문 제	분 야	점 수
B-1		

Scenario Step B

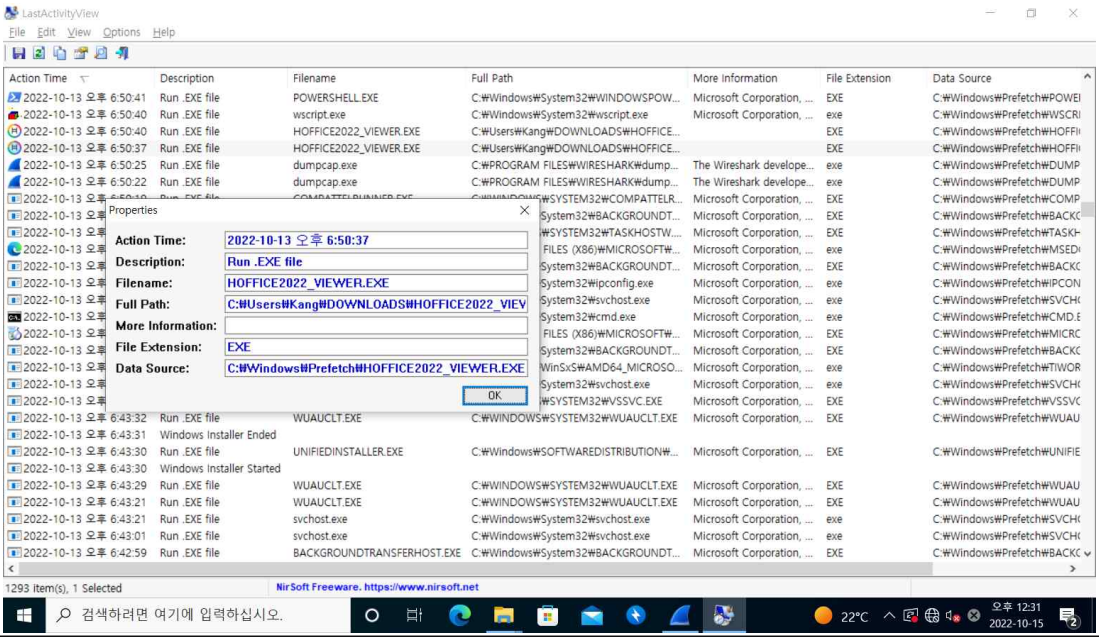
피해자는 공격자의 속임수에 넘어가 악성코드를 실행하였고,
결국 피해 PC에 악성 코드와 악성 도구들이 무차별적으로 설치되었다.
공격자가 사용한 드랍퍼 악성코드를 분석하여 피해 호스트에
설치된 악성코드에 대해 파악하라.

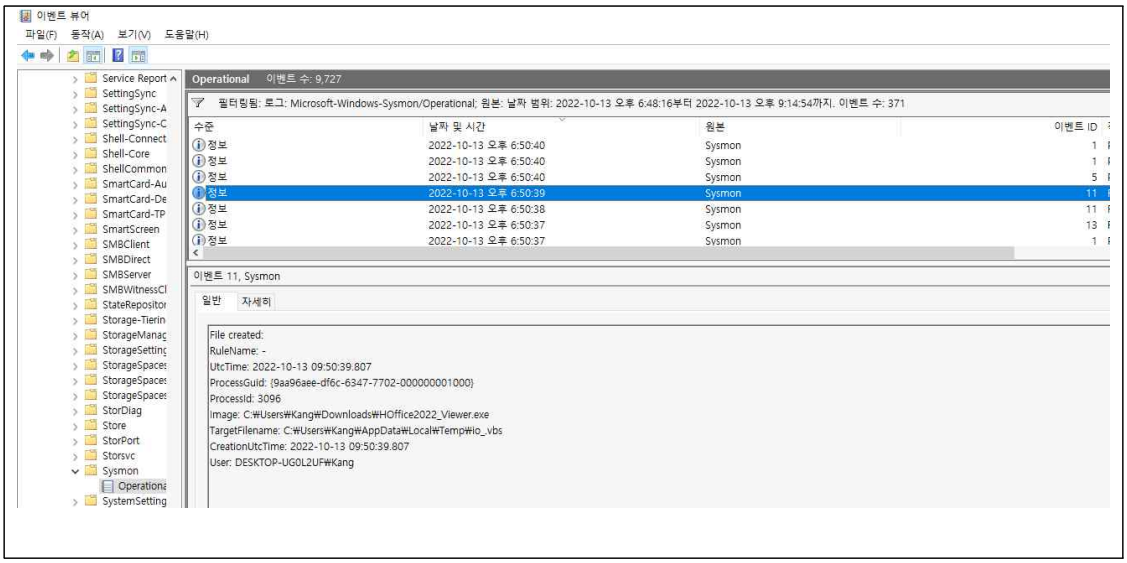
공격자가 초기 침투에 사용한 파일과, 해당 파일에 담겨있던 스크립트가 최초 실행된 시각은 언제인가?

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





문 제	분 야	점 수
B-2		

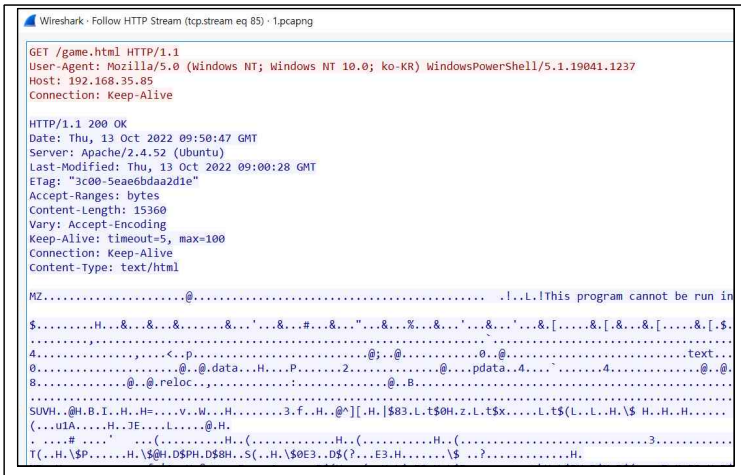
Scenario Step B

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)


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: "3c00-5eae6bdaa2d1e"
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.....,....<..p.....@;..@.....0..@.....text...
0.....@..@.data...H....P.....2.....@....pdata..4....`.....4.....@..@.
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$(L..L..H.\$ H..H..H.....
(...u1A.....H..JE....L.....@.H.
. ....# ....'   ...(.....H..(.....H..(.....H..(.....3.....
T(..H.\$P.....H.\$@H.D$PH.D$8H..S(..H.\$0E3..D$(?...E3.H.....\$ ..?.....H.

문 제	분 야	점 수
C-1		

Scenario Step C

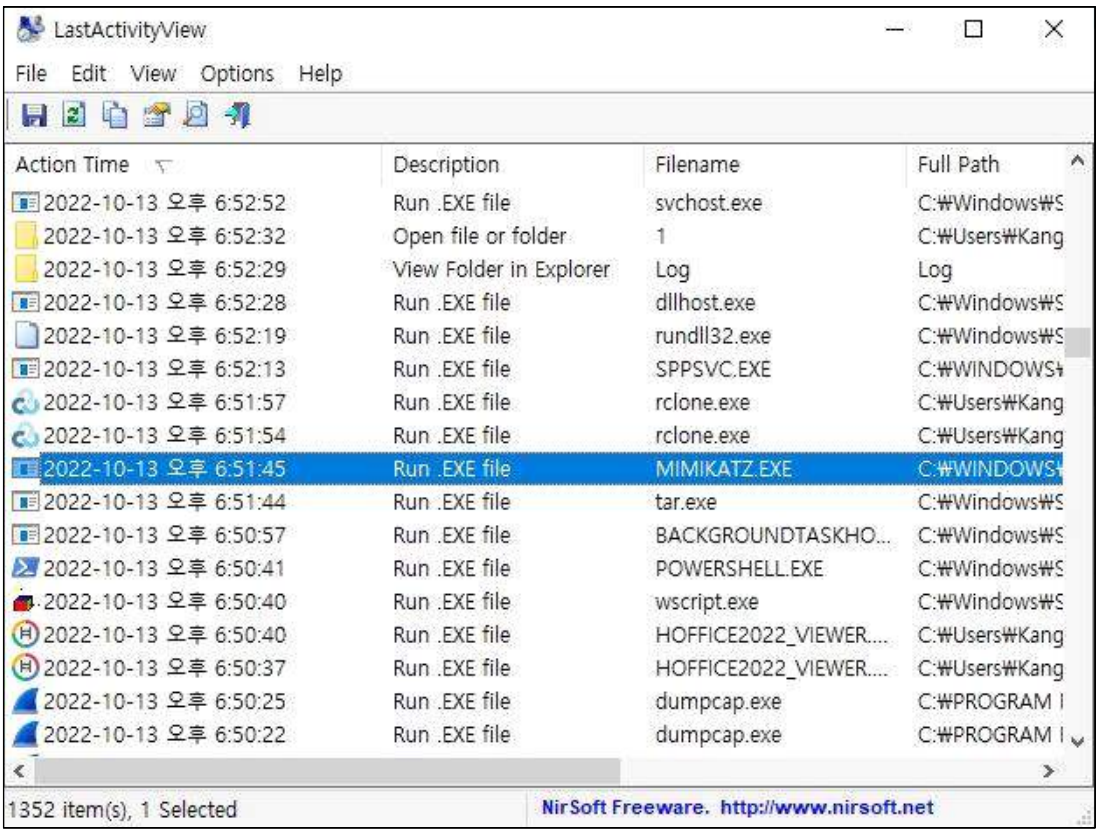
의문의 공격자는 계속해서 피해 PC 내부에 있는 중요 데이터를 수집하기 시작했다. 또한, 추적을 피하기 위해 데이터 유출 시 클라우드 서비스를 사용하는 등 주도면밀한 모습을 보여주었다. 피해 시스템을 분석하여 공격자가 유출한 민감한 데이터에 대해 식별하라.

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
정 답	FLAG{mimikatz.exe_20221013185145}

풀 이 과 정

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



문 제	분 야	점 수
C-2		

Scenario Step C

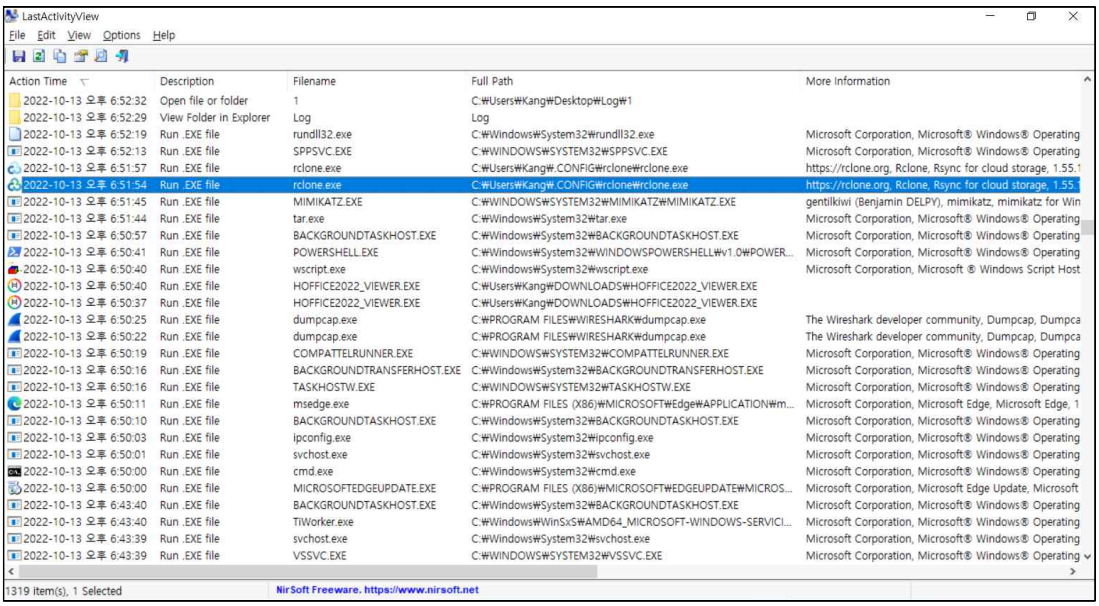
의문의 공격자는 계속해서 피해 PC 내부에 있는 중요 데이터를 수집하기 시작했다. 또한, 추적을 피하기 위해 데이터 유출 시 클라우드 서비스를 사용하는 등 주도면밀한 모습을 보여주었다. 피해 시스템을 분석하여 공격자가 유출한 민감한 데이터에 대해 식별하라.

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



문 제	분 야	점 수
C-3		

Scenario Step C

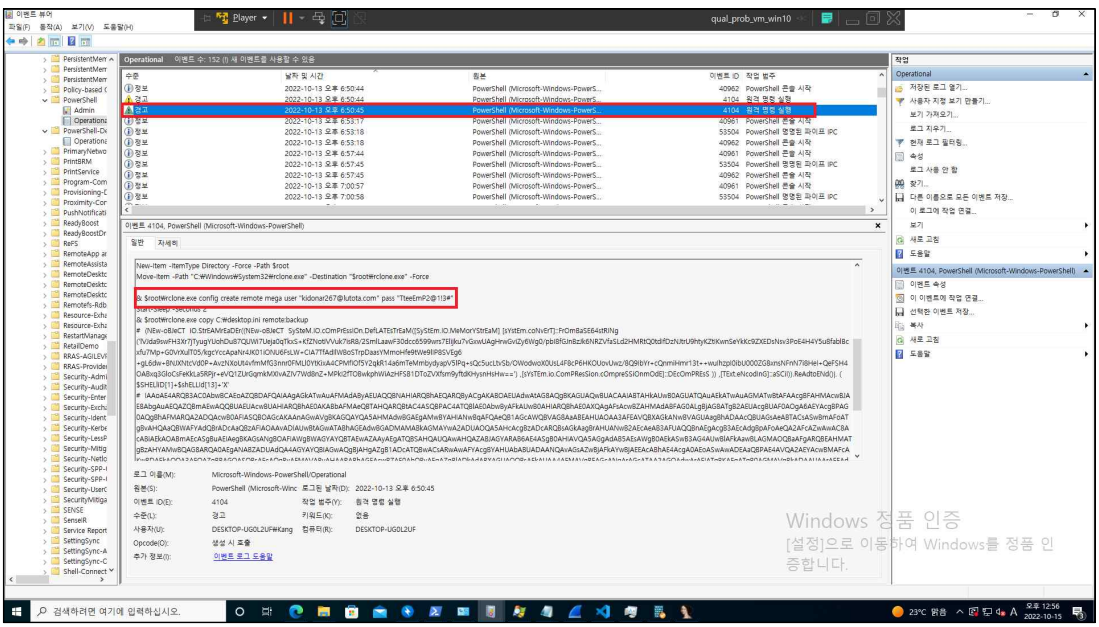
의문의 공격자는 계속해서 피해 PC 내부에 있는 중요 데이터를 수집하기 시작했다. 또한, 추적을 피하기 위해 데이터 유출 시 클라우드 서비스를 사용하는 등 주도면밀한 모습을 보여주었다. 피해 시스템을 분석하여 공격자가 유출한 민감한 데이터에 대해 식별하라.

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

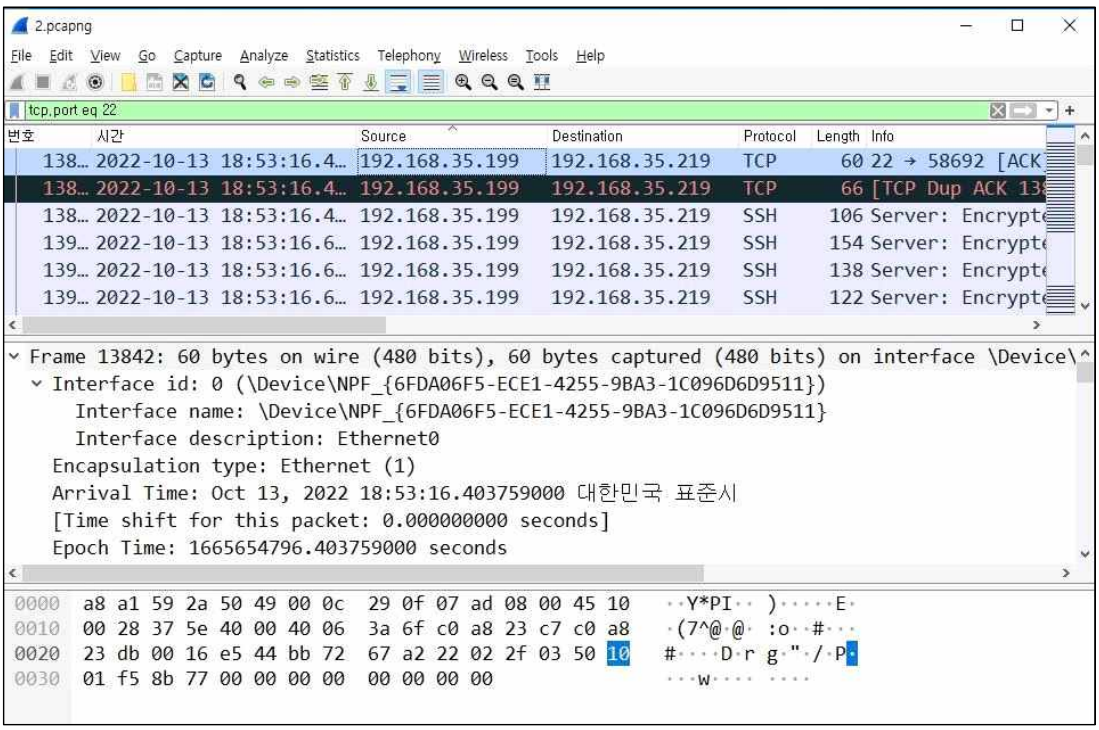
유출된 민감한 데이터 중에 PC 로그인과 관련된 정보가 있었는지, 공격자는 피해 PC에 원격 로그인을 한 뒤 무차별적으로 데이터를 수정하고 추가적인 악성 행위를 수행한다. 공격자가 수행한 원격 로그온에 대해 분석하라.

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



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 로그온에 대해 분석하라.

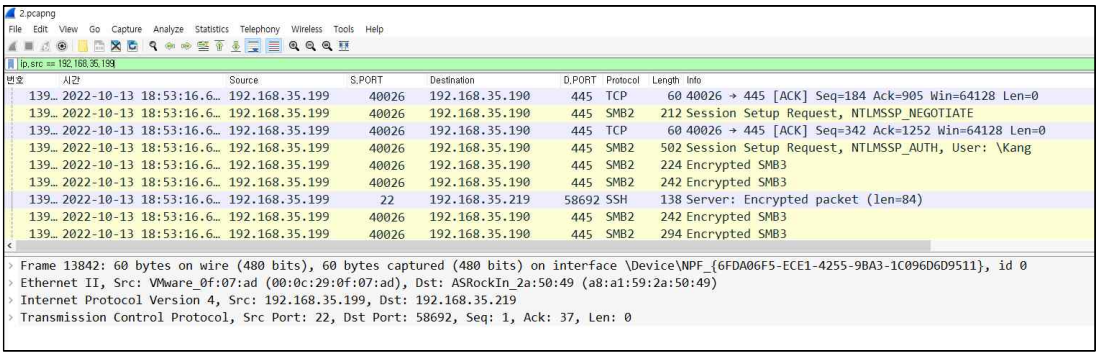
공격자가 피해 호스트에 접근할 때 사용한 도구와 프로토콜은?
(도구 : sysinternalsSuite)

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



문 제	분 야	점 수
D-3		

Scenario Step D

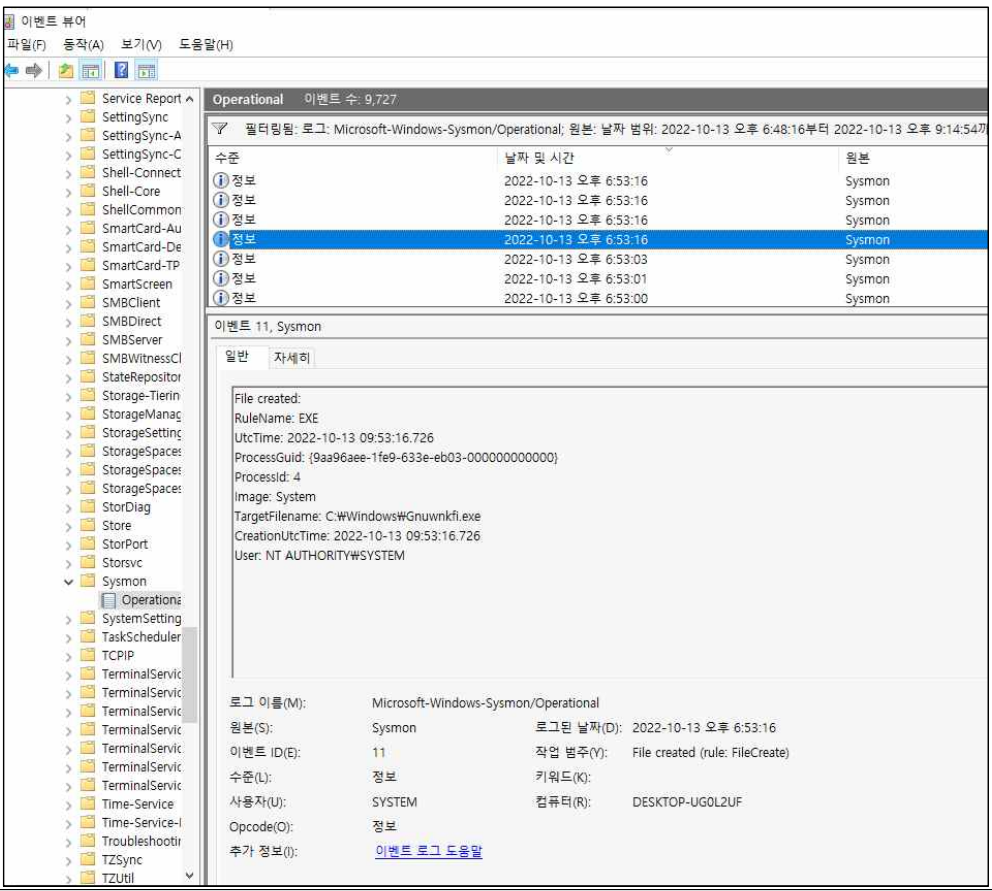
유출된 민감한 데이터 중에 PC 로그인과 관련된 정보가 있었는지, 공격자는 피해 PC에 원격 로그인을 한 뒤 무차별적으로 데이터를 수정하고 추가적인 악성 행위를 수행한다. 공격자가 수행한 원격 로그온에 대해 분석하라.

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



문 제	분 야	점 수
E-1		

Scenario Step E

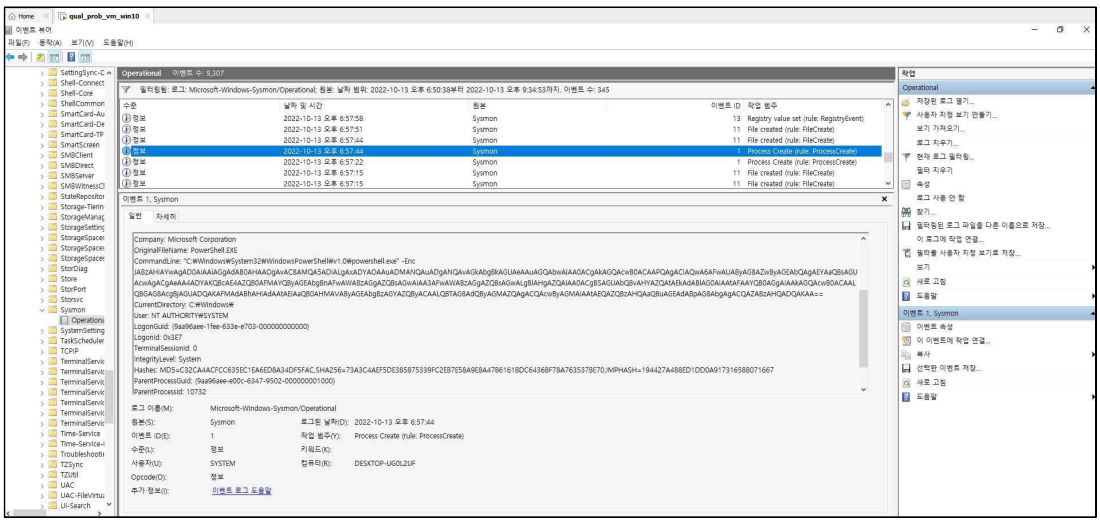
의문의 공격자는 악성 행위를 지속하기 위해 PC에 기존 설치되어 있던 프로그램을 삭제하고 재설치하는 등 행위를 했다. 공격자가 설치한 악성 행위 지속성 프로그램에 대해 분석하라.

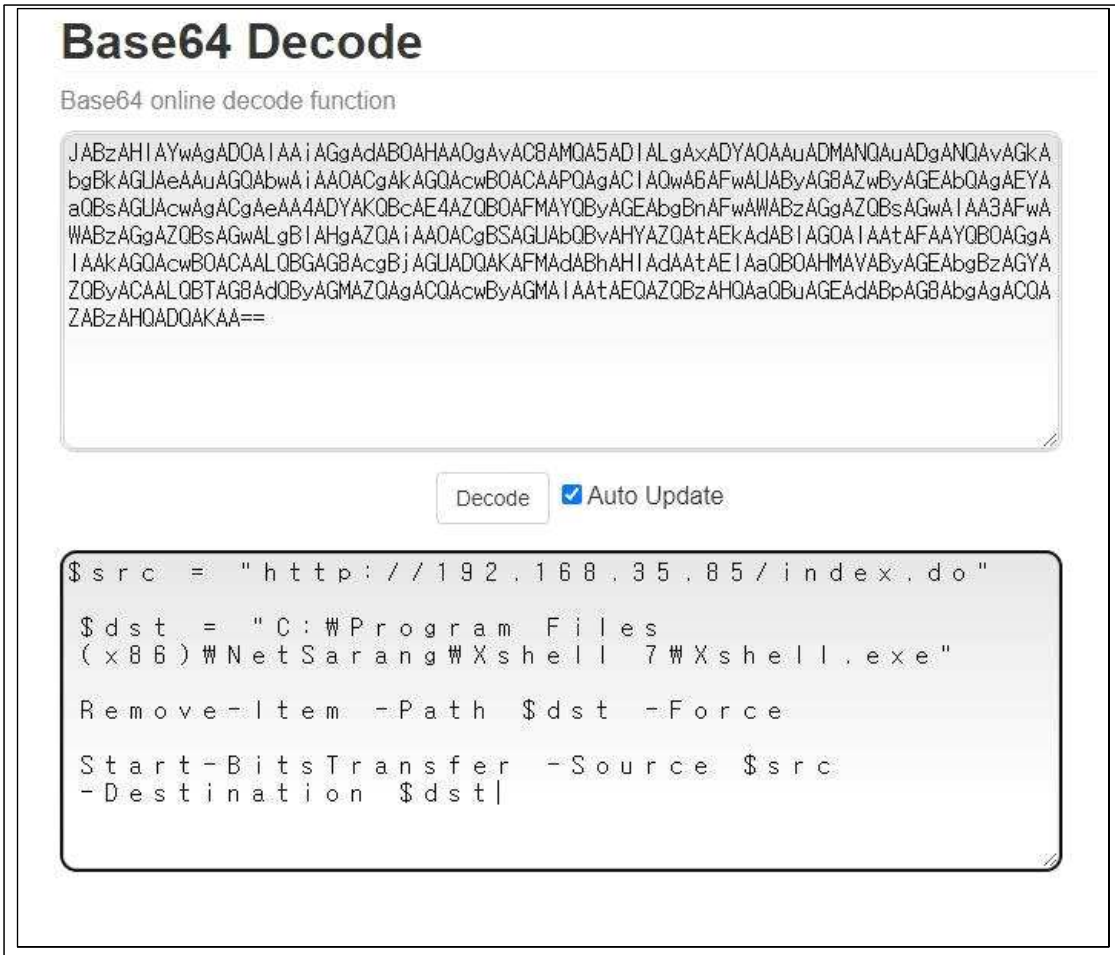
공격자가 기존 프로그램의 구성 요소를 삭제하고 악성코드를 설치한 시각은 언제인가? 공격자가 삭제한 프로그램 경로는 무엇인가?

풀이 절차	이벤트로그(sysmon)과 아티팩트 실행시간 확인
정 답	FLAG{C:₩Program Files (x86)₩NetSarang₩Xshell 7₩xshell.exe_20221013185744}

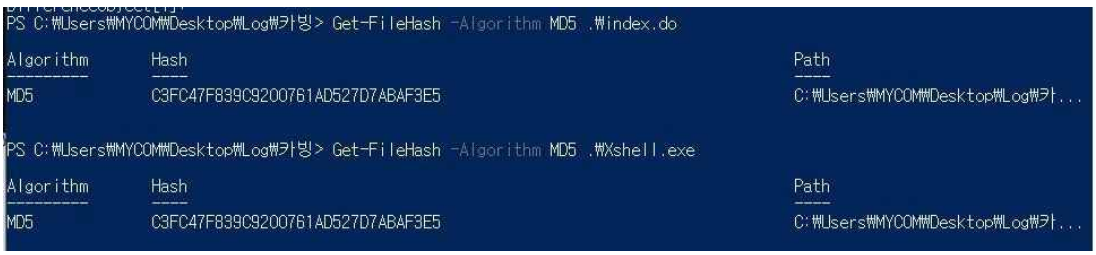
풀 이 과 정

이벤트 로그에서 파워쉘을 통하여 전달되는 Base64 코드 및 **설치시간** 확인





base64 디코딩결과 코드내용 중 **http://192.168.35.85/index.do를 Xshell.exe로 전송하는 내용확인**



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

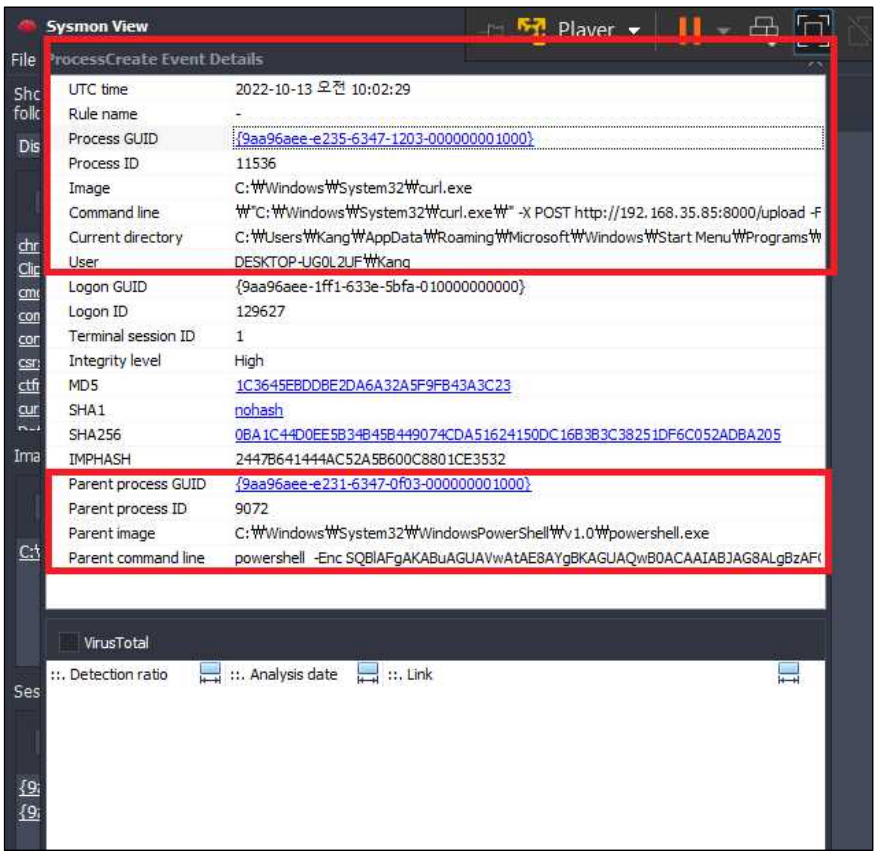
유출된 민감한 데이터 중에 PC 로그인과 관련된 정보가 있었는지, 공격자는 피해 PC에 원격 로그인을 한 뒤 무차별적으로 데이터를 수정하고 추가적인 악성 행위를 수행한다. 공격자가 수행한 원격 로그온에 대해 분석하라.

피해 호스트에 설치된 악성코드 중 시스템 부팅 시 피해 시스템의 파일을 유출하는 악성코드가 최초로 실행 된 시각과 당시 PID는 무엇인가?

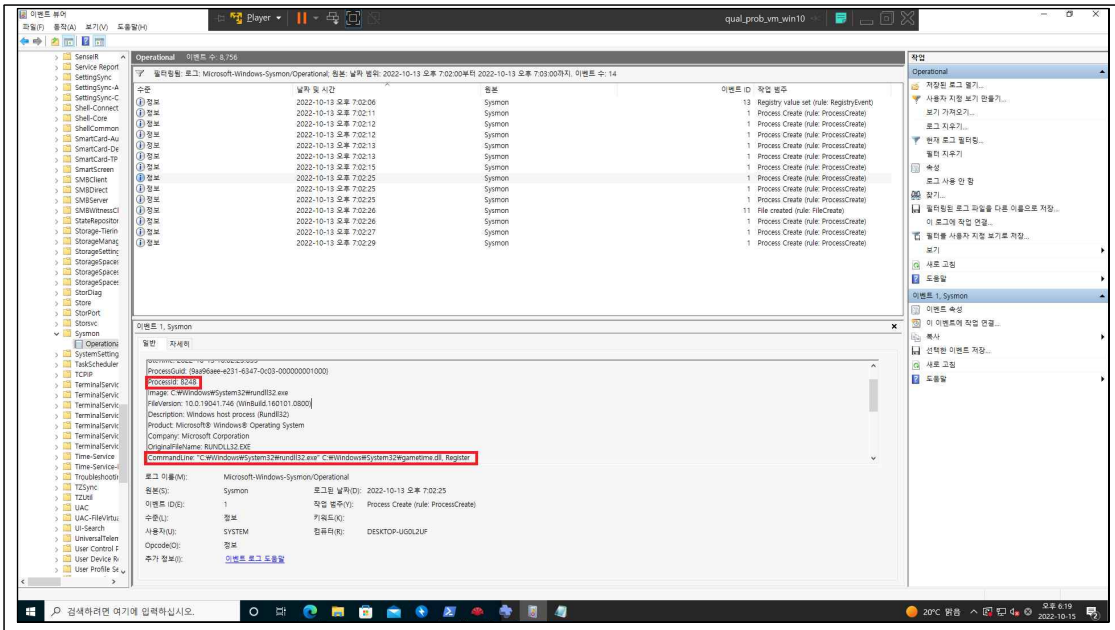
풀이 절차	이벤트로그(sysmon)과 시작프로그램 확인
정 답	FLAG{20221013190225_8248}

풀 이 과 정

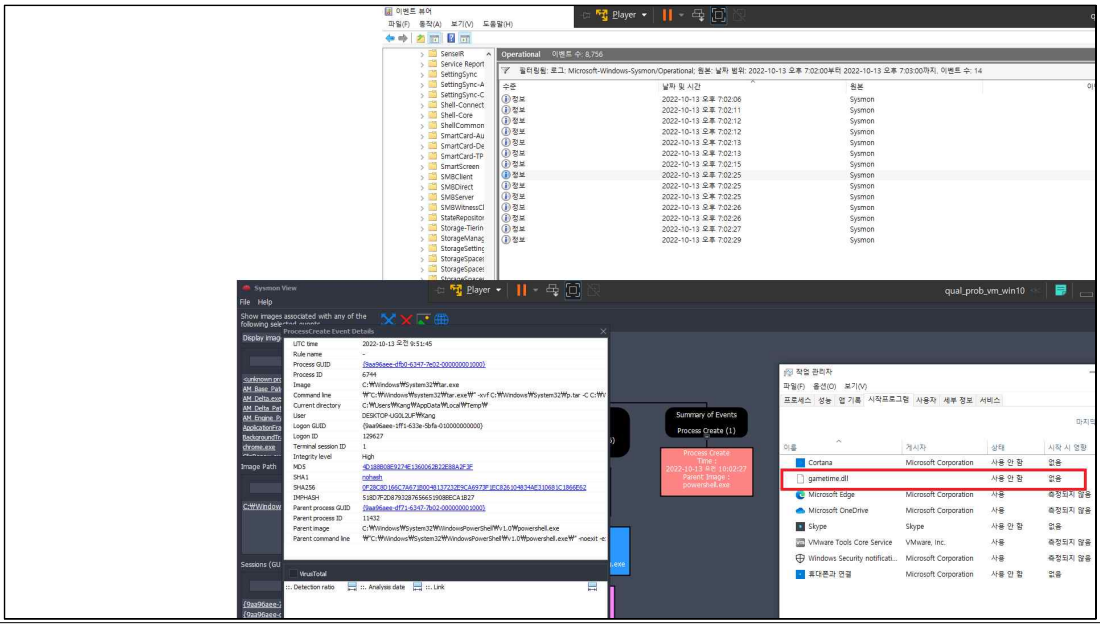
이벤트로그(sysmon)에서 curl_실행 흔적 확인



rundll32_gametime.dll_최초_재부팅시_실행시점_확인



시작프로그램_목록_검증



문 제	분 야	점 수
F-1		

Scenario Step F

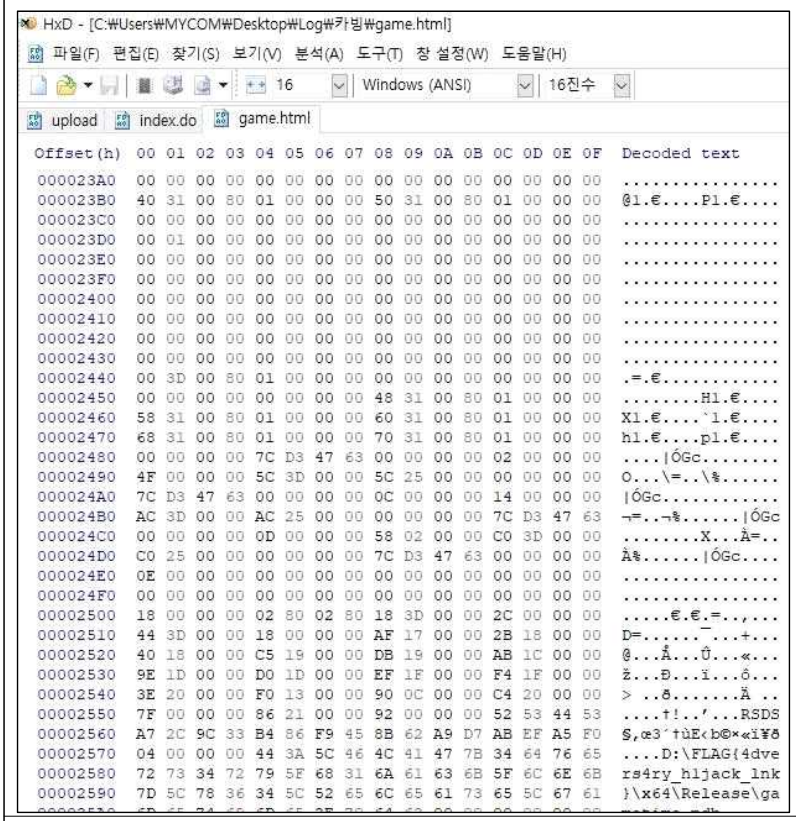
의문의 공격자는 악성 행위를 지속하기 위해 사용자가 PC를 부팅 시킬 때 마다 공격자가 지정한 명령을 수행하도록 시스템을 조작했다. 또한, 이 명령을 통해 피해 PC에 있는 중요 파일들을 추가적으로 유출한다. 공격자가 설치한 악성 행위 지속성 프로그램을 분석하라.

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

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

풀 이 과 정

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



문 제	분 야	점 수
F-2		

Scenario Step F

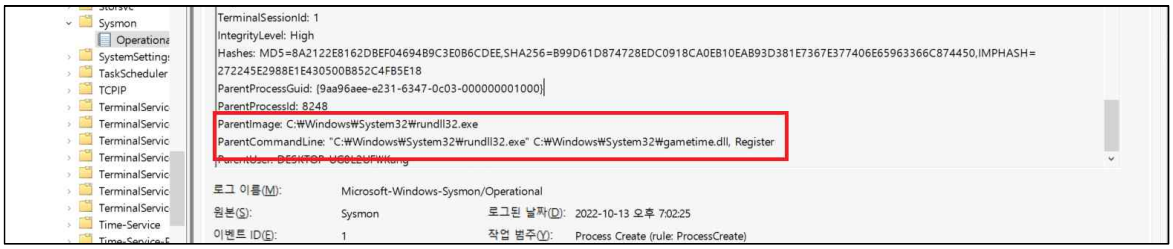
의문의 공격자는 악성 행위를 지속하기 위해 사용자가 PC를 부팅시킬 때 마다 공격자가 지정한 명령을 수행하도록 시스템을 조작했다.
또한, 이 명령을 통해 피해 PC에 있는 중요 파일들을 추가적으로 유출한다.
공격자가 설치한 악성 행위 지속성 프로그램을 분석하라.

공격자가 HTTP 프로토콜을 이용하여 최초로 데이터를 유출한 시각과 이 때 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
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

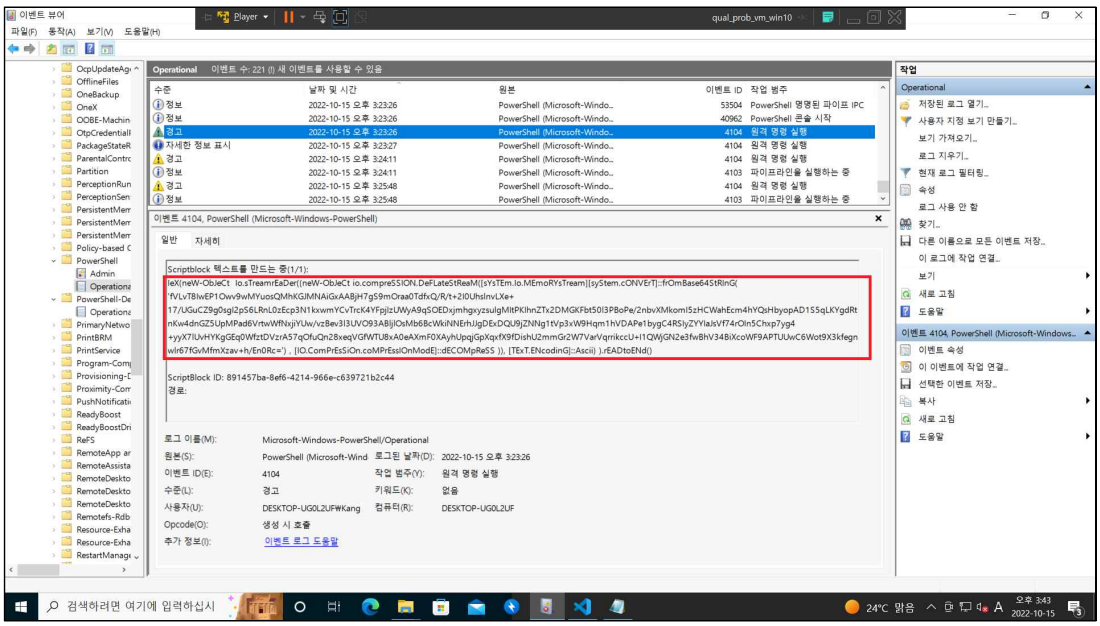
의문의 공격자는 악성 행위를 지속하기 위해 사용자가 PC를 부팅 시킬 때 마다 공격자가 지정한 명령을 수행하도록 시스템을 조작했다. 또한, 이 명령을 통해 피해 PC에 있는 중요 파일들을 추가적으로 유출한다. 공격자가 설치한 악성 행위 지속성 프로그램을 분석하라.

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

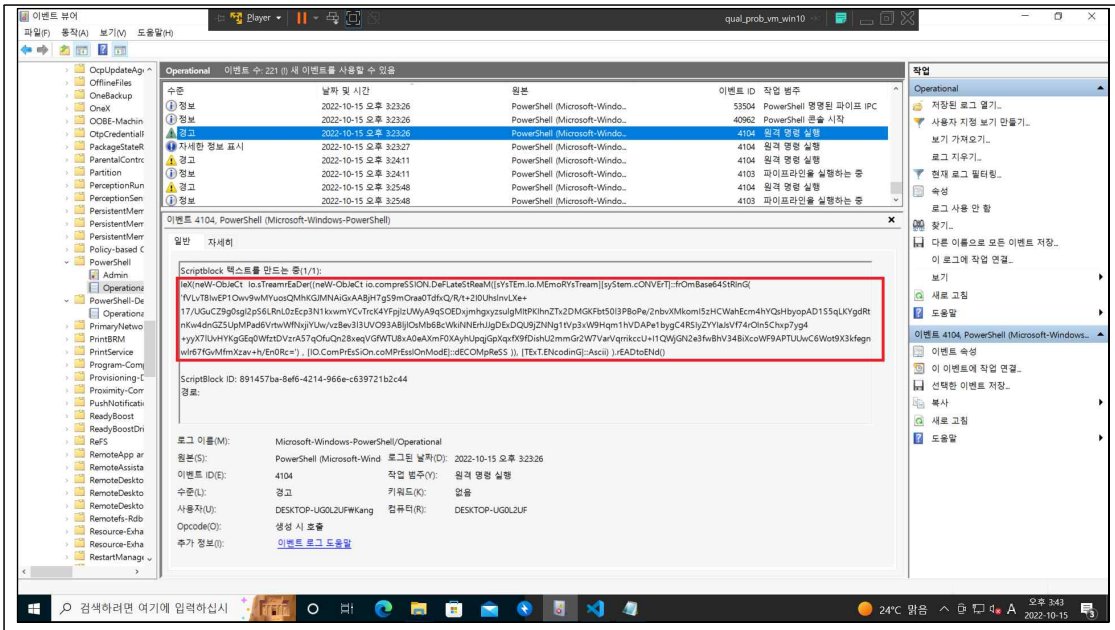
풀이 절차	이벤트로그(Powershell) 확인
정 답	FLAG{http://192.168.35.85:8000/upload_winlog.tar}

풀 이 과 정

암호화된_소스코드_실행_로그



소스코드_로깅_결과



문 제	분 야	점 수
F-4		

Scenario Step F

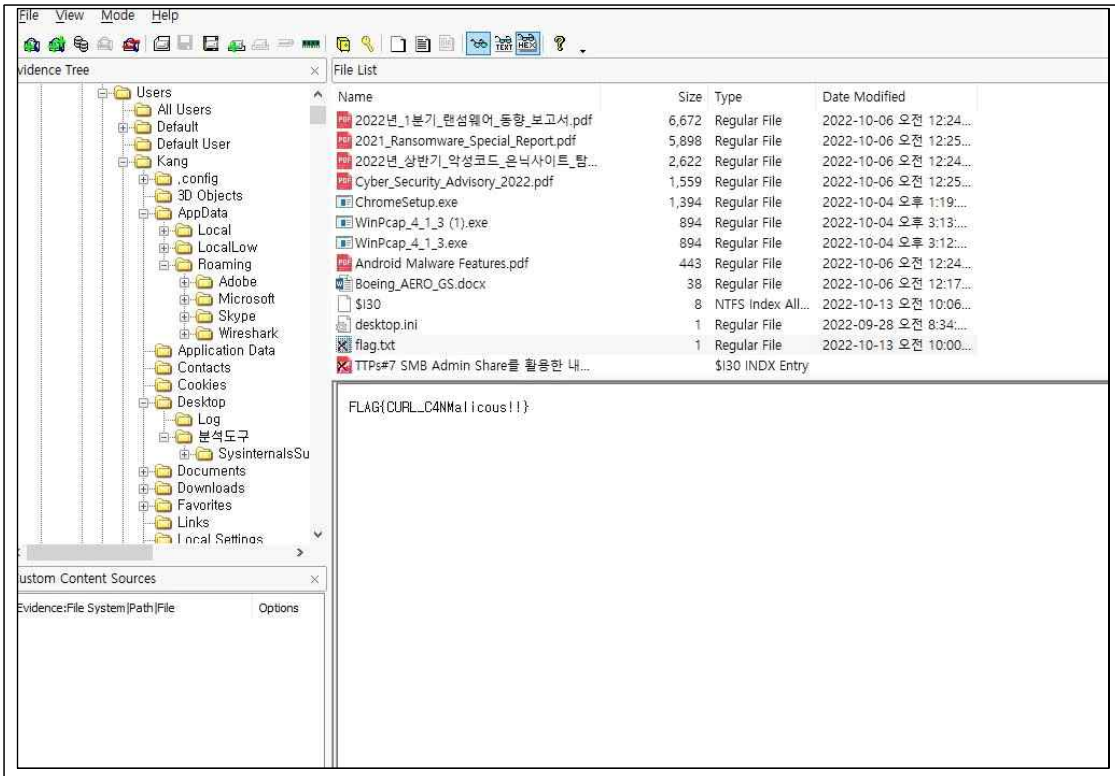
의문의 공격자는 악성 행위를 지속하기 위해 사용자가 PC를 부팅 시킬 때 마다 공격자가 지정한 명령을 수행하도록 시스템을 조작했다. 또한, 이 명령을 통해 피해 PC에 있는 중요 파일들을 추가적으로 유출한다. 공격자가 설치한 악성 행위 지속성 프로그램을 분석하라.

공격자가 피해 호스트에서 유출한 정보에서 플래그를 획득하여라.

풀이 절차	디스크 포렌식(FTK-Imager) 활용
정 답	FLAG{CURL_C4NMalicous!!}

풀 이 과 정

FTK Imager를 통하여 이미지 vmdk 내부에서 flag.txt 내용 확인결과 flag확인



문 제	분 야	점 수
G-1	시스템	-

Scenario Step G

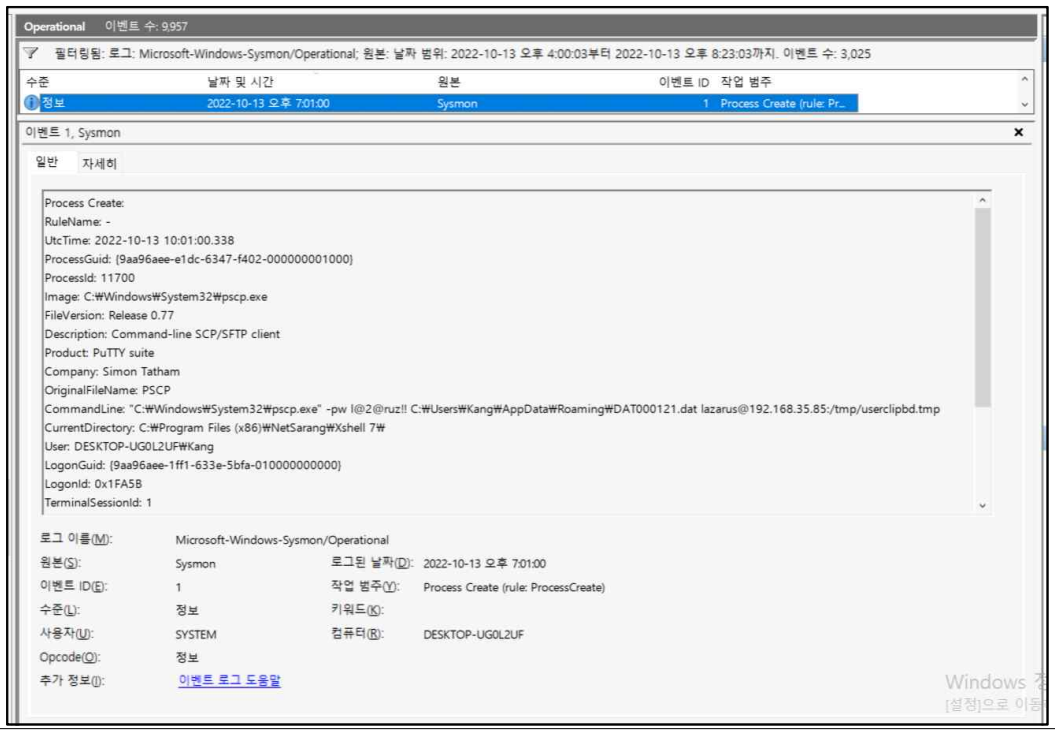
공격자는 이 뿐만 아니라 클립보드 데이터, 스크린샷 등
사용자가 행하는 다양한 행위에 대해 관찰하고 유출한다.
해당 악성 행위를 분석하여 추가적인 유출을 막아라.
클립보드 데이터가 최초로 유출된 시각은 언제이며, 유출에 사용된 도구의 당시 PID는?

풀이 절차	이벤트 뷰어 내 sysmon 로그 분석을 통하여 플래그를 획득함.
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



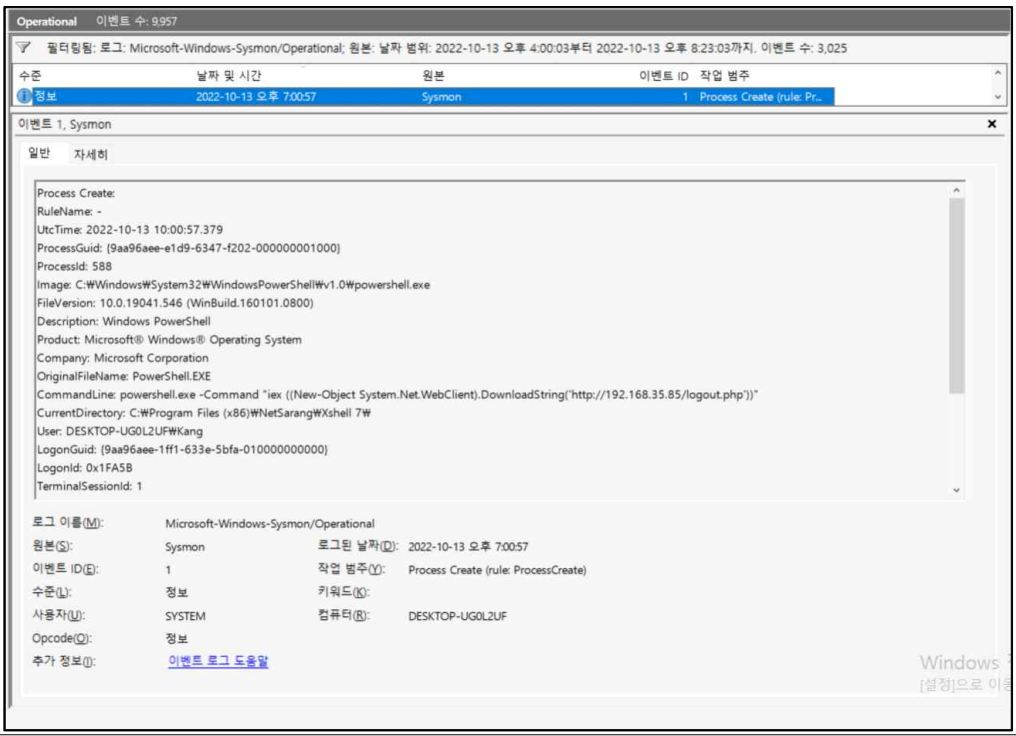
문 제	분 야	점 수
G-2	시스템	-

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.
정 답	FLAG{20221013190057_http192.168.35.85logout.php}

풀 이 과 정

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

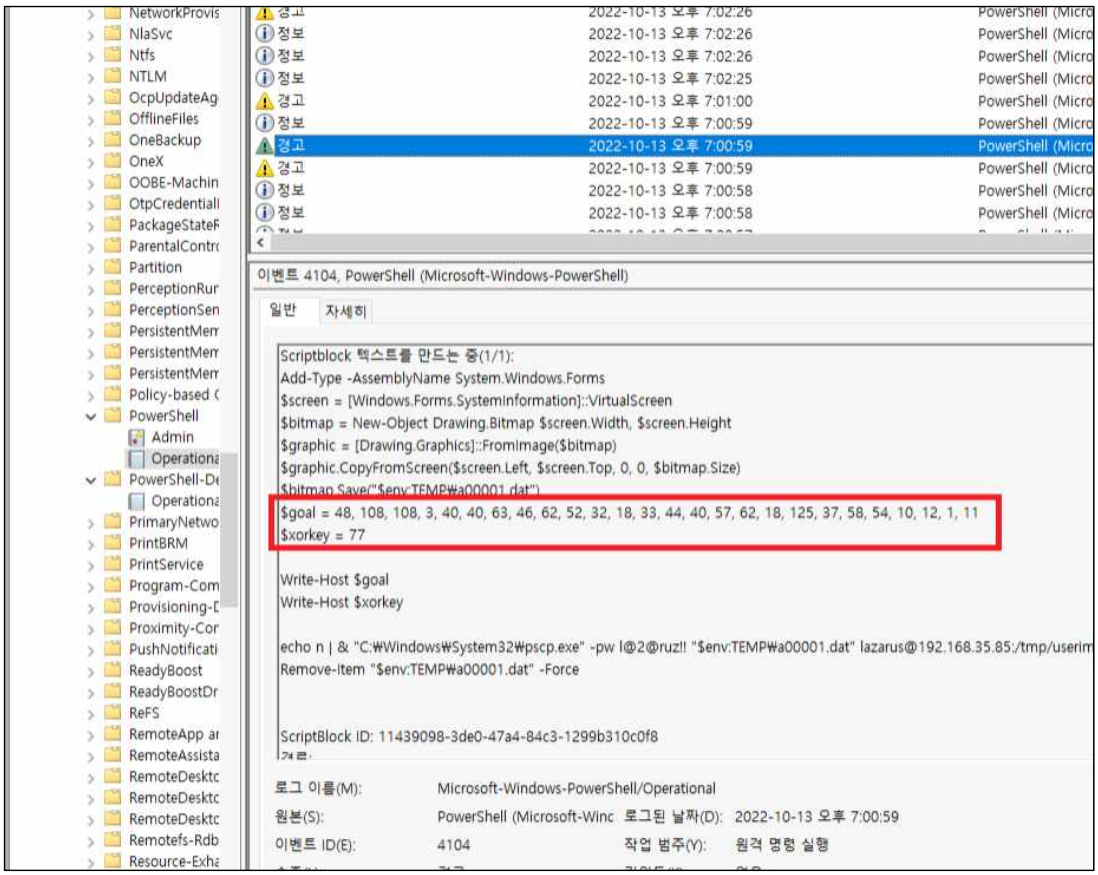
공격자는 PC를 탈취한 것을 과시하는 듯 자신이 사용한 공격 스크립트에 어떤한 메시지를 남겨놓았다.
우리는 배후가 누구인지 추적하기 위해 공격자에 대한 정보를 최대한 확보해야 한다.
공격자가 스크린 캡처를 위해 사용한 스크립트에서 플래그를 획득하라.
플래그 형식은 FLAG{...} 이다.

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

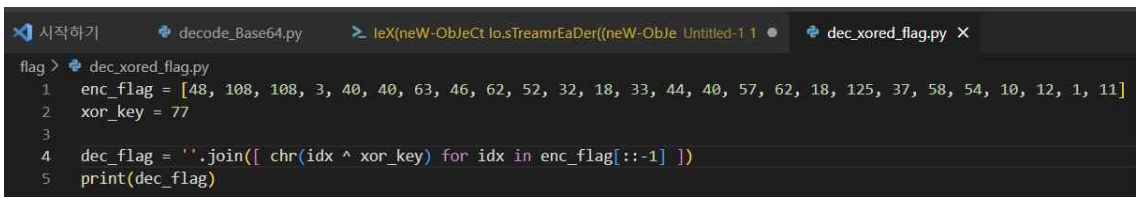
정 답	FLAG{wh0_steal_myscreeN!!}

풀 이 과 정

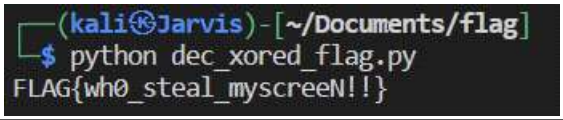
1. 이벤트 뷰어로 PowerShell 항목의 Operational 로그에 있는 로그 중 2022-10-13 오후 07:0059시 기준으로 Scriptblock 로그가 확인됨.



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



3. 스크립트를 구동하면 플래그값 확인 가능



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
정 답	FLAG{lazarus_l@2@ruz!!}

풀 이 과 정

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