



[XCZ Company Hacking Incident] Write-Up

작성자	김서영
분석 일자	2024.05.18.
작성 일자	2024.05.18.
분석 대상	Prob27.7z
문서 버전	2.0
작성자 E-mail	sykim1802@naver.com

0. 목차

1. 문제3

2. 분석 도구3

3. 환경3


4. Write-Up.....4

5. Flag.....7

6. 별도 첨부8

7. Reference9

1. 문제

URL	Prob27 (xcz.kr)
문제 내용	<p>어느 날 해커 'FORENSER' 는 BOSS 의 명령을 받고 계획까지 치밀하게 세운 뒤, "XCZ" 라는 회사의 내부에 침입하여 기밀문서를 찾아 외부로 유출하는 과정 중 현장에서 발각되었다.</p> <p>조사 중에서도 죄의식을 느끼지 못하고 질문에 답하지 않고 물어보았자 시간을 버리는 일이었다.</p> <p>결국 참다 못해 직접 나서서 찾기로 하였다.</p> <p>증거를 찾을 수 있는 단서는 'FORENSER' 가 가지고 있던 하드디스크 하나. 나는 일단 하드디스크에서 증거가 될 수 있을만한 것을 추려내었다.</p> <p>키 값을 찾으세요.</p>
문제 파일	 Prob27.7z
문제 유형	Disk forensics
난이도	1 / 3

2. 분석 도구

도구명	다운로드 링크	Version
Autopsy	Autopsy - Download	4.21.0
Mail Viewer	MiTeC Homepage	2.5.1.0

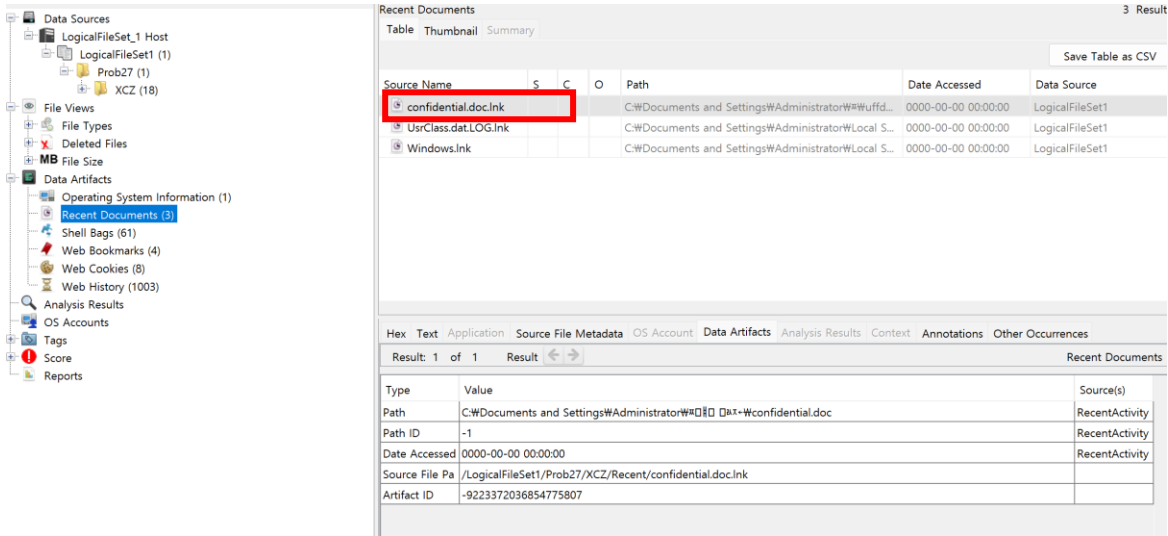
3. 환경

OS
Windows11 x64

4. Write-Up

파일명	Prob27.7z
용량	15,648kb
SHA256	d1e528b350ab1623711b668f48c316c9e38811f1b073f91e2a30a1b88786c7b6
Timestamp	2024-05-17 11:42:03

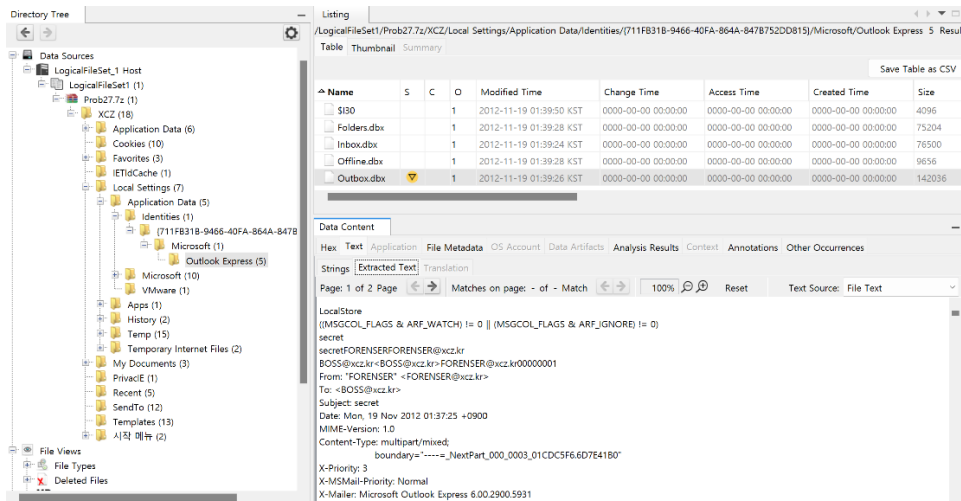
1. 문서 양이 많지 않아서 문서들 목록을 먼저 보게 되었다.



Source Name	S	C	O	Path	Date Accessed	Data Source
confidential.doc.lnk				C:\Documents and Settings\Administrator\Recent\confidential.doc	0000-00-00 00:00:00	LogicalFileSet1
UsrClass.dat.LOG.lnk				C:\Documents and Settings\Administrator\Local Settings\UsrClass.dat.LOG	0000-00-00 00:00:00	LogicalFileSet1
Windows.lnk				C:\Documents and Settings\Administrator\Local Settings\Windows	0000-00-00 00:00:00	LogicalFileSet1

[사진 1] Data Artifacts – Recent Documents

최근 문서 기록에 “Confidential.doc.lnk”가 남아있었다. Confidential(기밀)이라는 제목이 확 눈에 들어왔고, 링크가 남아있다는 뜻은 Confidential.doc 가 어딘가 있음을 의미하기에 파일 찾기에 몰두했다.



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
Outbox.dbx				2012-11-19 01:39:26 KST	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	142036

[사진 2] 수상한 dbx 파일

[WHS-2] .iso

숫자로 시작하는 파일 내부에서 outlook express 폴더를 찾았다. 기록과 텍스트 내용을 자세히 살펴보았다.

```
LocalStore
((MSGCOL_FLAGS & ARF_WATCH) != 0 || (MSGCOL_FLAGS & ARF_IGNORE) != 0)
secret
secretFORENSERFORENSER@xcz.kr
BOSS@xcz.kr<BOSS@xcz.kr> FORENSER@xcz.kr00000001
From: "FORENSER" <FORENSER@xcz.kr>
To: <BOSS@xcz.kr>
Subject: secret
Date: Mon, 19 Nov 2012 01:37:25 +0900
```

[사진 3] 수신자와 발신자

문제 내용에서 나온 해커 "Forenser"의 이름이 나왔고, 그가 발신자이다. 또한, 문제내용과 일치하게 수신자는 BOSS 다.

```
Content-Type: application/octet-stream;
    name="confidential.doc"
Content-Transfer-Encoding: base64
Content-Disposition: a
ttachment;
    filename="confidential.doc"
```

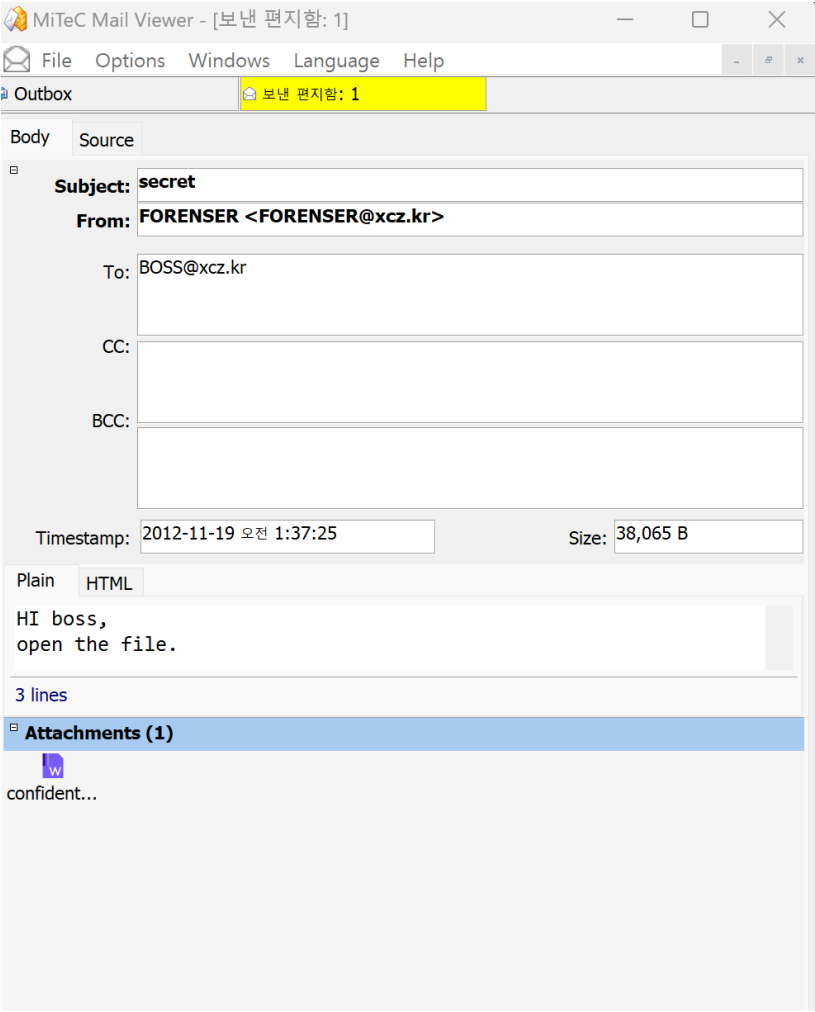
[사진 4] confidential.doc가 첨부되어 있다는 증거

Attachment – "confidential.doc"가 [사진 3]의 아래에 나와있어 결정적인 증거라고 확신했다. 이 이 메일을 추출하여 열어보면 confidential.doc도 함께 열릴 것으로 추측된다.

Outbox.dbx를 추출하여 확장자명은 .eml로 바꿔준 후 Outlook 메일 프로그램으로 열려고 시도 했다.

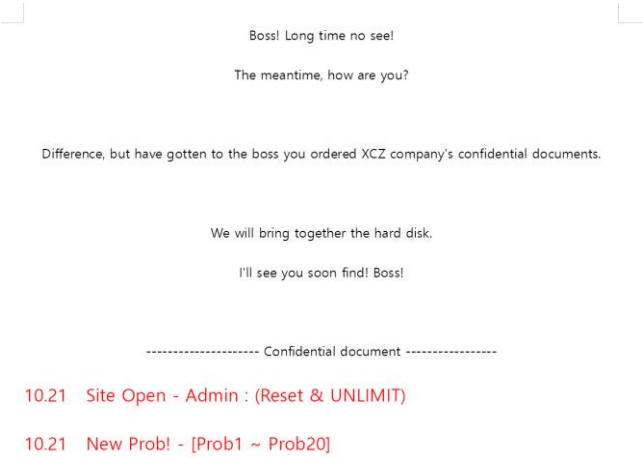
하지만, 확장자명을 바꾸는 건 역시나 한계가 뚜렷했다. 수신자와 발신자만 명시되어 있고, subject 에 secret 이 빠져있고, confidential.doc 를 다운받아서 여는 것은 불가능했다.

따라서 DBX viewer 를 다운 받아 [사진 2]의 Outbox.dbx 를 열어보았고,



[사진 5] Outbox.dbx로 이메일 복원

첨부파일인 confidential.doc를 열면,



[사진 6] confidential.doc 내용

맨 아래 빨간색 글자 옆을 드래그 한 후, 글씨 색을 바꾸면 key 값을 구할 수 있다.

5. Flag

Flag = Out10OkExpr3s5M4i1

6. 별도 첨부

7. Reference