

1. 메모리 덤프 분석 보고서

가. 3. 분석 과정 및 결과

1) 3.1 기본 정보 수집

명령어: imageinfo



```
imageinfo - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)
Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
AS Layer1 : IA32PagedMemoryPae (Kernel AS)
AS Layer2 : FileAddressSpace (C:\Wdf\memory\sample2.vmem)
PAE type : PAE
DTB : 0x319000L
KDBG : 0x80544ce0L
Number of Processors : 1
Image Type (Service Pack) : 2
KPCR for CPU 0 : 0xffdf000L
KUSER_SHARED_DATA : 0xffdf000L
Image date and time : 2010-08-15 19:17:56 UTC+0000
Image local date and time : 2010-08-15 15:17:56 -0400
```

- 결과 요약:

프로파일: WinXPSP2x86, WinXPSP3x86

메모리 레이어 : 메모리 페이징 구조가 PAE 방식 사용 (Physical Address Extension)


DTB : 0x319000L

KDBG : 0x80544ce0L

프로세서 수 : 단일 cpu 코어 사용

이미지 생성 시각 : 2010-08-15 19:17:56

connections

 connections.txt - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

Offset(V)	Local Address	Remote Address	Pid
-----------	---------------	----------------	-----

connscan

 connscan.txt - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

Offset(P)	Local Address	Remote Address	Pid
-----------	---------------	----------------	-----

0x02214988	172.16.176.143:1054	193.104.41.75:80	856
0x06015ab0	0.0.0.0:1056	193.104.41.75:80	856

connections에는 연결 결과가 표시 되지 않았지만 connscan에서는 856으로 연결된 것을 확인

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
0x810b1660	System	4	0	58	379	-----	0		
0xff2ab020	smss.exe	544	4	3	21	-----	0	2010-08-11 06:06:21 UTC+0000	
0xff1ecda0	csrss.exe	608	544	10	410	0	0	2010-08-11 06:06:23 UTC+0000	
0xff1ec978	winlogon.exe	632	544	24	536	0	0	2010-08-11 06:06:23 UTC+0000	
0xff247020	services.exe	676	632	16	288	0	0	2010-08-11 06:06:24 UTC+0000	
0xff255020	lsass.exe	688	632	21	405	0	0	2010-08-11 06:06:24 UTC+0000	
0xff218230	vmacthlp.exe	844	676	1	37	0	0	2010-08-11 06:06:24 UTC+0000	
0x80ff88d8	svchost.exe	856	676	29	336	0	0	2010-08-11 06:06:24 UTC+0000	
0xff217560	svchost.exe	936	676	11	288	0	0	2010-08-11 06:06:24 UTC+0000	
0x80bf910	svchost.exe	1028	676	88	1424	0	0	2010-08-11 06:06:24 UTC+0000	
0xff22d558	svchost.exe	1088	676	7	93	0	0	2010-08-11 06:06:25 UTC+0000	
0xff203b80	svchost.exe	1148	676	15	217	0	0	2010-08-11 06:06:26 UTC+0000	
0xff1d7da0	spoolsv.exe	1432	676	14	145	0	0	2010-08-11 06:06:26 UTC+0000	
0xff1b8b28	vmtoolsd.exe	1668	676	5	225	0	0	2010-08-11 06:06:35 UTC+0000	
0xff1fdc88	VMUpgradeHelper	1788	676	5	112	0	0	2010-08-11 06:06:38 UTC+0000	
0xff143b28	TPAutoConnSvc.e	1968	676	5	106	0	0	2010-08-11 06:06:39 UTC+0000	
0xff25a7e0	alg.exe	216	676	8	120	0	0	2010-08-11 06:06:39 UTC+0000	
0xff364310	wscntfy.exe	888	1028	1	40	0	0	2010-08-11 06:06:49 UTC+0000	
0xff38b5f8	TPAutoConnect.e	1084	1968	1	68	0	0	2010-08-11 06:06:52 UTC+0000	
0x80f60da0	wuauclt.exe	1732	1028	7	189	0	0	2010-08-11 06:07:44 UTC+0000	
0xff3865d0	explorer.exe	1724	1708	13	326	0	0	2010-08-11 06:09:29 UTC+0000	
0xff3667e8	VMwareTray.exe	432	1724	1	60	0	0	2010-08-11 06:09:31 UTC+0000	
0xff374980	VMwareUser.exe	452	1724	8	207	0	0	2010-08-11 06:09:32 UTC+0000	
0x80f94588	wuauclt.exe	468	1028	4	142	0	0	2010-08-11 06:09:37 UTC+0000	
0xff224020	cmd.exe	124	1668	0	-----	0	0	2010-08-15 19:17:55 UTC+0000	2010-08-15 19:17:56 UTC+0000

네트워크와 통신하는 프로세스 확인

svchost.exe(pid 856) 확인

```
malfind856.txt - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)
Process: svchost.exe Pid: 856 Address: 0xb70000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 38, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00b70000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
0x00b70010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@.....
0x00b70020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00b70030 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 00 .....

0x00b70000 4d      DEC EBP
0x00b70001 5a      POP EDX
0x00b70002 90      NOP
0x00b70003 0003     ADD [EBX], AL
0x00b70005 0000     ADD [EAX], AL
0x00b70007 000400   ADD [EAX+EAX], AL
0x00b7000a 0000     ADD [EAX], AL
0x00b7000c ff      DB 0xff
0x00b7000d ff00   INC DWORD [EAX]
0x00b7000f 00b800000000   ADD [EAX+0x0], BH
0x00b70015 0000     ADD [EAX], AL
0x00b70017 004000   ADD [EAX+0x0], AL
0x00b7001a 0000     ADD [EAX], AL
0x00b7001c 0000     ADD [EAX], AL
0x00b7001e 0000     ADD [EAX], AL
0x00b70020 0000     ADD [EAX], AL
0x00b70022 0000     ADD [EAX], AL
0x00b70024 0000     ADD [EAX], AL
0x00b70026 0000     ADD [EAX], AL
0x00b70028 0000     ADD [EAX], AL
```

malfind로 856 pid를 검색

dlldump로 메모리에 로드된 DLL(동적 링크 라이브러리)을 추출

Process(V) Name	Module Base	Module Name	Result
0x80ff88d8 svchost.exe	0x000b70000	UNKNOWN	OK: module.856.115b8d8.b70000.dll


string을 사용해서 문자열 추출

```
C:\df\memory\mem2>strings module.856.115b8d8.b70000.dll

Strings v2.54 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2021 Mark Russinovich
Sysinternals - www.sysinternals.com

!This program cannot be run in DOS mode.
wR#k332833283328
T}8
328
328
328l
328E
328p
8)328Rich3328
.text
.data
.reloc
B.data1
w5u
wxj
```

procdump 로 pid 856 덤프파일 저장

내 PC > 로컬 디스크 (C:) > df > memory > mem2 > procdump856		
이름	수정한 날짜	유형
 executable.856.exe	2024-11-19 오전 9:29	응용 프로그램

바이러스 토탈에 파일 검사

Domain	Detections	Created	Registrar
res.public.onecdn.static.microsoft	2 / 94	2023-05-05	MarkMonitor Inc.
watson.telemetry.microsoft.com	0 / 94	1991-05-02	MarkMonitor Inc.
www.microsoft.com	1 / 94	1991-05-02	MarkMonitor Inc.

Contacted IP addresses (48) ⓘ

IP	Detections	Autonomous System	Country
104.208.16.94	0 / 94	8075	US
104.86.182.58	0 / 94	20940	US
114.114.114.114	4 / 94	21859	CN
13.107.4.52	2 / 94	8068	US
13.89.179.12	0 / 94	8075	US
131.253.33.203	1 / 94	8068	US
184.25.191.235	0 / 94	16625	US
192.168.0.1	0 / 94	-	-
192.168.0.12	1 / 94	-	-
192.168.0.14	0 / 94	-	-

...

Execution Parents (43) ⓘ

Scanned	Detections	Type	Name
2023-10-30	6 / 63	ZIP	Winsrv.zip
2024-07-23	4 / 67	ZIP	zeus.zip
2024-07-23	5 / 67	ZIP	zeus-dll.zip
2024-05-13	5 / 67	ZIP	Zeus.zip
2024-06-04	5 / 66	ZIP	module.856.115b8d8.71a90000.zip
2024-06-04	5 / 68	ZIP	module.856.115b8d8.77f60000.zip
2023-10-30	6 / 64	ZIP	WinSRV.zip
2023-05-03	6 / 64	ZIP	856dlldump.zip
2024-07-23	4 / 67	ZIP	module.856.115b8d8.ff0000.zip
2024-12-09	5 / 66	ZIP	dlldump.zip