2018 디지털 범인을 찾아라!

목차

I. 서론

1. 사건 개요

2018 디지털 범인을 찾아라!

** 본 대회에서 문제 풀이자에게 제공하는 문제(파일 포함)는 가상의 시나리오를 대회 문제로 구현한 것입니다. 본 문제에서 획득할 수 있는 공격과 관련된 일체의 프로그램을 사용하여 발생하는 책임에 대해서는 문제 풀이자 본인에게 있음을 알립니다.

 # 문제 시나리오

국내의 영화제작사인 [무비아이 스튜디오]는 약 650억의 제작비를 투자받아 한국영화 역사상 가장 큰 규모의 영화 [Re:set]을 제작하기로 발표하였다. 영화 [Re:set]은 황폐해지고 오염된 지구를 구하기 위해 인류를 새롭게 탄생 시키자는 특정 국가의 거대한 프로젝트를 담은 영화이다. 시나리오 작업을 완료한 [무비아이 스튜디오]는 배우 또한 국내/외 톱스타들로 구성하여 전세계 영화 팬들로부터 큰 관심을 이끌어냈다.

그런데 개봉하기 3일 전, 영화 시나리오 완성본 일부가 캡쳐된 파일이 인터넷 커뮤니티 사이트에 업로드 되었다는 사실이 발견되어 캡쳐본을 살펴본 [무비아이 스튜디오]는 본인이 가지고 있던 시나리오 완성본의 일부라는 사실을 확인하고 경찰에 고소하였다.

경찰은 인터넷 커뮤니티 사이트에 글을 게시한 사용자의 IP를 추적해 용의자를 검거했고, 용의자는 이내 범행 사실을 인정했지만 어떤 방식으로 시나리오 완성본을 빼낸 것인지 진술하지 않았다. 여러분은 제공된 데이터를 토대로 유출방법과 과정, 피해상황을 파악하고 [무비아이 스튜디오]에 제공할 시스템 상 보안대책 방안을 수립하라!

2. 의뢰 내용

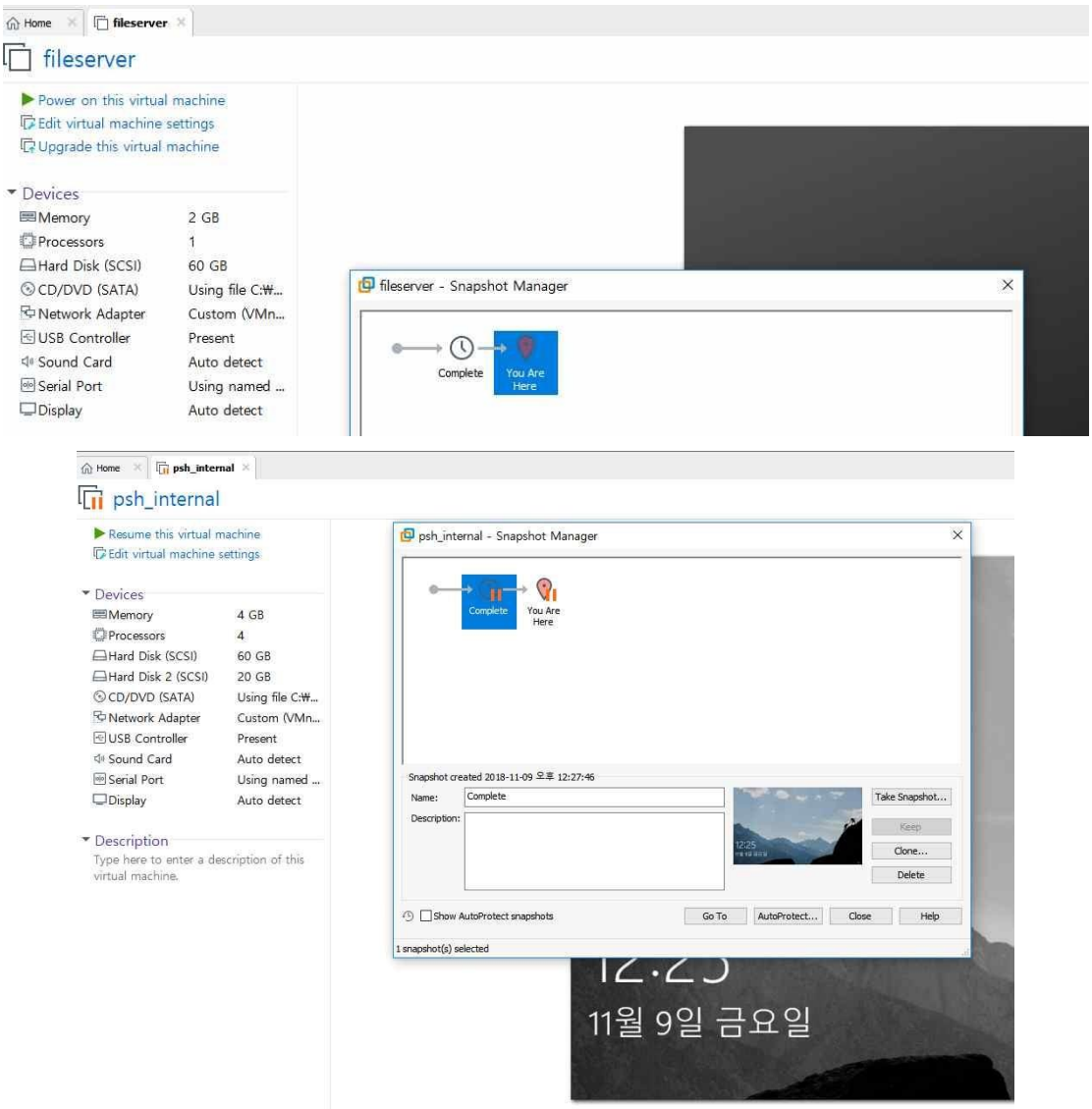
[무비아이 스튜디오]의 서버에 해커가 침입하여 File의 일부를 캡처 후 인터넷에 유출 시켰 다. 경찰은 해커를 잡는데 성공하였지만 침입 방법과 과정, 피해상황을 파악하지 못하였다. 해 커의 침입 방법과 과정, 피해 상황을 파악하고 [무비아이 스튜디오]에 제공할 시스템 상 보안 대책 방안을 수립하라. 이번 문제에 주어진 정보는 [무비아이 스튜디오]의 File Server, psh_internal Server이다.

II 사건 분석

1. 증거물 정보 및 증거물 보존 과정

이번 대회의 증거물로는 2개의 vmware 파일이 있다. 첫 번째 파일은 fileserver란 이름으로 유출된 시나리오 파일의 원본이 들어있는 windows server 2016 vmware 파일이다. 두 번째 로는 psh_internal 이란 파일로 운영체제는 windows 10으로 피해자의 PC로 추정된다.

이 두 개의 vmware 파일들은 그림 1과 같이 각각 하나의 스냅 샷을 가지고 있는 상태였으며 이 스냅 샷은 모두 Complete라는 이름으로 저장되어 있었다. 또한, fileserver는 전원이 꺼진 상태였으며 반대로 psh_internal은 일시정지 상태의 파일이었다.



[그림 1] vmware 파일들

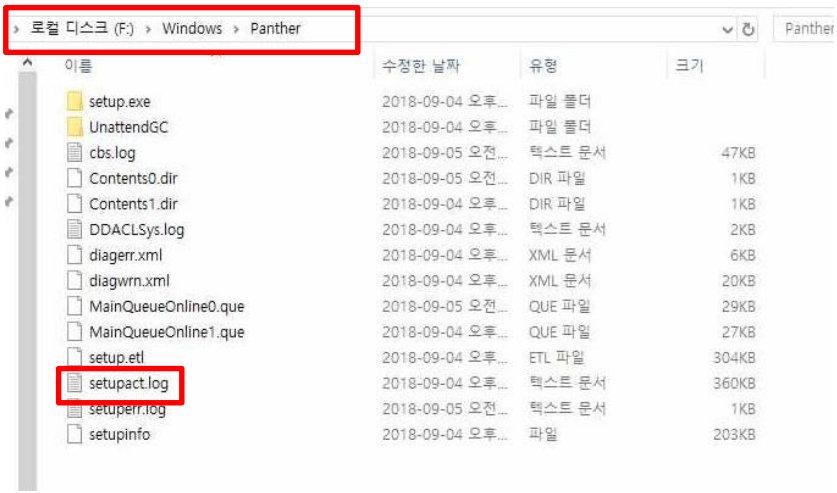
II 사건 분석

2. 상세 분석 결과

(1) 분석 대상 PC, 서버의 운영체제 버전과 설치 날짜는 무엇인가요? (3점)

윈도우는 이벤트 로그라는 바이너리 로깅 시스템을 이용하지만 호환성 유지를 위한 과거 텍 스트 파일 형태의 로그 역시 가지고 있다. 이 로그들을 확인하기 위해 툴을 이용하여 vm 디스크 파일을 VHD로 변환하여 분석을 진행하였다.

windows의 설치 로그 파일들이 있는 Panther 폴더로 이동 후 windows를 설치하는 동안의 설치 작업에 대한 정보를 기록해두는 setupact.log 파일을 열어 deviceinfo란 키워드로 검색을 한 결과 다음과 같이 Driver version = [10.0.14393.0]이라는 것을 발견할 수 있었다. 또한 가장 왼쪽에 설치 날짜 역시 표기가 되어있는 것을 확인할 수 있었다. 즉 가장 하단에 있는 설치 정보를 보면 설치가 완료된 시각 역시 알 수 있다.



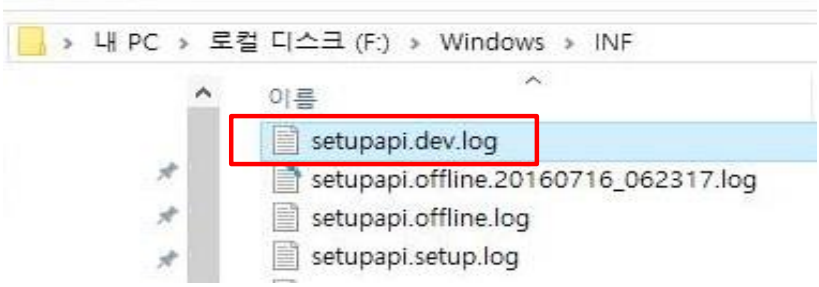
[그림 2] panther 폴더

[그림 3] setupact.log

확인 결과 fileserver의 운영체제 버전은 [10.0.14393.0], 설치 날짜는 UTC+9, 2018-09-04 13:50:39 이고 psh_internal 서버의 버전은 [10.0.17134.1]이며 설치 날짜는 UTC+9, 2018-09-04 13:13:05라고 할 수 있다.

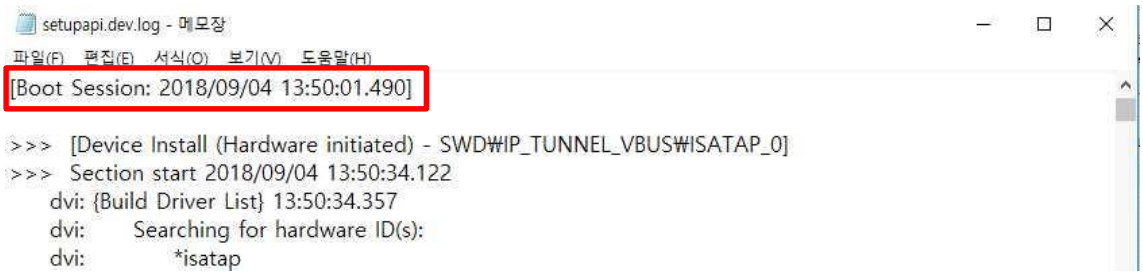
(2) 분석 대상 PC에 연결되었던 외부저장장치의 개수와 마지막에 연결된 외부저장장치의 시리 얼 번호와 연결 시각은 무엇인가요? (3점)

외부장치들은 각각 고유한 일련번호를 가지고 있으며 컴퓨터에 처음으로 연결을 시도할 시 Setupapi .dev.log 파일에 고유 정보를 남긴다. 즉, Setupapi.dev.log 파일을 확인 한다면 지 금까지 컴퓨터에 사용된 외부장치들의 정보를 확인 할 수 있다.



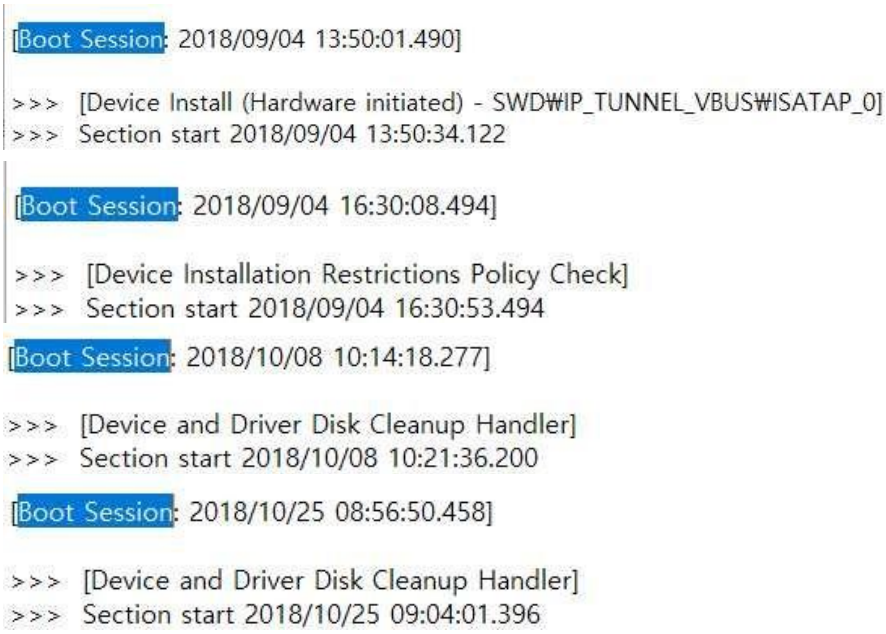
[그림 4] setupapi.dev.log

setupapi.dev.log 파일을 실행하면 다음과 같은 텍스트 파일이 실행된다. 이 파일에서 주의 깊게 봐야 하는 부분이 바로 Boot Session이다. Boot Session은 처음으로 꽂은 외부장치가 있을 때 생성된다. 즉, Boot Session의 개수가 바로 지금까지 컴퓨터에 접속한 외부장치의 개수이다. 또한 Boot Session은 날짜 역시 명시하고 있다.



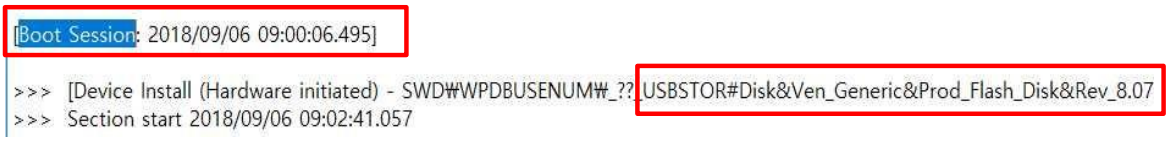
[그림 5] Boot Session

검색을 이용해 fileserver의 Boot Session 개수를 확인한 결과 총 4개의 외부장치가 USB PORT를 통해 연결된 흔적을 찾을 수 있었다. 하지만 확인 결과 4개의 외부장치 중 외부저장 장치인 USB의 흔적은 발견되지 않았다. 즉, fileserver에서는 USB가 사용된 적이 없었다.



[그림 6] 4개의 Boot Session

psh_internal 서버에서 역시 검색을 진행한 결과 총 14개의 Boot Session을 확인 할 수 있 었다. 또한 그중 하나의 세션이 USB 사용 기록인 것과 연결 시각을 확인할 수 있었다.



[그림 7] USB LOG

[그림 8] Serial Number

즉, 모든 Server를 통틀어서 외부저장장치인 USB는 단 하나만이 연결된 적이 있으며, 이 USB의 연결 시간은 UTC+9, 2018-09-06 09:00:06이고 Serial Number는 97DFB02C인 것을 확인할 수 있었다.

(3) 공격자가 보낸 메일을 처음 받은 시각은 언제인가요? (3점)

처음 이 문제를 풀기 시작 했을 때 제대로 된 결론을 낼 수 없었다. 메일을 찾을 수 없었기 때문이다. 레지스트리와 이벤트뷰어를 이용해 인터넷 접속 기록과 다운로드한 파일이 있는지 찾아보았지만 관련 기록을 찾을 수 없었고 메일 프로토콜도 찾을 수 없었다. 하지만 뒤에 있 는 문제를 풀이 중 3번 문제의 정답에 조금은 더 접근할 수 있었다. psh_internal 서버의 movie_psh 계정의 비밀번호를 알아낸 후 로그인한 다음 windows mail로 접근하니 다음과 같이 메일 기록을 찾을 수 있었던 것이다.

[그림 9] 받은 메일함

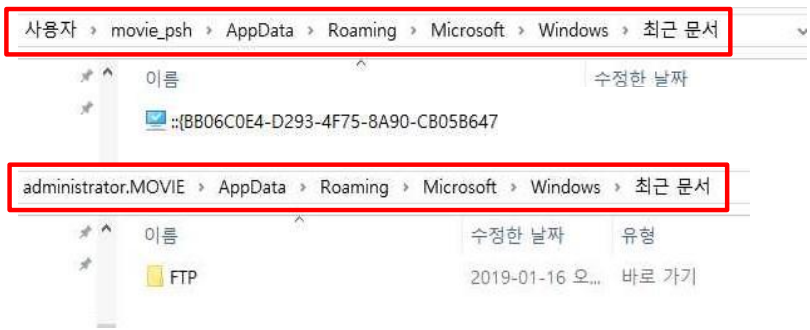
이 메일 중 악성코드가 처음 침투한 날인 11월 07일에 온 메일이 있어 확인하여 보니 다음 과 같이 악성코드가 들어있는 압축파일이 첨부되어 있다는 것을 확인할 수 있었다.

[그림 10] 메일 첨부 파일

즉 공격자는 ljh@kmcom.kr이란 메일로 위장하여 피해자의 PC로 악성코드가 첨부된 메일을 보낸 것이다. 피해자가 이 메일을 처음 받은 시각은 UTC+9, 2018-11-07 15:17:00이다.

(4) 분석 대상 PC에서 열람된 문서 파일을 모두 작성하세요. (3점)

열람된 문서 파일을 확인하기 위해서는 레지스트리를 확인하거나 최근 문서 항목을 확인하는 방법이 존재한다. 레지스트리를 확인하기 위해서는 레지스트리 뷰어라는 프로그램을 통해 확 인할 수 있으며, 최근 문서 항목은 가상 디스크의 User\사용자 계정\AppData\Roaming \Microsoft\Windows\Recent(최근 문서)에서 확인할 수 있다.

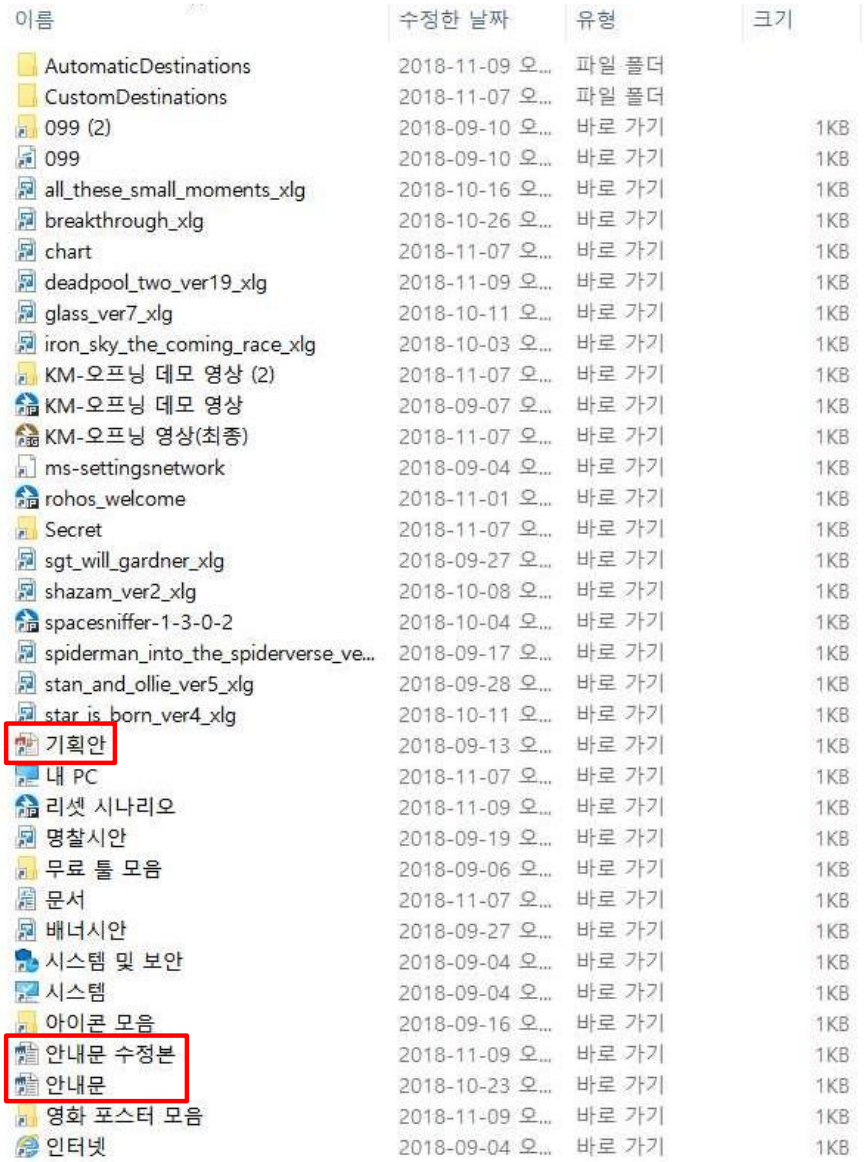


[그림 11] 각 계정의 최근 문서

최근 문서를 확인 결과 문서 파일은 발견할 수 없었다. 이에 이상하다는 생각이 들어 파일 복구 프로그램을 이용하여 삭제된 파일이 있는지 확인을 해보았다.

[그림 12] fileserver 최근 문서 복구

복구 프로그램을 이용하여 fileserver의 administrator.MOVIE 계정의 최근 문서 폴더의 삭 제된 파일들을 복구해보았더니 그림 11과 같은 결과를 확인할 수 있었다. 이 중 문서 파일은 리셋 시나리오가 존재하였다. 또한 psh_server의 movie_psh 계정 역시 복구를 해보니 그림 12와 같이 많은 파일들을 확인할 수 있었고 이 파일 중 문서 파일이 존재한다는 것을 확인 할 수 있었다.



이름	수정한 날짜	유형	크기
AutomaticDestinations	2018-11-09 오...	파일 폴더	
CustomDestinations	2018-11-07 오...	파일 폴더	
099 (2)	2018-09-10 오...	바로 가기	1KB
099	2018-09-10 오...	바로 가기	1KB
all_these_small_moments_xlg	2018-10-16 오...	바로 가기	1KB
breakthrough_xlg	2018-10-26 오...	바로 가기	1KB
chart	2018-11-07 오...	바로 가기	1KB
deadpool_two_ver19_xlg	2018-11-09 오...	바로 가기	1KB
glass_ver7_xlg	2018-10-11 오...	바로 가기	1KB
iron_sky_the_coming_race_xlg	2018-10-03 오...	바로 가기	1KB
KM-오프닝 데모 영상 (2)	2018-11-07 오...	바로 가기	1KB
KM-오프닝 데모 영상	2018-09-07 오...	바로 가기	1KB
KM-오프닝 영상(최종)	2018-11-07 오...	바로 가기	1KB
ms-settingsnetwork	2018-09-04 오...	바로 가기	1KB
rohos_welcome	2018-11-01 오...	바로 가기	1KB
Secret	2018-11-07 오...	바로 가기	1KB
sgt_will_gardner_xlg	2018-09-27 오...	바로 가기	1KB
shazam_ver2_xlg	2018-10-08 오...	바로 가기	1KB
spacesniffer-1-3-0-2	2018-10-04 오...	바로 가기	1KB
spiderman_into_the_spiderverse_ve...	2018-09-17 오...	바로 가기	1KB
stan_and_ollie_ver5_xlg	2018-09-28 오...	바로 가기	1KB
star_is_born_ver4_xlg	2018-10-11 오...	바로 가기	1KB
기획안	2018-09-13 오...	바로 가기	1KB
내 PC	2018-11-07 오...	바로 가기	1KB
리셋 시나리오	2018-11-09 오...	바로 가기	1KB
명찰시안	2018-09-19 오...	바로 가기	1KB
무료 틀 모음	2018-09-06 오...	바로 가기	1KB
문서	2018-11-07 오...	바로 가기	1KB
배너시안	2018-09-27 오...	바로 가기	1KB
시스템 및 보안	2018-09-04 오...	바로 가기	1KB
시스템	2018-09-04 오...	바로 가기	1KB
아이콘 모음	2018-09-16 오...	바로 가기	1KB
안내문 수정본	2018-11-09 오...	바로 가기	1KB
안내문	2018-10-23 오...	바로 가기	1KB
영화 포스터 모음	2018-11-09 오...	바로 가기	1KB
인터넷	2018-09-04 오...	바로 가기	1KB

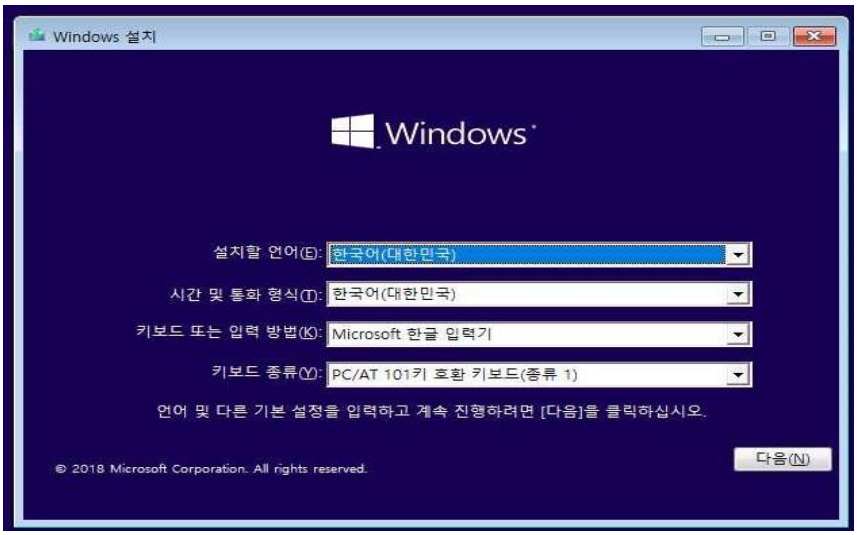
[그림 13] movie_psh 최근 문서 복구

확인 결과 fileserver의 administrator.MOVIE 계정의 최근 열람 문서는 리셋 시나리오가 있으며 psh_srver의 movie_psh 계정의 최근 열람 문서는 기획안, 안내문, 안내문 수정본이 있다.

(5) 무비아이 스튜디오의 AD 관리자 IP, 계정, 암호는 무엇인가요? (3점)

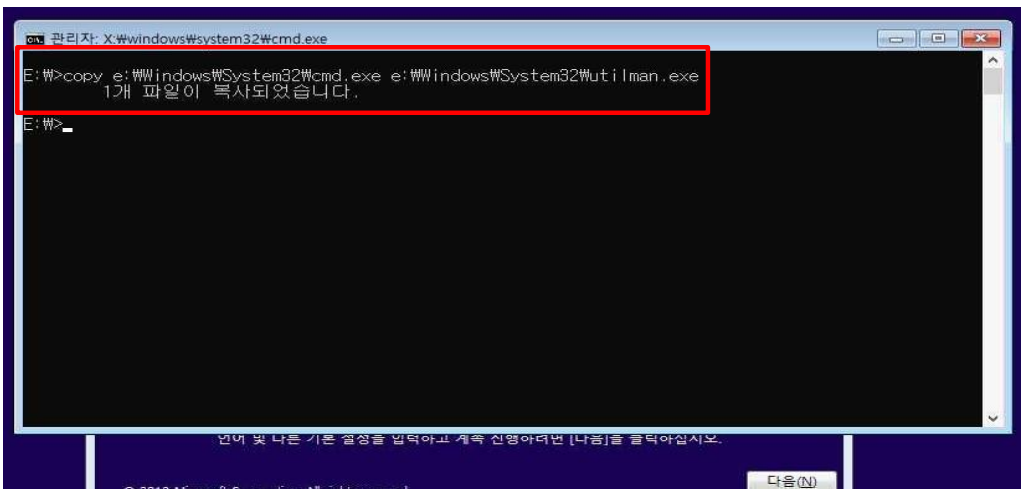
지급받은 VMware server의 AD 관리자 암호를 알게 되면 IP와 계정 정보를 알 수 있게 된다. 암호를 알기 위해서는 패스워드 크래킹이라는 작업이 필요하며 이 패스워드 크래킹을 위 한 다양한 방법과 툴들이 존재한다. 그중 mimikatz라는 툴이 있는데 이 툴을 이용할 시 비교 적 간단하게 패스워드를 크래킹 하는 것이 가능하다.

mimikatz를 이용하기 위해서는 해당 PC에 접속한 상태여야 한다. 이를 위해서는 Windows 로그인 화면에서 cmd를 이용할 수 있어야한다. 먼저 Windows를 포맷 할 시 많이 사용하는 부팅 USB를 준비한 후 VMware에서 USB 부팅을 통해 윈도우 설치 화면을 띄운다.



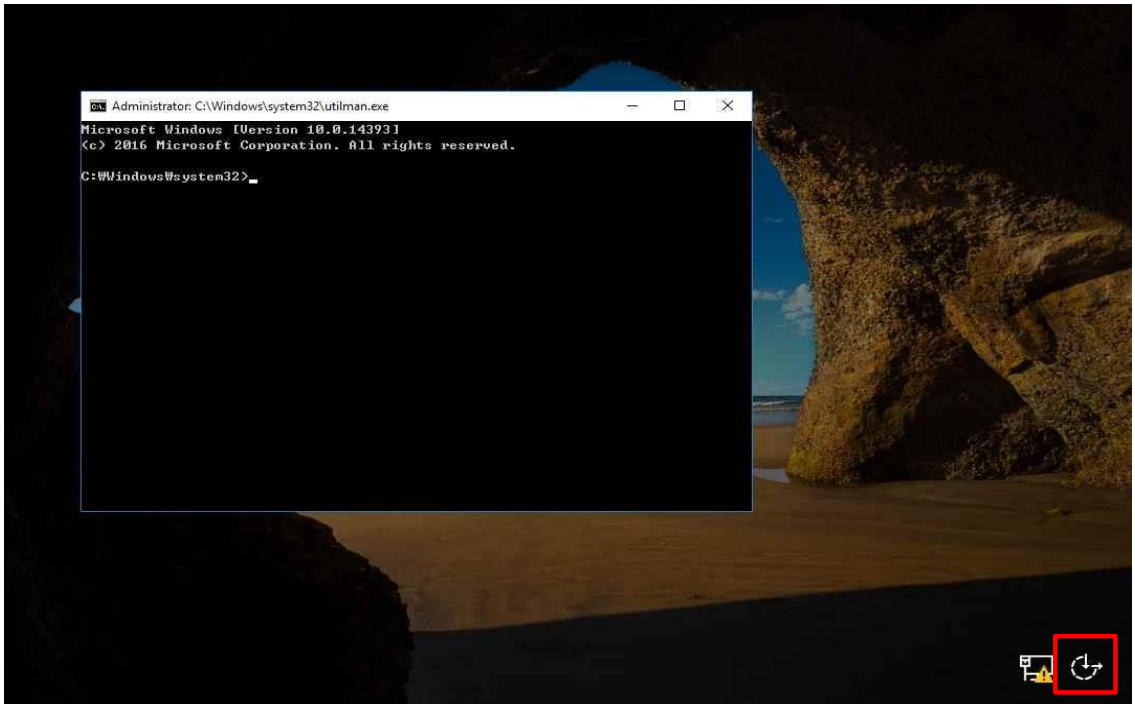
[그림 14] windows 설치 화면

Windows 설치 화면에서 Shift + F10을 누르면 cmd 창이 뜬다. 이 cmd 창에서 copy 명령 어를 이용해 메인 디스크의 \Windows\System32\cmd.exe를 같은 폴더에 utilman.exe란 이름으로 저장한다.



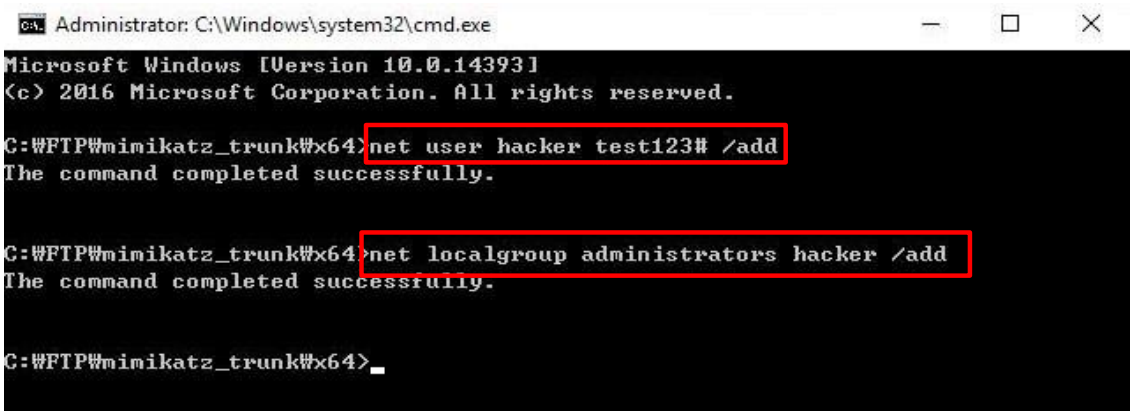
[그림 15] copy cmd

위 과정 마친 후 Windows를 종료 후 부팅 USB를 제거한 후 Windows를 실행하면 로그인 화면이 정상적으로 뜬다. 이 화면에서 오른쪽 밑에 있는 접근성 아이콘을 클릭하면 다음과 같 이 cmd 창이 뜨는 모습을 확인할 수 있다.



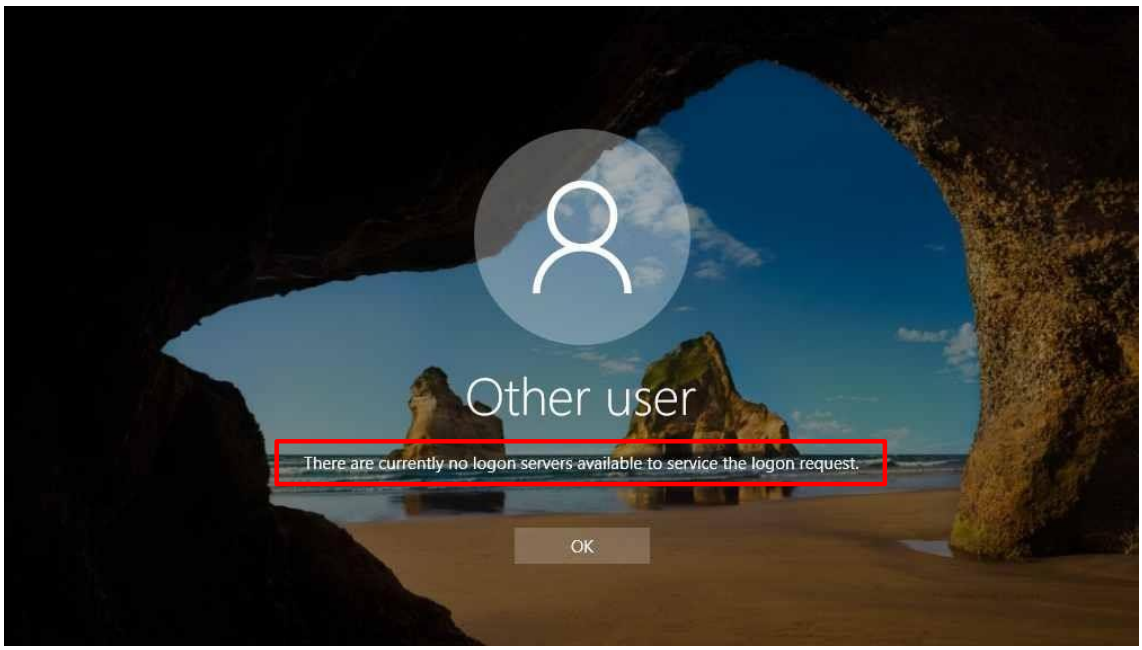
[그림 16] cmd 실행

먼저 Windows에 접속하기 위해 새로운 계정을 하나 만들어야 한다. 또한 그 계정을 Administrators 그룹에 속하도록 설정해줄 것이다. cmd 창에 net user [유저명] [비밀 번호] /add 라는 명령어를 입력하면 내가 지정한 유저명과 비밀번호로 생성된 계정 하나가 생긴다. 그 다음 net localgroup administrators [유저명] /add 란 명령어를 입력하면 hacker 계정을 administrators group에 추가해준다.



[그림 17] net 명령어

계정을 추가하였다면 추가한 계정으로 컴퓨터에 접속하는 것이 가능해진다. 로그인 화면에서 Other user를 선택한 후 추가한 계정으로 로그인을 하면 된다. 이때 도메인 서버 설정을 안 한다면 다음과 같은 error가 발생할 수 있다.



[그림 18] logon error

이 오류를 해결하기 위해서는 도메인 서버의 이름을 알아야 한다. Other user 화면에서 "Sign in to" 부분이 바로 현재 도메인 서버의 이름을 나타내는 부분이다. 이 도메인으로 접 속을 시도하였더니 오류가 뜬 것으로 보아 hacker 계정은 다른 도메인에 생성이 된 것을 알 수 있었다.

[그림 19] domain server name

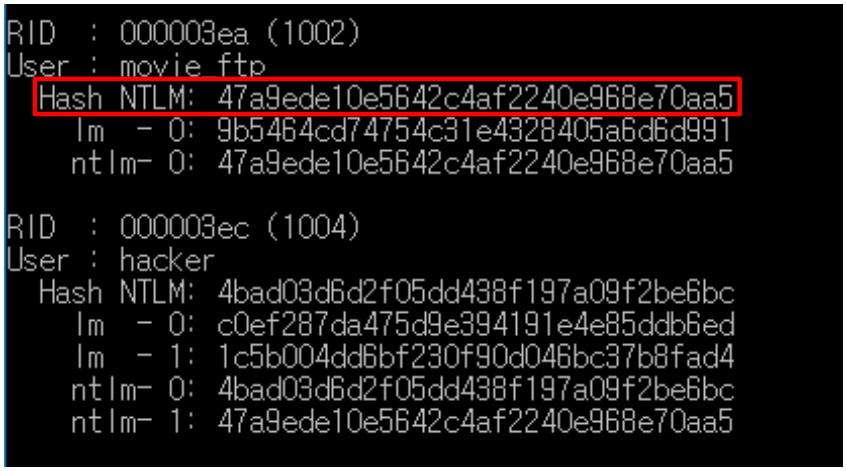
[그림 20] How do I sigh in to another domain?

그림 18을 보면 “sign in to” 바로 밑에 “How do I sigh in to another domain?”이라는 문구가 보인다. 이 문구를 클릭하면 그림 19와 같은 설명이 나오는데 이곳을 보면 다른 도메인의 접속 방법이 나와 있다. 그리고 가장 밑에 있는 문구를 보면 FILESERVER\local 유저만 이 PC에 접속할 수 있다고 나와 있는 것을 볼 수 있다.

이에 User name에 FILESERVER\을 입력하니 그림 20과 같이 “sign in to”가FILE SERVER로 바뀐 것을 확인할 수 있었다. “sign in to”가 FILESERVER로 바뀐 것을 확인 후 FILESERVER\hacker로 로그인을 시도하니 정상적으로 로그인을 할 수 있었다.

[그림 21] FILESERVER

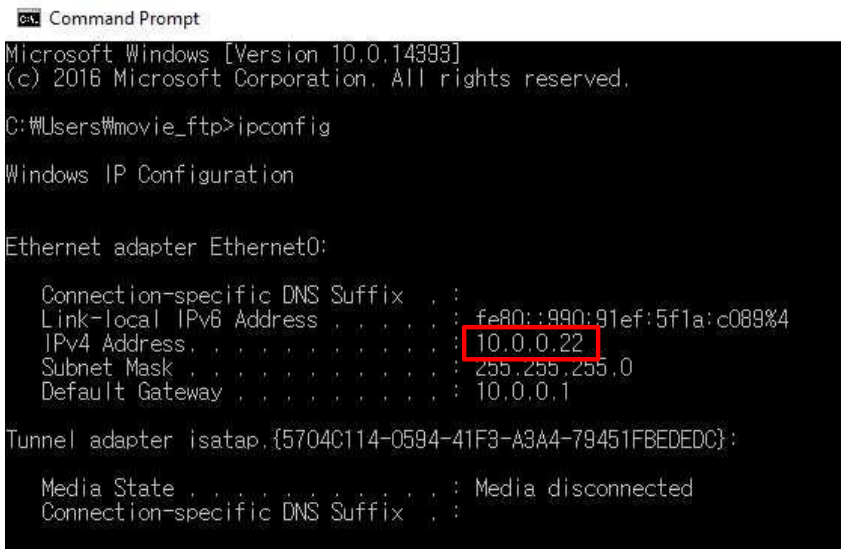
로그인을 한 후 mimikatz를 설치하면 지정한 위치에 폴더가 생성된다. 그곳으로 이동 후 mimikatz를 관리자 권한으로 실행시키면 된다. mimikatz를 실행시킨 후 명령어를 활용하여 NTLM 해시 값을 뽑아낸 후 인터넷을 통해 복호화하면 패스워드의 값을 알 수 있다.



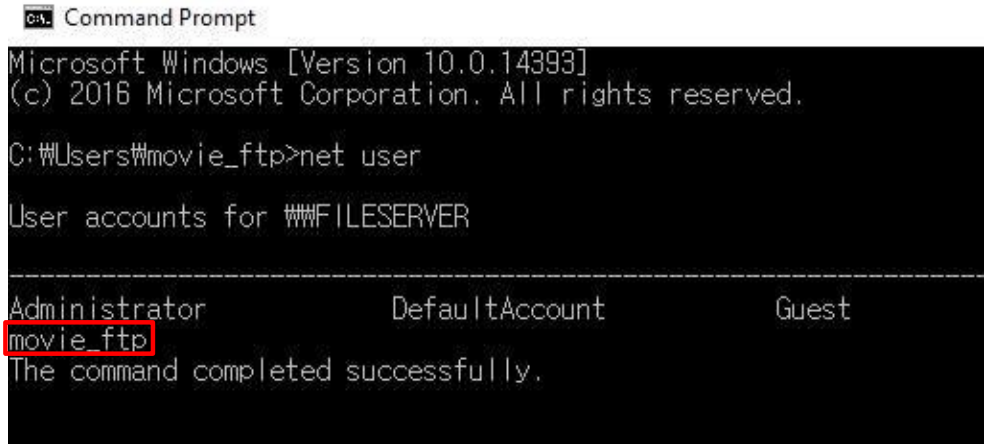
[그림 22] NTLM 해시

[그림 23] hash decrypte

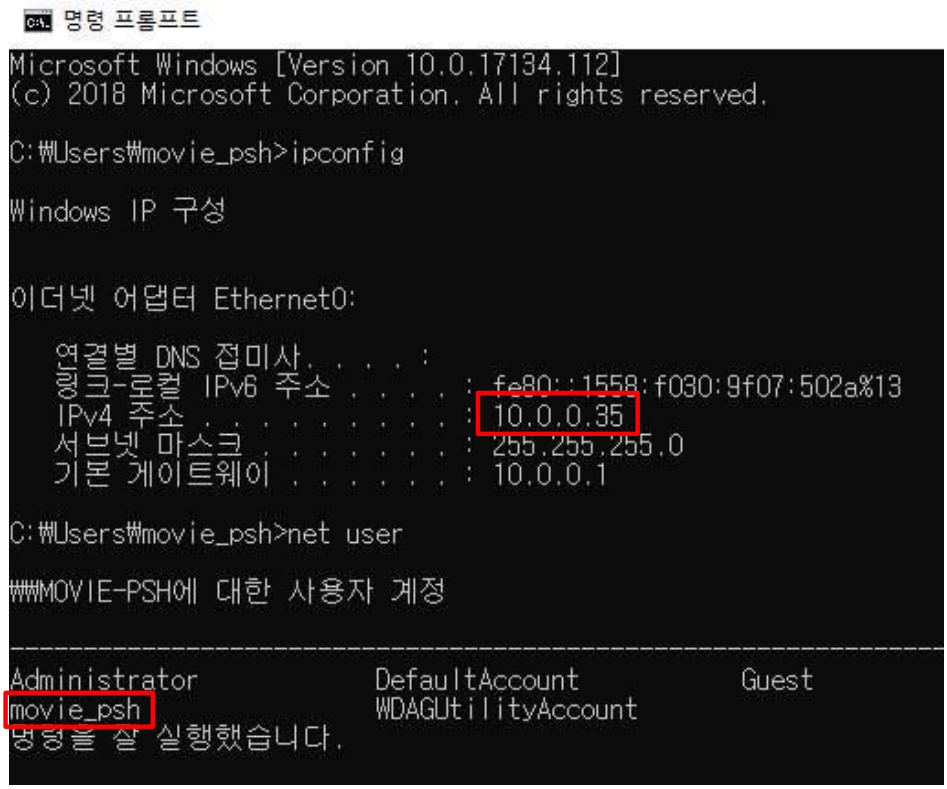
인터넷을 이용하여 NTLM 해시의 값을 decrypte를 해보니 asdf123#이라는 값이 나왔다. 이 값과 User명에 나온 movie_ftp란 이름으로 로그인을 시도한 결과 올바른 패스워드라는 사실 을 확인할 수 있었다. 또한 로그인을 한 후 cmd에서 ip와 유저에 대한 정보를 얻을 수 있었 다.



[그림 24] fileserver ip



[그림 25] net user

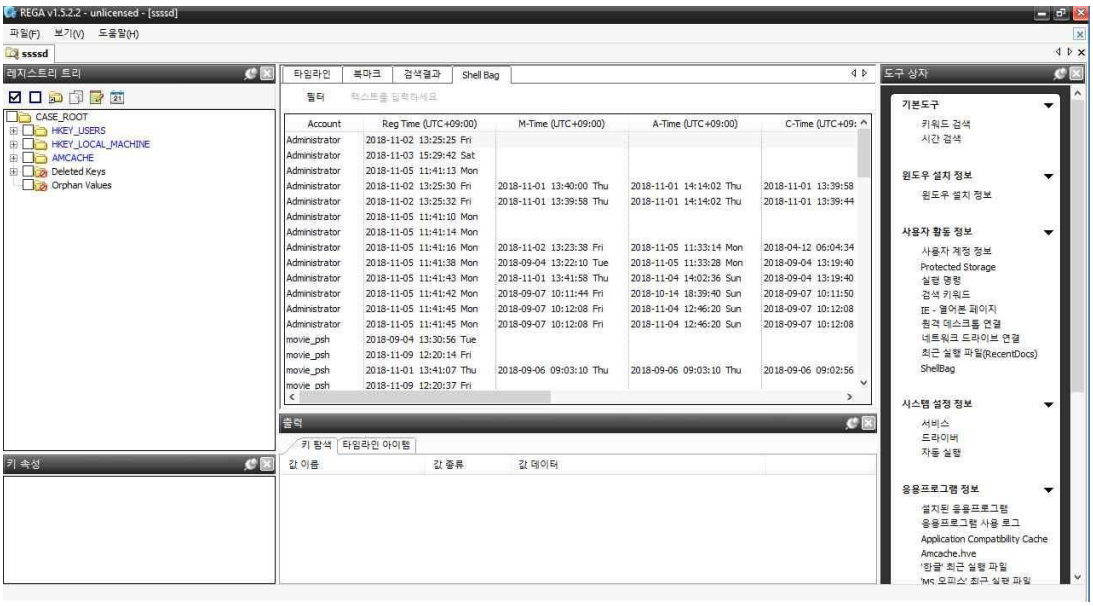


[그림 26] psh_internal ip & net user

확인 결과 fileserver의 AD 계정은 movie_ftp이며, ip는 10.0.0.22, 패스워드는 asdf123#이 다. 위와 같은 과정을 거쳐 확인해본 결과 psh_interanl의 AD계정은 movie_psh이며, ip는 10.0.0.35, 패스워드는 psh123#으로 확인되었다.

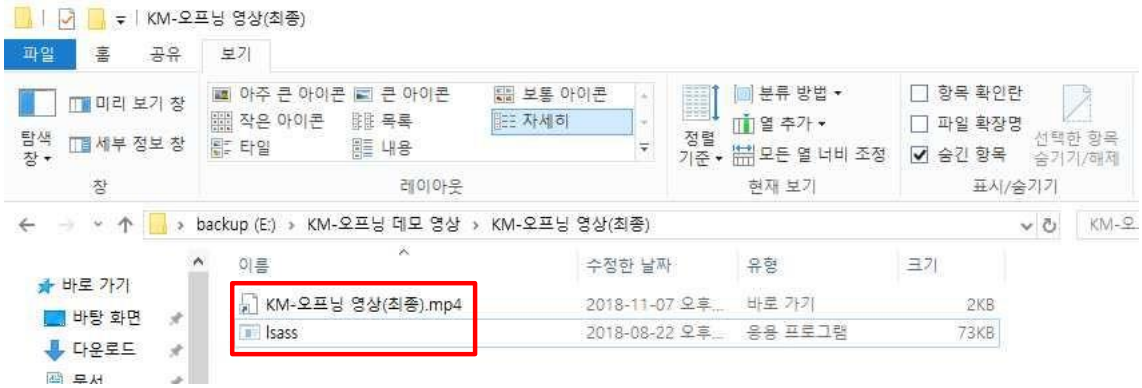
(6) 최초로 생성된 악성코드 파일의 해시 값과 악성코드 기능에 대해 작성하세요. (3점) 최초로 생성된 악성코드 파일의 해시 값과 악성코드 기능에 대해 알기 위해서는 우선 악성코 드의 위치에 대하여 파악하여야 한다. 먼저 fileserver와 psh_internal 서버에 악성코드가 있 는지 REGA라는 툴을 사용하여 조사해 보았다. REGA는 사용자 PC의 레지스트리 정보를 수 집하여 분석을 도와주는 툴로 삭제된 레지스트리까지 확인을 할 수 있다.

REGA를 이용해 각 서버의 응용 프로그램 실행 정보, Shellbag, 최근 실행 파일 등 여러 가지 로그를 분석결과 psh_internal 서버의 E 드라이브에 있는 KM-오프닝 영상(최종).mp4 파일에 접근한 기록 찾을 수 있었다. 하지만 E 드라이브를 확인한 결과 어떤 파일도 발견할 수 없었고 이에 복구 프로그램을 이용하여 삭제된 파일들을 복구하였다.



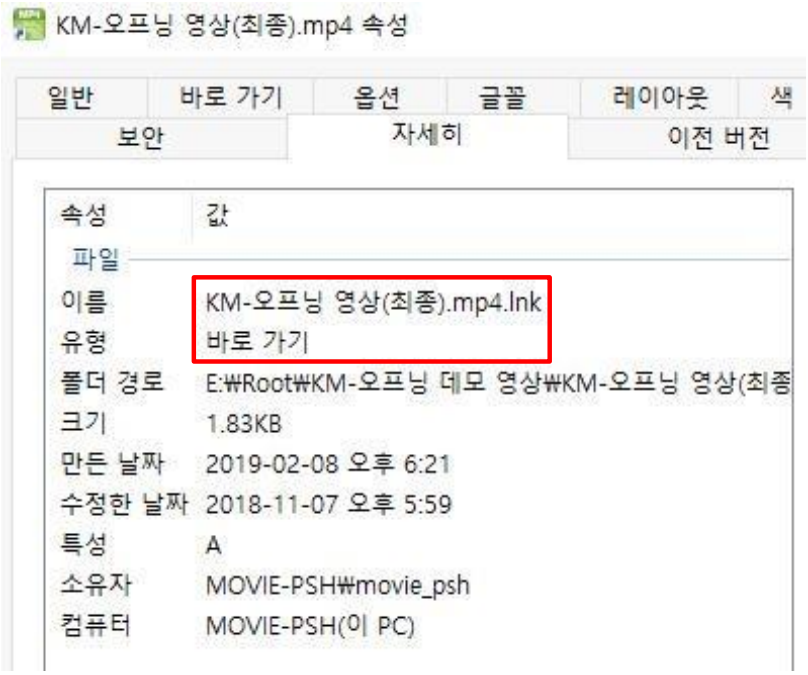
[그림 27] REGA

복구된 E 드라이브를 살피던 도중 KM-오프닝 영상(최종)이란 폴더에서 다음과 같이 2개의 파일을 발견하였다. 그 중 lsass.exe는 숨겨져 있고 KM-오프닝 영상(최종).mp4 파일은 확장 자 표시를 켜지 않았는데 확장자가 표시되어 자세히 살펴보았다.



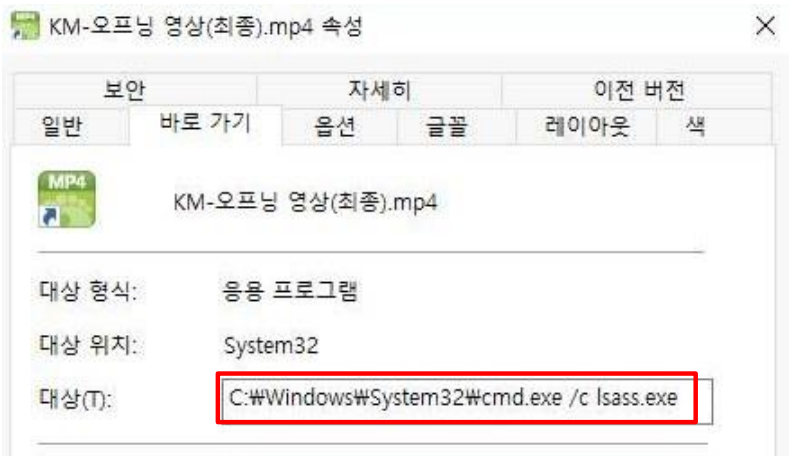
[그림 28] lsass.exe

KM-오프닝 영상(최종).mp4 파일을 보면 확장자가 mp4 같이 보인다. 하지만 현재 확장자 표시를 켜지 않은 상태인데 확장자가 표시되는 것이 이상하여 속성에서 자세히 확인해보았다.



[그림 29] KM-오프닝 영상(최종).mp4

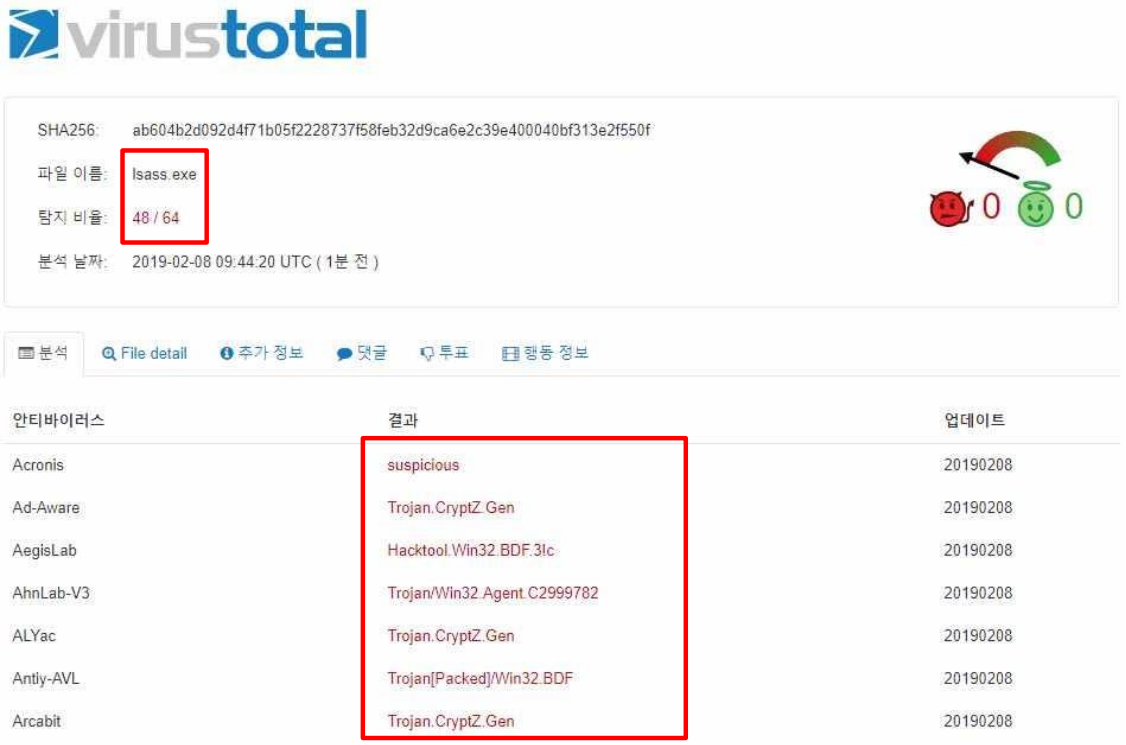
KM-오프닝 영상(최종).mp4 파일의 속성에 들어가 자세히 탭을 확인해 보니 파일의 확장자 가 mp4가 아닌 lnk로 되어있는 것을 확인 할 수 있다. 즉 확장자를 숨겨 놓은 것이다. 확인 결과 파일이 실행되면 cmd.exe를 실행시켜 같은 경로에 있던 lsass.exe 파일을 자동으로 실 행시키도록 만든 바로가기 파일이라는 것을 알 수 있었다.



[그림 30] cmd 실행 및 명령

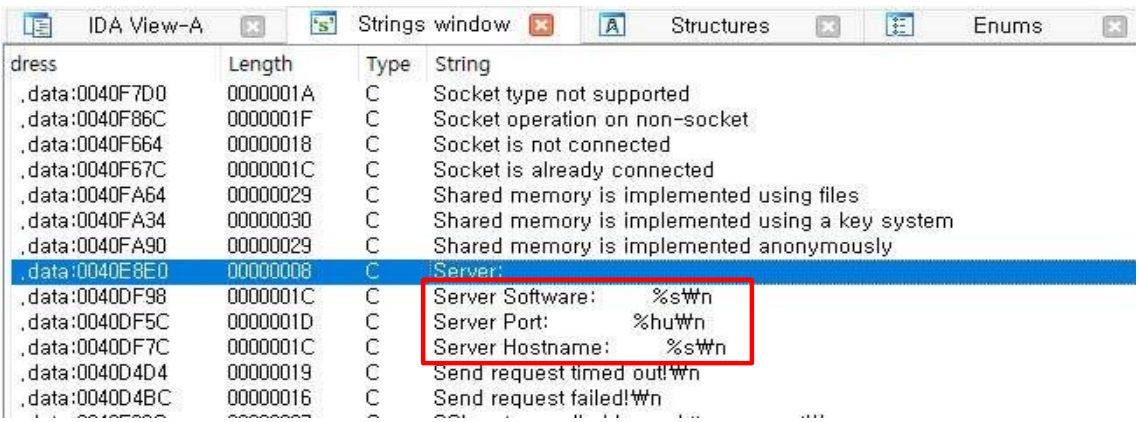
lsass.exe 파일은 Local Security Authority Subsystem Service(로컬 보안 인증 하위 시 스템 서비스)의 약자로 보안 정책을 강화하는 역할을 하는 윈도우 기본 프로세스이다. 이 파 일의 정상적인 경로는 C:\Windwos\System32\이다. 즉, E 드라이브에서 발견된 lsass.exe는 정상적인 윈도우 기본 프로세스가 아닐 수도 있는 것이다.

이에 E 드라이브에 있던 lsass.exe 파일을 악성코드 분석 사이트인 바이러스 토탈을 이용해 분석을 해본 결과 lsass.exe 파일이 트로이 목마형 악성코드라는 사실을 알아낼 수 있었다.



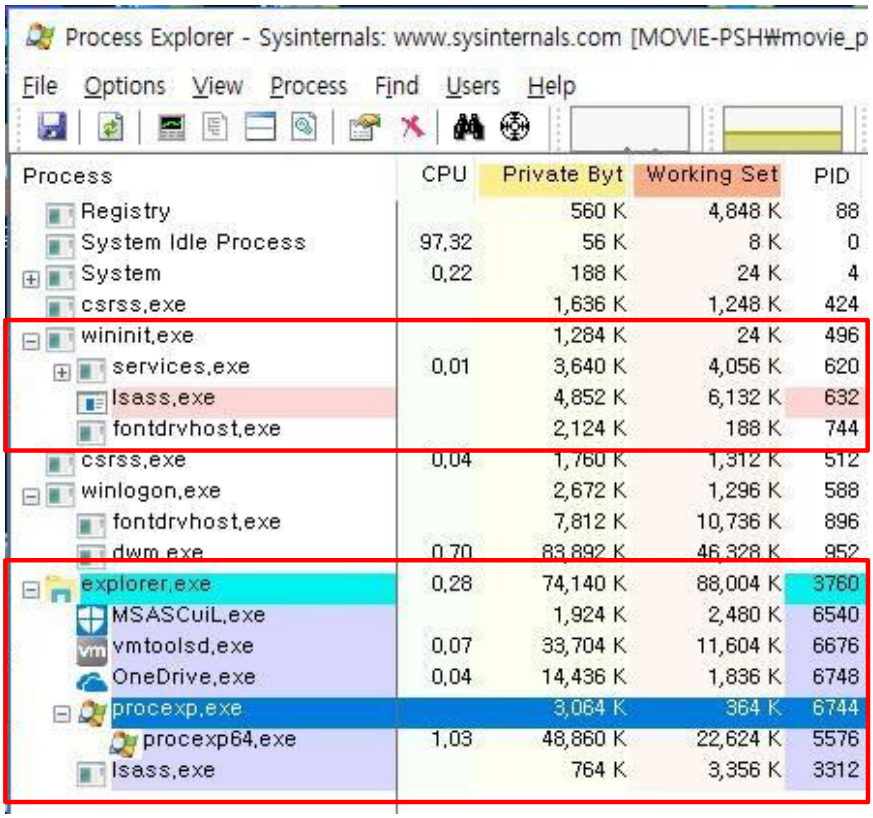
[그림 31] Virus Total

이 악성코드가 어떤 기능을 가지고 있는지 알기 위해 정적 분석 툴인 IDA를 이용하여 바이 너리를 확인해 보았다. 확인 결과 피해자 PC의 소프트웨어, IP, 포트 정보를 변수로 받아 이 정보를 어떤 인터넷 서버에 전송한다는 사실을 알아낼 수 있었다.



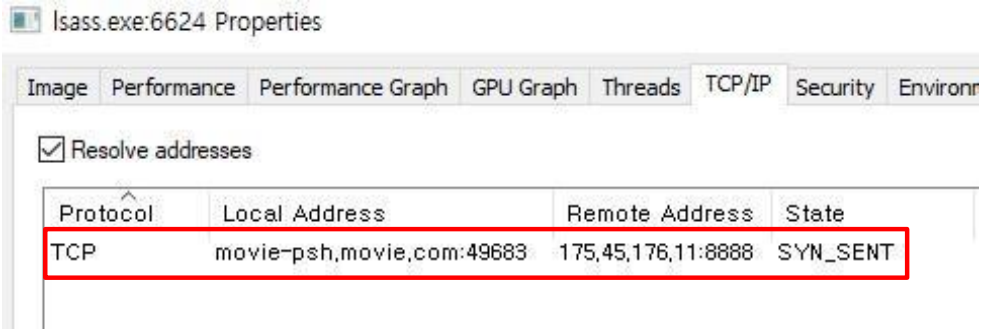
[그림 32] IDA 분석

더 정확한 분석을 위해 이 악성코드를 VMware에서 실행을 시킨 후 Process Explorer를 이용해 동적 분석을 진행하였다. 만약 lsass.exe가 정상적인 윈도우 기본 프로세스라면 explorer.exe 항목이 아닌 wininit.exe 항목의 하위에 위치해야 한다. 하지만 다음 그림과 같 이 explorer.exe 항목에서 lsass.exe가 실행되고 있다. 또한 정상적인 lsass.exe는 wininit. exe에서 제대로 돌아가고 있다는 것 또한 확인이 가능하다.



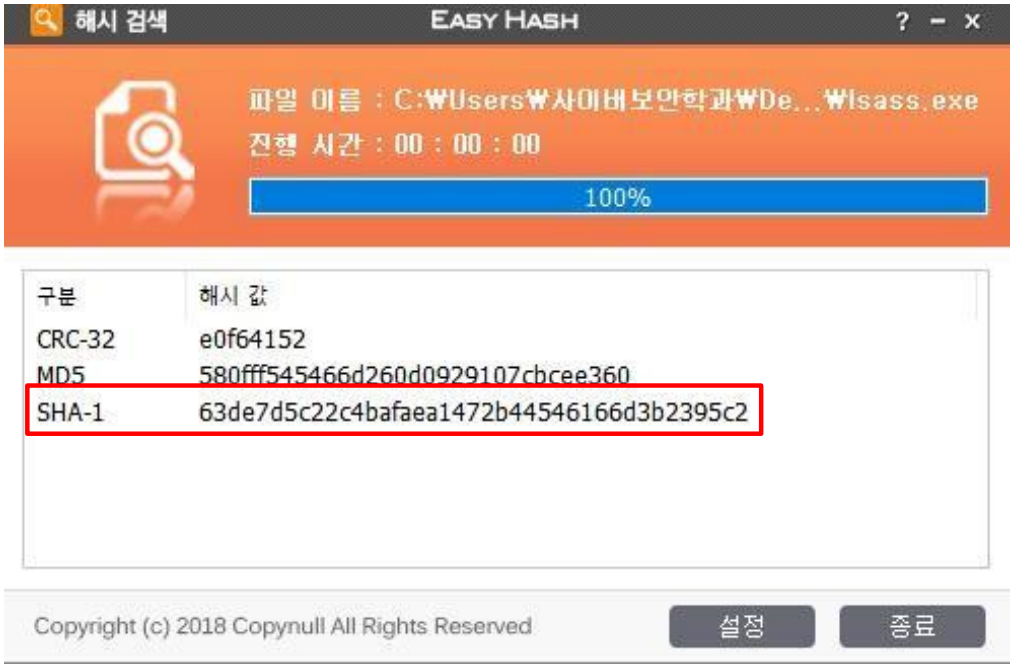
[그림 33] Process Explorer

explorer.exe에서 돌아가는 lsass.exe의 상세 정보를 확인해보니 TCP/IP 항목에서 175.45.176.11:8888로 SYN 신호를 지속적으로 보내고 있다는 것을 알 수 있었다.



[그림 34] SYN_SENT

lsass.exe의 Hash 값은 Easy Hash라는 툴을 이용하였으며 확인 결과 다음과 같은 Hash 값들이 나왔다. 그 중 SHA-1의 Hash 값은 63de7d5c22c4bafaea1472b44546166d3b2395c2 이다.

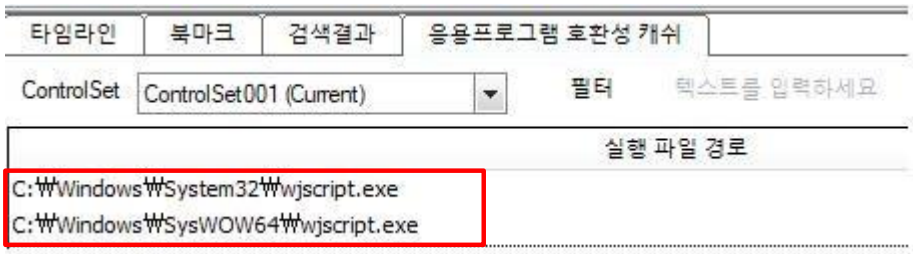


[그림 35] SHA-1 HASH

즉, 최초로 생성된 악성코드는 lsass.exe 파일로 전형적인 백도어형 악성코드로 피해자가 이 파일을 실행시키면 공격자의 인터넷 서버로 SYN 신호를 보내는 기능을 수행한다고 할 수 있 다. 이 신호를 받은 공격자는 피해자 PC에 원격 접속이나 조작이 가능할 것으로 예상할 수 있으며 이 파일의 Hash 값 중 SHA-1 값은 63de7d5c22c4bafaea1472b44546166d3b2395c2 이다.

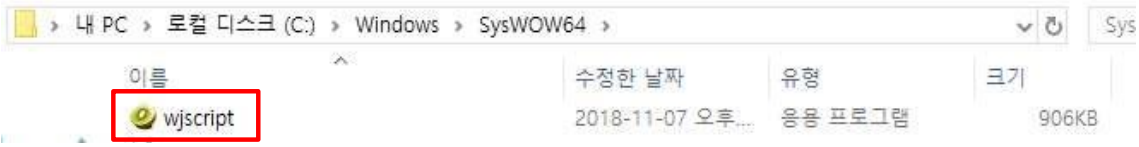
(7) 공격자가 추가적인 공격을 하기 위해 자격증명 탈취 도구를 사용하였습니다. 자격증명 탈 취 도구의 해시 값은 무엇이고, 자격증명 탈취 도구가 현재 어느 경로에 저장되어 있나요? (3 점)

최초의 악성코드 lsass.exe가 psh_internal 서버에서 최초로 실행된 날짜는 2018-11-07일 이다. 추가적인 공격은 같은 날에 이루어질 확률이 높기에 2018-11-07일을 중심적으로 REGA를 통해 레지스트리를 확인해본 결과 응용프로그램 호환성 캐시에서 다음과 같은 기록 을 발견할 수 있었다.



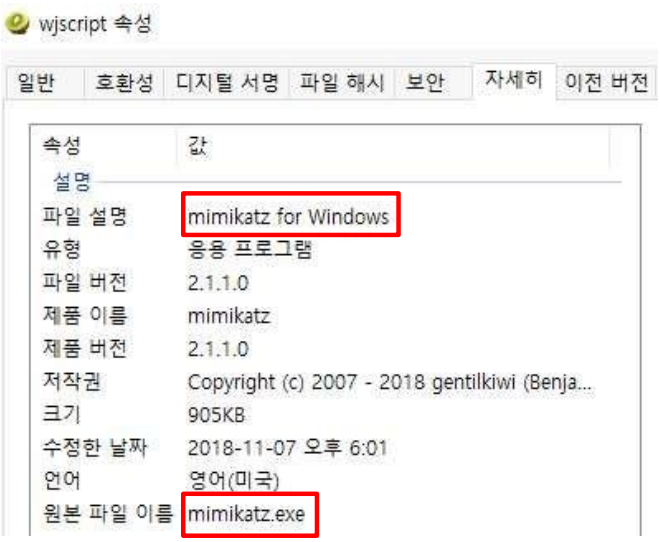
[그림 36] 응용프로그램 호환성 캐시

위에 있는 경로로 이동을 해본 결과 C:\Windows\System32\wjscript.exe는 찾을 수 없었 지만 C:\Windows\SysWOW64\wjscript.exe는 발견할 수 있었다.



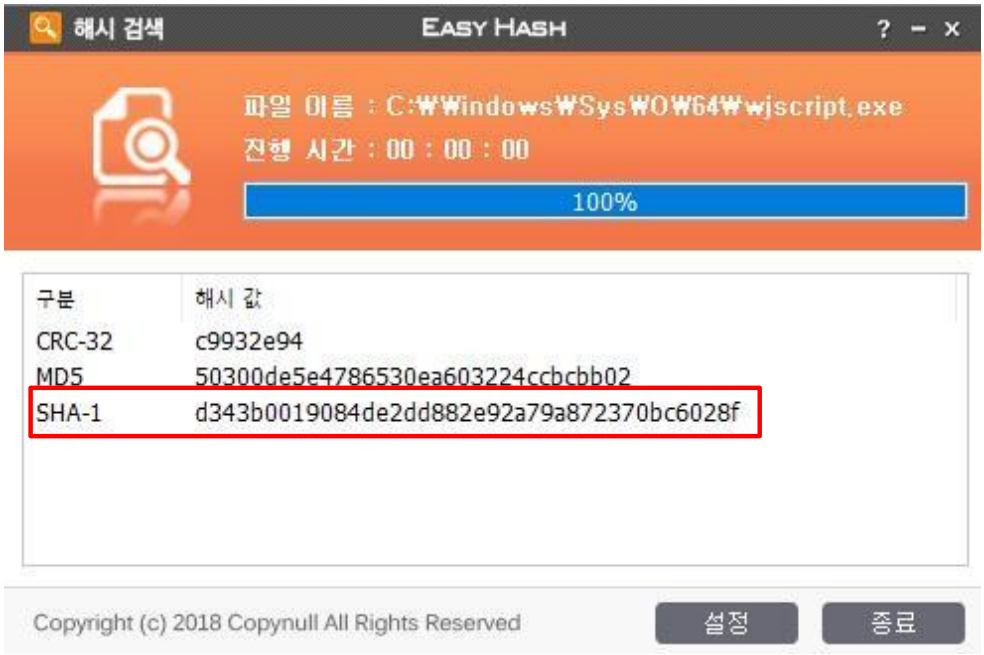
[그림 37] wjscript

이 파일의 속성을 확인해 보니 자격증명 탈취에 많이 쓰이는 툴인 mimikatz인 것을 확인할 수 있었다.



[그림 38] mimikatz

이 파일의 Hash 값을 확인 결과 SHA-1의 값은 d343b0019084de2dd882e92a79a872370b c6028f로 확인이 되었다.

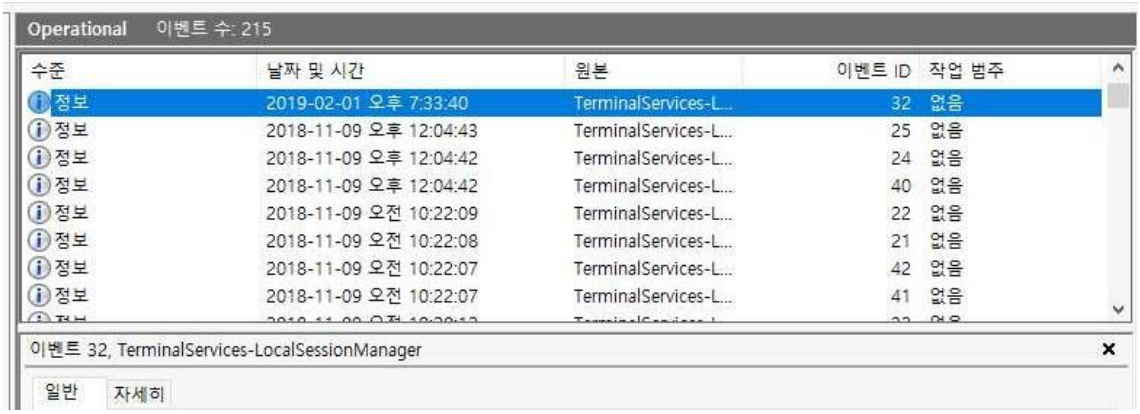


[그림 39] mimikatz SHA-1

즉, 추가 공격에 쓰인 자격증명 탈취 도구는 mimikatz가 발견이 되었으며 이 파일의 경로는 C:\Windows\SysWOW64\wjscript.exe이다. 또한 이 파일의 SHA-1 Hash 값은 d343b0019 084de2dd882e92a79a872370bc6028f이다.

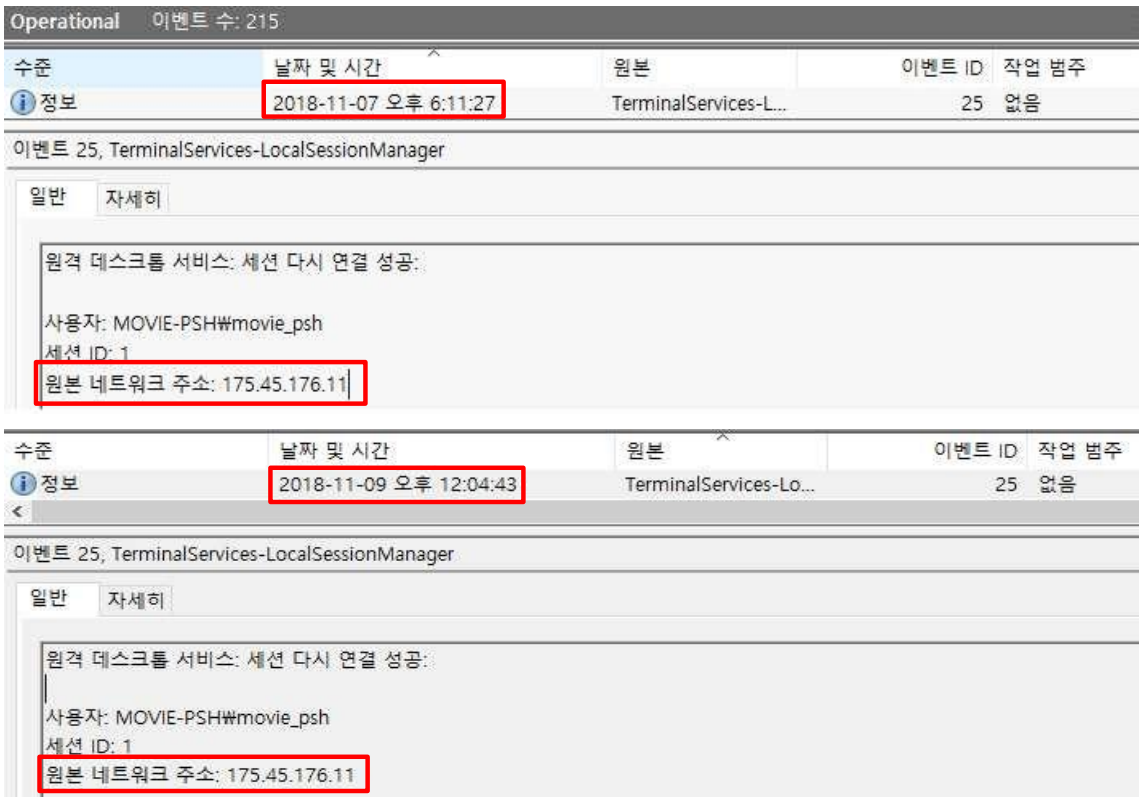
(8) 공격자가 원격 접속 프로토콜(RDP)을 이용해 접속한 시점은 언제인가요? (3점)

원격 접속 프로토콜의 Log는 이벤트 뷰어에서 확인이 가능하다. 이벤트 뷰어에서 응용프로그램 및 서비스로그 항목의 Microsoft, Windows, TerminalServices-LocalSessionManag er, Operational로 이동하면 원격 접속 프로토콜의 Log를 확인 가능하다.



[그림 40] 이벤트 뷰어

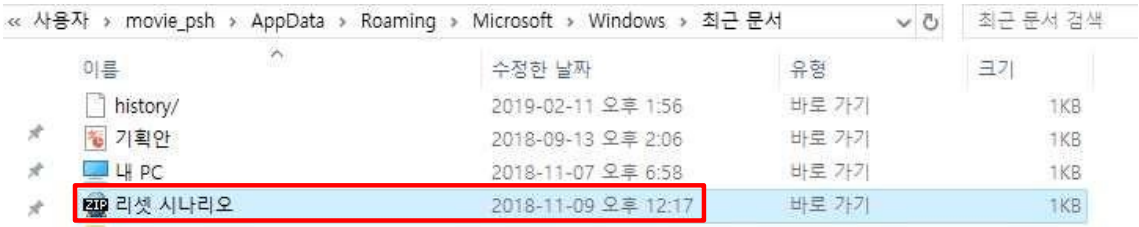
확인 결과 psh_internal 서버에서 175.45.176.11의 원격 접속 흔적을 발견할 수 있었다. 2018-11-07일에 처음으로 원격 접속을 하였으며 2018-11-09일에도 접속을 한 기록을 발견 할 수 있었다.



[그림 41] 원격 접속 로그

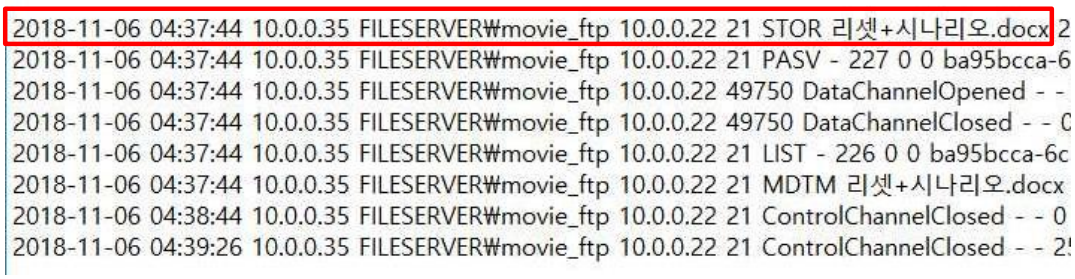
ip 주소 175.45.176.11은 공격자의 ip 주소이므로 위 Log들이 바로 공격자가 원격 접속을 한 시점이라고 할 수 있다. 즉 공격자는 UTC+9, 2018-11-07 18:11:27, UTC+9, 2018-11-09 12:04:43에 피해자의 PC에 원격접속을 한 것이라고 할 수 있다.

(9) 공격자가 탈취한 영화 시나리오의 압축 파일명과 해시 값은 무엇인가요? (3점) psh_internal 서버의 movie_psh 계정을 확인하던 도중 최근 문서에서 리셋 시나리오.zip을 발견할 수 있었다. 또한 이 파일의 마지막 수정 날짜가 공격자가 피해자의 PC에 마지막으로 원격 접속을 한 2018-11-09일이라는 것을 확인할 수 있었다. 이에 이 파일의 속성에서 파일 의 경로를 확인한 후 해당 경로를 확인해 보았다. 하지만 리셋 시나리오.zip 파일은 찾을 수 없었다. 파일 복구 프로그램을 이용하여 복구를 시도하여도 리셋 시나리오.zip 파일을 복구할 수는 없었다.



[그림 42] 최근 문서 리셋 시나리오.zip

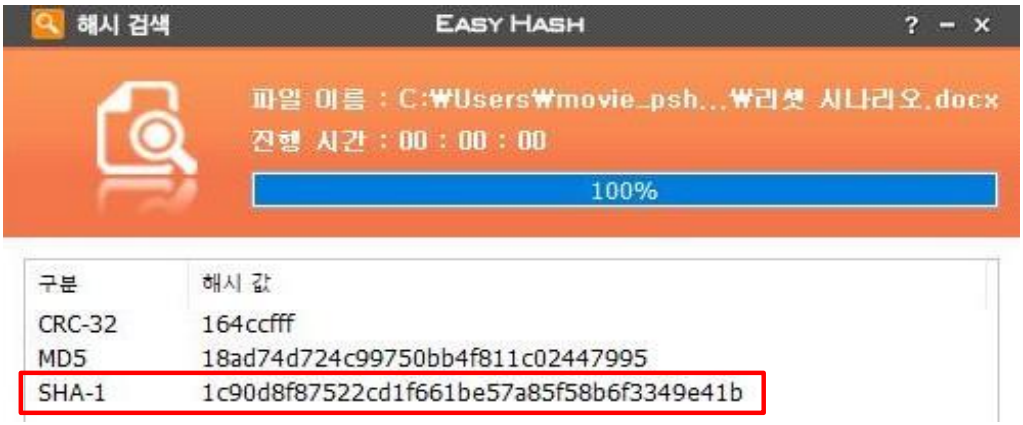
리셋 시나리오.zip을 복구를 할 수는 없었지만 원본 파일을 찾는다면 해시 값을 유출해 낼 수 있기에 압축되기 전인 원본 파일을 찾는데 주력하였다. 리셋 시나리오.zip의 원본 파일은 fileserver에서 찾을 수 있었다. fileserver의 C:\FTP 폴더에서 리셋 시나리오.docx 파일을 발견할 수 있었다. 또한 FTP 전송을 통해 2018-11-06일에 psh_internal 서버의 movie_psh 계정으로 리셋 시나리오.docx 파일을 전송한 기록을 찾을 수 있었다.



[그림 43] 리셋 시나리오.docx FTP 전송

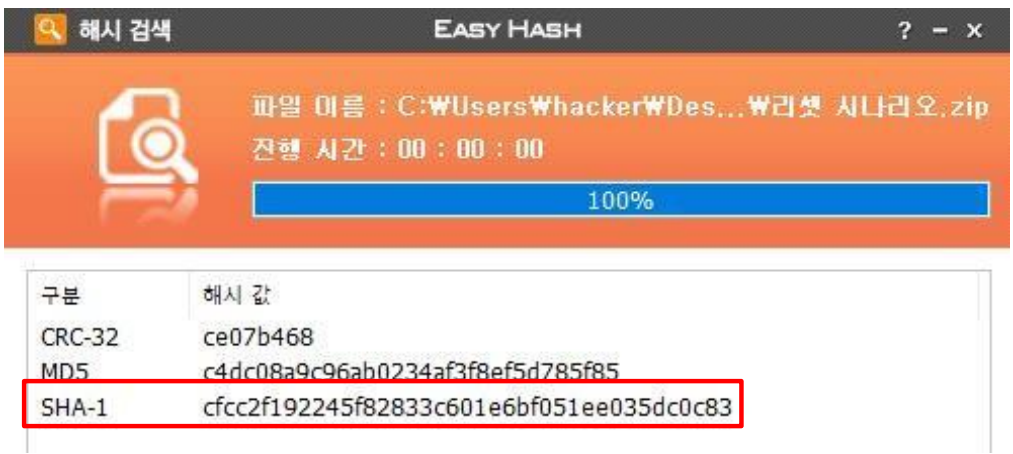
psh_internal 서버에서 리셋 시나리오.docx 파일을 찾아보았지만 리셋 시나리오.zip 파일과 마찬가지로 존재했었던 흔적만을 찾을 수 있었다. 복구 역시 불가능하였다. 이에 공격자가 파 일의 흔적을 지웠다고 판단하였다. 문제에서 요구하는 것은 해시 값이므로 만약 FTP를 통해 파일이 손상되지 않고 전송되었다면 해시 값에 변화가 없었을 것이다.

즉, FTP 전송을 통해 받은 psh_internal에 있었던 리셋 시나리오.docx 파일은 fileserver에 있는 리셋 시나리오.docx 파일과 같은 해시 값을 가지고 있었을 확률이 매우 높다고 판단된 다. 확인 결과 리셋 시나리오.docx의 해시 값은 1c90d8f87522cd1f661be57a85f58b6f3349e4 1b이며 정황 상 이 파일을 압축하여 탈취한 것으로 보인다.



[그림 44] 리셋 시나리오.docx HASH

파일을 압축하면 내부 파일의 해시는 변동이 없지만 새로운 압축 파일이 생기며 고유한 해시 값을 가진다. 이때 어떤 압축 프로그램을 사용하였는가에 따라 해시 값이 변경될 수 있다. psh_internal 서버를 보면 알집 압축 프로그램이 설치가 되어있다. 동일성을 위해 psh_internal에 설치되어 있는 알집 프로그램을 이용하여 파일을 압축한다면 공격자가 탈취 한 파일에 대한 해시 값과 동일한 해시 값이 나올 것이라 생각된다.



[그림 45] 리셋 시나리오.zip HASH

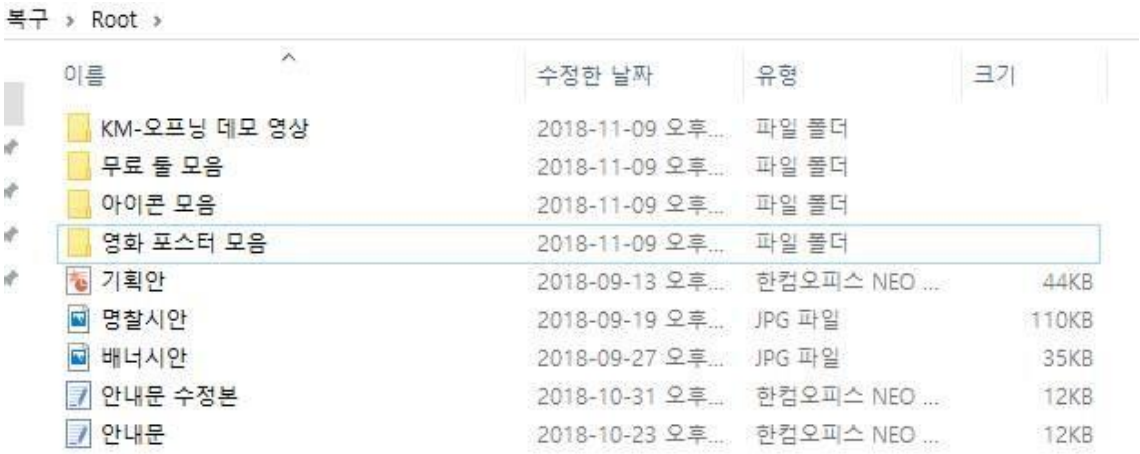
그림 44는 알집을 이용하여 리셋 시나리오.docx를 압축한 후 생성된 리셋 시나리오.zip 파일 의 해시 값을 구한 것이다. 그 결과 SHA-1 값은 cfcc2f192245f82833c601e6bf051ee035dc0 c83으로 나왔다.

정리해보면 탈취당한 영화 시나리오 파일명은 리셋 시나리오.zip이며 이 리셋 시나리오.zip의 원본 파일은 fileserver에 있는 리셋 시나리오.docx이고 이 원본 파일의 SHA-1 해시 값은 1c90d8f87522cd1f661be57a85f58b6f3349e41b이다. 또한 공격자가 탈취한 리셋 시나리 오.zip의 해시 값은 cfcc2f192245f82833c601e6bf051ee035dc0c83으로 추측된다.

(10) 공격자는 목적을 달성한 후 안티포렌식 행위를 한 것으로 보입니다. 공격자는 어떤 안티 포렌식 행위를 수행했나요? (3점)

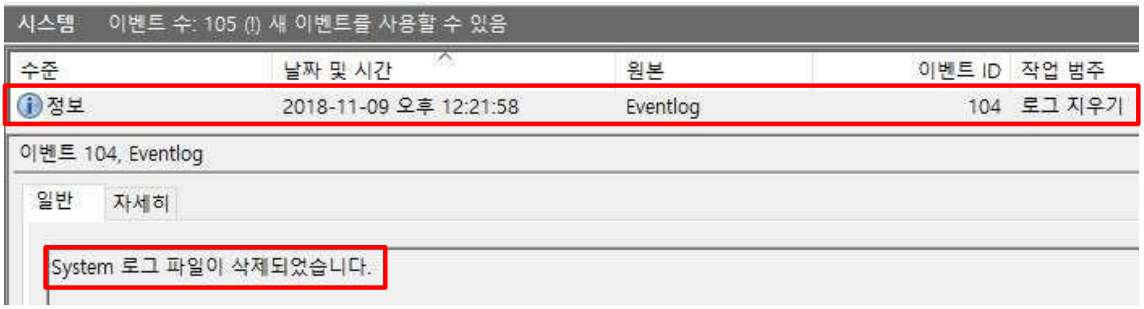
안티포렌식이란 공격자가 피해자의 PC에서 자신의 흔적을 지우는 행위를 말한다. 중요 데이터를 삭제하거나 훼손하는 행위라고 할 수 있다. 공격자는 psh_internal 서버에서의 흔적을 지우기 위해 다양한 안티포렌식 행위를 한 것으로 보인다.

우선 공격자는 psh_internal 서버의 E 드라이브에 있던 악성코드와 모든 파일들을 삭제하였다. 서버를 처음 확인할 때 E 드라이브는 어떤 파일도 찾아볼 수 없었는데 복구 프로그램을 이용하여 확인 결과 다양한 파일들이 삭제되었다는 것을 알 수 있었다. 또한 E 드라이브에서 는 해킹에 사용된 트로이 목마형 바이러스가 발견되기도 하였다.



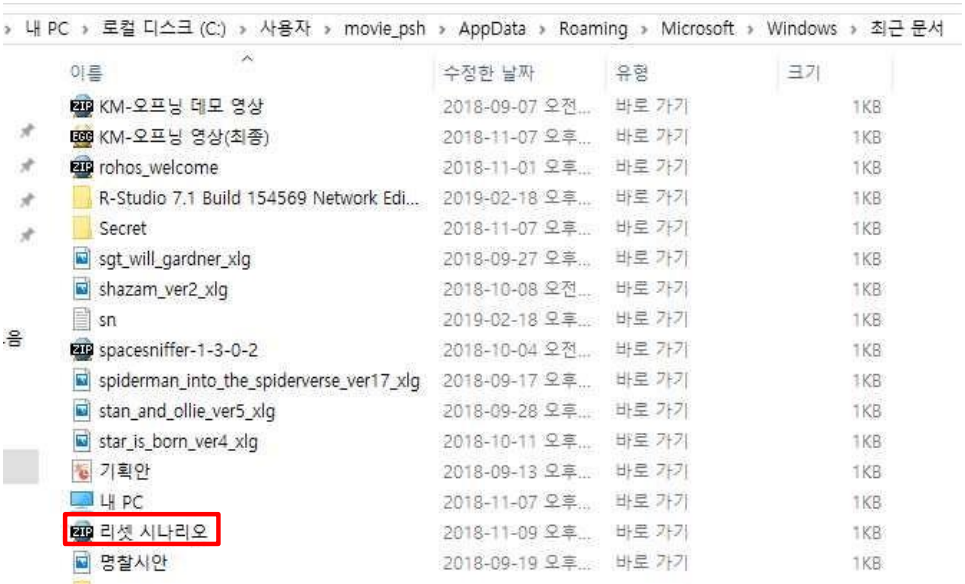
[그림 46] E 드라이브 복구 파일

또한 이벤트뷰어를 통해 확인해본 결과 마지막 침투 날짜인 2018-11-09일 시스템 로그가 삭제된 것을 확인할 수 있었다.

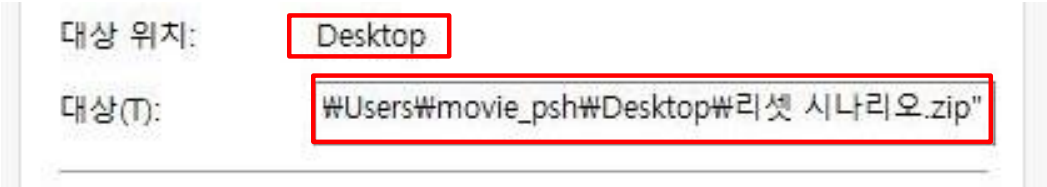


[그림 47] psh_internal 시스템 로그 삭제 기록

psh_internal 서버의 최근 문서에서 리셋 시나리오.zip 바로가기 파일을 통해 리셋 시나리 오.zip 파일이 바탕화면에 존재했었다는 기록을 발견할 수 있었다. 하지만 바탕화면에서는 리 셋 시나리오.zip 파일을 발견할 수 없었다. 이에 공격자가 바탕화면에 있는 리셋 시나리오.zip 파일을 삭제했었다는 사실을 알 수 있었다.

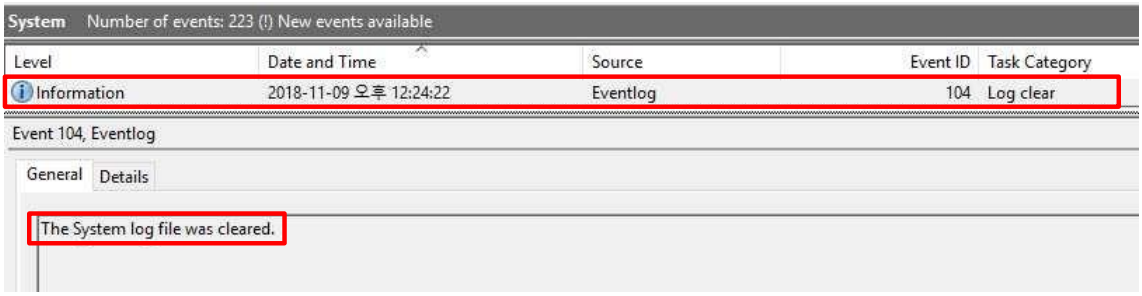


[그림 48] 최근 문서



[그림 49] 리셋 시나리오.zip 대상

fileserver 역시 확인 결과 공격자가 마지막으로 원격 접속을 한 2018-11-09일에 시스템 로 그가 삭제된 기록을 확인할 수 있었다.



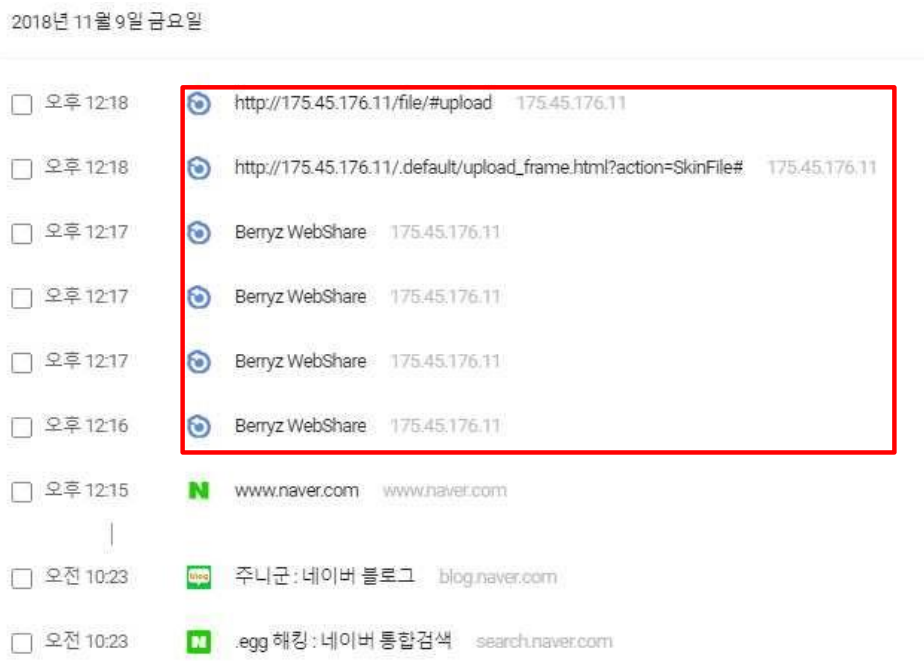
[그림 50] fileserver 시스템 로그 삭제 기록

공격자는 공격에 성공한 후 psh_internal 서버에서 E 드라이브 삭제, 이벤트로그 삭제, 탈취 파일 삭제를 fileserver에서는 이벤트로그 삭제와 같은 안티포렌식 행위를 한 것으로 보인다.

(11) 위 10문제 외 사고와 관련된 모든 공격자 행위와 흔적을 분석하세요. (70점)

분석을 진행하며 찾은 lsass.exe 악성코드를 살펴본 결과 공격자에게 SYN 신호를 보내는 기 능을 가지고 있었다. 이 신호를 받은 공격자는 원격으로 피해자의 PC를 조작하여 파일을 탈취한 것으로 보인다. 하지만 어떠한 방법으로 공격자가 자신의 PC로 리셋 시나리오.zip 파일 을 옮겼는지는 아직 알지 못한다.

이에 대한 해답은 인터넷 기록에서 찾을 수 있었다. 피해자는 네이버 웨일이란 인터넷 브라우저를 사용한 것으로 확인이 되어 이 네이버 웨일에서 인터넷 기록을 살펴보던 중 2018-11-09일 기록에서 이상한 점을 찾을 수 있었다.



[그림 51] Berryz WebShare

그림 49를 확인해보면 Berryz WebShare라는 기록을 발견할 수 있다. Berryz WebShare는 인터넷을 이용한 FTP 서비스를 제공하는 프로그램으로 보통 자신의 PC에서 다른 PC로 파일 을 쉽게 전송하기 위해 개인이 사용하기도 한다. 또한, 바로 옆에 하얀 글씨로 되어있는 ip주 소 역시 확인이 가능하다. 이 ip 주소는 악성 바이러스 lsass.exe 파일을 동적 분석을 하였을 때 확인이 가능했던 ip주소로 ip 175.45.176.11은 공격자의 PC라고 판단이 된다. 즉, 공격자 가 피해자의 PC에 마지막으로 접근한 2018-11-09일에 피해자의 PC에서 공격자의 인터넷 서 버로 접근하였다는 뜻이 된다.

자세히 분석하기 위해 그림 49의 가장 마지막 기록인 http://175.45.176.11/file/#upload로 접속을 시도해 보았다. 접속에는 실패했지만 남아있는 쿠키를 이용해 페이지의 소스를 열어보 니 그림 50과 같은 결과를 확인할 수 있었다.

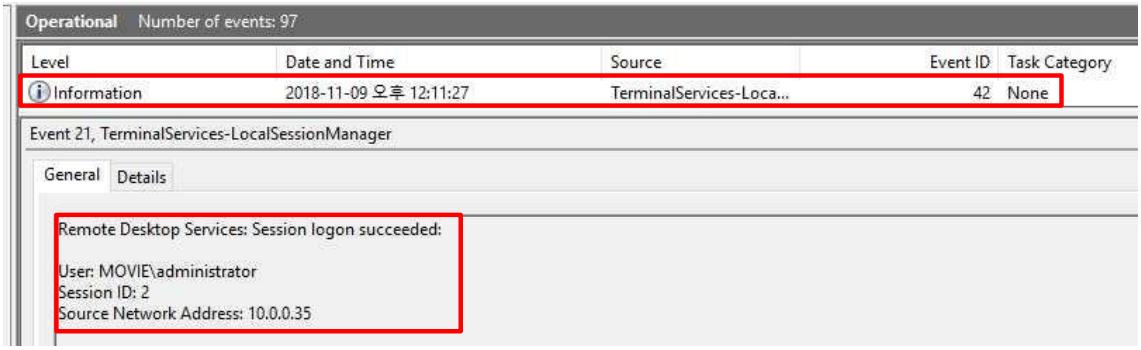
[그림 52] http://175.45.176.11/file/#upload 소스

이 소스의 129번째 줄을 살펴보면 밑에 그림 51과 같은 부분을 찾을 수 있을 것이다. 이 부 분을 확인하면 리셋 시나리오.zip 파일이 http://175.45.176.11/file/#upload에 올라가 있다 는 것을 확인할 수 있었다.

[그림 53] 리셋 시나리오.zip upload

즉, 공격자는 Berryz WebShare를 통해 피해자의 PC에서 파일을 탈취한 후 자신의 PC에서 다운로드 받아 파일을 유출 시켰을 것이다. 이외에도 Berryz WebShare에서 mimikatz 툴을 발견할 수 있었다.

8번 문제를 통해 우리는 공격자가 psh_internal 서버에 원격 접속한 시각을 알 수 있었다. 공격자는 2018-11-07일 오후 6시 11분경에 처음 원격 접속을 성공하였으며 2018-11-09일 오후 12시 04분경에 다시 원격 접속을 성공하였다. 그런데 필자는 fileserver의 이벤트로그를 확인하던 중 그림 53과 같은 로그를 발견할 수 있었다.



[그림 54] fileserver 원격 접속 기록

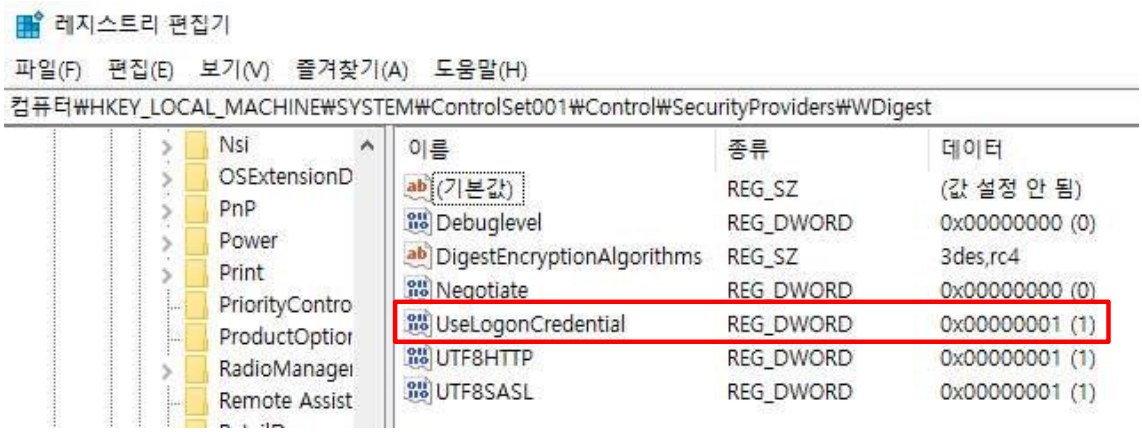
그림 53의 로그를 보면 2018-11-09일 오후 12시 11분경에 ip주소 10.0.0.35에서 원격 접속 을 한 것을 알 수 있다. ip주소 10.0.0.35는 바로 psh_internal의 ip 주소이다. 즉, 공격자가 psh_internal 서버를 조종하던 시각에 psh_internal 서버에서 fileserver로 원격 접속이 이 루어졌다는 것이다. 이에 필자는 그림 53의 원격 접속 로그는 공격자가 fileserver에 원격 접 속을 하였다는 증거라고 생각한다. 정리해 보면 공격자는 psh_internal에 원격 접속한 다음 다 시 psh_internal에서 fileserver로 원격 접속을 한 것이다. 그 시각은 UTC +9, 2018-11-09 12:11:31이다.

또한, 우리는 문제 지문 10번을 통해서 공격자가 fileserver의 시스템 로그를 지웠다는 사실을 알 수 있었다. 공격자가 시스템 로그를 지운 날짜는 2018-11-09일 12시 24분경으로 확인 되었으므로 공격자는 UTC +9, 2018-11-09 12:11:31에 fileserver에 원격 접속을 한 후 시스 템 로그 지우기와 같은 안티포렌식 행위를 한 것이라고 할 수 있다.

필자는 공격자가 mimikatz를 이용하였다는 것을 알아낸 후 psh_internal 서버의 레지스트 리 편집기를 확인하였다. 그 이유는 바로 windows KB2871997 업데이트 때문이다. 사용자가 PC에 로그온하면 자격증명이 생성되어 메모리에 저장된다. 이 자격증명 중에는 일반 텍스트 암호 역시 포함이 되어있었는데 이는 자격증명이 탈취 당할 경우 암호를 일반 텍스트로 바로 확인할 수 있기에 매우 위험하다. 이러한 이유로 일반 텍스트 암호가 더 이상 메모리에 저장 되지 않도록 해주는 것이 바로 windows KB2871997 업데이트이다. windows 10에서는 KB2871997 업데이트가 이미 적용이 되어 있는 상태이다. 즉, mimikatz를 이용해 자격증명을 탈취하여 텍스트 형식의 암호를 유출하기 위해서는 레지스트리의 변경이 반드시 필요하다.

[그림 55] 레지스트리 경로

레지스트리 편집기에서 그림 54의 경로로 이동하면 UseLogonCredential이라는 값이 있을 것이다. 만약 이 값이 0이라면 정상인 것이고 1이라면 자격증명에 일반 텍스트 암호를 저장한 다는 의미이므로 비정상이라 할 수 있다. psh_internal 서버의 UseLogonCredential 값을 확 인한 결과 그림 55와 같은 결과를 얻을 수 있었다.



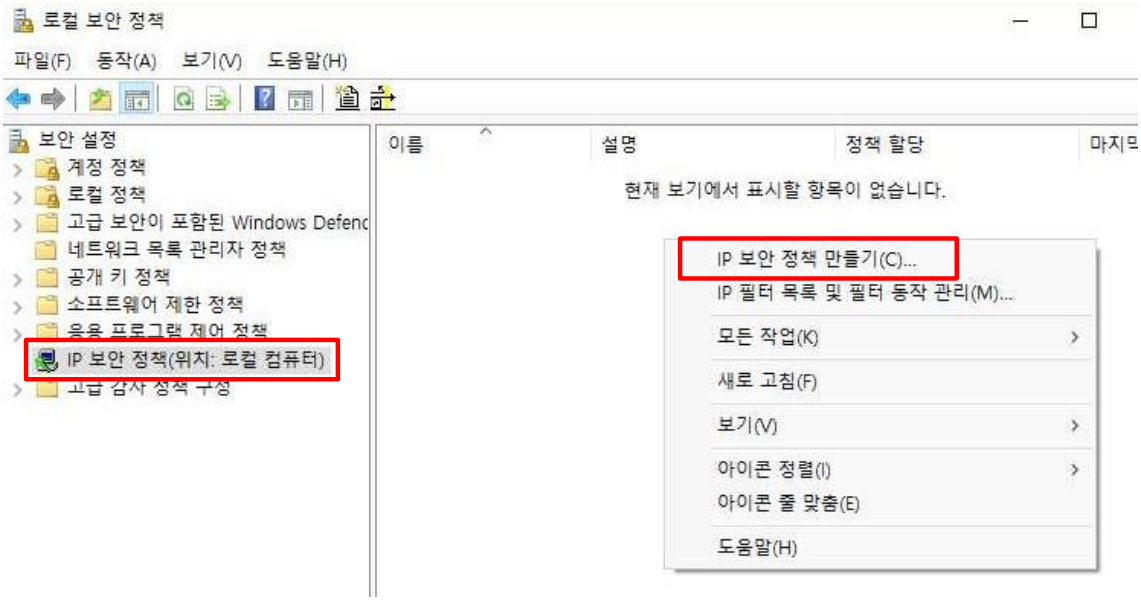
[그림 56] UseLogonCredential 값

확인 결과 psh_internal 서버의 UseLogonCredential 값은 1이었다. 즉, 자격증명 탈취로 일반 텍스트 암호를 알아낼 수 있는 것이다. 이것은 인위적으로 레지스트리가 변경되었다는 것을 의미하기도 한다. 공격자는 psh_internal 서버를 원격 조작한 후 이 레지스트리 값을 변 경하여 mimikatz를 이용해 자격증명을 탈취한 것으로 보인다.

III. 사고 대응 매뉴얼

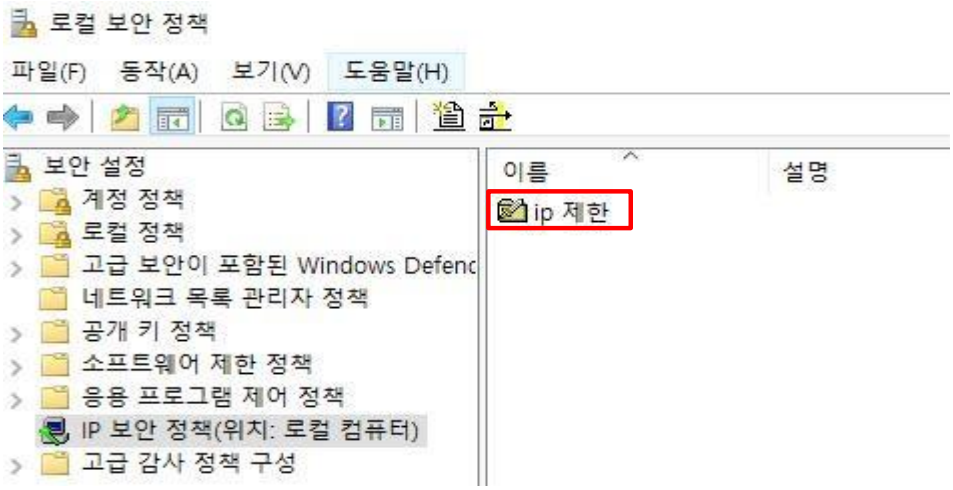
1. 원격 데스크톱 ip 제한

공격자는 백도어형 트로이 목마를 이용하여 침입을 한 후 자격증명을 탈취하여 피해자의 PC 에 원격 접속을 하였다. 이런 경우 만약 피해자의 PC에 특정 ip만 원격 접속을 허용한 상태 였다면 공격자는 피해자의 PC에 원격 접속 할 수 없었을 것이다. 원격 데스크톱의 특정 ip 제한은 로컬보안정책에서 설정할 수 있다. 다음 그림을 참조하기 바란다.



[그림 57] 로컬 보안 정책

로컬 보안 정책에서 ip 보안 정책으로 이동 후 오른쪽 마우를 클릭, ip 보안 정책 만들기를 누른다. 그 후 ip 보안 정책 마법사창이 뜨는데 ip 보안 정책의 이름만 설정해 준 후 다른 부 분은 아무것도 안 건드리고 넘기면 그림 58과 같이 새로운 정책이 생긴다.



[그림 58] 새로운 보안 정책

새로 만든 보안 정책의 속성을 열어 추가를 선택한 후 사용자에게 들어오는 포트 중 원격 접 속을 할 때 사용하는 TCP 3389를 막으면 모든 원격 접속에 대한 접근을 막을 수 있다.

[그림 59] 원격 접속 차단

이후 필터동작 역시 추가를 해야 한다. 필터동작은 다음과 같이 거부로 설정하면 된다.

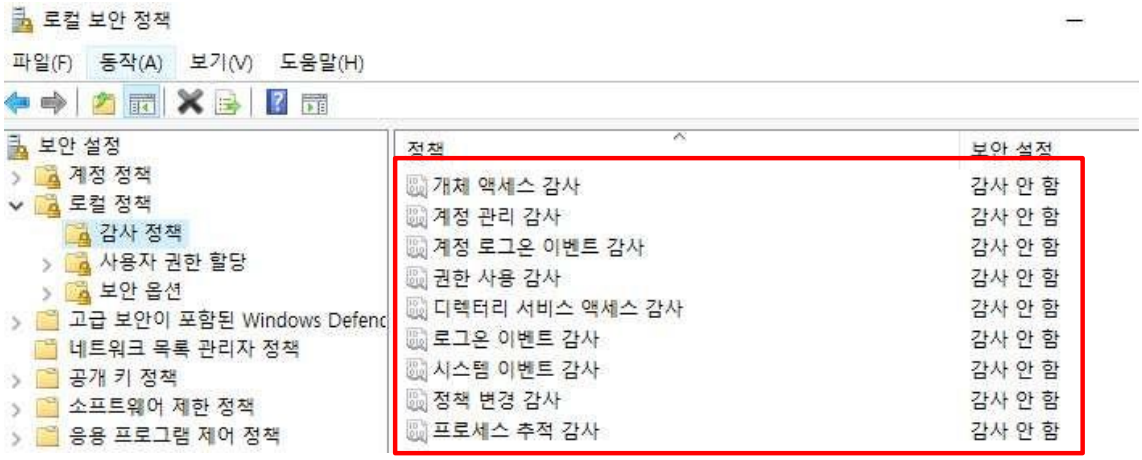
[그림 60] 필터 동작

여기서 주의할 점은 이렇게만 설정할 경우 모든 원격 데스크톱에 대해 차단하게 된다. 허용 해야하는 PC는 반드시 ip 필터 목록에 새롭게 추가 후 허용으로 설정을 해야만 한다. 이와 같은 과정을 거친 후 이 정책을 할당하게 되면 사용자가 지정한 ip만 원격 접속을 할 수 있 다.

III. 사고 대응 매뉴얼

2. 파일 감사 설정

만약 피해자가 파일 또는 폴더에 대한 기본 감사 정책을 적용해 놓았다면 공격자가 침입하 여 한 모든 행위가 로그로 남았을 것이다. 이런 감사 설정은 포렌식에 매우 큰 도움이 되기도 하며 중요한 파일들을 관리하기가 더욱 수월해지기도 한다. 감사 설정은 로컬 보안 정책의 로 컬 정책, 감사 정책에서 관리가 가능하다.



[그림 61] 감사 정책 설정

그림 61은 psh_internal 서버의 감사 정책으로 보는 것과 같이 모든 감사 설정이 감사 안함 으로 설정되어 있는 것을 확인할 수 있다. 이곳에서 감사 설정을 하면 보안에 더욱 도움이 된 다.

III. 사고 대응 매뉴얼

3. 백신 설치 및 활용

psh_internal 서버의 응용 프로그램을 확인해보면 어떠한 백신 프로그램도 확인할 수 없었 다. 이는 매우 위험한 일이라고 할 수 있다. 실제로 이번에 확인된 악성코드 lsass.exe 파일 역시 시중에서 많이 사용되는 백신들에서 모둔 잡을 수 있는 단순한 바이러스 중 하나였다. 다음 그림을 보면 V3 백신에서 lsass.exe 파일을 실시간으로 잡는 것을 확인할 수 있다.

[그림 62] V3 검사

lsass.exe를 백신이 설치된 PC로 옮기자마자 바로 악성 바이러스라고 뜨며 실시간으로 삭제 를 해버린다. 만약, 피해자의 PC에 이런 백신이 설치되어 있었다면 피해자가 바이러스를 실행 하기도 전에 백신에서 잡아낼 수 있었을 것이다.

IV. 마무리

1. 대회 후기

이번 겨울 방학을 맞아 무언가 의미 있는 일을 해보고 싶다는 생각에 이번 대회 참가 결정을 하였다. 사실 지금까지 포렌식을 접해 본적이 없어 문제 풀이를 진행하는데 조금 어려움이 있 었다. 하지만 한 문제, 한 문제 해결할 때마다 차오르는 기쁨에 매우 기뻐하며 대회를 진행하 였고 포렌식이란 학문에 매우 큰 흥미를 가지는 계기가 된 것 같아 매우 뿌듯하다. 사이버보안학과에 진학한 이후로 2년 만에 처음 출전한 대회지만 필자가 할 수 있는 모든 것을 보여주었다고 생각한다. 그동안 배운 것들을 활용하기도 하고 새로운 것들을 배울 수 있 는 매우 좋은 기회였다. 특히 이번 대회를 통해 매우 많은 것들을 배울 수 있었고 많은 툴들 의 사용법을 익히는 좋은 기회가 되어서 필자에게 매우 큰 도움이 되었던 시간이었다.

2. 사용 분석 도구 정보

VHD 변환 도구 : StarWindConverter 레
지스트리 분석 도구 : REGA
동적 분석 도구 : ProcessExplorer 정
적 분석 도구 : IDA Pro
시스템 파일 덤프 도구 : Dumplt 검
색 도구 : Everything
해시 확인 도구 : EasyHash
패스워드 크랙 도구 : mimikatz
그 외 활용 도구 : john the ripper, volatility