

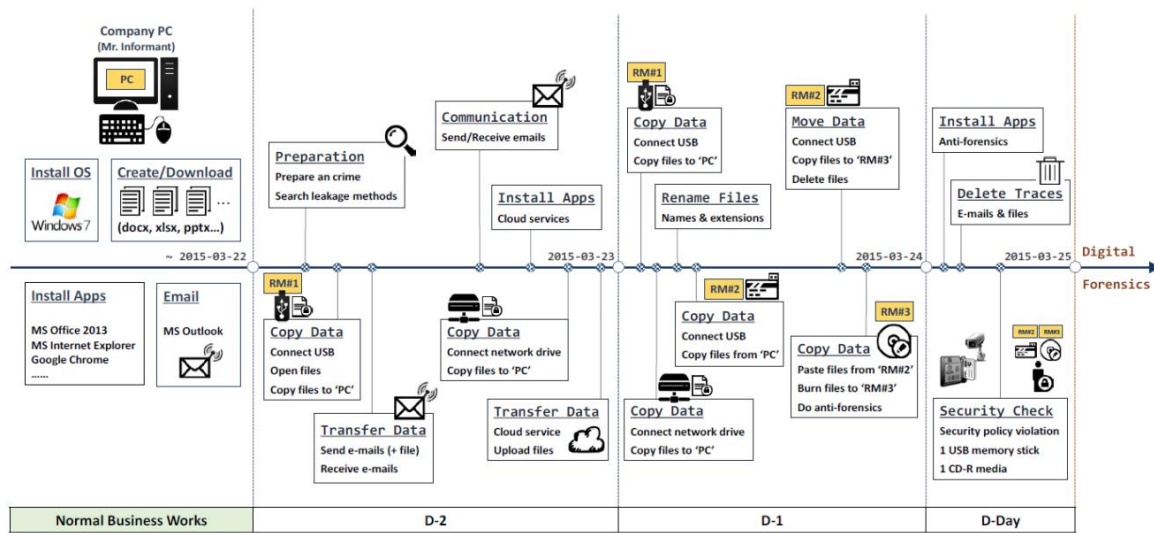
디지털 포렌식(01)

Assignment 3 Analyze Evidence from Storage

2171056 강승연

다음은 Data Leakage Case 과정이다.

Graphical Timeline of the Data Leakage Scenario



해당 보고서에서는 어째서 해당 이벤트가 결과로 도출되었는지 .dd 파일의 분석을 통해 근거를 찾아내는 것을 목적으로 한다.

분석 환경: Windows 11, Autopsy 4.21.0

Case Details

Case

Case Name: Assignment3

Case Number: Data Leakage

Created Date: 2024/06/16 12:24:23 (KST)

Case Directory: D:\Workplace\Study\2024-1\DigitalForensics\Assignment\HW3\Assignment3

Case Type: Single-user case

Database Name: D:\Workplace\Study\2024-1\DigitalForensics\Assignment\HW3\Assignment3\autopsy.db

Case UUID: assignment3 20240616 122423

Examiner

Name: SeungYeon Kang

Phone: 010-5595-9522

Email: syeon.dev@gmail.com

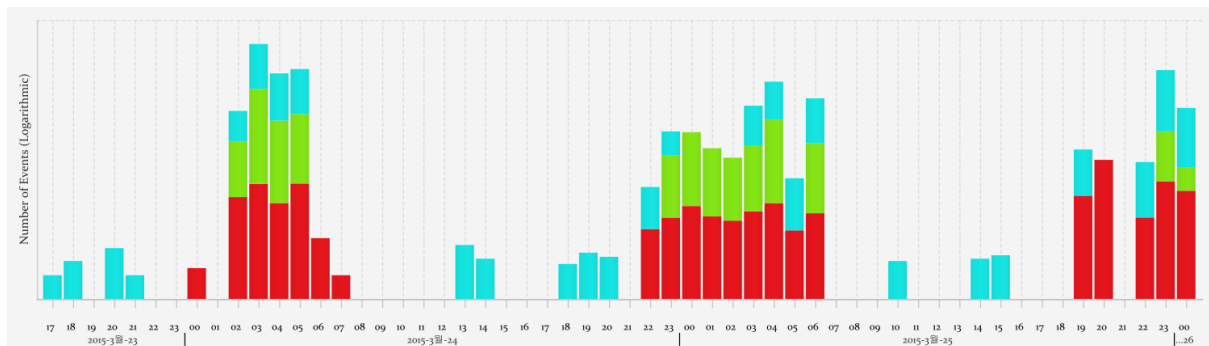
Notes:

[Copy Data]

데이터를 복사하기 위해서 USB를 사용했을 가능성이 높다.

그래서 USB Device Attached 를 확인해보니, 24일에 아래 USB 접근이 확인되었다.

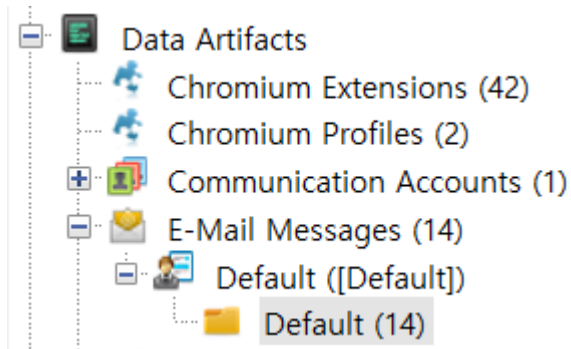
Source Name	S	C	O	△ Date/Time	Device Make	Device Model	Device ID
SYSTEM			2	2015-03-24 22:38:00 KST	SanDisk Corp.	Cruzer Fit	4C530012450531101593
SYSTEM			2	2015-03-24 22:38:00 KST	SanDisk Corp.	Cruzer Fit	4C530012450531101593
SYSTEM			2	2015-03-25 04:38:09 KST	SanDisk Corp.	Cruzer Fit	4C530012550531106501
SYSTEM			2	2015-03-25 04:38:09 KST	SanDisk Corp.	Cruzer Fit	4C530012550531106501



USB가 접속된 시간 후인 24일 10시 이후로 파일의 modified 가 급격히 증가함을 확인했다.

[Transfer Data]

전송된 데이터를 확인하기 위해 이메일을 확인했다.



그 결과 의심스러운 내용의 이메일과 전송된 데이터를 확인할 수 있었다.

From: iaman
Sent: Monday, March 23, 2015 4:39 PM
To: spy
Subject: It's me



Use links below,

<https://drive.google.com/file/d/0Bz0ye6gXtiZaVl8yVU5mWHlGbWc/view?usp=sharing>

<https://drive.google.com/file/d/0Bz0ye6gXtiZaakx6d3R3c0JmM1U/view?usp=sharing>

이를 미루어 보아 공격자는 해당 드라이브를 통해 데이터를 전송한 것으로 추정된다.

그래서 드라이브가 설치된 흔적이 있는지 확인해보았다.

 SOFTWARE		0	Google Drive v.1.20.8672.3137
 SOFTWARE		1	Google Drive v.1.20.8672.3137

Type	Value
Program Name	Google Drive v.1.20.8672.3137
Date/Time	2015-03-23 20:02:46 KST
Source File Path	/img_cfreds_2015_data_leakage_pc.dd/vol_vol3/Windows/System32/config/SOFTWARE
Artifact ID	-9223372036854775491

드라이브 다운을 위해 검색한 기록도 남아있다.

Web Search	
Term:	google drive
Time:	2015-03-24 04:56:04 KST
Domain:	google.com
Program Name:	Google Chrome

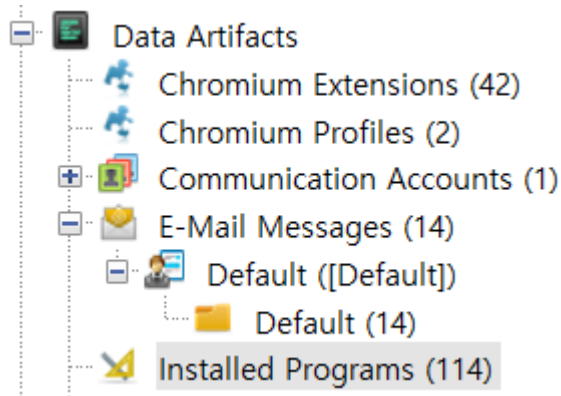
그리고 계속해서 의심스러운 기록들에 남아있는 유저인 informant의 AppData를 확인해보니, Google/Drive 폴더 안에 log 기록이 남아있었다.

```
2015-03-23 16:02:51,486 -0400 INFO pid=2576 1224:MainThread common.service.service:209 Creating paramed singleton service instance of '<class 'common.file_lock.FileLock'>'  
2015-03-23 16:02:51,563 -0400 INFO pid=2576 1224:MainThread resources.images.image_resources:246 Loading image resources#images#menu_warning.png  
2015-03-23 16:02:51,611 -0400 INFO pid=2576 1224:MainThread resources.images.image_resources:246 Loading image resources#images#ic_drawer_24.png  
2015-03-23 16:02:51,611 -0400 INFO pid=2576 1224:MainThread resources.images.image_resources:246 Loading image resources#images#menu_drive-logo.png  
2015-03-23 16:02:51,625 -0400 INFO pid=2576 1224:MainThread resources.images.image_resources:246 Loading image resources#images#menu_google-logo-gray.png  
2015-03-23 16:02:51,641 -0400 INFO pid=2576 1224:MainThread resources.images.image_resources:246 Loading image resources#images#ic_folder_mydrive_24.png  
2015-03-23 16:02:51,641 -0400 INFO pid=2576 1224:MainThread resources.images.image_resources:246 Loading image resources#images#ic_web_24.png  
2015-03-23 16:02:51,657 -0400 INFO pid=2576 1224:MainThread resources.images.image_resources:246 Loading image resources#images#menu_backups.png  
2015-03-23 16:02:51,657 -0400 INFO pid=2576 1224:MainThread resources.images.image_resources:246 Loading image resources#images#ic_sync_problem_24.png  
2015-03-23 16:02:51,673 -0400 INFO pid=2576 1224:MainThread resources.images.image_resources:246 Loading image resources#images#ic_done_24.png  
2015-03-23 16:02:51,750 -0400 INFO pid=2576 1224:MainThread resources.images.image_resources:246 Loading image resources#images#win7-inactive.png
```

Log 기록을 통해 파일이 이동했음을 알 수 있었다.

[Delete Trace] & [Install Apps]

제일 먼저 [Install Apps]를 분석하기 위해 Data Artifacts의 Installed Programs를 확인했다.

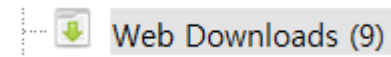


Date/Time을 기준으로 정렬하여 사건 발생 당일부터 포렌식 직전까지 설치된 파일을 확인했다.

그 결과 하드 드라이브에서 데이터를 완전히 삭제해 디지털 포렌식을 방해하는 프로그램인 Eraser가 발견되었다.

Type	Value	Source(s)
Program N	Eraser 6.2.0.2962 v.6.2.2962	Recent Act
Date/Time	2015-03-25 14:57:31 KST	Recent Act
Source File	/img_cfreds_2015_data_leakage_pc.dd/vol_vol3/Windows/System32/config/SOFTWARE	
Artifact ID	-9223372036854775534	

해당 데이터에 대한 근거는 Web Downloads 에서도 확인할 수 있었다.



Downloaded File

Domain:

URL:

Path: /Users/informant/Desktop/Download/Eraser 6.2.0.2962.exe

Program Name:

그리고 해당 프로그램이 실행된 것 또한 확인했다.

ERASER 6.2.0.2962.EXE-BE552234.pf		ERASER 6.2.0.2962.EXE		/USERS/INFORMANT/DESKTOP/DOWNLOAD		2015-03-25 23:50:14 KST		1		Prefetch Fi	
<div>HexTextApplicationSource File MetadataOS AccountData ArtifactsAnalysis ResultsContextAnnotationsOther Occurrences</div>											
Result: 1 of 1Result										Run Programs	
Type	Value								Source(s)		
Program Name	ERASER 6.2.0.2962.EXE								Windows Prefetch Analyzer		
Path	/USERS/INFORMANT/DESKTOP/DOWNLOAD								Windows Prefetch Analyzer		
Date/Time	2015-03-25 23:50:14 KST								Windows Prefetch Analyzer		
Count	1								Windows Prefetch Analyzer		
Comment	Prefetch File								Windows Prefetch Analyzer		
Source File Path	/img_cfreds_2015_data_leakage_pc.dd/vol_vol3/Windows/Prefetch/ERASER 6.2.0.2962.EXE-BE552234.pf										
Artifact ID	-9223372036854769219										

해당 프로그램이 어떤 데이터를 삭제했는지 확인하기 위해 Deleted files로 들어가 File System을 확인했다.



~\$rmalEmail.dotm



~iaman.informant@nist.gov.ost.tmp

Metadata

Name: /img_cfreds_2015_data_leakage_pc.dd/vol_vol3/Users/informant/AppData/Local/Microsoft/Outlook/~iaman.informant@nist.gov.ost.tmp
 Type: File System
 MIME Type: application/octet-stream
 Size: 131072
 File Name Allocation: Unallocated
 Metadata Allocation: Unallocated
 Modified: 2015-03-25 23:41:04 KST
 Accessed: 2015-03-25 23:41:04 KST
 Created: 2015-03-25 23:41:04 KST
 Changed: 2015-03-25 23:41:04 KST
 MD5: 5c9c687d4edd745de9e37aac48124a45
 SHA-256: 0f98c7254a5eabd22bd3fb2db1c51ce7e656cc01cf8cf42d25d9d9e14f6cd0c7
 Hash Lookup Results: UNKNOWN
 Internal ID: 7234

Metadata
















Name: /img_cfreds_2015_data_leakage_pc.dd/vol_vol3/Users/informant/AppData/Roaming/Microsoft/Templates/~\$rmalEmail.dotm
 Type: File System
 MIME Type: application/x-ms-owner
 Size: 162
 File Name Allocation: Unallocated
 Metadata Allocation: Unallocated
 Modified: 2015-03-25 23:41:10 KST
 Accessed: 2015-03-25 23:41:10 KST
 Created: 2015-03-25 23:41:10 KST
 Changed: 2015-03-25 23:41:10 KST
 MD5: 7e32b68efc53c0927d71742bae7d8f01
 SHA-256: 71ecbe26c71914a9e488869b43a5eb2da3bf6232234abde19f47be50a08058fe
 Hash Lookup Results: UNKNOWN
 Internal ID: 13461

그 결과 이메일 데이터가 삭제된 것을 확인할 수 있었다.

그리고 Eraser 또한 삭제되었음을 확인했다.




Result: 1 of 2 Result < >		Associated Object
Type	Value	Source(s)
Associated Artifact	-9223372036854769269	Recent Activity
Source File Path	/img_cfreds_2015_data_leakage_pc.dd/vol_vol3/Users/informant/Desktop/Download/Eraser 6.2.0.2962.exe	
Artifact ID	-9223372036854769268	

아래는 Eraser 설치 이후 삭제된 파일의 내역으로 아래 파일들 또한 공격자가 의도하여 삭제한 데이터로 추측해볼 수 있다.













 Eraser 6.2.0.2962.exe				2015-03-25 23:47:40 KST	2015-03-25 23:47:40 KST
 Eraser 6.2.0.2962.exe:Zone.Identifier				2015-03-25 23:47:40 KST	2015-03-25 23:47:40 KST
 ~DFC63A36FEE260F768.TMP				2015-03-25 23:46:06 KST	2015-03-25 23:46:06 KST
 jsonstrings[1].js				2015-03-25 23:41:13 KST	2015-03-25 23:41:13 KST
 ~\$malEmail.dotm				2015-03-25 23:41:10 KST	2015-03-25 23:41:10 KST
 ~iaman.informant@nist.gov.ost.tmp				2015-03-25 23:41:04 KST	2015-03-25 23:41:04 KST
 WebCacheV01.tmp				2015-03-25 23:41:04 KST	2015-03-25 23:41:04 KST
 IMpService925A3ACA-C353-458A-AC8D-A7E5EB3				2015-03-25 22:07:52 KST	2015-03-25 22:07:52 KST
 EtwRTMsMpPsSession7.etl				2015-03-25 22:07:52 KST	2015-03-25 22:07:52 KST
 tmp.edb				2015-03-25 22:06:17 KST	2015-03-25 22:06:17 KST
 usgthrsvc				2015-03-25 22:06:16 KST	2015-03-25 22:06:16 KST
 [current folder]				2015-03-25 22:06:16 KST	2015-03-25 22:06:16 KST
 EtwRTUBPM.etl				2015-03-25 22:05:48 KST	2015-03-25 22:05:48 KST
 EtwRTEventlog-Security.etl				2015-03-25 22:05:43 KST	2015-03-25 22:05:43 KST
 \$RIQGWTT.ini				2015-03-25 04:57:20 KST	2015-03-25 05:11:42 KST

[검색 기록]

추가로 의심스러운 검색 기록을 첨부한다.

 History			google.com	data leakage methods	Google Chrome	2015-03-24 03:02:09 KST
 History			google.com	leaking confidential information	Google Chrome	2015-03-24 03:02:44 KST
 History			google.com	information leakage cases	Google Chrome	2015-03-24 03:03:40 KST

아래 검색 기록들을 보아 고의적으로 디지털 포렌식을 방해하려고 했음을 알 수 있다.

 WebCacheV01.dat			bing.com	e-mail investigation	Microsoft Edge Analyzer	0000-00-00 00:00:00
 WebCacheV01.dat			bing.com	e-mail investigation	Microsoft Edge Analyzer	0000-00-00 00:00:00
 WebCacheV01.dat			bing.com	Forensic Email Investigation	Microsoft Edge Analyzer	0000-00-00 00:00:00
 WebCacheV01.dat			bing.com	what is windows system artifacts	Microsoft Edge Analyzer	0000-00-00 00:00:00
 WebCacheV01.dat			bing.com	investigation on windows machine	Microsoft Edge Analyzer	0000-00-00 00:00:00
 WebCacheV01.dat			bing.com	windows event logs	Microsoft Edge Analyzer	0000-00-00 00:00:00
 WebCacheV01.dat			bing.com	cd burning method	Microsoft Edge Analyzer	0000-00-00 00:00:00
 WebCacheV01.dat			bing.com	cd burning method in windows	Microsoft Edge Analyzer	0000-00-00 00:00:00
 WebCacheV01.dat			bing.com	external device and forensics	Microsoft Edge Analyzer	0000-00-00 00:00:00
 WebCacheV01.dat			bing.com	external device and forensics	Microsoft Edge Analyzer	0000-00-00 00:00:00
 WebCacheV01.dat			bing.com	anti-forensic tools	Microsoft Edge Analyzer	0000-00-00 00:00:00
 WebCacheV01.dat			bing.com	eraser	Microsoft Edge Analyzer	0000-00-00 00:00:00