

# 해킹방어실습

## 기말고사



학 번 : 2021671029

이 름 : 박예서

제출일 : 2023년 6월 9일

질문 1> 악성코드로 추정되는 프로세스의 PID 와 이름은 무엇입니까?

정답> PID : 2944, 이름 : 0.9981548333304334.exe

근거>

	H	I	J	K	L
	Signer	Company	Image Path	Version	Launch String
2					
3			File not found: File not found: KernCap.vbs		
4					cscript KernCap.vbs
5	(Verified) NAVER Corp.	NAVER Corp.	c:\Program Files\Naver\NaverCommon\NaverAdminAPISvc.exe	1.0.2.27	C:\Program Files\Naver\NaverCommon\NaverAdminAPISvc.exe
6	(Verified) Riverbed Technology, Inc.	Riverbed Technology, Inc.	c:\Program Files\WinPcap\Wpcapd.exe	4.1.0.2980	"%ProgramFiles%\WinPcap\Wpcapd.exe" -d -f "%ProgramFiles%\WinPcap\Wpcapd.ini"
7	(Verified) Oracle Corporation	Oracle Corporation	c:\Windows\System32\Wboxservice.exe	4.3.12.0	system32\WboxService.exe
8	(Not verified) VMware, Inc.	VMware, Inc.	c:\Program Files\VMware\VMware Tools\Wmware_VGAuthService.exe	3.10.5.20562	"C:\Program Files\VMware\VMware Tools\Wmware_VGAuthService.exe"
9	(Verified) VMware, Inc.	VMware, Inc.	c:\Program Files\VMware\VMware Tools\Wmtoolsd.exe	3.10.5.49873	"C:\Program Files\VMware\VMware Tools\Wmtoolsd.exe"
10					
11	(Verified) Riverbed Technology, Inc.	Riverbed Technology, Inc.	c:\Windows\System32\drivers\Wnpl.sys	4.1.0.2980	system32\drivers\Wnpl.sys
12	(Verified) Oracle Corporation	Oracle Corporation	c:\Windows\System32\drivers\Wboxguest.sys	4.3.12.0	system32\DRIVERS\WboxGuest.sys
13	(Verified) Oracle Corporation	Oracle Corporation	c:\Windows\System32\drivers\Wboxmouse.sys	4.3.12.0	system32\DRIVERS\WboxMouse.sys
14	(Verified) Oracle Corporation	Oracle Corporation	c:\Windows\System32\drivers\Wboxsf.sys	4.3.12.0	system32\drivers\WboxSF.sys
15	(Verified) Oracle Corporation	Oracle Corporation	c:\Windows\System32\drivers\Wboxvideo.sys	4.3.12.0	system32\DRIVERS\WboxVideo.sys
16			File not found: System32\drivers\Wdvgkmd.sys		System32\drivers\Wdvgkmd.sys
17	(Verified) VMware, Inc.	VMware, Inc.	c:\Windows\System32\drivers\Wm3dnp.sys	8.15.1.32	system32\DRIVERS\Wm3dnp.sys
18	(Verified) VMware, Inc.	VMware, Inc.	c:\Windows\System32\drivers\Wmci.sys	3.7.1.0	system32\DRIVERS\Wmci.sys
19	(Verified) VMware, Inc.	VMware, Inc.	c:\Windows\System32\drivers\Wmhghfs.sys	3.2.33.0	system32\drivers\Wmhghfs.sys
20	(Verified) VMware, Inc.	VMware, Inc.	c:\Program Files\Common Files\VMware\Drivers\Wmmemctl.sys	7.3.5.0	W??C:\Program Files\Common Files\VMware\Drivers\Wmmemctl.sys
21	(Verified) VMware, Inc.	VMware, Inc.	c:\Windows\System32\drivers\Wmmouse.sys	12.5.2.0	system32\DRIVERS\Wmmouse.sys
22	(Verified) VMware, Inc.	VMware, Inc.	c:\Program Files\VMware\VMware Tools\Wmrawdsk.sys	0.9.7.0	W??C:\Program Files\VMware\VMware Tools\Wmrawdsk.sys
23	(Verified) VMware, Inc.	VMware, Inc.	c:\Windows\System32\drivers\Wmusmouse.sys	12.5.4.0	system32\DRIVERS\Wmusmouse.sys
24	(Verified) VMware, Inc.	VMware, Inc.	c:\Windows\System32\drivers\Wsock.sys	3.7.0.0	system32\drivers\Wsock.sys
25					
26	(Verified) VMware, Inc.	VMware, Inc.	c:\Windows\System32\Wmhghfs.dll	8.2.4.0	%SystemRoot%\System32\Wmhghfs.dll
27	(Verified) Oracle Corporation	Oracle Corporation	c:\Windows\System32\Wboxmnp.dll	4.3.12.0	C:\Windows\System32\WboxMNP.dll
28					
29	(Verified) VMware, Inc.	VMware, Inc.	c:\Windows\System32\Wsocklib.dll	3.7.0.0	%windir%\System32\Wsocklib.dll
30	(Verified) VMware, Inc.	VMware, Inc.	c:\Windows\System32\Wsocklib.dll	3.7.0.0	%windir%\System32\Wsocklib.dll
31					
32	(Verified) Microsoft Windows	Microsoft Corporation	c:\Windows\System32\cmd.exe	6.1.7601.17514	cmd.exe
33					
34	(Verified) Oracle Corporation	Oracle Corporation	c:\Windows\System32\Wboxtray.exe	4.3.12.0	C:\Windows\System32\WboxTray.exe
35	(Verified) Oracle America, Inc.	Sun Microsystems, Inc.	c:\Program Files\Common Files\Java\Update\WuSchad.exe	2.1.5.3	"c:\Program Files\Common Files\Java\Update\WuSchad.exe"
36			c:\Users\admin\AppData\Local\Temp\0.9981548333304334.exe		"C:\Users\admin\AppData\Local\Temp\0.9981548333304334.exe"

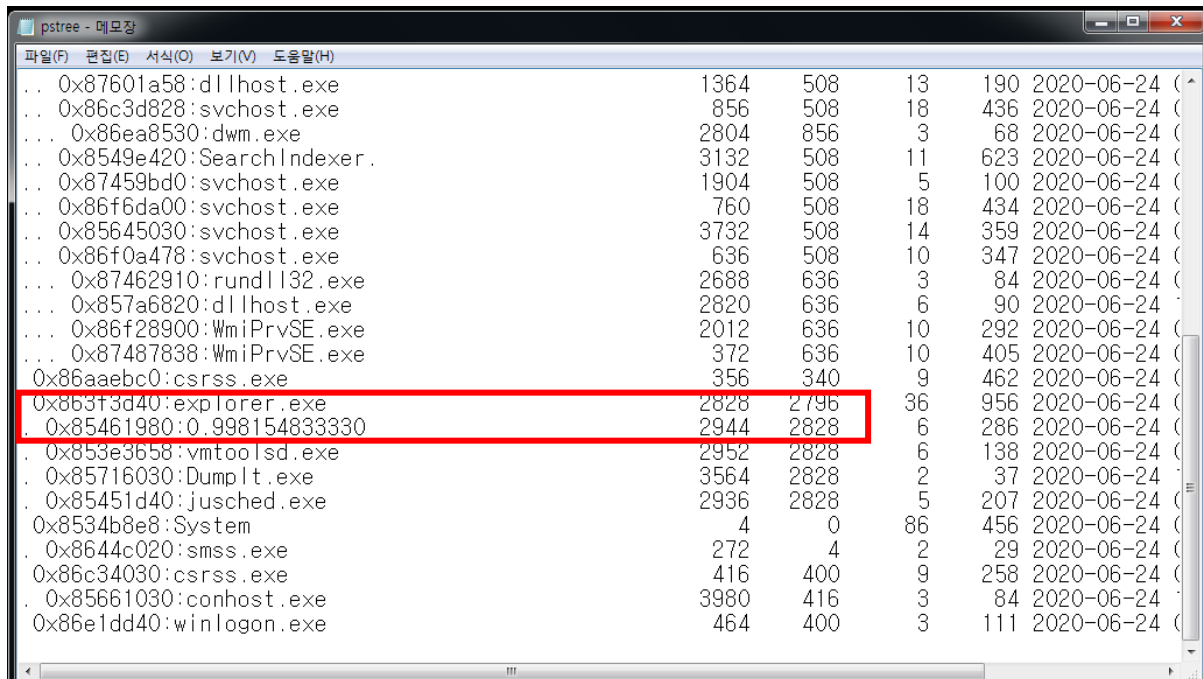
파일(F)	편집(E)	서식(O)	보기(V)	도움말(H)
svchost	856	8	17	424
svchost	904	8	44	1119
svchost	1080	8	14	596
svchost	1176	8	23	632
spoolsv	1292	8	12	264
svchost	1328	8	17	305
svchost	1440	8	14	233
NaverAdminAPISvc	1472	8	10	228
VGAuthService	1588	8	4	92
vmtoolsd	1612	13	9	290
svchost	1904	8	5	100
WmiPrvSE	2012	8	10	292
WmiPrvSE	372	8	12	414
dlhst	1364	8	13	190
msdtc	2108	8	12	131
taskhost	2396	8	9	166
sppsvc	2488	8	4	148
rundll32	2688	8	3	84
dwm	2804	8	3	68
explorer	2828	8	23	793
WuSchad	2936	8	5	207
0.9981548333304334	2944	8	8	292
vmtoolsd	2952	8	6	138
SearchIndexer	3132	8	11	621
svchost	3732	8	14	354
cmd	676	8	1	28
conhost	3332	8	3	86
TrustedInstaller	3048	8	6	212
msiexec	3568	8	4	104
pslist	2864	13	1	139

autoruns.csv 파일을 열어 보면 0.998154833330.exe 는 윈도우 운영체제의 빌트인 프로세스가 아니고, 실행 경로가 temp 폴더로 일반적이지 않고, (C:\Users\admin\AppData\Local\Temp\), 파일의 버전, 밴더 등과 관련된 정보가 없는 것으로 보아 악성코드임을 추측할 수 있다. 또한 pslist 를 확인한 결과 해당 프로세스의 pid 는 2944 임이 확인되었다.

질문 2> 질문 1에서 발견된 악성 프로세스의 부모 프로세스 PID와 이름은 무엇입니까?

정답> PID : 2828, 이름 : explorer.exe

근거>



Process Name	PID	PPID	Other Info
0x87601a58:dllhost.exe	1364	508	13 190 2020-06-24
0x86c3d828:svchost.exe	856	508	18 436 2020-06-24
0x86ea8530:dwm.exe	2804	856	3 68 2020-06-24
0x8549e420:SearchIndexer.exe	3132	508	11 623 2020-06-24
0x87459bd0:svchost.exe	1904	508	5 100 2020-06-24
0x86f6da00:svchost.exe	760	508	18 434 2020-06-24
0x85645030:svchost.exe	3732	508	14 359 2020-06-24
0x86f0a478:svchost.exe	636	508	10 347 2020-06-24
0x87462910:rundll32.exe	2688	636	3 84 2020-06-24
0x857a6820:dllhost.exe	2820	636	6 90 2020-06-24
0x86f28900:WmiPrvSE.exe	2012	636	10 292 2020-06-24
0x87487838:WmiPrvSE.exe	372	636	10 405 2020-06-24
0x86aaebc0:csrss.exe	356	340	9 462 2020-06-24
0x863f3d40:explorer.exe	2828	2796	36 956 2020-06-24
0x85461980:0.998154833330	2944	2828	6 286 2020-06-24
0x853e3658:vmtoolsd.exe	2952	2828	6 138 2020-06-24
0x85716030:DumpIt.exe	3564	2828	2 37 2020-06-24
0x85451d40:jusched.exe	2936	2828	5 207 2020-06-24
0x8534b8e8:System	4	0	86 456 2020-06-24
0x8644c020:smss.exe	272	4	2 29 2020-06-24
0x86c34030:csrss.exe	416	400	9 258 2020-06-24
0x85661030:conhost.exe	3980	416	3 84 2020-06-24
0x86e1dd40:winlogon.exe	464	400	3 111 2020-06-24

volatility 를 통해 수집한 pstree.txt 를 확인해 보면 부모 프로세스는 explorer.exe 이고 해당 프로세스의 pid 는 2828 임을 확인할 수 있다.

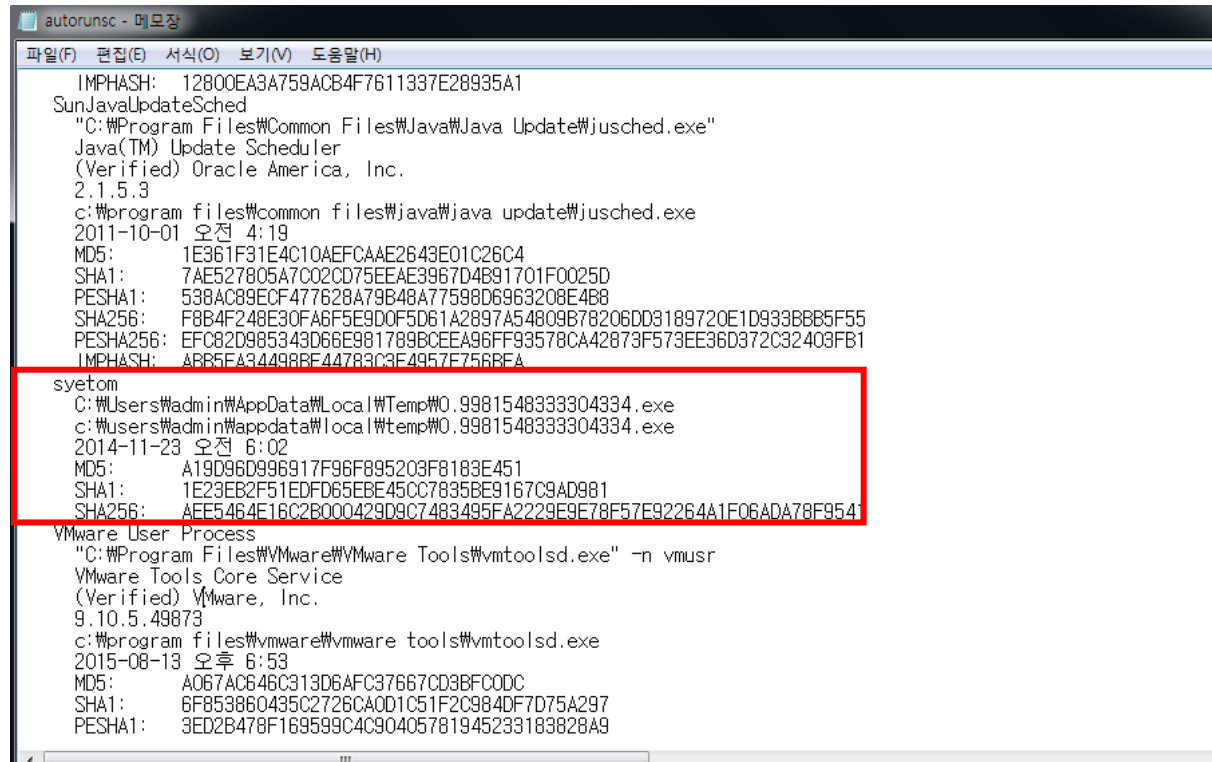
질문 3> 질문 1에서 발견된 악성 프로세스의 파일에 대한 Persistence(제어지속)을 위해 조작된 레지스트리의 1)키경로, 2)값이름, 3)데이터는 무엇입니까?

정답> 키경로 : HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

값이름 : syetom

데이터 : C:\Users\admin\AppData\Local\Temp\0.9981548333304334.exe

근거>



```
autorunsc - 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)
IMPHASH: 12800EA3A759ACB4F7611337E28935A1
SunJavaUpdateSched
"C:\Program Files\Common Files\Java\Java Update\jusched.exe"
Java(TM) Update Scheduler
(Verified) Oracle America, Inc.
2.1.5.3
c:\program files\common files\java\java update\jusched.exe
2011-10-01 오전 4:19
MD5: 1E361F31E4C10AEFCAAE2643E01C26C4
SHA1: 7AE527805A7C02CD75EEAE3967D4B91701F0025D
PESHA1: 538AC89ECF477628A79B48A77598D6963208E4B8
SHA256: F8B4F248E30FA6F5E9D0F5D61A2897A54809B78206DD3189720E1D933BBB5F55
PESHA256: EFC82D985343D66E981789BCCEA96FF93578CA42873F573EE36D372C32403FB1
IMPHASH: ABB5FA34498BF44783C3E4957F756BFA
syetom
C:\Users\admin\AppData\Local\Temp\0.9981548333304334.exe
C:\Users\admin\AppData\Local\Temp\0.9981548333304334.exe
2014-11-23 오전 6:02
MD5: A19D96D996917F96F895203F8183E451
SHA1: 1E23EB2F51EDF065EBE45CC7835BE9167C9AD981
SHA256: AEE5464E16C2B000429D9C7483495FA2229E9E78F57E92264A1F06ADA78F9541
VMware User Process
"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr
VMware Tools Core Service
(Verified) VMware, Inc.
9.10.5.49873
c:\program files\vmware\vmware tools\vmtoolsd.exe
2015-08-13 오후 6:53
MD5: A067AC646C313D6AFC37667CD3BFC0DC
SHA1: 6F853860435C2726CA0D1C51F2C984DF7D75A297
PESHA1: 3ED2B478F169599C4C90405781945233183828A9
```

autorunsc.txt 에서 syetom 값 데이터에 0.9981548333304334.exe 가 발견되었으니 syetom 이 조작된 레지스트리이다.

2014-11-23 오전 6:02	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	syetom	enabled	Login	System-wide
36	C:\Users\admin\AppData\Local\Temp\0.9981548333304334.exe	C:\Users\admin\AppData\Local\Temp\0.9981548333304334.exe			

1번 문제에서 확인했던 autorunsc.csv 파일을 열어 보면 해당 악성코드의 레지스트리 경로를 알 수 있다. 따라서 레지스트리의 경로는

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 이고 값 이름은 syetom이며, 데이터는 C:\Users\admin\AppData\Local\Temp\0.9981548333304334.exe이다.

질문 4> 질문 1에서 발견된 악성 코드가 존재하는 파일 시스템상 경로는 무엇 입니까? (경로에 포함된 모든 영문자를 소문자로 적어 주시고, 폴더 문자는 역슬래시("\")를 사용합니다. (E.G c:\windows\temp\malware.exe)

정답> c:\users\admin\appdata\local\temp\0.998154833304334.exe

근거>

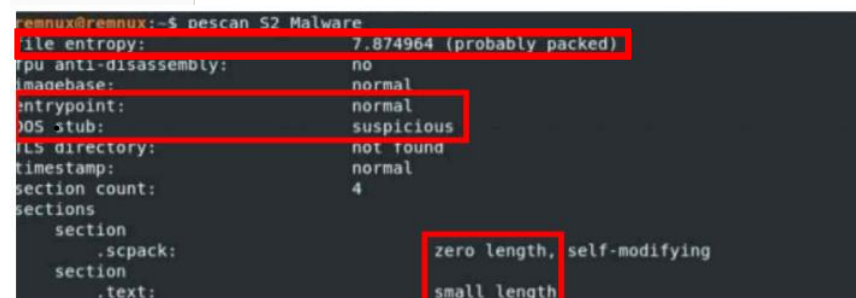
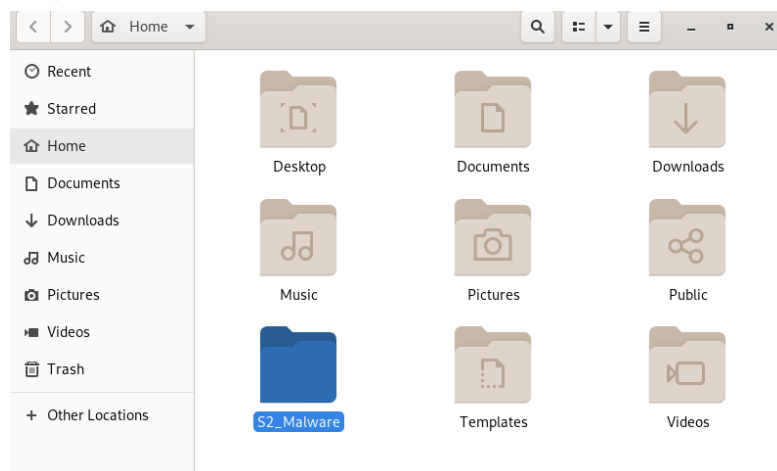


확인했던 autoruns.csv 파일의 Image Path 항목을 보면 해당 악성코드가 존재하는 경로를 알 수 있다.

질문 5> 질문 1에서 발견된 악성 코드는 질문 4의 답으로 패스워드가 설정된 상태로 압축되어 있습니다. 해당 파일을 PESCANNER 도구를 이용하여 분석한 후 발견되는 이상 징후를 모두 서술하세요.

정답> “SUSPICIOUS”라는 글자, 엔트로피 값이 7 이상, .spac 섹션이 0, .text 섹션이 작음,

근거>



해당 악성 코드를 remnux로 이동시킨 뒤 remnux의 pscanner를 이용하여 해당 악성코드를 분석한 결과 “SUSPICIOUS”라는 글자가 뜨고, 엔트로피 값이 7이상으로 높으며, 섹션들의 크기가 0 또는 작으므로 이상 징후로 판단된다고 할 수 있다.

질문 6> 질문 1에서 발견된 악성 코드가 파일 시스템에 생성된 시간을 찾으세요.

정답> 2015.06.23. 21:21:50

근거>

1 /Users/admin/AppData/LocalLow/Sun/Java/Deployment/cache/6.0/lastAccessed	2015-06-23 21:21:50.3	2015-06-
1 /Users/admin/AppData/LocalLow/Sun/Java/Deployment/cache/6.0/18/99c4792-5292ca67.idx	2015-06-23 21:21:50.3	2015-06-
1 /Users/admin/AppData/LocalLow/Sun/Java/Deployment/cache/6.0/18/00c4792-5292ca67	2015-06-23 21:21:50.3	2015-06-
2 /Users/admin/AppData/Local/Temp/0.998154833304334.exe	2015-06-23 21:21:50.7	2015-06-
1 /Users/admin/AppData/LocalLow/Sun/Java/Deployment/cache/6.0/39/ba8243e7-bc52846f.idx	2015-06-23 21:21:50.7	2015-06-
1 /Users/admin/AppData/LocalLow/Sun/Java/Deployment/cache/6.0/39/5a8243e7-bc52846f	2015-06-23 21:21:50.7	2015-06-
2 /Users/admin/AppData/Local/Temp/Internet Files/Content.IE5/ABD/C6DS/ahewalcnma11	2015-06-23 21:21:50.7	2015-06-

MFT의 \$FN의 생성시간을 확인한 결과 2015.06.23. 21:21:50임이 확인되었다.

질문 7> 질문 1에서 발견된 악성 코드가 최초로 실행된 시간(추정값)을 찾으세요.

정답> 2015.06.23. 21:21:50

근거>

Windows/Prefetch/0.998154833304334.EXE-0DF40D6A.pf	2015-06-23 21:22:00.3201
--	--------------------------

/Windows/Prefetch/0.998154833304334.EXE-0DF40D6A.pf의 Std Info Creation date 탭을 확인한 결과 2015-06-23 21:22:00에 실행되었고 악성코드의 최초 실행 시간은 생성시간에서 10초를 뺀 2015.06.23. 21:21:50 이다.