

303 – Audit My Corporation

Team Information

Team Name: kimbabasaksaksak

Team Member: Jaeheon Kim, Donghyun Kim, Soyoung Yoo, Minhee Lee

Email Address : uaaoong@gmail.com

Instructions

Description We have discovered that the report of a highly confidential forensic analysis project has been leaked to a competing company. To identify the suspect among the employees involved in the project, we have obtained audit logs and Google Drive files from the Google Workspace, which is our internal groupware system. Please analyze these logs and files to determine the leaked documents, identify the suspect, and investigate the circumstances surrounding the leak.

Target	Hash (MD5)
dfc_corp_audit.ad1	58190A85B3ACDA88F46C5650B312DEDF

Questions

- 1) Who is the person responsible for leaking the highly confidential report? (50 points)
- 2) Describe in a timeline the entirety of the suspect's actions and describe the leak process. (100 points)
- 3) Find the original leaked confidential report. (MD5 Hash) (150 points)

Teams must:

- Develop and document the step-by-step approach used to solve this problem to allow another examiner to replicate team actions and results.
- Specify all tools used in deriving the conclusion(s).

Tools used:

Name:	X-Ways Forensics	Publisher:	X-Ways Software
Version:	20.7		
URL:	https://www.x-ways.net/forensics		

Name:	010 Editor	Publisher:	SweetScape
Version:	13.0.2		
URL:	https://www.sweetscape.com/010editor		

Name:	IDA	Publisher:	Hex-rays
Version:	6.8.150423		
URL:	https://hex-rays.com		

Step-by-step methodology:

Q1. Who is the person responsible for leaking the highly confidential report?
(50 points)

- **Name: delta dfc, Email: delta.dfc@nomean.org**

제공된 ad1 이미지 파일에 주요 로그가 저장되어 있는 폴더로는 takeout 폴더가 존재한다. takeout 폴더에는 포렌식 분석 프로젝트 참석 인원의 Gmail, Google Calendar, Google Chat, Google Drive 등의 데이터가 저장되어 있다. Google Takeout은 Google 계정과 관련된 데이터를 다운로드하고 보관할 수 있도록 제공되는 서비스이다.

#Native_Export#takeout		9 hours ago
Name	Path	Full path
Native_Export (166,593)	#	#Native_Export
takeout (224)	#Native_Export	#Native_Export#takeout
takeout-20230530T060930Z-001 (197)	#Native_Export#takeout	#Native_Export#takeout#takeout-20230530T060930Z-001
takeout-20230530T061028Z-001 (5)	#Native_Export#takeout	#Native_Export#takeout#takeout-20230530T061028Z-001
takeout-20230530T062010Z-001 (5)	#Native_Export#takeout	#Native_Export#takeout#takeout-20230530T062010Z-001
takeout-20230530T062102Z-001 (10)	#Native_Export#takeout	#Native_Export#takeout#takeout-20230530T062102Z-001
takeout-20230530T062325Z-001 (6)	#Native_Export#takeout	#Native_Export#takeout#takeout-20230530T062325Z-001
\$I30	#Native_Export#takeout	#Native_Export#takeout#\$I30

또한, vault 폴더에도 주요 로그가 저장되어 있다. vault 폴더에는 포렌식 분석 프로젝트 참석 인원의 Gmail, Google Chat, Google Drive 등의 데이터가 저장되어 있다. Google Vault는 기업이나 조직이 전자적 데이터 보존 및 검색 등을 수행할 수 있도록 지원하는 Google의 클라우드 기반 서비스이다.

#Native_Export#vault		
Name	Path	Full path
Native_Export (166,640)	#	#Native_Export
vault (80,485)	#Native_Export	#Native_Export#vault
vault_google_chat-1 (1)	#Native_Export#va...	#Native_Export#vault#vault_google_chat-1
vault_google_chat-2 (1)	#Native_Export#va...	#Native_Export#vault#vault_google_chat-2
vault_google_drive_0 (20)	#Native_Export#va...	#Native_Export#vault#vault_google_drive_0
vault_google_drive_shared_all_0 (65,536)	#Native_Export#va...	#Native_Export#vault#vault_google_drive_shared_all_0
vault_google_drive_shared_all_1 (14,911)	#Native_Export#va...	#Native_Export#vault#vault_google_drive_shared_all_1
vault_google_mail-1 (10)	#Native_Export#va...	#Native_Export#vault#vault_google_mail-1
work_chat_room-1 (1)	#Native_Export#va...	#Native_Export#vault#work_chat_room-1
\$I30	#Native_Export#va...	#Native_Export#vault#\$I30
vault_google_drive-custodian-docid.csv	#Native_Export#va...	#Native_Export#vault#vault_google_drive-custodian-docid.csv
vault_google_drive_shared_all-custodian-docid.csv	#Native_Export#va...	#Native_Export#vault#vault_google_drive_shared_all-custodian-docid.csv
vault_google_mail-metadata.csv	#Native_Export#va...	#Native_Export#vault#vault_google_mail-metadata.csv
vault_google_mail-result-counts.csv	#Native_Export#va...	#Native_Export#vault#vault_google_mail-result-counts.csv

그리고 주요 로그 파일인 Google Workspace 감사 로그(google_workspace_audit_report.json)도 존재한다.

Name	Path	Full path
Native_Export (166.640)	#	#Native_Export
google_workspace_audit_report.json	#	#google_workspace_audit_report.json

Google Workspace 감사 로그 파일과 vault 폴더에 존재하는 메일 로그를 확인하면 프로젝트 팀은 'admin jin'(관리자), 'alice dfc', 'bravo dfc', 'Charlie dfc', 'delta dfc', 'echo dfc'으로 6명인 것을 알 수 있다.

[Notice] Regret Regarding Information Leak and Internal Audit
Admin Jin <admin@nomean.org> <admin@nomean.org>
Sent time: 05/30/2023 02:21:21 PM
Received time: 05/30/2023 02:21:30 PM
To: [alice dfc <alice.dfc@nomean.org>](#); [bravo dfc <bravo.dfc@nomean.org>](#); [charlie dfc <charlie.dfc@nomean.org>](#); [delta dfc <delta.dfc@nomean.org>](#); [echo dfc <echo.dfc@nomean.org>](#)

Dear Team,

I hope this email finds you well. I am writing to address a recent and unfortunate incident that has come to my attention. It has been brought to my notice that our forensic report has been leaked, compromising the confidentiality and integrity of our work. I deeply regret this unfortunate event, and I understand the concerns and implications it raises for each of us.

I want to assure you that we are taking this matter extremely seriously. The leaked report contains sensitive information, and we recognize the importance of identifying the root cause and preventing such incidents from happening in the future. In light of this, we will be conducting an immediate and comprehensive internal audit to assess our security protocols, systems, and potential vulnerabilities.

The purpose of this audit is to determine the source of the leak, evaluate our existing safeguards, and implement any necessary enhancements to ensure the utmost security and confidentiality of our work. I encourage each team member to cooperate fully and provide any information or insights that may assist in the investigation.

I understand that this incident may have caused distress and uncertainty among all of us. Rest assured, we are committed to transparency throughout this process. Regular updates will be provided to keep you informed about the progress of the audit, and any additional measures that need to be taken to safeguard our work.

I want to emphasize the importance of teamwork, support, and maintaining a positive mindset during this challenging time. We have a strong and resilient team, and together we will overcome this setback. Our dedication to upholding the highest standards in our forensic practice remains unwavering.

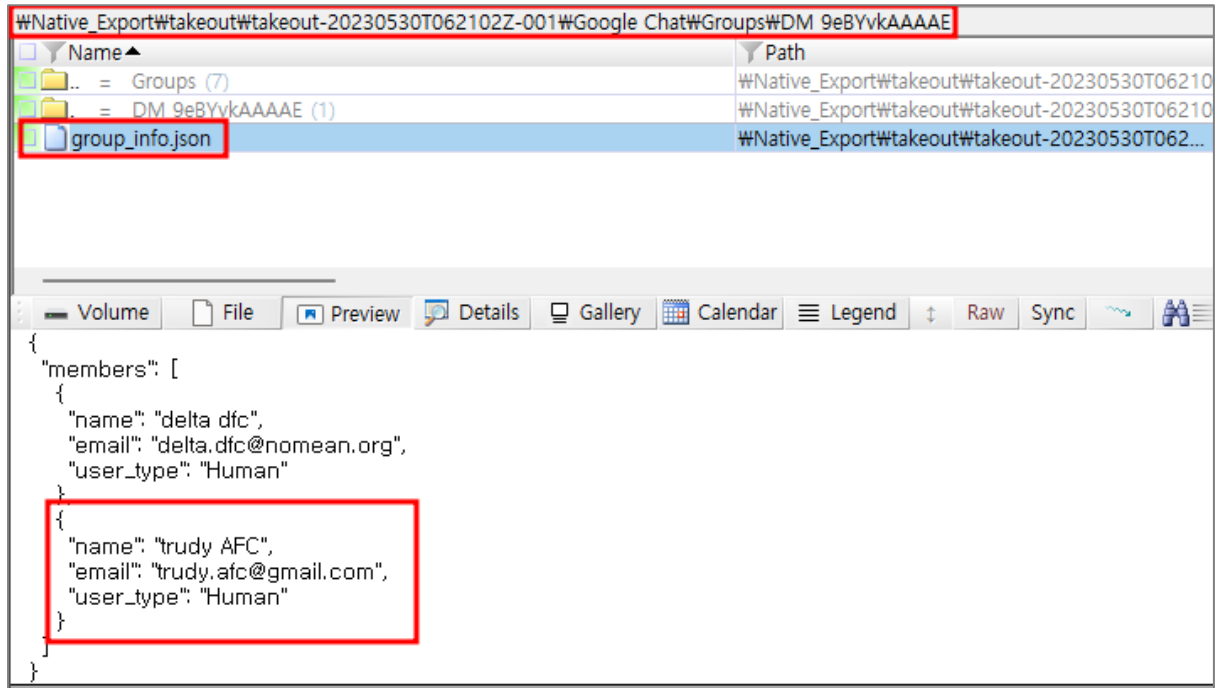
If any team member has concerns, questions, or suggestions regarding the ongoing audit or any other related matter, please do not hesitate to reach out to me directly. Your input and involvement are vital as we navigate through this situation.

Thank you for your understanding, professionalism, and commitment to the integrity of our work. Let us remain united as we carry out the necessary steps to rectify the situation and reinforce the trust placed in us.

Best regards,

Mail 로그: WNative_ExportWvaultWvault_google_mail-1Wvault_google_mail--delta.dfc@nomean.org-flw0Bc.pst

takeout 폴더에는 프로젝트 인원별로 채팅 로그가 저장되어 있다. 유저 정보가 저장되어 있는 user_info.json 파일과 채팅 그룹 정보가 저장되어 있는 group_info.json 파일을 확인한 결과, delta dfc 만 유일하게 프로젝트 참여 인원이 아닌 사람(trudy AFC)과 1:1 채팅을 진행한 사실이 확인되었다.



또한, delta dfc와 trudy AFC가 주고받은 내용을 확인하기 위하여 주요 로그 파일 3개를 확인하면, delta dfc가 trudy AFC에게 암호화된 포렌식 프로젝트 극비 문서 파일과 해당 문서 파일을 복호화할 수 있는 실행 파일을 유출한 것을 알 수 있다. (* 상세 내용은 Q2 참고)

- 주요 로그 파일:

- Google Workspace 감사 로그: #google_workspace_audit_report.json
- Chat 로그: #Native_Export#vault#vault_google_chat-1#vault_google_chat_0.pst.zip#vault_google_chat_0.pst
- Mail 로그: #Native_Export#vault#vault_google_mail-1#vault_google_mail--delta.dfc@nomean.org-flw0Bc.pst

Q2. Describe in a timeline the entirety of the suspect's actions and describe the leak process. (100 points)

- 용의자 행동 타임라인

@ 이벤트 시각: 2023-05-26 14:52:01 (UTC+0)

- 아티팩트: vault_google_chat_0.pst
- 이벤트 내용: delta.dfc@nomean.org가 trudy.afc@gmail.com에게 chat 메시지 전달 (* 두 사람은 2023-05-26일에 16:10:45 시각까지 1:1 채팅 진행)
 - * chat room id: 9eBYvkAAAAE
 - * chat type: direct message
 - * 채팅 내용(한글 번역) :

- delta.dfc@nomean.org 2023년 5월 26일 14:52:01 UTC+0
안녕, 트루디 거기 있니?

- trudy.afc@gmail.com 2023년 5월 26일 14:53:57 UTC+0
네, 여기 있어요. 우리 도시에 도착했니??

- delta.dfc@nomean.org 2023년 5월 26일 14:54:35 UTC+0
물론 준비 되셨나요?

- trudy.afc@gmail.com 2023년 5월 26일 14:55:39 UTC+0
응. 은밀하게 진행하는 것을 잊지 마십시오. 당신과 함께 오는 사람은 눈치 채지 못합니다.

- delta.dfc@nomean.org 2023년 5월 26일 14:55:55 UTC+0
곧 보자.

- trudy.afc@gmail.com 2023년 5월 26일 14:56:07 UTC+0
좋아요. 행운을 빌어요

- delta.dfc@nomean.org 2023년 5월 26일 15:18:00 UTC+0
초대장 잘 받으셨나요?

- trudy.afc@gmail.com 2023년 5월 26일 15:18:28 UTC+0
물론 나는 이미 회의에 참여하고 있습니다.

- delta.dfc@nomean.org 2023년 5월 26일 16:07:16 UTC+0
Invoice_1284672213.pdf (파일 첨부)

- delta.dfc@nomean.org 2023년 5월 26일 16:07:57 UTC+0
vimrc (파일 첨부)

- delta.dfc@nomean.org 2023년 5월 26일 16:08:26 UTC+0

fakeSMTP-latest.zip (파일 첨부)

- delta.dfc@nomean.org 2023년 5월 26일 16:10:45 UTC+0

샘플 보고서는 다음과 같습니다.

CyberSleuth_Report_Sample.pdf (파일 첨부)

@ 이벤트 시각: 2023-05-26 14:52:13 (UTC+0)

- 아티팩트: google_workspace_audit_report.json
- 이벤트 내용: delta.dfc@nomean.org의 9eBYvkAAAAE chat room에 trudy.afc@gmail.com가 추가됨 (trudy.afc@gmail.com가 1:1 채팅방에 입장)
- * chat room id: 9eBYvkAAAAE
- * chat type: direct message

```
"kind": "admin#reports#activity",|
"id": {
  "time": "2023-05-26T14:52:13.519Z",
  "uniqueQualifier": "7761636385924348146",
  "applicationName": "chat",
  "customerId": "C038fhwe2"
},
"etag": "\"82YgmLpRVC5iA-bU28dUqy2uCKS7KM1DQDk3vW-TM2Y/5vepAbXqebo009x8v51FNRpG3Ao\"",
"actor": {
  "callerType": "USER",
  "email": "delta.dfc@nomean.org",
  "profileId": "115830431782957231483"
},
"events": [
  {
    "type": "user_action",
    "name": "add_room_member",
    "parameters": [
      {
        "name": "target_users",
        "multiValue": [
          "trudy.afc@gmail.com"
        ]
      },
      {
        "name": "room_id",
        "value": "9eBYvkAAAAE"
      },
      {
        "name": "timestamp_ms",
        "value": "1685112733519668"
      },
      {
        "name": "actor",
        "value": "delta.dfc@nomean.org"
      }
    ]
  }
]
```


@ 이벤트 시각: 2023-05-26 14:57:48 (UTC+0)

- 아티팩트: vault_google_mail--delta.dfc@nomean.org-flw0Bc.pst
 - 이벤트 내용: delta.dfc@nomean.org가 admin@nomean.org, bravo.dfc@nomean.org, echo.dfc@nomean.org, trudy.afc@gmail.com에게 'collaboration meeting with APC.' Google Meet 초대
- * 회의 예정 시간:
- 시작시간: 2023-05-26 15:00:00 (UTC+0)
 - 종료시간: 2023-05-26 17:00:00 (UTC+0)

```


1 BEGIN:VCALENDAR
2 PRODID:-//Google Inc//Google Calendar 70.9054//EN
3 VERSION:2.0
4 CALSCALE:GREGORIAN
5 METHOD:REPLY
6 BEGIN:VEVENT
7 DTSTART:20230526T150000Z
8 DTEND:20230526T170000Z
9 DTSTAMP:20230526T151718Z
10 ORGANIZER;CN=delta.dfc@nomean.org:mailto:delta.dfc@nomean.org
11 UID:1ffgmr7u6bdij4len8i0ec0fgp@google.com
12 ATTENDEE;CUTYPE=INDIVIDUAL;ROLE=REQ-PARTICIPANT;PARTSTAT=ACCEPTED;CN=trudy.
13   afc@gmail.com;X-NUM-GUESTS=0:mailto:trudy.afc@gmail.com
14 X-GOOGLE-CONFERENCE:https://meet.google.com/vdd-vzue-vfi
15 CREATED:20230526T145748Z
16 DESCRIPTION:-~~~~~\nJoin with Google Meet: https://meet.google.com/vd
17   d-vzue-vfi\nOr dial: (US) +1 724-491-2016 PIN: 669221341#\nMore phone numbe
18   rs: https://tel.meet/vdd-vzue-vfi?pin=9283529487321&hs=7\n\nLearn more abou
19   t Meet at: https://support.google.com/a/users/answer/9282720\n\nPlease do n
20   ot edit this section.\n~~~~~
21   ~~~~~
22 LAST-MODIFIED:20230526T151718Z
23 LOCATION:
24 SEQUENCE:0
25 STATUS:CONFIRMED
26 SUMMARY:collaboration meeting with APC.
27 TRANSP:OPAQUE
28 END:VEVENT
29 END:VCALENDAR

```

@ 이벤트 시각: 2023-05-26 15:17:18 (UTC+0)

- 아티팩트: vault_google_mail--delta.dfc@nomean.org-flw0Bc.pst
- 이벤트 내용: trudy.afc@gmail.com가 'collaboration meeting with APC.' Google Meet 초대 수락
- * 회의 참여자: trudy.afc@gmail.com 뿐만 아니라, admin@nomean.org, bravo.dfc@nomean.org, echo.dfc@nomean.org도 초대에 수락하여 회의 진행

Accepted: collaboration meeting with APC. @ Sat 27 May 2023 12am - 2am (KST) (delta.dfc@nomean.org)
delta.dfc@nomean.org
Sent time:
Received time:
To:
Attachments:

05/27/2023 12:17:18 AM
05/27/2023 12:17:19 AM
delta.dfc@nomean.org
 [invite.ics](#)

UTC+9가 적용된 시각

trudy AFC has accepted this invitation. [Learn more](#) <>

@ 이벤트 시각: 2023-05-26 16:04:15 (UTC+0)

- 아티팩트: google_workspace_audit_report.json
- 이벤트 내용: delta.dfc@nomean.org가 Google Meet으로 presentation 시작

```
"kind": "admin#reports#activity",
"id": {
  "time": "2023-05-26T16:04:15.327Z",
  "uniqueQualifier": "1545701139495466283",
  "applicationName": "meet",
  "customerId": "C038fhwe2"
},
"etag": "\"82YgmLpRVC5iA-bU28dUqy2uCKS7KM1DQDk3vW-TM2Y/h0somjEkr_zz6WCSCNdudzIy0P68\"",
"actor": {
  "callerType": "USER",
  "email": "delta.dfc@nomean.org",
  "profileId": "115830431782957231483"
},
"events": [
  {
    "type": "conference_action",
    "name": "presentation_started",
    "parameters": [
      {
        "name": "is_external",
        "boolValue": false
      },
      {
        "name": "meeting_code",
        "value": "VDDVZUEVFI"
      },
      {
        "name": "conference_id",
        "value": "e_QW58tTmrNDIrxAYSYeDxIROAkBMgIoABgJCIOcIAQI"
      },
      {
        "name": "action_time",
        "value": "2023-05-26T16:04:15.327662Z"
      },
      {
        "name": "identifier",
        "value": "delta.dfc@nomean.org"
      },
      {
        "name": "identifier_type",
        "value": "email_address"
      }
    ]
  }
]
```

@ 이벤트 시각: 2023-05-26 16:04:48 (UTC+0)

- 아티팩트: google_workspace_audit_report.json
- 이벤트 내용: delta.dfc@nomean.org가 Google Meet으로 진행하던 presentation 종료

```
{
  "kind": "admin#reports#activity",
  "id": {
    "time": "2023-05-26T16:04:48.378Z",
    "uniqueQualifier": "-4883775868486114604",
    "applicationName": "meet",
    "customerId": "C038fhwe2"
  },
  "etag": "\"82YgmLpRVC5iA-bU28dUqy2uCKS7KM1DQDk3vW-TM2Y/Q_7FUz6FBN53IeGcr5vU26WzMDc\"",
  "actor": {
    "callerType": "USER",
    "email": "delta.dfc@nomean.org",
    "profileId": "115830431782957231483"
  },
  "events": [
    {
      "type": "conference_action",
      "name": "presentation_stopped",
      "parameters": [
        {
          "name": "is_external",
          "boolValue": false
        },
        {
          "name": "meeting_code",
          "value": "VDDVZUEVFI"
        },
        {
          "name": "conference_id",
          "value": "e_QW58tTmrNDIrxAYSYeDxIROAkBMgIoABgJCioCIAQI"
        },
        {
          "name": "action_time",
          "value": "2023-05-26T16:04:48.378487Z"
        },
        {
          "name": "identifier",
          "value": "delta.dfc@nomean.org"
        },
        {
          "name": "identifier_type",
          "value": "email_address"
        }
      ]
    }
  ]
}
```

@ 이벤트 시각: 2023-05-26 16:16:52 (UTC+0)

- 아티팩트: google_workspace_audit_report.json

- 이벤트 내용: delta.dfc@nomean.org가 'collaboration meeting with APC.' Google Meet 회의 종료 (3277초간 진행)

* 회의 참여자: delta.dfc@nomean.org, admin@nomean.org, bravo.dfc@nomean.org, echo.dfc@nomean.org, trudy.afc@gmail.com

* 추가 정보: trudy.afc@gmail.com는 2023-05-26 16:09:03 (UTC+0)에 회의 종료 (3097초간 진행)

```
{
  "kind": "admin#reports#activity",
  "id": {
    "time": "2023-05-26T16:16:52.652Z",
    "uniqueQualifier": "-6250333425119936041",
    "applicationName": "meet",
    "customerId": "C038fhwe2"
  },
  "etag": "\"82YgmLpRVC5iA-bU28dUqy2uCKS7KMLDQDk3vW-TM2Y/NbHvPy52tqvnD0IeQc7EB54EaYw\"",
  "actor": {
    "callerType": "USER",
    "email": "delta.dfc@nomean.org",
    "profileId": "115830431782957231483"
  },
  "events": [
    {
      "type": "call",
      "name": "call_ended",
      "parameters": [
        {
          "name": "video_send_seconds",
          "intValue": "3270"
        },
        {
          "name": "location_country",
          "value": "KR"
        },
        {
          "name": "identifier_type",
          "value": "email_address"
        },
        {
          "name": "audio_send_bitrate_kbps_mean",
          "intValue": "0"
        },
        {
          "name": "video_send_packet_loss_max",
          "intValue": "0"
        },
        {
          "name": "endpoint_id",
          "value": "boq_hlane_5RKJzFwdXZ6"
        },
        {
          "name": "device_type",
          "value": "web"
        }
      ]
    }
  ]
}
```

@ 이벤트 시각: 2023-05-29 03:08:35 (UTC+0)

- 아티팩트: vault_google_mail--delta.dfc@nomean.org-flw0Bc.pst
- 이벤트 내용: delta.dfc@nomean.org가 trudy.afc@gmail.com에게 'work meeting' Google Meet 초대
- * 회의 예정 시간:
 - 시작시간: 2023-05-29 17:00:00 (UTC+0)
 - 종료시간: 2023-05-29 18:00:00 (UTC+0)
- * 회의 위치 정보: Gimpo International Airport, 112 Haneul-gil, Gangseo-gu, Seoul, South Korea

```

1 BEGIN:VCALENDAR
2 PRODID:-//Google Inc//Google Calendar 70.9054//EN
3 VERSION:2.0
4 CALSCALE:GREGORIAN
5 METHOD:REPLY
6 BEGIN:VEVENT
7 DTSTART:20230529T170000Z
8 DTEND:20230529T180000Z
9 DTSTAMP:20230529T172504Z
10 ORGANIZER;CN=delta.dfc@nomean.org:mailto:delta.dfc@nomean.org
11 UID:25dqdcat1lc72dvlpc9bi7mghk@google.com
12 ATTENDEE;CUTYPE=INDIVIDUAL;ROLE=REQ-PARTICIPANT;PARTSTAT=ACCEPTED;CN=trudy.
13   afc@gmail.com;X-NUM-GUESTS=0:mailto:trudy.afc@gmail.com
14 X-GOOGLE-CONFERENCE:https://meet.google.com/dms-hbhc-anb
15 CLASS:PRIVATE
16 CREATED:20230529T030835Z
17 DESCRIPTION:~~~~~\nJoin with Google Meet: https://meet.google.com/dm
18   s-hbhc-anb\nOr dial: (US) +1 276-335-0245 PIN: 833499106#\nMore phone numbe
19   rs: https://tel.meet/dms-hbhc-anb?pin=8475158645533&hs=7\n\nLearn more abou
20   t Meet at: https://support.google.com/a/users/answer/9282720\n\nPlease do n
21   ot edit this section.\n~~~~~
22   ~::~::~~
23   LAST-MODIFIED:20230529T172504Z
24 LOCATION:Gimpo International Airport\, 112 Haneul-gil\, Gangseo-gu\, Seoul\
25   \, South Korea
26 SEQUENCE:1
27 STATUS:CONFIRMED
28 SUMMARY:work meeting
29 TRANSP:OPAQUE
30 END:VEVENT
31 END:VCALENDAR
32

```

@ 이벤트 시각: 2023-05-29 16:10:01 (UTC+0)

- 아티팩트: google_workspace_audit_report.json
- 이벤트 내용: delta.dfc@nomean.org가 드라이브의 '[DFC]_Forensic_Report.docx' 파일 접근
- * 문서 정보:
 - 문서 이름: [DFC]_Forensic_Report.docx
 - 문서 id: 1C9sDRd2DgqC8MhOfn3v81Hh82hGk_Avq
 - 업로드한 유저: admin@nomean.org (* 업로드 시간: 2023-05-29 15:47:52 UTC+0)
 - 추가 설명: 해당 문서 파일은 admin@nomean.org가 업로드한 후, 프로젝트 참여 인원인 admin@nomean.org, alice.dfc@nomean.org, charlie.dfc@nomean.org, echo.dfc@nomean.org, bravo.dfc@nomean.org, delta.dfc@nomean.org가 지속적으로 접근 및 수정

```
{
  "kind": "admin#reports#activity",
  "id": {
    "time": "2023-05-29T16:10:01.703Z",
    "uniqueQualifier": "-41045b35466838130388",
    "applicationName": "drive",
    "customerId": "C038fhwe2"
  },
  "etag": "\"82YgmLpRVC5iA-bU28dUqy2uCKS7KM1DQDk3vW-TM2Y/6Mz1YwaoHPEcRyoCfwufxLSO-d8\"",
  "actor": {
    "email": "delta.dfc@nomean.org",
    "profileId": "115830431782957231483"
  },
  "ipAddress": "58.77.95.37",
  "events": [
    {
      "type": "access",
      "name": "view",
      "parameters": [
        {
          "name": "primary_event",
          "boolValue": true
        },
        {
          "name": "billable",
          "boolValue": true
        },
        {
          "name": "owner_is_shared_drive",
          "boolValue": true
        },
        {
          "name": "owner_team_drive_id",
          "value": "0ANP7Tzn9-C6GUk9PVA"
        },
        {
          "name": "owner",
          "value": "DFC_Shared"
        },
        {
          "name": "doc_id",
          "value": "1C9sDRd2DgqC8MhOfn3v81Hh82hGk_Avq"
        },
        {
          "name": "doc_type",
          "value": "msword"
        },
        {
          "name": "is_encrypted",
          "boolValue": false
        },
        {
          "name": "doc_title",
          "value": "[DFC]_Forensic_Report.docx"
        },
        {
          "name": "visibility",

```

@ 이벤트 시각: 2023-05-29 16:35:43 (UTC+0)

- 아티팩트: google_workspace_audit_report.json

- 이벤트 내용: delta.dfc@nomean.org가 드라이브의 '[DFC]_Forensic_Report.docx' 파일 수정

* 문서 정보:

- 문서 이름: [DFC]_Forensic_Report.docx

- 문서 id: 1C9sDRd2DgqC8MhOfn3v81Hh82hGk_Avq

- 업로드한 유저: admin@nomean.org (* 업로드 시간: 2023-05-29 15:47:52 UTC+0)

- 추가 설명: 해당 문서 파일은 admin@nomean.org가 업로드한 후, 프로젝트 참여 인원인 admin@nomean.org, alice.dfc@nomean.org, charlie.dfc@nomean.org, echo.dfc@nomean.org, bravo.dfc@nomean.org, delta.dfc@nomean.org가 지속적으로 접근 및 수정

```
{
  "kind": "admin#reports#activity",
  "id": {
    "time": "2023-05-29T16:35:43.022Z",
    "uniqueQualifier": "-9043159485135928416",
    "applicationName": "drive",
    "customerId": "C038fhwe2"
  },
  "etag": "\"82YgmLpRVC5iA-bU28dUqy2uCKS7KM1DQDk3vW-TM2Y/UwjyoRYesPxfiVa8PAPr6r9X1e0\"",
  "actor": {
    "email": "delta.dfc@nomean.org",
    "profileId": "115830431782957231483"
  },
  "ipAddress": "58.77.95.37",
  "events": [
    {
      "type": "access",
      "name": "edit",
      "parameters": [
        {
          "name": "primary_event",
          "boolValue": true
        },
        {
          "name": "billable",
          "boolValue": true
        },
        {
          "name": "owner_is_shared_drive",
          "boolValue": true
        },
        {
          "name": "owner_team_drive_id",
          "value": "0ANP7Tzn9-C6Guk9PVA"
        },
        {
          "name": "owner",
          "value": "DFC_Shared"
        },
        {
          "name": "doc_id",
          "value": "1C9sDRd2DgqC8MhOfn3v81Hh82hGk_Avq"
        },
        {
          "name": "doc_type",
          "value": "msword"
        },
        {
          "name": "is_encrypted",
          "boolValue": false
        },
        {
          "name": "doc_title",
          "value": "[DFC]_Forensic_Report.docx"
        }
      ]
    }
  ]
}
```


@ 이벤트 시각: 2023-05-29 16:51:33 (UTC+0)

- 아티팩트: google_workspace_audit_report.json
- 이벤트 내용: delta.dfc@nomean.org가 드라이브의 '[DFC]_Forensic_Report.docx' 파일 다운로드
- * 문서 정보:
 - 문서 이름: [DFC]_Forensic_Report.docx
 - 문서 id: 1C9sDRd2DgqC8MhOfn3v81Hh82hGk_Avq
 - 업로드한 유저: admin@nomean.org (* 업로드 시간: 2023-05-29 15:47:52 UTC+0)
 - 추가 설명: 해당 문서 파일은 admin@nomean.org가 업로드한 후, 프로젝트 참여 인원인 admin@nomean.org, alice.dfc@nomean.org, charlie.dfc@nomean.org, echo.dfc@nomean.org, bravo.dfc@nomean.org, delta.dfc@nomean.org가 지속적으로 접근 및 수정

```
{
  "kind": "admin#reports#activity",
  "id": {
    "time": "2023-05-29T16:51:33.039Z",
    "uniqueQualifier": "2607964422789261322",
    "applicationName": "drive",
    "customerId": "C038fhwe2"
  },
  "etag": "\"82YgmLpRVC5iA-bU28dUqy2uCKS7KM1DQDk3vW-TM2Y/dAwWb_03tdZ1AWLre_h-eFvgFns\"",
  "actor": {
    "email": "delta.dfc@nomean.org",
    "profileId": "115830431782957231483"
  },
  "ipAddress": "58.77.95.37",
  "events": [
    {
      "type": "access",
      "name": "download",
      "parameters": [
        {
          "name": "primary_event",
          "boolValue": true
        },
        {
          "name": "billable",
          "boolValue": true
        },
        {
          "name": "owner_is_shared_drive",
          "boolValue": true
        },
        {
          "name": "owner_team_drive_id",
          "value": "0ANP7Tzn9-C6GUK9PVA"
        },
        {
          "name": "owner",
          "value": "DFC_Shared"
        },
        {
          "name": "doc_id",
          "value": "1C9sDRd2DgqC8MhOfn3v81Hh82hGk_Avq"
        },
        {
          "name": "doc_type",
          "value": "msword"
        },
        {
          "name": "is_encrypted",
          "boolValue": false
        },
        {
          "name": "doc_title",
          "value": "[DFC]_Forensic_Report.docx"
        },
        {
          "name": "visibility",
          "value": "shared_internally"
        }
      ]
    }
  ]
}
```

@ 이벤트 시각: 2023-05-29 17:22:32 (UTC+0)

- 아티팩트: google_workspace_audit_report.json
- 이벤트 내용: delta.dfc@nomean.org가 드라이브의 '[DFC]_Forensic_Report.docx' 파일을 휴지통으로 이동
- * 문서 정보:
 - 문서 이름: [DFC]_Forensic_Report.docx
 - 문서 id: 1C9sDRd2DgqC8MhOfn3v81Hh82hGk_Avq
 - 업로드한 유저: admin@nomean.org (* 업로드 시간: 2023-05-29 15:47:52 UTC+0)
 - 추가 설명: 해당 문서 파일은 admin@nomean.org가 업로드한 후, 프로젝트 참여 인원인 admin@nomean.org, alice.dfc@nomean.org, charlie.dfc@nomean.org, echo.dfc@nomean.org, bravo.dfc@nomean.org, delta.dfc@nomean.org가 지속적으로 접근 및 수정

```
{
  "kind": "admin#reports#activity",
  "id": {
    "time": "2023-05-29T17:22:32.045Z",
    "uniqueQualifier": "3839777008290187968",
    "applicationName": "drive",
    "customerId": "C038fhwe2"
  },
  "etag": "\"\\82YgmLpRVC5iA-bU28dUqy2uCKS7KMlDQDk3vW-TM2Y/80I59wFImuCdZpWHZkkEhy0MkAA\\\"",
  "actor": {
    "email": "delta.dfc@nomean.org",
    "profileId": "115830431782957231483"
  },
  "ipAddress": "58.77.95.37",
  "events": [
    {
      "type": "access",
      "name": "trash",
      "parameters": [
        {
          "name": "primary_event",
          "boolValue": true
        },
        {
          "name": "billable",
          "boolValue": true
        },
        {
          "name": "owner_is_shared_drive",
          "boolValue": true
        },
        {
          "name": "owner_team_drive_id",
          "value": "0ANP7Tzn9-C6Guk9PVA"
        },
        {
          "name": "owner",
          "value": "DFC_Shared"
        },
        {
          "name": "doc_id",
          "value": "1C9sDRd2DgqC8MhOfn3v81Hh82hGk_Avq"
        },
        {
          "name": "doc_type",
          "value": "msword"
        },
        {
          "name": "is_encrypted",
          "boolValue": false
        },
        {
          "name": "doc_title",
          "value": "[DFC]_Forensic_Report.docx"
        }
      ]
    }
  ]
}
```

@ 이벤트 시각: 2023-05-29 17:23:15 (UTC+0)

- 아티팩트: google_workspace_audit_report.json
- 이벤트 내용: delta.dfc@nomean.org가 '[DFC]_Forensic_Report.docx' 파일을 드라이브에 업로드

*** 문서 정보:**

- 문서 이름: [DFC]_Forensic_Report.docx
- 문서 id: 1C1Viz_EbP50SDSmZ5G2AVFYWkduDuSZE

```
{
  "kind": "admin#reports#activity",
  "id": {
    "time": "2023-05-29T17:23:15.620Z",
    "uniqueQualifier": "-4651326229468613003",
    "applicationName": "drive",
    "customerId": "C038fhwe2"
  },
  "etag": "\"82YgmLpRVC5iA-bU28dUqy2uCKS7KMlDQDk3vW-TM2Y/tBKkgrZPmebaaqP1_5nDeF2bSEI\"",
  "actor": {
    "email": "delta.dfc@nomean.org",
    "profileId": "115830431782957231483"
  },
  "ipAddress": "58.77.95.37",
  "events": [
    {
      "type": "access",
      "name": "upload",
      "parameters": [
        {
          "name": "primary_event",
          "boolValue": true
        },
        {
          "name": "billable",
          "boolValue": true
        },
        {
          "name": "owner_is_shared_drive",
          "boolValue": true
        },
        {
          "name": "owner_team_drive_id",
          "value": "0ANP7Tzn9-C6Guk9PVA"
        },
        {
          "name": "owner",
          "value": "DFC_Shared"
        },
        {
          "name": "doc_id",
          "value": "1C1Viz_EbP50SDSmZ5G2AVFYWkduDuSZE"
        },
        {
          "name": "doc_type",
          "value": "msword"
        },
        {
          "name": "is_encrypted",
          "boolValue": false
        },
        {
          "name": "doc_title",
          "value": "[DFC]_Forensic_Report.docx"
        }
      ]
    }
  ]
}
```

@ 이벤트 시각: 2023-05-29 17:23:29 (UTC+0)

- 아티팩트: google_workspace_audit_report.json
- 이벤트 내용: delta.dfc@nomean.org가 드라이브의 '[DFC]_Forensic_Report.docx' 파일을 복사하여, '[DFC]_Forensic_Report.docx'의 사본' 파일로 생성

*** 문서 정보:**

- 복사 대상 문서 이름: [DFC]_Forensic_Report.docx
- 복사 대상 문서 id: 1C1Viz_EbP50SDSmZ5G2AVFYWkduDuSZE
- 생성된 문서 이름: [DFC]_Forensic_Report.docx의 사본
- 생성된 문서 id: 12sVRnsytVypNPu93xmkSkrkFyH9tHw3x

```
{
  "type": "access",
  "name": "copy",
  "parameters": [
    {
      "name": "billable",
      "boolValue": true
    },
    {
      "name": "primary_event",
      "boolValue": true
    },
    {
      "name": "copy_type",
      "value": "internal"
    },
    {
      "name": "old_value",
      "multiValue": [
        "[DFC]_Forensic_Report.docx"
      ]
    },
    {
      "name": "new_value",
      "multiValue": [
        "[DFC]_Forensic_Report.docx\uc758 \uc0ac\ubcf8"
      ]
    },
    {
      "name": "owner_is_shared_drive",
      "boolValue": true
    },
    {
      "name": "owner_team_drive_id",
      "value": "0ANP7Tzn9-C6Guk9PVA"
    },
    {
      "name": "owner",
      "value": "DFC_Shared"
    },
    {
      "name": "doc_id",
      "value": "12sVRnsytVypNPu93xmkSkrkFyH9tHw3x"
    },
    {
      "name": "doc_type",
      "value": "msword"
    }
  ]
}
```

@ 이벤트 시각: 2023-05-29 17:23:47 (UTC+0)

- 아티팩트: google_workspace_audit_report.json
- 이벤트 내용: delta.dfc@nomean.org가 드라이브의 '[DFC]_Forensic_Report.docx'의 사본' 파일을 'Sample_Template.docx'로 이름 변경

* 문서 정보:

- 변경 전 문서 이름: [DFC]_Forensic_Report.docx의 사본
- 변경 전 문서 id: 12sVRnsytVypNPu93xmkSkrkFyH9tHw3x
- 변경 후 문서 이름: 'Sample_Template.docx
- 변경 후 문서 id: 12sVRnsytVypNPu93xmkSkrkFyH9tHw3x

```
{
  "type": "access",
  "name": "rename",
  "parameters": [
    {
      "name": "primary_event",
      "boolValue": true
    },
    {
      "name": "billable",
      "boolValue": true
    },
    {
      "name": "old_value",
      "multiValue": [
        "[DFC]_Forensic_Report.docx\u2013"
      ]
    },
    {
      "name": "new_value",
      "multiValue": [
        "Sample_Template.docx"
      ]
    },
    {
      "name": "owner_is_shared_drive",
      "boolValue": true
    },
    {
      "name": "owner_team_drive_id",
      "value": "0ANP7Tzn9-C6Guk9PVA"
    },
    {
      "name": "owner",
      "value": "DFC_Shared"
    },
    {
      "name": "doc_id",
      "value": "12sVRnsytVypNPu93xmkSkrkFyH9tHw3x"
    },
    {
      "name": "doc_type",
      "value": "msword"
    },
    {
      "name": "is_encrypted",
      "boolValue": false
    },
    {
      "name": "doc_title",
      "value": "Sample_Template.docx"
    }
  ],
  "value": "Sample_Template.docx"
}
```

@ 이벤트 시각: 2023-05-29 17:25:04 (UTC+0)

- 아티팩트: vault_google_mail--delta.dfc@nomean.org-flw0Bc.pst
- 이벤트 내용: trudy.afc@gmail.com가 'work meeting' Google Meet 초대 수락
- * 회의 참여자: delta.dfc@nomean.org와 trudy.afc@gmail.com가 1:1 회의 진행


Accepted: work meeting @ Tue 30 May 2023 2am - 3am (KST) (delta.dfc@nomean.org)

delta.dfc@nomean.org

Sent time: 05/30/2023 02:25:04 AM

Received time: 05/30/2023 02:25:05 AM

To: delta.dfc@nomean.org

Attachments:  [invite.ics](#)

trudy AFC has accepted this invitation. [Learn more <>](#)

@ 이벤트 시각: 2023-05-29 17:25:24 (UTC+0)

- 아티팩트: google_workspace_audit_report.json
- 이벤트 내용: delta.dfc@nomean.org가 'Sample_Template.docx' 파일 권한을 private에서 people_with_link로 수정

* 문서 정보:

- 문서 이름: Sample_Template.docx
- 문서 id: 12sVRnsytVypNPu93xmkSkrkFyH9tHw3x

* 권한 정보:

- visibility: people_with_link (링크가 있는 모든 사용자)
- access_scope: can_view (뷰어 권한)

```
{
  "type": "acl_change",
  "name": "change_document_visibility",
  "parameters": [
    {
      "name": "primary_event",
      "boolValue": true
    },
    {
      "name": "billable",
      "boolValue": true
    },
    {
      "name": "visibility_change",
      "value": "external"
    },
    {
      "name": "target_domain",
      "value": "all"
    },
    {
      "name": "old_value",
      "multiValue": [
        "private"
      ]
    },
    {
      "name": "new_value",
      "multiValue": [
        "people_with_link"
      ]
    },
    {
      "name": "old_visibility"
    }
  ]
}
```

```
{
  "type": "acl_change",
  "name": "change_document_access_scope",
  "parameters": [
    {
      "name": "primary_event",
      "boolValue": true
    },
    {
      "name": "billable",
      "boolValue": true
    },
    {
      "name": "visibility_change",
      "value": "external"
    },
    {
      "name": "target_domain",
      "value": "all"
    },
    {
      "name": "old_value",
      "multiValue": [
        "none"
      ]
    },
    {
      "name": "new_value",
      "multiValue": [
        "can_view"
      ]
    },
    {
      "name": "old_visibility",
      "value": "shared_internally"
    }
  ]
}
```

@ 이벤트 시각: 2023-05-29 17:26:25 (UTC+0)

- 아티팩트: google_workspace_audit_report.json
- 이벤트 내용: delta.dfc@nomean.org가 공유한 'Sample_Template.docx' 파일에 trudy AFC가 링크를 통해 접근한 것으로 추정
- * 문서 정보:
 - 문서 이름: Sample_Template.docx
 - 문서 id: 12sVRnsytVypNPu93xmkSkrkFyH9tHw3x

```
{
  "kind": "admin#reports#activity",
  "id": {
    "time": "2023-05-29T17:26:25.856Z",
    "uniqueQualifier": "680722678291178994",
    "applicationName": "drive",
    "customerId": "C038fhwe2"
  },
  "etag": "\"82YgmLpRVC5iA-bU28dUqy2uCKS7KM1DQDk3vW-TM2Y/Gn0ZcoD1q0_F3vq8K8GZ_e7XC5o\"",
  "actor": {
    "email": "",
    "profileId": "105250506097979753968"
  },
  "events": [
    {
      "type": "access",
      "name": "view",
      "parameters": [
        {
          "name": "primary_event",
          "boolValue": true
        },
        {
          "name": "billable",
          "boolValue": false
        },
        {
          "name": "owner_is_shared_drive",
          "boolValue": true
        },
        {
          "name": "owner_team_drive_id",
          "value": "0ANP7Tzn9-C6Guk9PVA"
        },
        {
          "name": "owner",
          "value": "DFC_Shared"
        },
        {
          "name": "doc_id",
          "value": "12sVRnsytVypNPu93xmkSkrkFyH9tHw3x"
        },
        {
          "name": "doc_type",
          "value": "mword"
        },
        {
          "name": "is_encrypted",
          "boolValue": false
        },
        {
          "name": "doc_title",
          "value": "Sample_Template.docx"
        },
        {
          "name": "visibility",
          "value": "people_with_link"
        }
      ]
    }
  ]
}
```


@ 이벤트 시각: 2023-05-29 17:26:26 (UTC+0)

- 아티팩트: google_workspace_audit_report.json

- 이벤트 내용: delta.dfc@nomean.org가 공유한 'Sample_Template.docx' 파일을 trudy AFC가 다운로드한 것으로 추정

* 문서 정보:

- 문서 이름: Sample_Template.docx

- 문서 id: 12sVRnsytVypNPu93xmkSkrkFyH9tHw3x

```
{
  "kind": "admin#reports#activity",
  "id": {
    "time": "2023-05-29T17:26:26.336Z",
    "uniqueQualifier": "6679896063690497792",
    "applicationName": "drive",
    "customerId": "C038fhwe2"
  },
  "etag": "\"82YgmLpRVC5iA-bU28dUqy2uCKS7KMLDQDk3vW-TM2Y/8VBhi_Eqy-rIEn8GvQwpWwDk4i0\"",
  "actor": {
    "email": "",
    "profileId": "105250506097979753968"
  },
  "events": [
    {
      "type": "access",
      "name": "download",
      "parameters": [
        {
          "name": "primary_event",
          "boolValue": true
        },
        {
          "name": "billable",
          "boolValue": false
        },
        {
          "name": "owner_is_shared_drive",
          "boolValue": true
        },
        {
          "name": "owner_team_drive_id",
          "value": "0ANP7Tzn9-C6GUK9PVA"
        },
        {
          "name": "owner",
          "value": "DFC_Shared"
        },
        {
          "name": "doc_id",
          "value": "12sVRnsytVypNPu93xmkSkrkFyH9tHw3x"
        },
        {
          "name": "doc_type",
          "value": "msword"
        },
        {
          "name": "is_encrypted",
          "boolValue": false
        }
      ]
    }
  ]
}
```

@ 이벤트 시각: 2023-05-29 17:31:07 (UTC+0)

- 아티팩트: google_workspace_audit_report.json
- 이벤트 내용: delta.dfc@nomean.org와 trudy.afc@gmail.com의 'work meeting' Google Meet 회의 종료 (380초간 진행)

```
{
  "kind": "admin#reports#activity",
  "id": {
    "time": "2023-05-29T17:31:07.852Z",
    "uniqueQualifier": "6735984409692950308",
    "applicationName": "meet",
    "customerId": "C038fhwe2"
  },
  "etag": "\"82YgmLpRVC5iA-bU28dUqy2uCKS7KM1DQDk3vW-TM2Y/h-hVHTtz5VBiB2iKo_rsthb4dc\"",
  "actor": {
    "callerType": "KEY",
    "key": "HANGOUTS_EXTERNAL_OR_ANONYMOUS"
  },
  "events": [
    {
      "type": "call",
      "name": "call_ended",
      "parameters": [
        {
          "name": "video_send_seconds",
          "intValue": "0"
        },
        {
          "name": "identifier_type",
          "value": "email_address"
        },
        {
          "name": "audio_send_bitrate_kbps_mean",
          "intValue": "1"
        },
        {
          "name": "endpoint_id",
          "value": "duo_android_7751141951371110819"
        },
        {
          "name": "device_type",
          "value": "android"
        },
        {
          "name": "calendar_event_id",
          "value": "25dqdcatl1lc72dvlpc9bi7mghk"
        },
        {
          "name": "screencast_send_seconds",
          "intValue": "0"
        },
        {
          "name": "audio_send_packet_loss_max",
          "intValue": "0"
        }
      ]
    }
  ]
}
```

@ 이벤트 시각: 2023-05-29 17:41:21 (UTC+0)

- 아티팩트: google_workspace_audit_report.json
- 이벤트 내용: delta.dfc@nomean.org와 trudy.afc@gmail.com의 'work meeting' Google Meet 회의 종료 (548초간 진행)

```
{
  "kind": "admin#reports#activity",
  "id": {
    "time": "2023-05-29T17:41:21.102Z",
    "uniqueQualifier": "3738209707242555465",
    "applicationName": "meet",
    "customerId": "C038fhwe2"
  },
  "etag": "\"82YgmLpRVC5iA-bU28dUqy2uCKS7KM1DQDk3vW-TM2Y/9W1kZbwNRaRG6NwmOHu5GFNKpw\"",
  "actor": {
    "callerType": "KEY",
    "key": "HANGOUTS_EXTERNAL_OR_ANONYMOUS"
  },
  "events": [
    {
      "type": "call",
      "name": "call_ended",
      "parameters": [
        {
          "name": "video_send_seconds",
          "intValue": "0"
        },
        {
          "name": "identifier_type",
          "value": "email_address"
        },
        {
          "name": "audio_send_bitrate_kbps_mean",
          "intValue": "1"
        },
        {
          "name": "endpoint_id",
          "value": "duo_android_4440672412571046997"
        },
        {
          "name": "device_type",
          "value": "android"
        },
        {
          "name": "calendar_event_id",
          "value": "25dqdcatllc72dvlpc9bi7mghk"
        },
        {
          "name": "screencast_send_seconds",
          "intValue": "0"
        },
        {
          "name": "audio_send_packet_loss_max",
          "intValue": "0"
        }
      ]
    }
  ]
}
```

@ 이벤트 시각: 2023-05-29 17:42:30 (UTC+0)

- 아티팩트: vault_google_chat_0.pst
- 이벤트 내용: delta.dfc@nomean.org가 trudy.afc@gmail.com와 채팅 시작 (* 두 사람은 2023-05-29일에 18:05:28 시각까지 1:1 채팅 진행)
 - * chat room id: 9eBYvkAAAAE
 - * chat type: direct message
 - * 채팅 내용(한글 번역) :

- delta.dfc@nomean.org 2023년 5월 29일 17:42:30
이봐 트루디 다운로드 됐어??

- trudy.afc@gmail.com 2023년 5월 29일 17:43:14
네. 나는 그것을 다운로드했다. 근데 확인이 안되네요???

- delta.dfc@nomean.org 2023년 5월 29일 17:44:11
보안을 위해 암호화가 적용됩니다. 더 암호화된 채널로 전달하겠습니다. 기다리고 보자

- delta.dfc@nomean.org 2023년 5월 29일 17:48:49
우선 이것을 잘 받아서 보관하세요. 곧 연락 드리겠습니다. 이것은 데이터로 이어질 수 있습니다.
presentation.pptx (파일 첨부)

- delta.dfc@nomean.org 2023년 5월 29일 17:49:08
다운로드했는지 알려주세요

- trudy.afc@gmail.com 2023년 5월 29일 17:49:55
액세스할 수 없습니다. 링크에 대해 공유해 주시겠습니까??

- delta.dfc@nomean.org 2023년 5월 29일 17:50:37
알겠습니다.
https://docs.google.com/presentation/d/1_pJAoOwqMu2nWveJi6pmUNw5IPlbiqXv/edit?usp=share_link&ouid=115830431782957231483&rtpof=true&sd=true입니다.

https://docs.google.com/presentation/d/1_pJAoOwqMu2nWveJi6pmUNw5IPlbiqXv/edit?usp=share_link&ouid=115830431782957231483&rtpof=true&sd=true

https://drive.google.com/open?id=1_pJAoOwqMu2nWveJi6pmUNw5IPlbiqXv

- trudy.afc@gmail.com 2023년 5월 29일 17:59:51
다운로드할 수 없습니다. 다른 방법은???

- delta.dfc@nomean.org 2023년 5월 29일 18:00:04
그래 기다려..

- delta.dfc@nomean.org 2023년 5월 29일 18:04:03

여기!!

presentation.zip (파일 첨부)

- trudy.afc@gmail.com 2023년 5월 29일 18:04:54

알겠습니다. 나는 그것을 다운로드했다!

- delta.dfc@nomean.org 2023년 5월 29일 18:05:28

좋아요. 이 채팅방을 나가겠습니다

@ 이벤트 시각: 2023-05-29 17:45:36 (UTC+0)

- 아티팩트: google_workspace_audit_report.json
- 이벤트 내용: delta.dfc@nomean.org가 'presentation.pptx' 파일을 드라이브에 업로드

* 문서 정보:

- 문서 이름: presentation.pptx
- 문서 id: 1_pJAoOwqMu2nWveJi6pmUNw5IPlbqXv

```
{
  "kind": "admin#reports#activity",
  "id": {
    "time": "2023-05-29T17:45:36.940Z",
    "uniqueQualifier": "551387429788039385",
    "applicationName": "drive",
    "customerId": "C038fhwe2"
  },
  "etag": "\"82YgmLpRVC5iA-bU28dUqy2uCKS7KM1DQDk3vW-TM2Y/1zVNstRK33iIJInnmNwO_QH4aak\"",
  "actor": {
    "email": "delta.dfc@nomean.org",
    "profileId": "115830431782957231483"
  },
  "ipAddress": "58.77.95.37",
  "events": [
    {
      "type": "access",
      "name": "upload",
      "parameters": [
        {
          "name": "primary_event",
          "boolValue": true
        },
        {
          "name": "billable",
          "boolValue": true
        },
        {
          "name": "owner_is_shared_drive",
          "boolValue": true
        },
        {
          "name": "owner_team_drive_id",
          "value": "0ANP7Tzn9-C6GUk9PVA"
        },
        {
          "name": "owner",
          "value": "DFC_Shared"
        },
        {
          "name": "doc_id",
          "value": "1_pJAoOwqMu2nWveJi6pmUNw5IPlbqXv"
        },
        {
          "name": "doc_type",
          "value": "mspowerpoint"
        },
        {
          "name": "is_encrypted",
          "boolValue": false
        },
        {
          "name": "doc_title",
          "value": "presentation.pptx"
        }
      ]
    }
  ]
}
```

@ 이벤트 시각: 2023-05-29 17:48:49 (UTC+0)

- 아티팩트: google_workspace_audit_report.json
- 이벤트 내용: delta.dfc@nomean.org가 'presentation.pptx' 파일을 trudy.afc@gmail.com와의 chat에 첨부 파일 업로드
- * chat room id: 9eBYvkAAAAE
- * chat type: direct message

```
{
  "kind": "admin#reports#activity",
  "id": {
    "time": "2023-05-29T17:48:49.429Z",
    "uniqueQualifier": "-2562307178191074499",
    "applicationName": "chat",
    "customerId": "C038fhwe2"
  },
  "etag": "\"82YgmLpRVC5iA-bU28dUqy2uCKS7KMLDQDk3vW-TM2Y/gr-RGiUQH2_B4Xm4rUPVgXDefK8\"",
  "actor": {
    "callerType": "USER",
    "email": "delta.dfc@nomean.org",
    "profileId": "115830431782957231483"
  },
  "events": [
    {
      "type": "user_action",
      "name": "attachment_upload",
      "parameters": [
        {
          "name": "message_id",
          "value": "spaces/9eBYvkAAAAE/messages/ZoiaCj4ApDc.ZoiaCj4ApDc"
        },
        {
          "name": "room_id",
          "value": "9eBYvkAAAAE"
        },
        {
          "name": "timestamp_ms",
          "value": "1685382529429151"
        },
        {
          "name": "actor",
          "value": "delta.dfc@nomean.org"
        },
        {
          "name": "attachment_name",
          "value": "presentation.pptx"
        },
        {
          "name": "attachment_hash",
          "value": "0ebdca4abc6ea14bc3f01139c9e027cc84f2ad88852ee34918bf98a981372f33"
        },
        {
          "name": "retention_state",
          "value": "PERMANENT"
        },
        {
          "name": "room_name",
          "value": ""
        },
        {
          "name": "dlp_scan_status",
          "value": "DLP_SCANNED"
        }
      ]
    }
  ]
}
```

@ 이벤트 시각: 2023-05-29 17:50:16 (UTC+0)

- 아티팩트: google_workspace_audit_report.json

- 이벤트 내용: delta.dfc@nomean.org가 'presentation.pptx' 파일 권한을 private에서 people_with_link로 수정

* 문서 정보:

- 문서 이름: presentation.pptx

- 문서 id: 1_pJAoOwqMu2nWveJi6pmUNw5IPlbqXv

* 권한 정보:

- visibility: people_with_link (링크가 있는 모든 사용자)

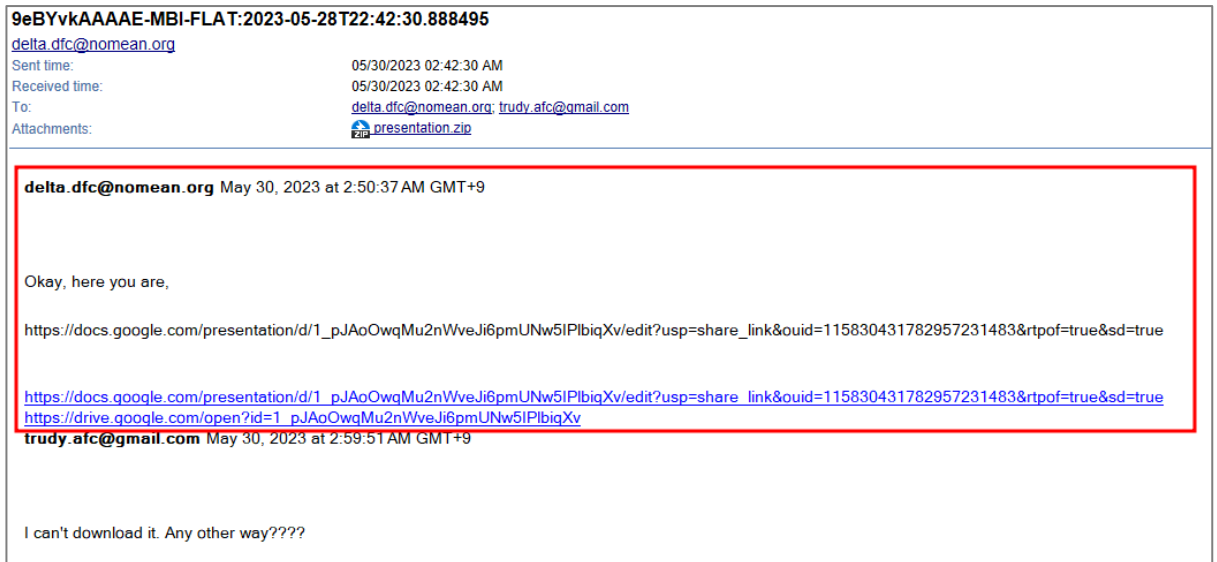
- access_scope: can_view (뷰어 권한)

```
{
  "type": "acl_change",
  "name": "change_document_visibility",
  "parameters": [
    {
      "name": "primary_event",
      "boolValue": true
    },
    {
      "name": "billable",
      "boolValue": true
    },
    {
      "name": "visibility_change",
      "value": "external"
    },
    {
      "name": "target_domain",
      "value": "all"
    },
    {
      "name": "old_value",
      "multiValue": [
        "private"
      ]
    },
    {
      "name": "new_value",
      "multiValue": [
        "people_with_link"
      ]
    }
  ],
  {}
}
```

```
{
  "type": "acl_change",
  "name": "change_document_access_scope",
  "parameters": [
    {
      "name": "primary_event",
      "boolValue": true
    },
    {
      "name": "billable",
      "boolValue": true
    },
    {
      "name": "visibility_change",
      "value": "external"
    },
    {
      "name": "target_domain",
      "value": "all"
    },
    {
      "name": "old_value",
      "multiValue": [
        "none"
      ]
    },
    {
      "name": "new_value",
      "multiValue": [
        "can_view"
      ]
    }
  ],
  {}
}
```


@ 이벤트 시각: 2023-05-29 17:50:37 (UTC+0)

- 아티팩트: vault_google_chat_0.pst
- 이벤트 내용: delta.dfc@nomean.org가 'presentation.pptx'에 접근할 수 있는 링크를 trudy.afc@gmail.com에게 chat으로 전달



@ 이벤트 시각: 2023-05-29 18:04:03 (UTC+0)

- 아티팩트: google_workspace_audit_report.json

- 이벤트 내용: delta.dfc@nomean.org가 'presentation.zip' 파일을 trudy.afc@gmail.com와의 chat에 첨부 파일 업로드

* chat room id: 9eBYvkAAAAE

* chat type: direct message

```
{
  "kind": "admin#reports#activity",
  "id": {
    "time": "2023-05-29T18:04:03.303Z",
    "uniqueQualifier": "611541353938606086",
    "applicationName": "chat",
    "customerId": "C038fhwe2"
  },
  "etag": "\"82YgmLpRVC5iA-bU28dUqy2uCKS7KM1DQDk3vW-TM2Y/qT9n881jgJ4NV6DMYGcUoIi--Ng\"",
  "actor": {
    "callerType": "USER",
    "email": "delta.dfc@nomean.org",
    "profileId": "115830431782957231483"
  },
  "events": [
    {
      "type": "user_action",
      "name": "attachment_upload",
      "parameters": [
        {
          "name": "message_id",
          "value": "spaces/9eBYvkAAAAE/messages/AfFzpiVrDiA.AfFzpiVrDiA"
        },
        {
          "name": "room_id",
          "value": "9eBYvkAAAAE"
        },
        {
          "name": "timestamp_ms",
          "value": "1685383443303727"
        },
        {
          "name": "actor",
          "value": "delta.dfc@nomean.org"
        },
        {
          "name": "attachment_name",
          "value": "presentation.zip"
        },
        {
          "name": "attachment_hash",
          "value": "fb1afa8815f71effd097aed0b82d9a9b397c5286b42122b041cb59646f0d6a91"
        },
        {
          "name": "retention_state",
          "value": "PERMANENT"
        },
        {
          "name": "room_name",
          "value": ""
        },
        {
          "name": "dlp_scan_status",
          "value": "DLP_SCAN_FAILED"
        }
      ]
    }
  ]
}
```

@ 이벤트 시각: 2023-05-29 18:07:31 (UTC+0)

- 아티팩트: vault_google_mail--delta.dfc@nomean.org-flw0Bc.pst
- 이벤트 내용: delta.dfc@nomean.org가 trudy.afc@gmail.com에게 'work meeting' Google Meet 초대 (회의 설명에 첫 번째 암호화 키 '6c4575c9ec1709de06f48546004a7d0f' 문자열 전달)

* 회의 예정 시간:

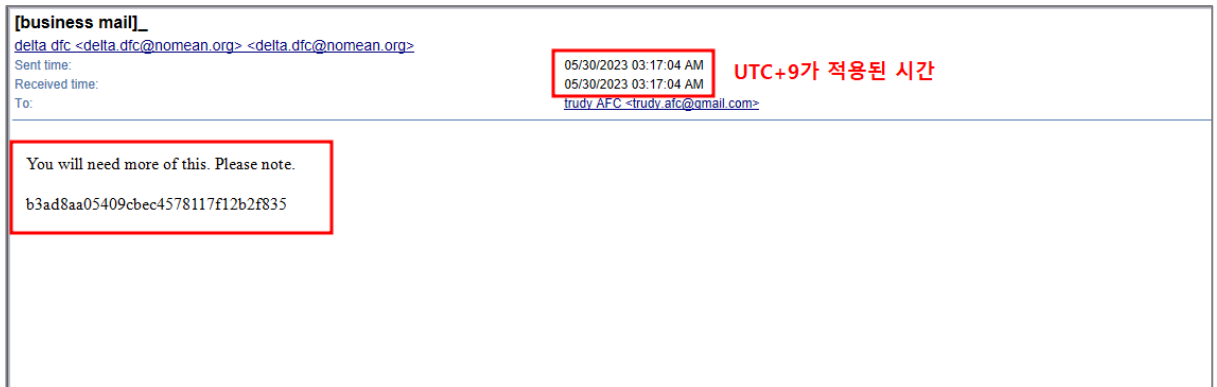
- 시작시간: 2023-05-29 23:00:00 (UTC+0)
- 종료시간: 2023-05-30 00:00:00 (UTC+0)

* 회의 설명: Hey, take a look at this. it is first. 6c4575c9ec1709de06f48546004a7d0f

[illegible]

@ 이벤트 시각: 2023-05-29 18:17:04 (UTC+0)

- 아티팩트: vault_google_mail--delta.dfc@nomean.org-flw0Bc.pst
- 이벤트 내용: delta.dfc@nomean.org가 trudy.afc@gmail.com에게 '[business mail]_' 제목의 메일을 전송 (메일 본문에 두 번째 암호화 키 'b3ad8aa05409cbec4578117f12b2f835' 문자열 전달)



@ 이벤트 시각: 2023-05-30 05:21:30 (UTC+0)

- 아티팩트: vault_google_mail--delta.dfc@nomean.org-flw0Bc.pst
- 이벤트 내용: admin@nomean.org에게 포렌식 보고서가 유출되어 내부 감사가 진행될 것이라는 사실을 알리는 '[Notice] Regret Regarding Information Leak and Internal Audit' 메일을 전달받음

[Notice] Regret Regarding Information Leak and Internal Audit
Admin Jin <admin@nomean.org> <admin@nomean.org>
Sent time: 05/30/2023 02:21:21 PM
Received time: 05/30/2023 02:21:30 PM UTC+9가 적용된 시간
To: alice.dfc <alice.dfc@nomean.org>; bravo.dfc <bravo.dfc@nomean.org>; charlie.dfc <charlie.dfc@nomean.org>; delta.dfc <delta.dfc@nomean.org>; echo.dfc <echo.dfc@nomean.org>

Dear Team,

I hope this email finds you well. I am writing to address a recent and unfortunate incident that has come to my attention. It has been brought to my notice that our forensic report has been leaked, compromising the confidentiality and integrity of our work. I deeply regret this unfortunate event, and I understand the concerns and implications it raises for each of us.

I want to assure you that we are taking this matter extremely seriously. The leaked report contains sensitive information, and we recognize the importance of identifying the root cause and preventing such incidents from happening in the future. In light of this, we will be conducting an immediate and comprehensive internal audit to assess our security protocols, systems, and potential vulnerabilities.

The purpose of this audit is to determine the source of the leak, evaluate our existing safeguards, and implement any necessary enhancements to ensure the utmost security and confidentiality of our work. I encourage each team member to cooperate fully and provide any information or insights that may assist in the investigation.

I understand that this incident may have caused distress and uncertainty among all of us. Rest assured, we are committed to transparency throughout this process. Regular updates will be provided to keep you informed about the progress of the audit, and any additional measures that need to be taken to safeguard our work.

I want to emphasize the importance of teamwork, support, and maintaining a positive mindset during this challenging time. We have a strong and resilient team, and together we will overcome this setback. Our dedication to upholding the highest standards in our forensic practice remains unwavering.

If any team member has concerns, questions, or suggestions regarding the ongoing audit or any other related matter, please do not hesitate to reach out to me directly. Your input and involvement are vital as we navigate through this situation.

Thank you for your understanding, professionalism, and commitment to the integrity of our work. Let us remain united as we carry out the necessary steps to rectify the situation and reinforce the trust placed in us.

Best regards,

- 유출 과정 요약

1. delta dfc는 DFC Corp 기업의 구글 드라이브인 DFC_Shared에 존재하는 프로젝트 극비 문서 파일 '[DFC]_Forensic_Report.docx'를 복사하여 '[DFC]_Forensic_Report.docx의 사본' 파일로 생성

* 프로젝트 극비 문서 파일 '[DFC]_Forensic_Report.docx' 파일은 admin jin이 업로드한 후, 프로젝트 참여 인원들이 지속적으로 접근 및 수정함. delta dfc는 해당 파일을 다운로드하고 드라이브에서 삭제하였음. 그 후, delta dfc는 '[DFC]_Forensic_Report.docx' 파일을 드라이브에 다시 업로드하였음. '[DFC]_Forensic_Report.docx의 사본' 파일의 복사 대상 파일은 admin jin이 업로드했던 파일이 아닌, delta dfc가 업로드한 파일임.

2. delta dfc는 구글 드라이브에 존재하는 '[DFC]_Forensic_Report.docx의 사본' 파일을 'Sample_Template.docx'로 이름 변경

3. delta dfc는 'Sample_Template.docx' 파일의 접근 권한을 '링크가 있는 모든 사용자 (뷰어 권한)'로 변경

4. delta dfc는 trudy AFC와 'work meeting' Google Meet 회의를 진행하며, 'Sample_Template.docx' 파일을 접근할 수 있는 링크를 전달한 것으로 추정됨. trudy AFC로 추정되는 인물이 링크로 접근하여 해당 파일을 다운로드 하였음.

5. 'Sample_Template.docx' 파일은 암호화되어 있는 파일임. 그러므로 delta dfc는 해당 파일을 복호화할 수 있는 실행 파일인 'presentation.pptx' 파일을 압축하여, 'presentation.zip' 파일을 trudy AFC에게 chat으로 전달 (* 'presentation.pptx' 파일은 확장자만 pptx인 exe 파일)

* delta dfc는 'presentation.pptx' 파일을 trudy AFC에게 chat으로 전달했었으나, trudy AFC가 해당 파일에 액세스 할 수 없었음. 그 후, delta dfc는 'presentation.pptx' 권한을 '링크가 있는 모든 사용자 (뷰어 권한)'으로 변경하여, 파일 접근 링크를 trudy AFC에게 chat으로 전달했음. 하지만, trudy AFC는 공유된 'presentation.pptx' 파일을 다운로드할 수 없었음. delta dfc는 마지막으로 'presentation.pptx' 파일을 압축한 'presentation.zip' 파일을 chat으로 trudy AFC에게 전달하였고 trudy AFC는 해당 파일을 성공적으로 다운로드 했음

6. 'presentation.pptx'는 실행 파일로 'Sample_Template.docx' 파일을 복호화할 때 사용됨. 단, 복호화 하기 위해서 암호 문자열 2개가 필요함. delta dfc는 trudy AFC에게 'work meeting' Google Meet 을 초대하며, 회의 설명에 첫 번째 암호 문자열 '6c4575c9ec1709de06f48546004a7d0f'을 기입하여 전달

7. delta dfc는 trudy AFC에게 '[business mail]_' 제목의 메일을 전송하여, 메일 본문에 두 번째 암호 문자열 'b3ad8aa05409cbec4578117f12b2f835'을 기입하여 전달

Q3. Find the original leaked confidential report. (MD5 Hash) (150 points)

- 986c8fc0d4a91c26388af65633898cfe

delta dfc가 trudy AFC에게 전달한 'presentation.pptx' 파일은 'DFCWNative_ExportWproject' 경로에 존재하며, 010 Editor 도구로 해당 파일의 구조를 확인해본 결과, pptx 파일이 아닌 PE 구조를 가진 64비트 실행파일임을 확인하였다.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h	4D	5A	90	00	03	00	04	00	00	00	00	00	FF	FF	00	00	MZ.....ÿÿ..
0010h	8B	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00@.....
0020h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0030h	00	00	00	00	00	00	00	00	00	00	00	00	80	00	00	00€...
0040h	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	..°...!..!..!Th
0050h	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program canno
0060h	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t be run in DOS
0070h	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode....\$.....
0080h	50	45	00	00	64	86	0D	00	00	00	00	00	00	16	20	00	PE..dt.....
0090h	23	0A	00	00	F0	00	22	02	0B	02	03	00	00	2C	0A	00	#...ä..".....
00A0h	00	B8	01	00	00	00	00	00	80	02	06	00	00	10	00	00€.....
00B0h	00	00	40	00	00	00	00	00	00	10	00	00	00	02	00	00	..@.....
00C0h	06	00	01	00	01	00	00	00	06	00	01	00	00	00	00	00
00D0h	00	D0	27	00	00	06	00	00	00	00	00	00	03	00	60	81	.D'.....
00E0h	00	00	20	00	00	00	00	00	00	10	00	00	00	00	00	00
00F0h	00	00	10	00	00	00	00	00	00	10	00	00	00	00	00	00

IDA로 해당 실행 파일을 분석한 결과, 암호화된 문서 파일을 복호화하기 위해서는 2개의 암호화 키 값과 함께 복호화 명령 코드인 'dec'가 필요한 것을 확인하였다.

```
56 v9 = main_decodeHexKey(*(os_Args + 48), os_Args, v8, v5, v4, a3); // 암호화 키 1
57 v11 = os_Args;
58 v12 = qword_56E288;
59 if ( qword_56E288 <= 4 )
60 LABEL_25:
61 runtime_panicIndex(v5, v12, v11);
62 v26 = v10;
63 v32 = v9;
64 v25 = v8;
65 v13 = *(os_Args + 72);
66 v31 = main_decodeHexKey(*(os_Args + 64), os_Args, v13, v5, qword_56E288, a3); // 암호화 키 2
67 v24 = v14;
68 v34 = main_getOutputFileName(v33, &unk_4C02AB, v27, 4LL, v12, a3);
69 v28 = v27;
70 v5 = 4LL;
71 main_getOutputFileName(v33, &unk_4C02A7, v27, 4LL, v12, a3);
72 if ( v29 != 3 )
73 {
74 LABEL_24:
75 runtime_gopanic(4LL, v12, v15, v29, v16, v17);
76 goto LABEL_25;
77 }
78 v15 = v30;
79 if ( *v30 != 'ne' )
80 {
81 v18 = v29 == 3;
82 goto LABEL_15;
83 }
84 if ( *(v30 + 2) != 'c' )
85 {
86 v18 = v29 == 3;
87 LABEL_15:
88 if ( v18 && *v30 == 'ed' && *(v30 + 2) == 'c' ) // 명령코드 "dec" 존재할 경우 파일 복호화 수행
89 {
90 v22 = main_decryptFile(v27, v27, v32, v25, v26, &off_4CA608, a3, v31, v13, v24); // 파일 복호화 함수
91 if ( v22 )
```

IDA를 통해 분석한 내용을 바탕으로, delta dfc가 trudy AFC에게 전송한 첫 번째 암호화 키 '6c4575c9ec1709de06f48546004a7d0f'와 두 번째 암호화 키 'b3ad8aa05409cbec4578117f12b2f835'를 파일 복호화에 사용한다는 것을 확인할 수 있었다.

위 내용을 토대로 delta dfc가 trudy AFC에게 전달한 암호화된 문서 파일 'DFC\Native_Export\project\report\Sample_Template.docx'을 복호화할 수 있었으며, 복호화된 원본 문서 파일의 MD5 값은 '986c8fc0d4a91c26388af65633898cfe'이다.

* 복호화 명령어: `presentation.pptx dec Sample_Template.docx 6c4575c9ec1709de06f48546004a7d0f b3ad8aa05409cbec4578117f12b2f835`

```
C:\Windows\System32\cmd.exe
(c) Microsoft Corporation. All rights reserved.

D:\Users\mini\Desktop\DFC\Native_Export\project\report>presentation.pptx dec Sample_Template.docx
6c4575c9ec1709de06f48546004a7d0f b3ad8aa05409cbec4578117f12b2f835
File decrypted successfully.
```

