2018
Volatility Analysis Contest

[2018 PyeongChang Olympic Destroyer]

MalGround

(malground7@gmail.com)

INDEX

1. INTRODUCTION

1.1 Profile

1) Team Name : MalGround

2) Country : South Korea

3) Member

- Han Eol LEE
- Tae Woo KIM
- Han Sol KIM
- Eun Jin JEON
- Ji Heouk HAN
- Jong Min KIM
- Jong Hyeon KIM

1.2 Summary of Malware

Name	Olympic_Session_V10_공지용.xls
Size	109KB
Characteristics	Connect with attacker server
MD5	A3EA62825308F53E8E9CCEA3D4F93C4B
SHA-1	CAE31C5C30DA3B388204F4AF74EDF4554FC6A867
SHA-256	663A82A81804EE35B9BFD1CFBD8743D43362554FD7F1EB985EEDB33EC3152EFC

Name	OlympicDestroyerer.exe
Size	1.77MB
Characteristics	System destruction
MD5	E47A8628CE9DDA4F31B335A79E753583
SHA-1	6CC7C454CC3B00C7E0D12B89B941D47A5EBAA42A
SHA-256	BC4E00970BB3FB22A21D087B59488FC806D115D51B6088B4B861FB9A04285D2E

1.3 Analysis Environment

	OS	Computer Name	Domain
Active Directory Server	Windows Server 2008 R2 standard x64	Server	Pyeongchang2018.com
Victim PC	Windows 7 Ultimate K x86	Victim	Pyeongchang2018.com
Attacker PC	Linux Kali x64		

- Analysis performed with the volatility 2.6 release.

1.4 Background

"Olympic Destroyer: who hacked the Olympics?"

The PyeongChang Winter Olympic Games started with a scandal: unknown hackers attacked the servers just before the opening ceremonies and many spectators were unable to attend the ceremonies as they were unable to print out tickets.

[Article 1] Kaspersky_180309

[Figure 1] BBC PyeongChang cyber attack report and error screen

At the opening ceremony of the PyeongChang Winter Olympics on February 9, 2018, there was a failure in the field of wired and wireless network systems. In succession, the official website operation for the transmission of the Wi-Fi service and the sale and output of the IPTV video from the main press center (MPC) was suspended.

This was a hacker's cyber attack to disrupt the Olympics, and the initial route of infection was revealed through a spear phishing Email. It is expected that this method is intended to disrupt operation or operation of IT-based services by destroying systems with destructive malware. The malware was named the "Olympic Destroyer".

Based on the above actual events, we will analyze the re-intervention incidents. The parts not working in the "Olympic Destroyer" used at the time were modified to make them work, and the Email content and infection paths are reconstructed based on reality and may differ from the actual ones.

---

1) [Article 1] https://www.kaspersky.com/blog/olympic-destroyer/21494/

2. OVERVIEW OF THE INCIDENT

2-1. Incident scenario

On the eve of the opening ceremony of the 2018 PyeongChang Winter Olympic Games on September 24, 2018, an Email arrived from the organizing committee in front of the Olympic ticket manager, Mr. OOO. It means that the schedule for the Olympic Games has been updated.

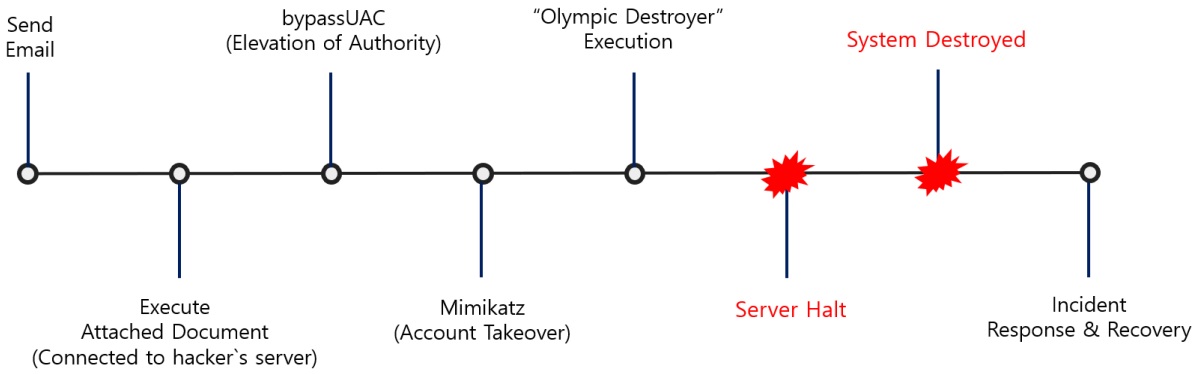
Mr. OOO checked the attached file "Olympic_Session_V10" in the mail and updated the schedule on the homepage.

The next day, the official PyeongChang Olympic homepage server was shut down, and PC on the site were interrupted one after another. Right after the accident, the security team dumped memory from the PC that was believed to have been infected for the first time.

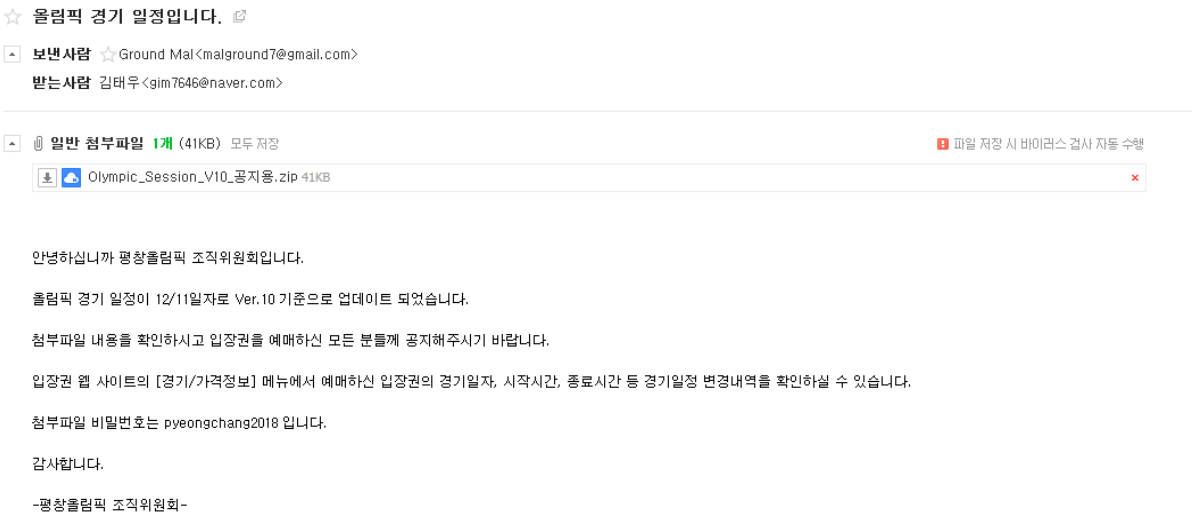
2-2. Summary of incident

Classification	Description
Infection path and method of document type malware	- Downloaded document type malware by spear phishing Email - After PC user execute the document, connected with hacker server
Attacker behavior	- Using Empire(Malware platform using PowerShell script) 1) Elevated the authority by bypassUAC module 2) Acquisition of Credentials in Active Directory environment by using a Mimikatz module 3) Inflow malware remotely by shellcode hacker injected and execute
Malware feature	- Through the captured Credentials, did Lateral Movement - After malware Lateral spread, it destroys MBR section
Incident feature	- Spread malware in Active Directory environment - System destroyed and unrecoverable after malware execution

2-3. Incident timeline



(1) Sent a Spear Phishing Email with document type malware attached to Olympic ticket manager


올림픽 경기 일정입니다.

보낸사람 Ground Mal<malground7@gmail.com>

받는사람 김태우<gim7646@naver.com>

일반 첨부파일 1개 (41KB) 모두 저장 — 파일 저장 시 바이러스 검사 자동 수행

Olympic_Session_V10_공지용.zip 41KB

안녕하십니까 평창올림픽 조직위원회입니다.

올림픽 경기 일정이 12/11일자로 Ver.10 기준으로 업데이트 되었습니다.

첨부파일 내용을 확인하시고 입장권을 예매하신 모든 분들께 공지해주시기 바랍니다.

입장권 웹 사이트의 [경기/가격정보] 메뉴에서 예매하신 입장권의 경기일자, 시작시간, 종료시간 등 경기일정 변경내역을 확인하실 수 있습니다.

첨부파일 비밀번호는 pyeongchang2018 입니다.

감사합니다.

-평창올림픽 조직위원회-

<Translated Email Content>

Title: Olympic games schedule

Attached File: Olympic_Session_v10_for Notice.zip

Hello, this is PyeongChang Olympic Organizing Committee.

The Olympic Games schedule was updated on December 11 as Ver10.

Please confirm the contents of the attached file and inform all those who reserved the ticket.

You can check the details of the game schedule, such as the date, start time, and end time of tickets you have booked from the [Match / Price Info] menu of the admission website.

The attachment file password is pyeongchang2018.

Thank you.

- PyeongChang Olympic Organizing Committee -

(2) When the document file attached to the Email is downloaded and viewed, malicious code contained in the document file is executed and connected to the server of the hacker.

(3) Hacker acquires AD Environment Credentials of Bot using Empire

  ㄴ Module used: bypassUAC, Mimikatz

(4) Inflow Malware(Olympic Destroyer)

  ㄴ ShellCode used

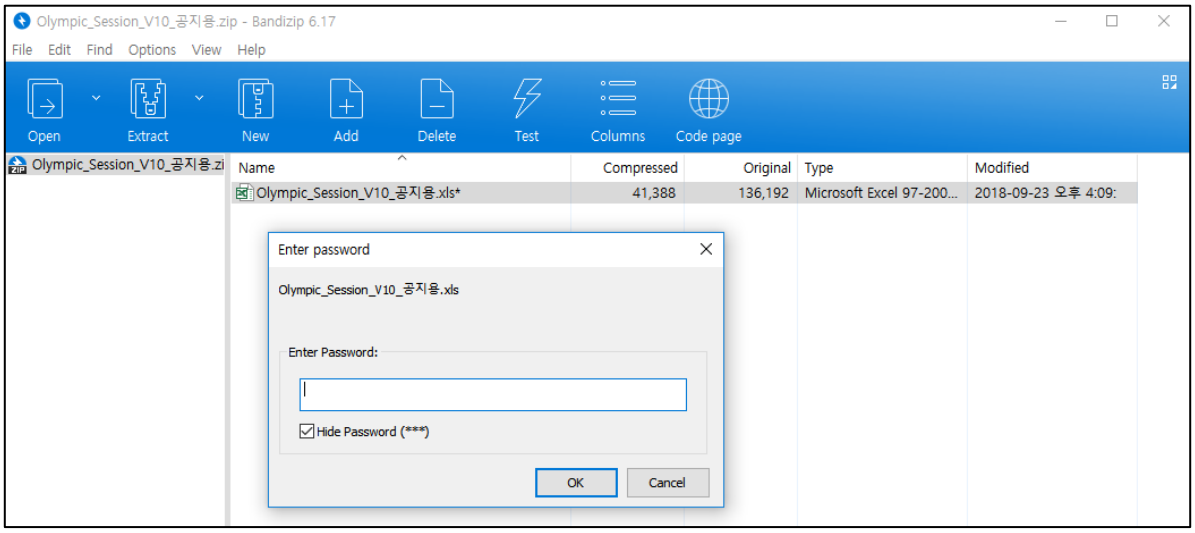
(5) Malware Spread by Credentials and executing itself

(6) Destroy System(MBR Section Destroy)

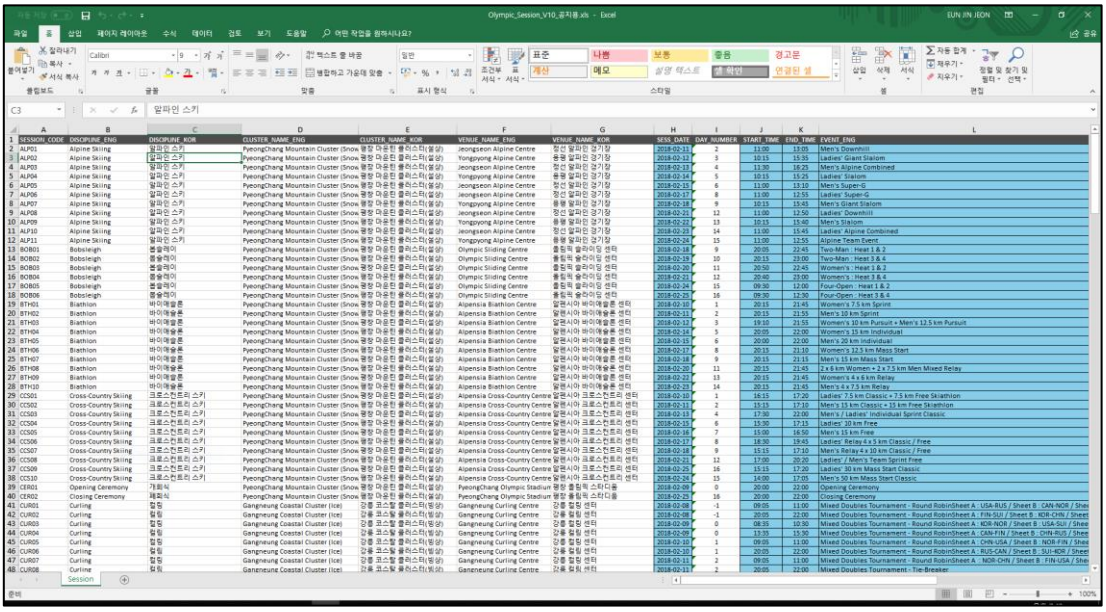
3. INCIDENT ANALYSIS

3.1 Method of malware infection

The attacker sent a spear phishing Email with a malicious document file to Olympic ticket manager. The user is connected to the attacker's server when viewing the file. The attachment is a compressed file that encrypted MS Excel file (.xls) and the password is written in an Email.



[Figure 2] Compressed file attached to spear phishing Email(ZIP)

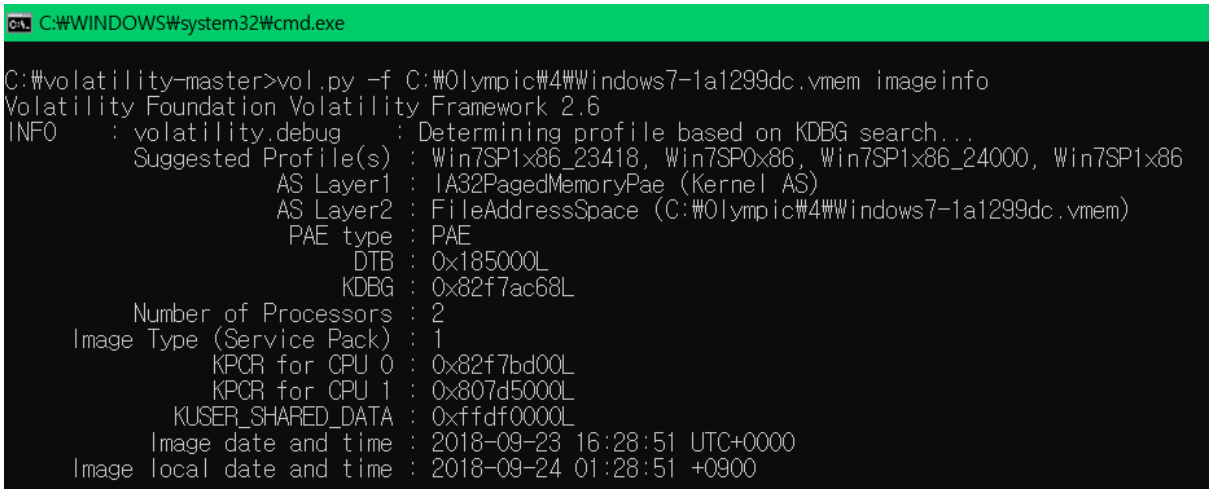


[Figure 3] Part of "Olympic_Session_V10_공지용.xls"

The content of the Email is that the schedule of the game has changed, so the ticket manager who is the target of the attack has no choice but to view it.

3.2 In-depth analysis

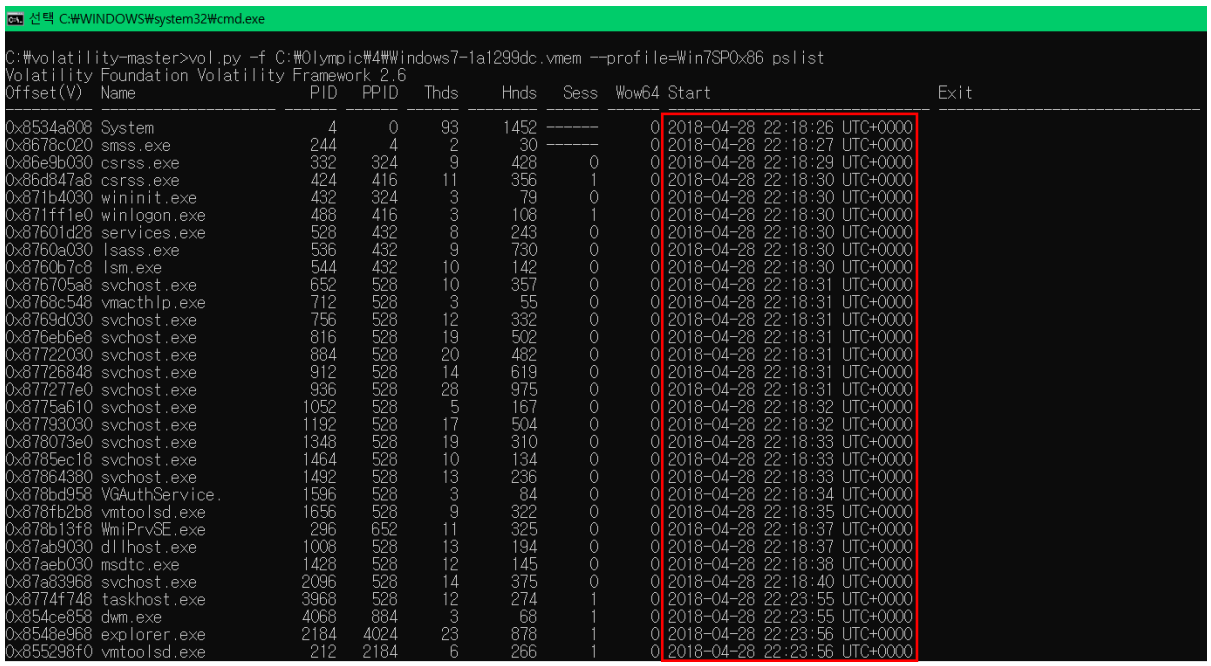
As shown below, operationg system information was identified by using "imageinfo" plugin.



[Figure 4] imageinfo

As a result of identification, victim's PC was running a Windows 7 32bit operating system, and since there are two fields related to KPCR, victim's PC has two central processing units.

After identifying the operating system according to NIST 800-86 and IETF RFC 3227, the result of checking the start time of processes are divided into four major parts as shown below.



[Figure 5] Process Start Time Part 1

It can be expected that the basic processes are loaded since the term of processes start time is relatively short 2018-04-28 22:18:26 to 2018-04-28 22:23:56 and most of process's name is windows basic process.

선택 C:₩WINDOWS₩system32₩cmd.exe

0x8548e968	explorer.exe	2184	4024	23	878	1	0	2018-04-28 22:23:56 UTC+0000	
0x855298f0	vmtoolsd.exe	212	2184	6	266	1	0	2018-04-28 22:23:56 UTC+0000	
0x85c948e0	spoolsv.exe	3132	528	12	334	0	0	2018-09-23 06:22:49 UTC+0000	
0x85b4a030	armsvc.exe	3764	528	4	63	0	0	2018-09-23 06:33:30 UTC+0000	
0x85c6e2b8	SearchIndexer.	2264	528	13	588	0	0	2018-09-23 07:23:28 UTC+0000	
0x85addd28	OSPPSVC.EXE	1700	528	3	123	0	0	2018-09-23 07:25:32 UTC+0000	
0x857319c8	powershell.exe	596	296	13	448	1	0	2018-09-23 07:25:51 UTC+0000	
0x857148e8	conhost.exe	620	424	2	30	1	0	2018-09-23 07:25:51 UTC+0000	
0x85742b78	OlympicDestroy	3528	596	8	220	1	0	2018-09-23 16:16:56 UTC+0000	
0x859ce348	ocxip.exe	3340	3528	0	--------	1	0	2018-09-23 16:16:56 UTC+0000	2018-09-23 16:16:56 UTC+0000
0x85883030	teikv.exe	1648	3528	0	--------	1	0	2018-09-23 16:16:56 UTC+0000	2018-09-23 16:16:56 UTC+0000
0x859e0cc0	_xut.exe	2432	3528	3	70	1	0	2018-09-23 16:16:57 UTC+0000	
0x85a1bb38	taskeng.exe	2192	936	4	79	0	0	2018-09-23 16:24:23 UTC+0000	
0x859ded28	cmd.exe	152	1656	0	--------	0	0	2018-09-23 16:28:51 UTC+0000	2018-09-23 16:28:51 UTC+0000
0x85756d28	conhost.exe	2588	332	0	29	0	0	2018-09-23 16:28:51 UTC+0000	2018-09-23 16:28:51 UTC+0000

[Figure 6] Process Start Time Part 2

The second time, between 2018-09-23 06:22:49 and 2018-09-23 06:33:30. It can see the spool sv.exe which is a process Windows basic process and armsvc.exe which is a process related to Adobe Reader which is Adobe's product. And can't identify distinct features.

선택 C:₩WINDOWS₩system32₩cmd.exe

0x8548e968	explorer.exe	2184	4024	23	878	1	0	2018-04-28 22:23:56 UTC+0000	
0x855298f0	vmtoolsd.exe	212	2184	6	266	1	0	2018-04-28 22:23:56 UTC+0000	
0x85c948e0	spoolsv.exe	3132	528	12	334	0	0	2018-09-23 06:22:49 UTC+0000	
0x85b4a030	armsvc.exe	3764	528	4	63	0	0	2018-09-23 06:33:30 UTC+0000	
0x85c6e2b8	SearchIndexer.	2264	528	13	588	0	0	2018-09-23 07:23:28 UTC+0000	
0x85addd28	OSPPSVC.EXE	1700	528	3	123	0	0	2018-09-23 07:25:32 UTC+0000	
0x857319c8	powershell.exe	596	296	13	448	1	0	2018-09-23 07:25:51 UTC+0000	
0x857148e8	conhost.exe	620	424	2	30	1	0	2018-09-23 07:25:51 UTC+0000	
0x85742b78	OlympicDestroy	3528	596	8	220	1	0	2018-09-23 16:16:56 UTC+0000	
0x859ce348	ocxip.exe	3340	3528	0	--------	1	0	2018-09-23 16:16:56 UTC+0000	2018-09-23 16:16:56 UTC+0000
0x85883030	teikv.exe	1648	3528	0	--------	1	0	2018-09-23 16:16:56 UTC+0000	2018-09-23 16:16:56 UTC+0000
0x859e0cc0	_xut.exe	2432	3528	3	70	1	0	2018-09-23 16:16:57 UTC+0000	
0x85a1bb38	taskeng.exe	2192	936	4	79	0	0	2018-09-23 16:24:23 UTC+0000	
0x859ded28	cmd.exe	152	1656	0	--------	0	0	2018-09-23 16:28:51 UTC+0000	2018-09-23 16:28:51 UTC+0000
0x85756d28	conhost.exe	2588	332	0	29	0	0	2018-09-23 16:28:51 UTC+0000	2018-09-23 16:28:51 UTC+0000

[Figure 7] Process Start Time Part 3

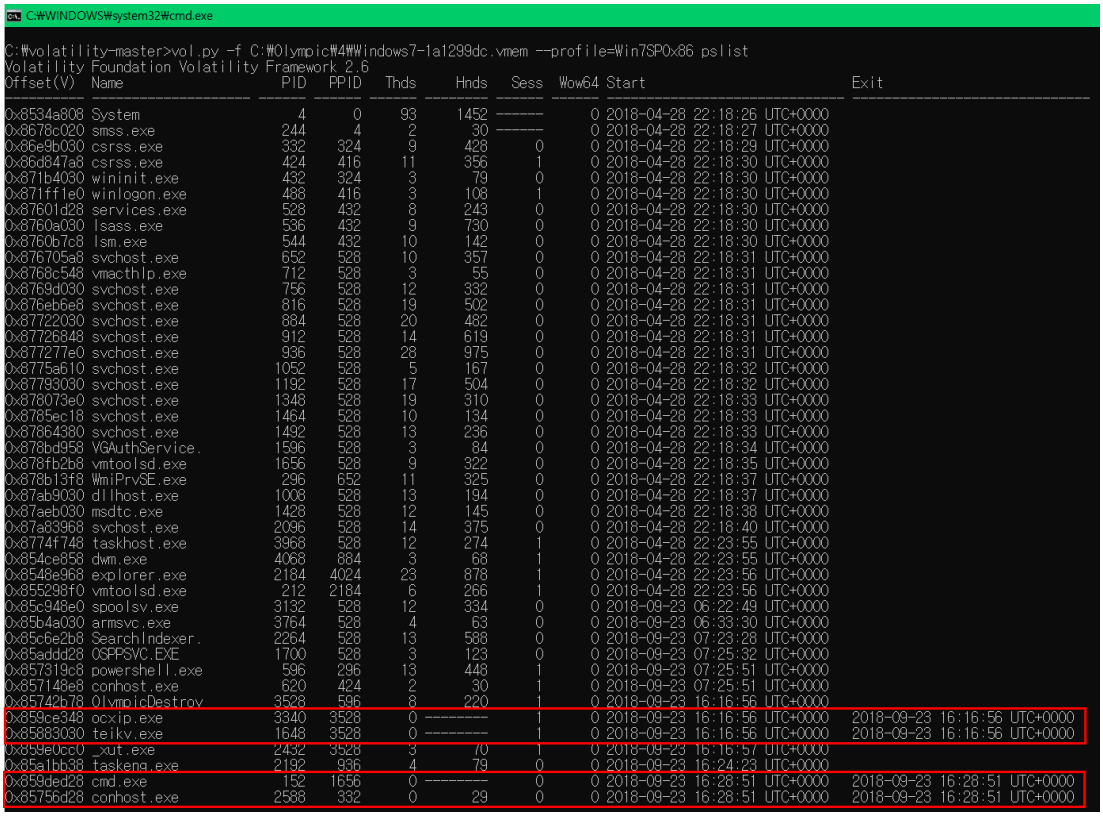
Compared with the processes start time shown in [Figure 6], It can be confirmed that the execution was performed at intervals of about 50 minutes.

선택 C:₩WINDOWS₩system32₩cmd.exe

0x8548e968	explorer.exe	2184	4024	23	878	1	0	2018-04-28 22:23:56 UTC+0000	
0x855298f0	vmtoolsd.exe	212	2184	6	266	1	0	2018-04-28 22:23:56 UTC+0000	
0x85c948e0	spoolsv.exe	3132	528	12	334	0	0	2018-09-23 06:22:49 UTC+0000	
0x85b4a030	armsvc.exe	3764	528	4	63	0	0	2018-09-23 06:33:30 UTC+0000	
0x85c6e2b8	SearchIndexer.	2264	528	13	588	0	0	2018-09-23 07:23:28 UTC+0000	
0x85addd28	OSPPSVC.EXE	1700	528	3	123	0	0	2018-09-23 07:25:32 UTC+0000	
0x857319c8	powershell.exe	596	296	13	448	1	0	2018-09-23 07:25:51 UTC+0000	
0x857148e8	conhost.exe	620	424	2	30	1	0	2018-09-23 07:25:51 UTC+0000	
0x85742b78	OlympicDestroy	3528	596	8	220	1	0	2018-09-23 16:16:56 UTC+0000	
0x859ce348	ocxip.exe	3340	3528	0	--------	1	0	2018-09-23 16:16:56 UTC+0000	2018-09-23 16:16:56 UTC+0000
0x85883030	teikv.exe	1648	3528	0	--------	1	0	2018-09-23 16:16:56 UTC+0000	2018-09-23 16:16:56 UTC+0000
0x859e0cc0	_xut.exe	2432	3528	3	70	1	0	2018-09-23 16:16:57 UTC+0000	
0x85a1bb38	taskeng.exe	2192	936	4	79	0	0	2018-09-23 16:24:23 UTC+0000	
0x859ded28	cmd.exe	152	1656	0	--------	0	0	2018-09-23 16:28:51 UTC+0000	2018-09-23 16:28:51 UTC+0000
0x85756d28	conhost.exe	2588	332	0	29	0	0	2018-09-23 16:28:51 UTC+0000	2018-09-23 16:28:51 UTC+0000

[Figure 8] Process Start Time Part 4

Compared with the time zone in [Figure 7], there are about 9hour intervals and there are many suspicious parts.



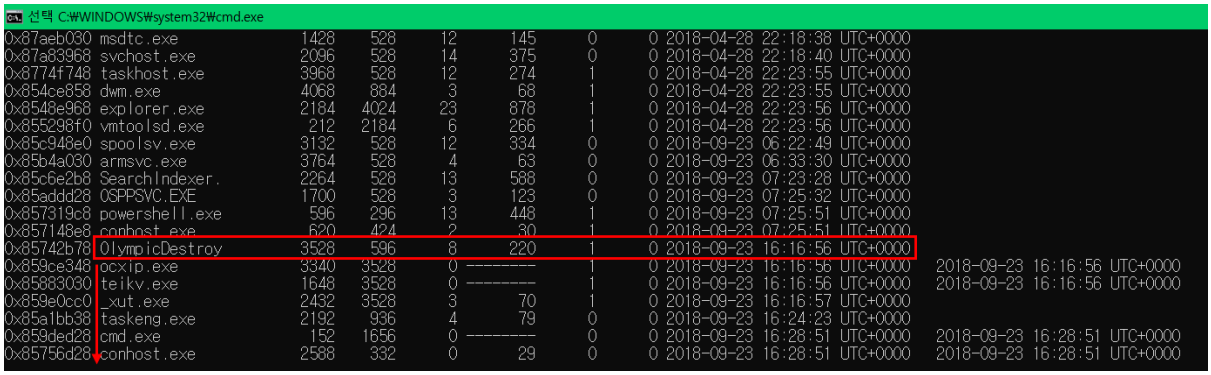
```
C:₩WINDOWS₩system32₩cmd.exe

C:₩volatility-master>vol.py -f C:₩Olympic₩4₩Windows7-1a1299dc.vmem --profile=Win7SP0x86 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x8534a808 System                    4      0     93     1452 ------      0 2018-04-28 22:18:26 UTC+0000
0x8678c020 smss.exe                244      4      2       30 ------      0 2018-04-28 22:18:27 UTC+0000
0x86e9b030 csrss.exe               332    324      9      428      0      0 2018-04-28 22:18:29 UTC+0000
0x86d847a8 csrss.exe               424    416     11      356      1      0 2018-04-28 22:18:30 UTC+0000
0x871b4030 wininit.exe             432    324      3       79      0      0 2018-04-28 22:18:30 UTC+0000
0x871ff1e0 winlogon.exe            488    416      3      108      1      0 2018-04-28 22:18:30 UTC+0000
0x87601d28 services.exe            528    432      8      243      0      0 2018-04-28 22:18:30 UTC+0000
0x8760a030 lsass.exe               536    432      9      730      0      0 2018-04-28 22:18:30 UTC+0000
0x8760b7c8 lsm.exe                 544    432     10      142      0      0 2018-04-28 22:18:30 UTC+0000
0x876705a8 svchost.exe             652    528     10      357      0      0 2018-04-28 22:18:31 UTC+0000
0x8768c548 vmacthlp.exe            712    528      3       55      0      0 2018-04-28 22:18:31 UTC+0000
0x8769d030 svchost.exe             756    528     12      332      0      0 2018-04-28 22:18:31 UTC+0000
0x876eb6e8 svchost.exe             816    528     19      502      0      0 2018-04-28 22:18:31 UTC+0000
0x87722030 svchost.exe             884    528     20      482      0      0 2018-04-28 22:18:31 UTC+0000
0x87726848 svchost.exe             912    528     14      619      0      0 2018-04-28 22:18:31 UTC+0000
0x877277e0 svchost.exe             936    528     28      975      0      0 2018-04-28 22:18:31 UTC+0000
0x8775a610 svchost.exe            1052    528      5      167      0      0 2018-04-28 22:18:32 UTC+0000
0x87793030 svchost.exe            1192    528     17      504      0      0 2018-04-28 22:18:32 UTC+0000
0x878073e0 svchost.exe            1348    528     19      310      0      0 2018-04-28 22:18:33 UTC+0000
0x8785ec18 svchost.exe            1464    528     10      134      0      0 2018-04-28 22:18:33 UTC+0000
0x87864380 svchost.exe            1492    528     13      236      0      0 2018-04-28 22:18:33 UTC+0000
0x878bd958 VGAuthService.         1596    528      3       84      0      0 2018-04-28 22:18:34 UTC+0000
0x878fb2b8 vmtoolsd.exe           1656    528      9      322      0      0 2018-04-28 22:18:35 UTC+0000
0x878b13f8 WmiPrvSE.exe            296    652     11      325      0      0 2018-04-28 22:18:37 UTC+0000
0x87ab9030 dllhost.exe            1008    528     13      194      0      0 2018-04-28 22:18:37 UTC+0000
0x87aeb030 msdtc.exe              1428    528     12      145      0      0 2018-04-28 22:18:38 UTC+0000
0x87a83968 svchost.exe            2096    528     14      375      0      0 2018-04-28 22:18:40 UTC+0000
0x8774f748 taskhost.exe           3968    528     12      274      1      0 2018-04-28 22:23:55 UTC+0000
0x854ce858 dwm.exe                4068    884      3       68      1      0 2018-04-28 22:23:55 UTC+0000
0x8548e968 explorer.exe           2184   4024     23      878      1      0 2018-04-28 22:23:56 UTC+0000
0x855298f0 vmtoolsd.exe            212   2184      6      266      1      0 2018-04-28 22:23:56 UTC+0000
0x85c948e0 spoolsv.exe            3132    528     12      334      0      0 2018-09-23 06:22:49 UTC+0000
0x85b4a030 armsvc.exe             3764    528      4       63      0      0 2018-09-23 06:33:30 UTC+0000
0x85c6e2b8 SearchIndexer.         2264    528     13      588      0      0 2018-09-23 07:23:28 UTC+0000
0x85addd28 OSPPSVC.EXE            1700    528      3      123      0      0 2018-09-23 07:25:32 UTC+0000
0x857319c8 powershell.exe          596    296     13      448      1      0 2018-09-23 07:25:51 UTC+0000
0x857148e8 conhost.exe             620    424      2       30      1      0 2018-09-23 07:25:51 UTC+0000
0x85742b78 OlympicDestroy         3528    596      8      220      1      0 2018-09-23 16:16:56 UTC+0000
0x859ce348 ocxip.exe              3340   3528      0 --------      1      0 2018-09-23 16:16:56 UTC+0000   2018-09-23 16:16:56 UTC+0000
0x85883030 teikv.exe              1648   3528      0 --------      1      0 2018-09-23 16:16:56 UTC+0000   2018-09-23 16:16:56 UTC+0000
0x859e0cc0 _xut.exe               2432   3528      3       70      1      0 2018-09-23 16:16:57 UTC+0000
0x85a1bb38 taskeng.exe            2192    936      4       79      0      0 2018-09-23 16:24:23 UTC+0000
0x859ded28 cmd.exe                 152   1656      0 --------      0      0 2018-09-23 16:28:51 UTC+0000   2018-09-23 16:28:51 UTC+0000
0x85756d28 conhost.exe            2588    332      0       29      0      0 2018-09-23 16:28:51 UTC+0000   2018-09-23 16:28:51 UTC+0000
```

[Figure 9] Remarkable processes

[Figure 9] shows the first thing that stands out the overall result of the pslist, and It can be confirmed that processes are terminated as soon as it is started, as you can get enough suspicion.

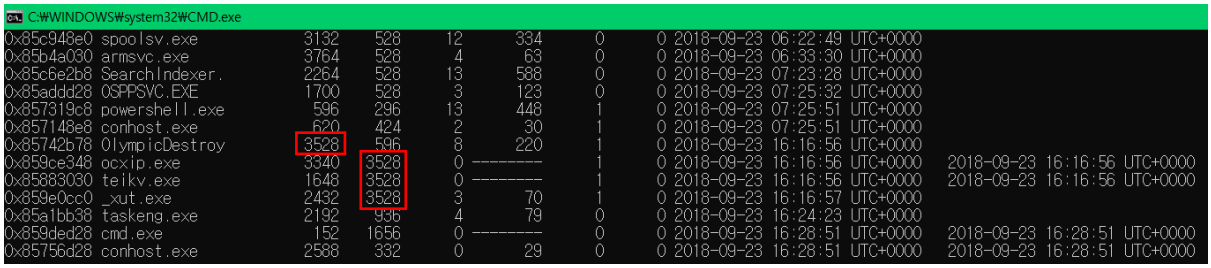
- Ocxip.exe (Start : 2018-09-23 16:16:56 UTC+0000, Exit : 2018-09-23 16:16:56 UTC+0000)
- Teikv.exe (Start : 2018-09-23 16:16:56 UTC+0000, Exit : 2018-09-23 16:16:56 UTC+0000)
- Cmd.exe (Start : 2018-09-23 16:28:51 UTC+0000, Exit : 2018-09-23 16:28:51 UTC+0000)
- Conhost.exe(Start : 2018-09-23 16:28:51 UTC+0000, Exit : 2018-09-23 16:28:51 UTC+0000)

Usually, if a process terminated immediately after it is started, the possibility that the process has committed malicious activity is usually very high and should be the focus of analysis.



[Figure 10] Checking OlympicDestroyer

Before execution of remarkable processes in [Figure 9], It can be confirmed that suspicious process name of "OlympicDestroyer" which has a pid 3528, and as you can see in below, three child processes are created.

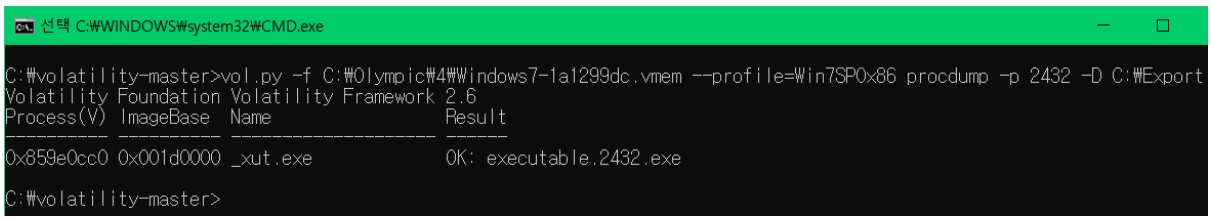


[Figure 11] Checking child processes

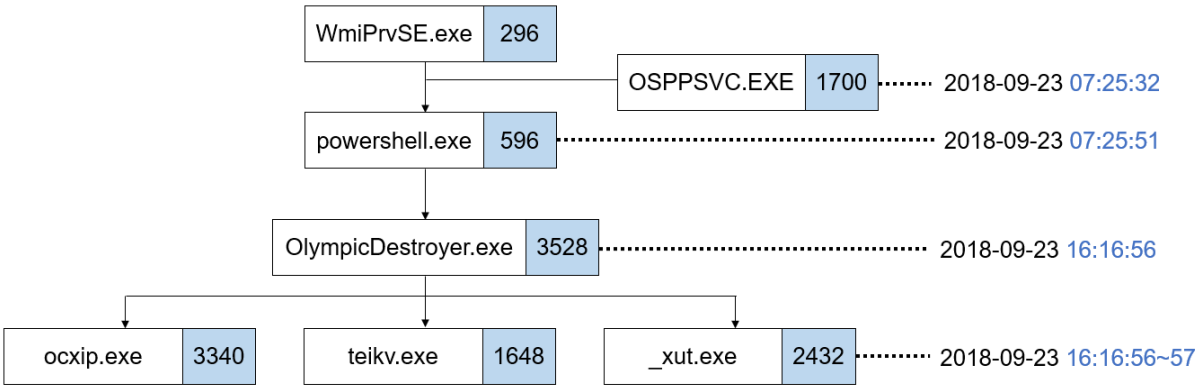
The list of Child processes of OlympicDestroyer is as follows.

- Ocxip.exe (PID 3340, PPID 3528)
- Teikv.exe (PID 1648, PPID 3528)
- _xut.exe (PID 2432, PPID 3528)

It is difficult to judge that the process names of the above processes to have a special meaning, and It can infer that processes name are created randomly by OlympicDestroyer, and since _xut.exe is currently active, the processes were extracted and checked the data as shown below.

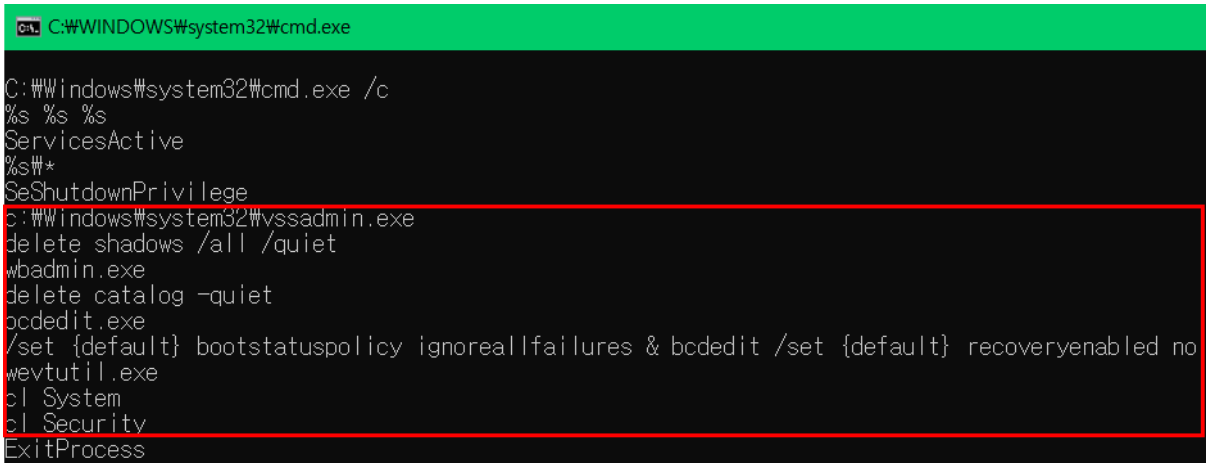


[Figure 12] Extracting _xut.exe



[Figure 13] Process tree and Timeline

After performing the extraction process as above, the malicious behavior as shown below was checked by using "string" command.



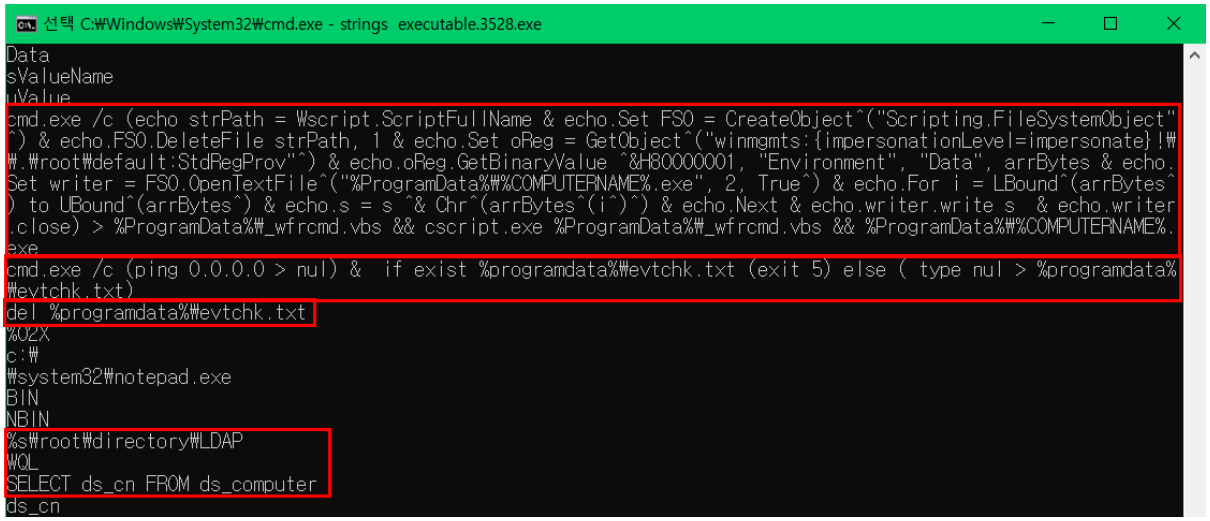
[Figure 14] Checking malicious behavior

1. All the Volume Shadow Copy are deleted using vssadmin.exe
2. All the Windows Backup Catalog are deleted using wbadmin.exe
3. Windows Error Recovery Alert and Recovery mode are disabled using Bcdedit.exe
4. Disable windows error recovery alerts and recovery mode using bcdedit.exe
5. Delete System and Security log using wevtutil.exe

It can be confirmed that the attacker intends to disturb availability of victim's PC by removing system's available recovery means, and The OlympicDestroyer currently active was extracted in order to confirm additional activity as shown below.

[Figure 15] Extracting OlympicDestroyer

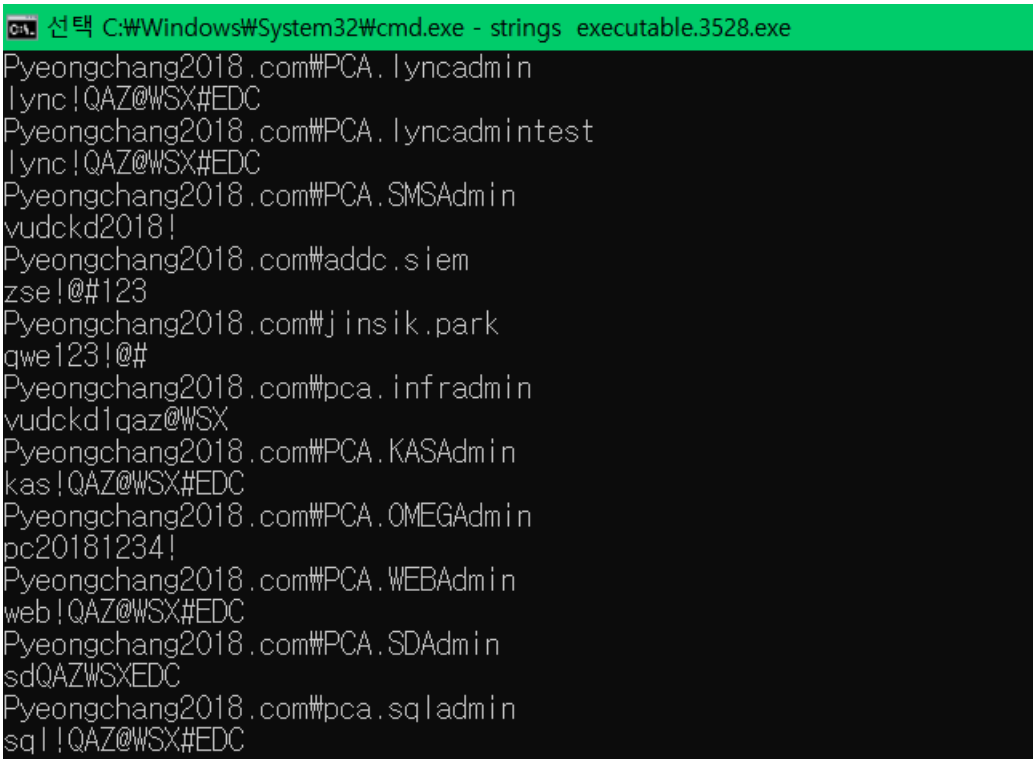
As shown in [Figure 14], The string value in the binary was checked by using the strings command, and remarkable points of the result were as below.



[Figure 16] Checking malicious activity

As shown in [Figure 16], you can see "ping 0.0.0.0 > nul" and this command is a type of activity to earning time, and It can be shown that attacker delete the evtchk.txt.

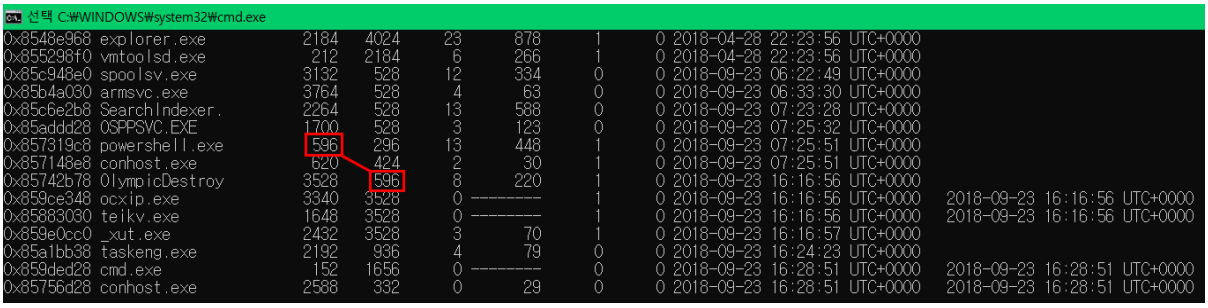
Also, it can be confirmed that attacker attempt to lateral movement using LDAP(Lightweight Directory Access Protocol) and WQL(Windows Query Language). "SELECT ds_cn FROM ds_computer" query shows the value of all the system in Active Directory.



[Figure 17] Checking accounts information

In addition, it can be assumed that the attacker obtained the credentials in advance and put them in the code because the data in binary is similar with account information.

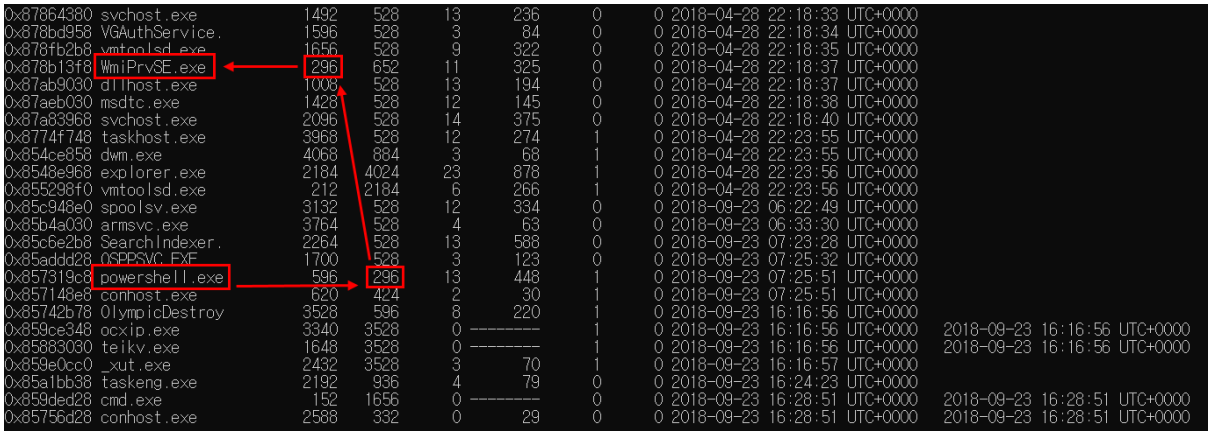
Then, OlympicDestroyer was confirmed that a child process of powershell.exe



[Figure 18] Checking processes correlation

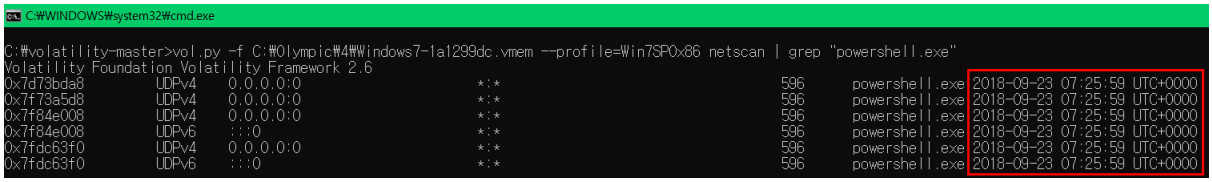
Through processes correlation, OlympicDestroyer was checked that it was executed by powershell.exe. And characteristic of such an attack using powershell is mainly use to lateral movement and it can RCE, Credentials/Password dumping, reverse shell, code/DLL Injection, and Toolkits that provide this functionality include powershell Empire, PowerSploit and MetaSploit.

Also, it has a characteristic that powershell is combined with WMI, frequently it used to remote execution on the attacker by calling Win32_Process Create method.



[Figure 19] Checking WmiPrSE.exe

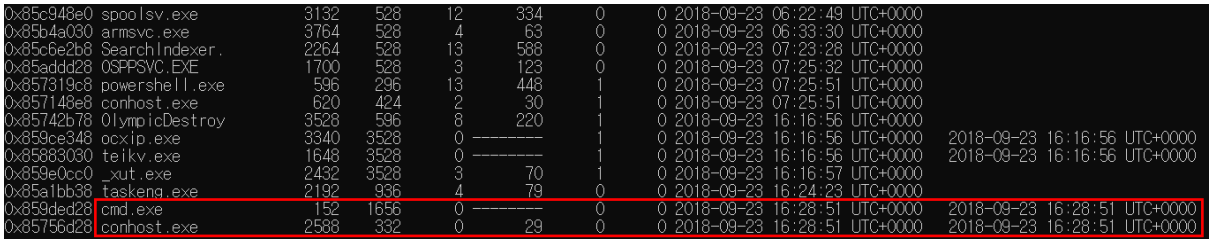
The result of checking powershell's PPID that has a characteristic that combining with WMI, it could be confirmed that WmiPrvSE.exe is residing that providing WMI service. As OlympicDestroyer was run by powershell, and after checking the information about the powershell related network connection considering remote control, the following results were obtained.



[Figure 20] Checking network artifacts though powershell

As a result, the network was connected at the point of time when the process of powershell.exe was created, 2018-09-23 07:25:51, 8 seconds after 2018-09-23 07:25:59.

After running powershell.exe, it is possible to expect that the OlympicDestroyer is dropped on victim's PC over the network.



[Figure 21] Checking command prompt

Normally, cmd.exe, which should operate as a child process of explorer.exe, was enough to buy suspicions because it was running under vmtoolsd.exe. The result of using "consoles" to check the command that was issued at the command prompt is as follows.

```
C:₩WINDOWS₩system32₩cmd.exe

C:₩volatility-master>vol.py -f C:₩Olympic₩4₩Windows7-1a1299dc.vmem --profile=Win7SP0x86 consoles
Volatility Foundation Volatility Framework 2.6
**************************************************
ConsoleProcess: conhost.exe Pid: 620
Console: 0x1681c0 CommandHistorySize: 50
HistoryBufferCount: 2 HistoryBufferMax: 4
OriginalTitle: %SystemRoot%₩System32₩WindowsPowerShell₩v1.0₩powershell.exe
Title: ???: C:₩Windows₩System32₩WindowsPowerShell₩v1.0₩powershell.exe
AttachedProcess: powershell.exe Pid: 596 Handle: 0x60
----
CommandHistory: 0x29fc60 Application: whoami.exe Flags:
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x0
----
CommandHistory: 0x29fb68 Application: powershell.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
----
Screen 0x26e730 X:80 Y:300
Dump:
```

[Figure 22] Result of "consoles"

The conhost.exe is played a role of handling input commands at the command prompt. Through the consoles, trace of running powershell can be shown from the command prompt.

In addition, you can see that OSPPSVC.EXE is running as shown below in the process just before powershell is executed.

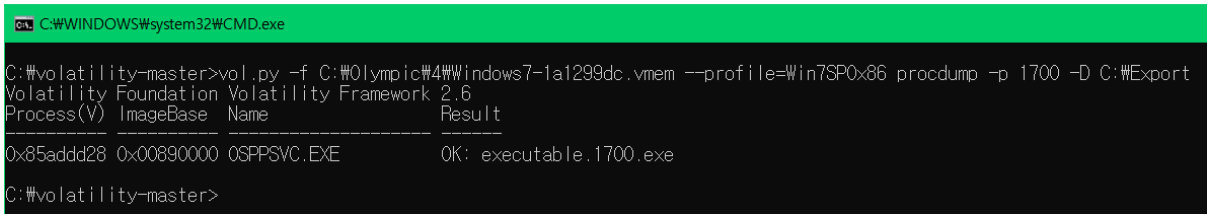
```
0x85b4a030 armsvc.exe          3764    528      4       63      0      0 2018-09-23 06:33:30 UTC+0000
0x85c6e2b8 SearchIndexer.      2264    528     13      588      0      0 2018-09-23 07:23:28 UTC+0000
0x85addd28 OSPPSVC.EXE         1700    528      3      123      0      0 2018-09-23 07:25:32 UTC+0000
0x857319c8 powershell.exe       596    296     13      448      1      0 2018-09-23 07:25:51 UTC+0000
0x857148e8 conhost.exe          620    424      2       30      1      0 2018-09-23 07:25:51 UTC+0000
0x85742b78 OlympicDestroy      3528    596      8      220      1      0 2018-09-23 16:16:56 UTC+0000
0x859ce348 ocxip.exe           3340   3528      0 --------      1      0 2018-09-23 16:16:56 UTC+0000   2018-09-23 16:16:56 UTC+0000
0x85883030 teikv.exe           1648   3528      0 --------      1      0 2018-09-23 16:16:56 UTC+0000   2018-09-23 16:16:56 UTC+0000
0x859e0cc0 _xut.exe            2432   3528      3       70      1      0 2018-09-23 16:16:57 UTC+0000
0x85a1bb38 taskeng.exe         2192    936      4       79      0      0 2018-09-23 16:24:23 UTC+0000
0x859ded28 cmd.exe              152   1656      0 --------      0      0 2018-09-23 16:28:51 UTC+0000   2018-09-23 16:28:51 UTC+0000
0x85756d28 conhost.exe         2588    332      0       29      0      0 2018-09-23 16:28:51 UTC+0000   2018-09-23 16:28:51 UTC+0000
```

[Figure 23] Checking execution of OSPPSVC.EXE

The OSPPSVC.EXE is a process that provides Microsoft Office services, you can see that powershell.exe is running after OSPPSVC.EXE is run at 2018-09-23 07:25:32 during the time the process resides, it can be assumed that OSPPSVC.EXE acts as a launcher to launch powershell.

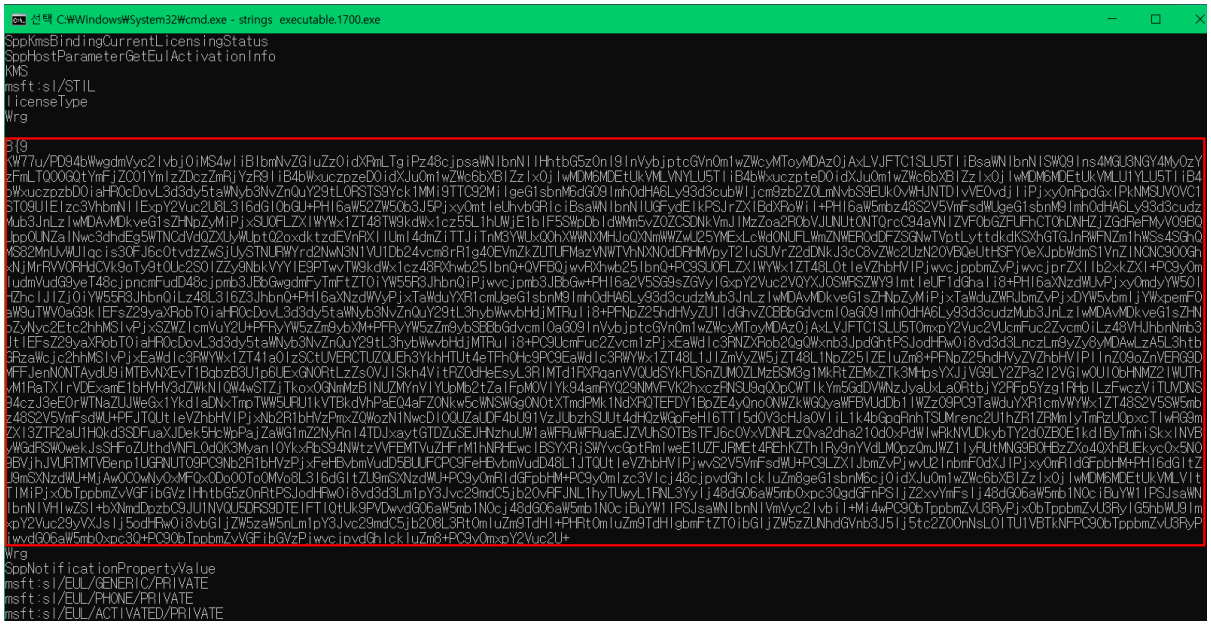
In addition, it is highly likely that the type of document malware is malicious code when the office is executed Also, malicious act started when the office was running, thus Document type macro is likely to be malicious code.

To proceed analyze as shown below, process was extracted.



[Figure 24] Extracting OSPPSVC.EXE

After extracting, the result of checking binary data using strings are same as shown below.



[Figure 25] Checking encoded string data

It is difficult to recognize, but one thing that you should know for sure is that it is a string that nomally does not exist.

Malfind and apihooks used in order to investigate additional behavior. As a result, It could be confirmed traces related to the suspicious behavior of code injection and API hooking as below. However, for detailed analysis, static analysis of malicious code through IDA need.

```
C:₩WINDOWS₩system32₩CMD.exe
Process: powershell.exe Pid: 596 Address: 0x7ff40000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, PrivateMemory: 1, Protection: 6

0x7ff40000  00 00 00 00 97 19 00 00 00 00 00 00 45 00 00 00   ............E...
0x7ff40010  68 00 00 00 00 e9 da 38 17 82 68 01 00 00 00 e9   h......8..h.....
0x7ff40020  d0 38 17 82 68 02 00 00 00 e9 c6 38 17 82 68 03   .8..h......8..h.
0x7ff40030  00 00 00 e9 bc 38 17 82 68 04 00 00 00 e9 b2 38   .....8..h......8

0x7ff40000 0000              ADD [EAX], AL
0x7ff40002 0000              ADD [EAX], AL
0x7ff40004 97                XCHG EDI, EAX
0x7ff40005 1900              SBB [EAX], EAX
0x7ff40007 0000              ADD [EAX], AL
0x7ff40009 0000              ADD [EAX], AL
0x7ff4000b 004500            ADD [EBP+0x0], AL
0x7ff4000e 0000              ADD [EAX], AL
0x7ff40010 6800000000        PUSH DWORD 0x0
0x7ff40015 e9da381782        JMP 0x20b38f4
0x7ff4001a 6801000000        PUSH DWORD 0x1
0x7ff4001f e9d0381782        JMP 0x20b38f4
0x7ff40024 6802000000        PUSH DWORD 0x2
0x7ff40029 e9c6381782        JMP 0x20b38f4
0x7ff4002e 6803000000        PUSH DWORD 0x3
0x7ff40033 e9bc381782        JMP 0x20b38f4
0x7ff40038 6804000000        PUSH DWORD 0x4
0x7ff4003d e9                DB 0xe9
0x7ff4003e b238              MOV DL, 0x38
```

[Figure 26] Result of "malfind"

Malfind can be used to identify pages that are suspected to be code-injected as above, but malfind is expected to require additional functionality improvements due to high false positives.

To investigate the additional functionality of OlympicDestroyer, apihooks was used as below.

```
C:₩WINDOWS₩system32₩cmd.exe - vol.py  -f C:₩Olympic₩4₩Windows7-1a1299dc.vmem --profile=Win7SP0x86 apihooks -p 3528

C:₩volatility-master>vol.py -f C:₩Olympic₩4₩Windows7-1a1299dc.vmem --profile=Win7SP0x86 apihooks -p 3528
Volatility Foundation Volatility Framework 2.6
************************************************************************
Hook mode: Usermode
Hook type: Import Address Table (IAT)
Process: 3528 (OlympicDestroy)
Victim module: OlympicDestroyer3.exe (0xc40000 - 0xe0b000)
Function: netapi32.dll!NetGetDCName
Hook address: 0x75045eb2
Hooking module: LOGONCLI.DLL

Disassembly(0):
0x75045eb2 6a54              PUSH 0x54
0x75045eb4 68505f0475        PUSH DWORD 0x75045f50
0x75045eb9 e8d2000000        CALL 0x75045f90
0x75045ebe 8b7508            MOV ESI, [EBP+0x8]
0x75045ec1 8975a8            MOV [EBP-0x58], ESI
0x75045ec4 8b450c            MOV EAX, [EBP+0xc]
0x75045ec7 8945b4            MOV [EBP-0x4c], EAX
```

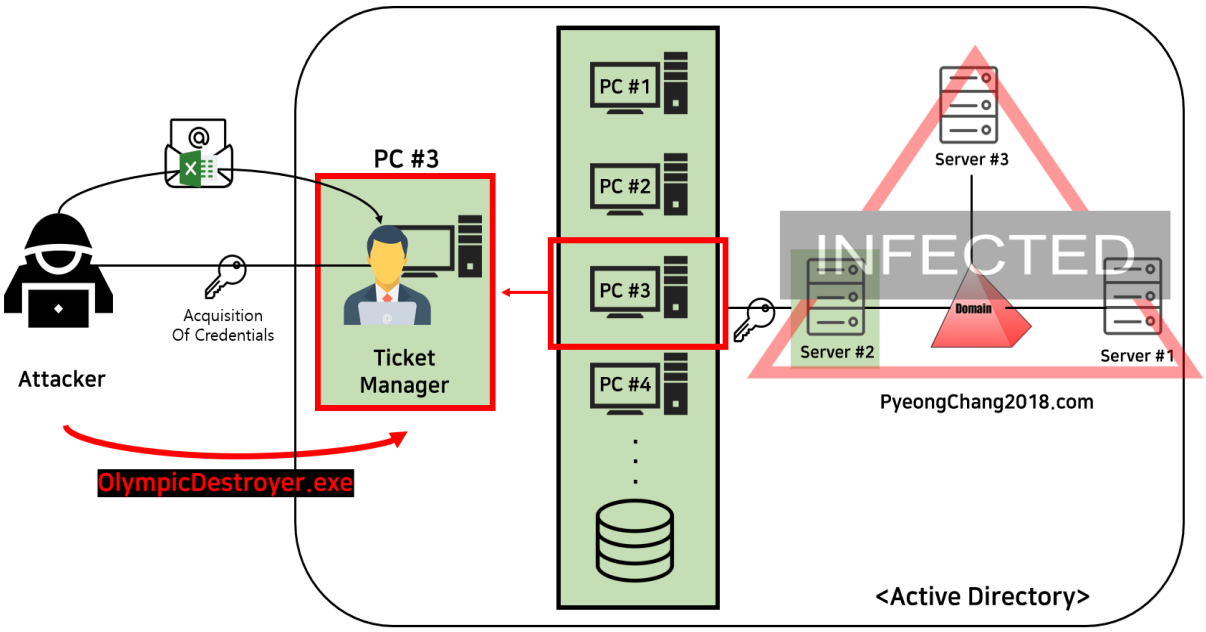
[Figure 27] Result of "apihooks"

As a result of confirming the information using apihooks, it can be confirmed that the user mode IAT is hooked, and that the function of fetching the name of the network domain controller is performed by hooking the NetGetDCName function.

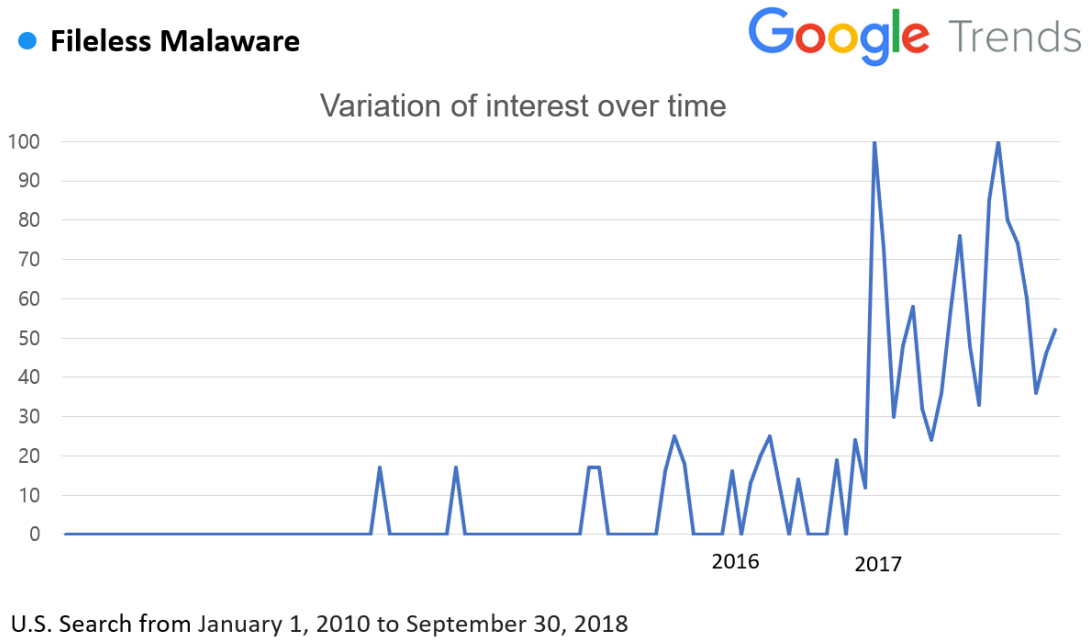
The analysis I have conducted is as follows. The overall contents are as follows.

1. 2018-09-23 07:25:32 Office document type malicious code execution
2. As it executes, powershell.exe is created, which downloads OlympicDestroyer
3. As OlympicDestroyer runs, the processes ocxip.exe, teikv.exe, and _xut.exe are created as child processes
4. As a result of analysis of _xut.exe, you can check for malicious behavior that deletes all the information related to backup
5. As a result of examining the string value of OlympicDestroyer, we confirm the traces estimated as lateral movement
6. After looking at the string in OSPPSVC.EXE, you can see the encrypted data, which can be guessed as C & C connecting with the hacker

4. DIAGRAM


PC #3
PC #1
PC #2
PC #3
PC #4
Server #3
INFECTED
Server #2
Domain
Server #1
Acquisition
Of Credentials
Attacker
Ticket
Manager
OlympicDestroyer.exe
PyeongChang2018.com
<Active Directory>

5. WHY THE SUBMISSION SHOULD WIN THE CONTEST



[Figure 28] Searching for Fileless Malware in Google Trends

Fileless malware is malware that does not store its body directly onto a memory. As you can see in [Figure 28] above, this type of malware became more popular in 2017 because of the increasing complexity of its detection and remediation. As a result, memory analysis become more important.

So we reconstruct the malware called "Olympic Destroyer" that appeared at the opening ceremony of the 2018 PyeongChang Olympics. In response to recent trends in malware, we have reproduced "Olympic Destroyer" using a representative fileless attack shellcode and an attack framework, Empire. And we found traces of it by using various modules provided by Volatility.

"Olympic Destroyer" is used in the actual situation. But at that time, it did not work properly due to some errors. We modified it to make it work properly and created using the latest trend, fileless attack scenario.

This analysis is of great value because it was reconstructed according to recent trends using malicious code that was actually used.