



Memory Forensics with CTF

Memory Forensics?



메모리 포렌식이란

- 디지털 포렌식에서의 사고 대응(Incident Response) 방안 중에 하나로 휘발성의 특징을 가지고있는 메모리에 대해 정보를 수집하는 것

메모리 포렌식의 필요성

- 컴퓨터 시스템의 특성으로 인하여 메모리에는 파일이 실행되는 과정이나 실행되었던 특유의 정보가 존재하기 때문이다.

분석 정보

- 프로세스와 스레드 정보 : 프로그램이나 파일이 실행 중이거나 이미 종료되었지만 메모리에 남아 있는 정보 추출
- 모듈과 라이브러리 정보 : 프로그램이나 파일이 실행 중이거나 이미 종료된 프로세스 관련 모듈과 라이브러리 정보 추출
- 실행된 파일이나 소켓 정보 : 실행 중이거나 이미 종료된 파일 정보와 네트워크 연결을 위해 사용되었거나 사용중인 소켓 정보 추출
- 다양한 데이터 구조 정보 : 메모리에만 존재하는 운영체제, 소프트웨어 및 파일과 관련된 다양한 데이터 구조의 정보 추출

Problem 1



GrrCON 2015 #1

1

(1~16번 문제파일 : Target1-1dd8701f.vmss)

프런트 데스크 직원들은 보안 업데이트라고 생각하고 이상한 이메일을 클릭한 것을 당신에게 보고했다. 프런트 데스크 사용자의 메일주소로 이메일을 보낸 전자 메일 주소는 무엇인가?

Target1-
1dd8701f.vmss

Key

SUBMIT

Problem 1



vmss



volatility

Vmss : 가상 머신에서 일시 중지 상태일 때 운영체제 상태를 저장한 파일 확장자

volatility : Python으로 제작된 메모리 포렌식 분석 프로그램

Problem 1



```
C:\Users\User\Desktop\TOOL\volatility\volatility2\volatility3>volatility.exe -f problem1.vms 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 : KDBGPageMemoryPae (Kernel AS)
AS Layer2 : VMWareAddressSpace (Unnamed AS)
AS Layer3 : FileAddressSpace (C:\Users\User\Desktop\TOOL\volatility\volatility2\volatility3\problem1.vms)
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
```

pslist

```
C:\Users\User\Desktop\TOOL\volatility\volatility2\volatility3>volatility.exe -f problem1.vms --profile=Win7SP0x86 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V) Name PID PPID Thds Hnds Sess Wow64 Start Exit
-----
0x85d0d030 iexplore.exe 2996 2984 6 463 1 0 2015-10-09 11:31:27 UTC+0000
0x85cd3d40 OUTLOOK.EXE 3196 2116 22 1678 1 0 2015-10-09 11:31:32 UTC+0000
0x85d01510 svchost.exe 3232 528 9 131 0 0 2015-10-09 11:31:34 UTC+0000
```

Problem 1



memdump

```
C:\Users\User\Desktop\TOOL\volatility\volatility2\volatility3>volatility.exe -f problem1.vms --profile=Win7SP0x86 memdump -p 3196 -D ./
Volatility Foundation Volatility Framework 2.6
*****
Writing OUTLOOK.EXE [ 3196] to 3196.dmp
```

Strings.exe

```
C:\Users\User\Desktop\TOOL>strings.exe 3196.dmp > 3196.txt

Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com
```

Problem 1



```
152336 Update Your VPN Client
152337 The Whit3R0s3
152338 SMTP
152339 [REDACTED]
152340 Update Your VPN Client
152341 >j+
152342 The Whit3R0s3
152343 SMTP
152344 [REDACTED]
152345 front desk<CALwgF5bo54VoNzmLrOs4R500JQ-zifiDB=UxCyiEZTisogfmCQ@mail.gmail.com>
152346 iH
152347 Hello Mr. Wellick,
152348 In order to provide the best service, in the most secure manner, AllSafe has recently updated our remote VPN software. Please download the update from the link below.
152349 http://180.76.254.120/AnyConnectInstaller.exe
152350 If you have an
```

Flag!!!

Problem 2



GrrCON 2015 #2

2

(1~16번 문제파일 : Target1-1dd8701fvmss)

공격자가 프론트 데스크 직원들의 이메일로 첨부해서 보낸 파일의 이름은 무엇인가?

KEY Format : xxx.exe

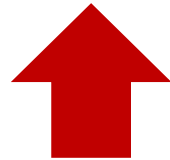
Key

SUBMIT

Problem 2



```
152336 Update Your VPN Client
152337 The Whit3R0s3
152338 SMTP
152339 [REDACTED]
152340 Update Your VPN Client
152341 >j+
152342 The Whit3R0s3
152343 SMTP
152344 [REDACTED]
152345 front desk<CALwgF5bo54VoNzmLrOs4R500JQ-zifiDB=UxCyiEZTisogfmCQ@mail.gmail.com>
152346 iH
152347 Hello Mr. Wellick,
152348 In order to provide the best service, in the most secure manner, AllSafe has recently updated our remote VPN software. Please download the update from the link below.
152349 http://180.76.254.120/[REDACTED]
152350 If you have an
```



첨부 파일명

Problem 3



GrrCON 2015 #3

3

(1~16번 문제파일 : Target1-1dd8701f.vms)

공격자는 AllSafeCyberSec 사용자들을 피싱한 것으로 보인다. 사용된 악성 코드의 이름은 무엇인가?

KEY Format : zeus

Key

SUBMIT

Problem 3



filescan

```
C:\Users\User\Desktop\TOOL\volatility>volatility.exe -f problem1.vms --profile=Win7SP0x86 filescan | findstr AnyConnect
Installer.exe
Volatility Foundation Volatility Framework 2.6
0x000000003df12dd0      2      0 RW-rwd \Device\HarddiskVolume2\Users\Wanyconnect\AnyConnect\AnyConnectInstaller.exe
0x000000003df1cf00      4      0 R--r-d \Device\HarddiskVolume2\Users\Wanyconnect\AnyConnect\AnyConnectInstaller.exe
0x000000003e0bc5e0      7      0 R--r-d \Device\HarddiskVolume2\Users\frontdesk\Downloads\AnyConnectInstaller.exe
0x000000003e2559b0      8      0 R--rwd \Device\HarddiskVolume2\Users\frontdesk\Downloads\AnyConnectInstaller.exe
0x000000003e2ae8e0      8      0 RWD--- \Device\HarddiskVolume2\Users\Wanyconnect\AnyConnect\AnyConnectInstaller.exe
0x000000003ed57968      4      0 R--r-d \Device\HarddiskVolume2\Users\frontdesk\Downloads\AnyConnectInstaller.exe
```



dumpfiles

```
C:\Users\User\Desktop\TOOL\volatility>volatility.exe -f problem1.vms --profile=Win7SP0x86 dumpfiles -Q 0x000000003df12dd0 -D ./
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x3df12dd0 None \Device\HarddiskVolume2\Users\Wanyconnect\AnyConnect\AnyConnectInstaller.exe

C:\Users\User\Desktop\TOOL\volatility>volatility.exe -f problem1.vms --profile=Win7SP0x86 dumpfiles -Q 0x000000003df1cf00 -D ./
Volatility Foundation Volatility Framework 2.6
ImageSectionObject 0x3df1cf00 None \Device\HarddiskVolume2\Users\Wanyconnect\AnyConnect\AnyConnectInstaller.exe
DataSectionObject 0x3df1cf00 None \Device\HarddiskVolume2\Users\Wanyconnect\AnyConnect\AnyConnectInstaller.exe
```

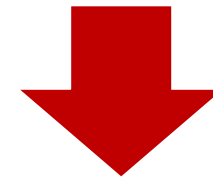
Problem 3



 file.None.0x85d1c6c0.img	2019-07-14 오후...	ALZip IMG File	227KB
 file.None.0x85d12b18.dat	2019-07-14 오후...	DAT 파일	228KB

Worm:Win32/Xtrat.0!D	심각 ▼
2019-07-14	
Worm:Win32/Xtrat.0!D	심각 ▼
2019-07-14	

Xtrat virus ???



Xtream virus

Xtream virus : 2012년 이스라엘과 시리아 정부를 공격하는데 사용된 원격 액세스 트로이 목마



QnA