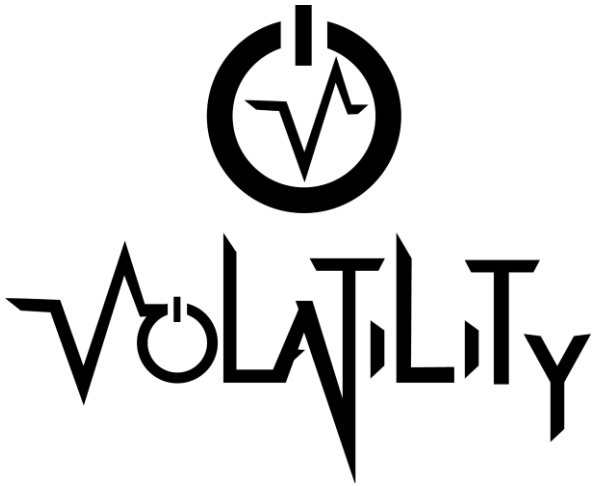
Memorize

크래시 덤프

절전 덤프

02 메모리 포렌식

메모리 덤프 분석 도구



03 Volatility

Volatility 플러그인

Imageinfo : vola.exe –f [메모리덤프 파일 이름] imageinfo

```
C:₩Users₩eunhe₩Desktop₩volatility>volatility.exe -f test.vmss imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : VMWareAddressSpace (Unnamed AS)
                     AS Layer3 : FileAddressSpace (C:₩Users₩eunhe₩Desktop₩volatility₩test.vmss)
                      PAE type : PAE
                           DTB : 0x185000L
                          KDBG : 0x82765be8L
          Number of Processors : 2
     Image Type (Service Pack) : 0
                KPCR for CPU 0 : 0x82766c00L
                KPCR for CPU 1 : 0x807c5000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2015-10-09 12:53:02 UTC+0000
     Image local date and time : 2015-10-09 08:53:02 -0400
```

03 Volatility

vola.exe-f[메모리덤프파일이름]—profile = [운영체제종류] 플러그인

Volatility 플러그인

pslist :프로세스 리스트 출력(가상주소)

psscan: 프로세스 리스트 출력(물리적주소)

pstree : 프로세스를 트리 구조로 출력

prodump : 프로세스 실행파일 추출

memdump : 프로세스가 사용한 전체 메모리 영역 덤프

. . .

https://github.com/volatilityfoundation/volatility/wiki/Command-Reference#imageinfo

04 실습

CTF-d

Memory

GrrCON 2015 #1 1	GrrCON 2015 #2 2	GrrCON 2015 #3 3	GrrCON 2015 #4 4	GrrCON 2015 #5 5	GrrCON 2015 #6 6
GrrCON 2015 #7 7	GrrCON 2015 #8 8	GrrCON 2015 #9 9	GrrCON 2015 #10 10	GrrCON 2015 #11 11	GrrCON 2015 #12 12
GrrCON 2015 #13 13	GrrCON 2015 #14 14	GrrCON 2015 #15 15	GrrCON 2015 #16 16	GrrCON 2015 #17 17	GrrCON 2015 #18 18
GrrCON 2015 #19 19	GrrCON 2015 #20 20	GrrCON 2015 #21 21	GrrCON 2015 #22 22	GrrCON 2015 #23 23	GrrCON 2015 #24 24

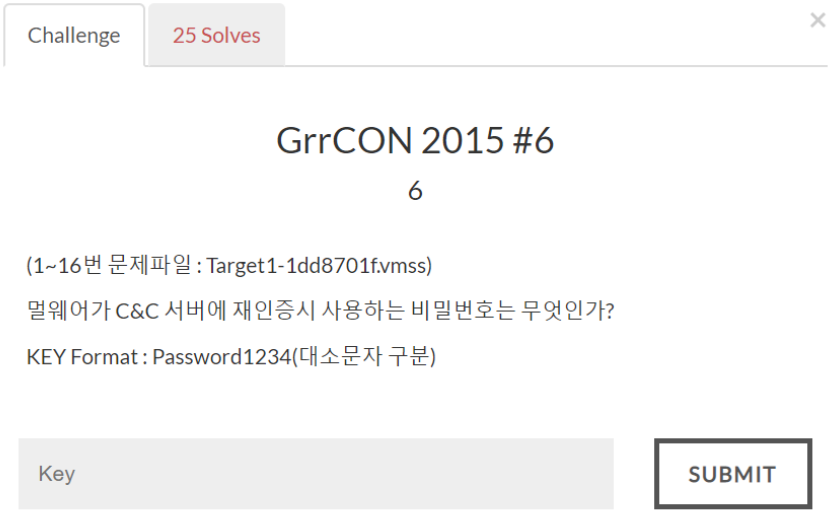
04 실습

CTF-d

Memory

GrrCON 2015 #1 1	GrrCON 2015 #2 2	GrrCON 2015 #3 3	GrrCON 2015 #4 4	GrrCON 2015 #5 5	GrrCON 2015 #6 6
GrrCON 2015 #7 7	GrrCON 2015 #8 8	GrrCON 2015 #9 9	GrrCON 2015 #10 10	GrrCON 2015 #11 11	GrrCON 2015 #12 12
GrrCON 2015 #13 13	GrrCON 2015 #14 14	GrrCON 2015 #15 15	GrrCON 2015 #16 16	GrrCON 2015 #17 17	GrrCON 2015 #18 18
GrrCON 2015 #19 19	GrrCON 2015 #20 20	GrrCON 2015 #21 21	GrrCON 2015 #22 22	GrrCON 2015 #23 23	GrrCON 2015 #24 24

04 실습


Challenge
25 Solves
GrrCON 2015 #6
6
(1~16번 문제파일 : Target1-1dd8701f.vmss)
멀웨어가 C&C 서버에 재인증시 사용하는 비밀번호는 무엇인가?
KEY Format : Password1234(대소문자 구분)
Key
SUBMIT

문제 1


Challenge
24 Solves
GrrCON 2015 #22
22
(22~25번 문제파일 : pos1.vmss)
멀웨어의 C&C 서버는 무엇인가?
KEY Format : 192.168.1.2
pos1.vmss
Key
SUBMIT

문제 2

04 실습

멀웨어?

정상적인 작동을 방해하거나 사용자의 컴퓨터, 휴대폰, 테블릿 또는 기타 디바이스를 감염시키도록 설계된 악성코드를 총칭하는 이름

C&C 서버?

감염된 좀비 PC가 해커가 원하는 공격을 수행하도록 원격지에 명령을 내리거나, 악성코드를 제어하는 서버를 말한다.

04 실습

lexplore.exe?

Microsoft사에서 만든 인터넷 브라우저 프로그램인 windows internet Exploerer를 실행하는 파일이다.

간혹 비정상적인 이름이나 경로를 가진 iexplorer.exe혹은 비슷한 이름의 프로세스가 작업관리자에 떠 있다면 바이러스나 웜을 의심해볼만 하다.

Explorer.exe의 자식프로세스로 돌아간다.

Explorere.exe

윈도우 탐색기 프로세스

04 실습

문제 1을 pstree로 봤을 때

```
0x85c1e5f8:explorer.exe                2116   2060     23      912 2015-10-09 11:31:04 UTC+0000
. 0x83eb5d40:cmd.exe                   2496   2116      1       22 2015-10-09 11:33:42 UTC+0000
. 0x83f1ed40:mstsc.exe                 2844   2116     11      484 2015-10-09 12:12:03 UTC+0000
. 0x83fb86a8:cmd.exe                   3064   2116      1       22 2015-10-09 11:37:32 UTC+0000
. 0x859281f0:vmtoolsd.exe              2388   2116      7      164 2015-10-09 11:31:04 UTC+0000
. 0x85cd3d40:OUTLOOK.EXE               3196   2116     22     1678 2015-10-09 11:31:32 UTC+0000
0x855f6d40:csrss.exe                    432    412     11      366 2015-10-09 11:30:48 UTC+0000
. 0x83f13d40:conhost.exe               1624    432      3       81 2015-10-09 11:35:15 UTC+0000
. 0x83fa9030:conhost.exe                676    432      3       83 2015-10-09 11:37:32 UTC+0000
. 0x83e5cd40:conhost.exe                916    432      3       83 2015-10-09 11:33:42 UTC+0000
. 0x83fc7c08:conhost.exe               1824    432      3       85 2015-10-09 11:39:22 UTC+0000
0x8561d030:winlogon.exe                 480    412      3      115 2015-10-09 11:30:48 UTC+0000
0x85d0d030:iexplore.exe                2996   2984      6      463 2015-10-09 11:31:27 UTC+0000
. 0x83f105f0:cmd.exe                   1856   2996      1       33 2015-10-09 11:35:15 UTC+0000
```

04 실습

문제 2을 pstree로 봤을 때

```
C:₩Users₩eunhe₩Desktop₩volatility>volatility.exe -f pos1.vmss --profile=Win7SP0x86 pstree
Volatility Foundation Volatility Framework 2.6
Name                                                 Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x83e92b50:explorer.exe                             1836   3348     24    995 2015-10-09 05:25:15 UTC+0000
. 0x83d9b368:regsvr32.exe                            2928   1836      0 ------ 2015-10-09 05:25:18 UTC+0000
. 0x83f11958:OUTLOOK.EXE                             3376   1836     29   2185 2015-10-09 06:21:35 UTC+0000
. 0x84ae9668:notepad.exe                             2700   1836      4    261 2015-10-09 05:30:12 UTC+0000
. 0x8462c610:vmtoolsd.exe                            1200   1836      7    156 2015-10-09 05:25:35 UTC+0000
. 0x84627d40:jusched.exe                             2832   1836      2    119 2015-10-09 05:25:35 UTC+0000
. 0x83e55030:EXCEL.EXE                               2092   1836     11    386 2015-10-09 09:47:28 UTC+0000
 0x83d38bb0:System                                      4      0     93    534 2015-10-09 03:37:36 UTC+0000
. 0x84edc020:smss.exe                                280      4      2     33 2015-10-09 03:37:38 UTC+0000
 0x85ad1608:explorer.exe                             2200   2084     20    849 2015-10-09 03:39:33 UTC+0000
. 0x846fd030:vmtoolsd.exe                            2444   2200      7    145 2015-10-09 03:39:38 UTC+0000
. 0x859afd10:WINWORD.EXE                             3740   2200     10    419 2015-10-09 05:21:27 UTC+0000
. 0x846fd920:jusched.exe                             2464   2200      5    361 2015-10-09 03:39:38 UTC+0000
. 0x85989030:chrome.exe                              1960   2200      0 ------ 2015-10-09 05:05:58 UTC+0000
 0x83f324d8:iexplore.exe                             3208   3324     11    214 2015-10-09 12:35:57 UTC+0000
. 0x855d86d0:iexplore.exe                            3136   3208      2     32 2015-10-09 12:35:57 UTC+0000
 0x85409030:csrss.exe                                 368    360      9    463 2015-10-09 03:37:42 UTC+0000
 0x83dd6458:wininit.exe                               432    360      3     79 2015-10-09 03:37:58 UTC+0000
```

04 실습

1번의 경우 재인증시 사용하는 비밀번호를 물었음

0x85c1e5f8:explorer.exe	2116	2060	23	912	2015-10-09 11:31:04 UTC+0000
. 0x83eb5d40:cmd.exe	2496	2116	1	22	2015-10-09 11:33:42 UTC+0000
. 0x83f1ed40:mstsc.exe	2844	2116	11	484	2015-10-09 12:12:03 UTC+0000
. 0x83fb86a8:cmd.exe	3064	2116	1	22	2015-10-09 11:37:32 UTC+0000
. 0x859281f0:vmtoolsd.exe	2388	2116	7	164	2015-10-09 11:31:04 UTC+0000
. 0x85cd3d40:OUTLOOK.EXE	3196	2116	22	1678	2015-10-09 11:31:32 UTC+0000
0x855f6d40:csrss.exe	432	412	11	366	2015-10-09 11:30:48 UTC+0000
. 0x83f13d40:conhost.exe	1624	432	3	81	2015-10-09 11:35:15 UTC+0000
. 0x83fa9030:conhost.exe	676	432	3	83	2015-10-09 11:37:32 UTC+0000
. 0x83e5cd40:conhost.exe	916	432	3	83	2015-10-09 11:33:42 UTC+0000
. 0x83fc7c08:conhost.exe	1824	432	3	85	2015-10-09 11:39:22 UTC+0000
0x8561d030:winlogon.exe	480	412	3	115	2015-10-09 11:30:48 UTC+0000
0x85d0d030:iexplore.exe	2996	2984	6	463	2015-10-09 11:31:27 UTC+0000
. 0x83f105f0:cmd.exe	1856	2996	1	33	2015-10-09 11:35:15 UTC+0000

04 실습

2번의 경우 C&C서버를 물어보았다

```
C:₩Users₩eunhe₩Desktop₩volatility>volatility.exe -f pos1.vmss --profile=Win7SP0x86 pstree
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x83e92b50:explorer.exe                             1836   3348     24    995 2015-10-09 05:25:15 UTC+0000
. 0x83d9b368:regsvr32.exe                            2928   1836      0 ------ 2015-10-09 05:25:18 UTC+0000
. 0x83f11958:OUTLOOK.EXE                             3376   1836     29   2185 2015-10-09 06:21:35 UTC+0000
. 0x84ae9668:notepad.exe                             2700   1836      4    261 2015-10-09 05:30:12 UTC+0000
. 0x8462c610:vmtoolsd.exe                            1200   1836      7    156 2015-10-09 05:25:35 UTC+0000
. 0x84627d40:jusched.exe                             2832   1836      2    119 2015-10-09 05:25:35 UTC+0000
. 0x83e55030:EXCEL.EXE                               2092   1836     11    386 2015-10-09 09:47:28 UTC+0000
 0x83d38bb0:System                                      4      0     93    534 2015-10-09 03:37:36 UTC+0000
. 0x84edc020:smss.exe                                280      4      2     33 2015-10-09 03:37:38 UTC+0000
 0x85ad1608:explorer.exe                             2200   2084     20    849 2015-10-09 03:39:33 UTC+0000
. 0x846fd030:vmtoolsd.exe                            2444   2200      7    145 2015-10-09 03:39:38 UTC+0000
. 0x859afd10:WINWORD.EXE                             3740   2200     10    419 2015-10-09 05:21:27 UTC+0000
. 0x846fd920:jusched.exe                             2464   2200      5    361 2015-10-09 03:39:38 UTC+0000
. 0x85989030:chrome.exe                              1960   2200      0 ------ 2015-10-09 05:05:58 UTC+0000
 0x83f324d8:iexplore.exe                             3208   3324     11    214 2015-10-09 12:35:57 UTC+0000
. 0x855d86d0:iexplore.exe                            3136   3208      2     32 2015-10-09 12:35:57 UTC+0000
 0x85409030:csrss.exe                                 368    360      9    463 2015-10-09 03:37:42 UTC+0000
 0x83dd6458:wininit.exe                               432    360      3     79 2015-10-09 03:37:58 UTC+0000
```

04 실습

2번의 경우 C&C서버를 물어보았다

Offset(P)	Proto	Local Address	Foreign Address	State	Pid	Owner
0x3e6cf270	TCPv4	0.0.0.0:49154	0.0.0.0:0	LISTENING	900	svchost.exe
0x3e0f90e8	TCPv4	10.1.1.10:64532	10.1.1.3:80	ESTABLISHED	3376	OUTLOOK.EXE
0x3e135df8	TCPv4	10.1.1.10:58751	54.84.237.92:80	CLOSE_WAIT	3208	iexplore.exe
0x3e24c7d0	TCPv4	10.1.1.10:49201	23.203.149.112:443	CLOSE_WAIT	2464	jusched.exe

Netscan 명령어로 활성화된 네트워크 연결 정보와 함께 이미 종료된 연결정보도 알 수 있다.