




[Skimming device] Write-Up

| | |
|------------|--|
| 작성자 | Team C |
| 분석 일자 | 2024.05.28 |
| 작성 일자 | 2024.05.30 |
| 분석 대상 | skimmer_microSD_Physical |
| 문서 버전 | 2.0 |
| 작성자 E-mail | rd002@naver.com |

0. 목차

- 1. 문제3
- 2. 분석 도구3
- 3. 환경3
- 4. Write-Up.....4
- 5. Flag..... 12
- 6. 별도 첨부 13
- 7. Reference 14

1. 문제

| | |
|-------|---|
| URL | - |
| 문제 내용 | 문제가 너무 긴 관계로 별도첨부에 문제 및 번역본을 업로드하겠다. |
| 문제 파일 |  skimmer_microSD _Physical.e01 |
| 문제 유형 | System Forensics |
| 난이도 | 3 / 3 |

2. 분석 도구

| 도구명 | 다운로드 링크 | Version |
|---------------------------|---|---------|
| Autopsy | https://www.autopsy.com/download/ | 4.20.0 |
| Foremost | https://sourceforge.net/projects/foremost/ | 1.5.7 |
| Audacity | https://www.audacityteam.org/ | 3.5.1 |
| Magnetice Stipde Decorder | https://github.com/jtarrio/MagstripeDecoder | 1.0.0 |

3. 환경

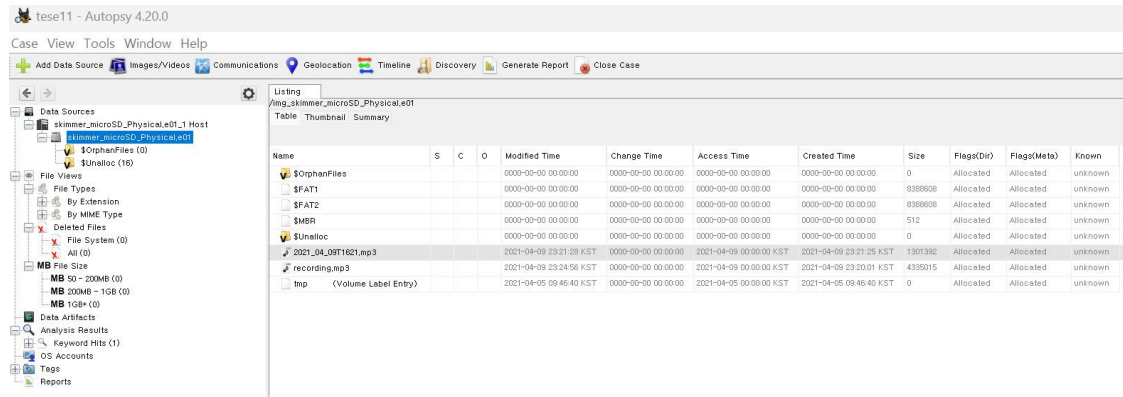
| OS |
|----------------|
| Windos Home 11 |

4. Write-Up

| | |
|------------------|--|
| 파일명 | skimmer_microSD_Physical |
| 용량 | 34.9MB |
| SHA256 | 6cf9c4bc23fe60ddbf79b734c06e85dffe8007d86339994776f6927e62dc4942 |
| Timestamp | 2021-07-28 09:32:00 |

1. 파일 수집

Autopsy 로 파일을 열어보았다.



[그림 1] autopsy로 연 문제 파일

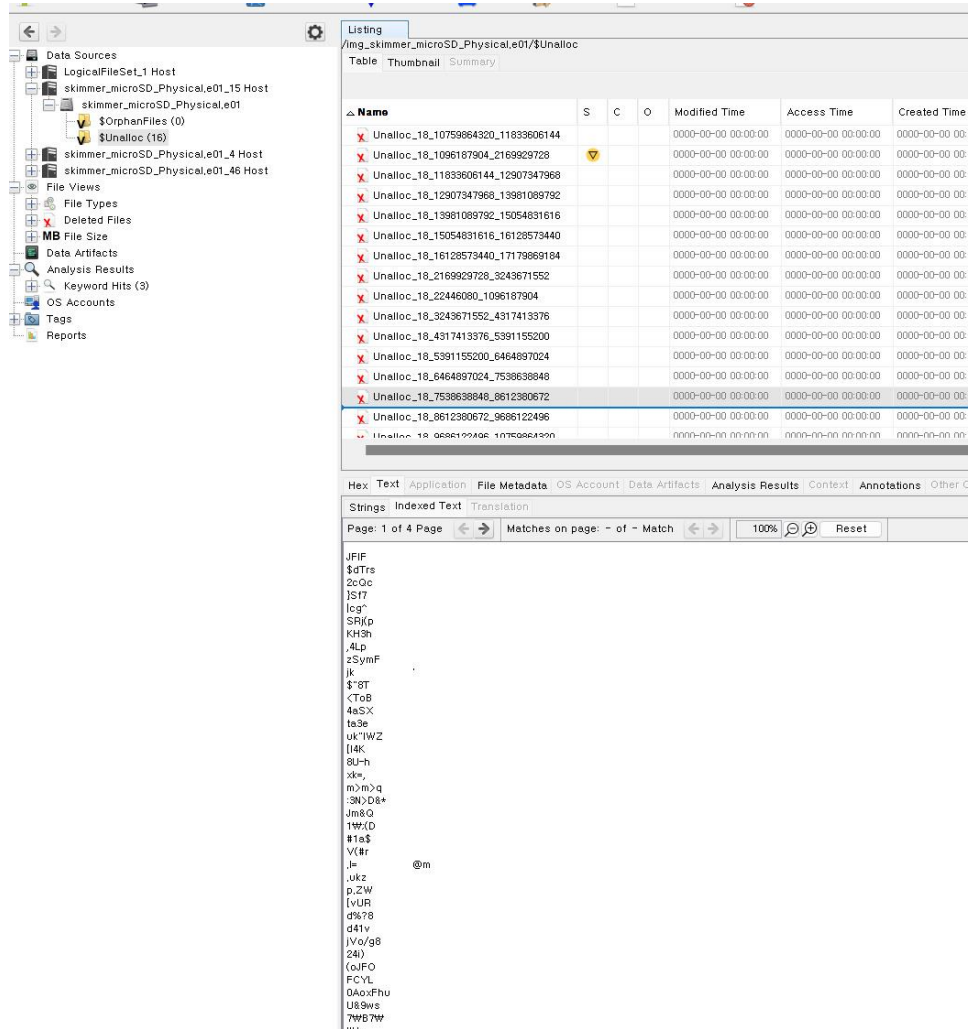
눈으로 확인할 수 있는 파일은 2021_04_09T1621.mp3 파일과 recording.mp3파일을 확인할 수 있었다. 간단하게 정리하고 넘어가자.

| 파일명 | 파일 형식 | 파일 용량 | 주석 |
|-----------------|-------|--------|---------------|
| 2021_04_09T1621 | mp3 | 1.24MB | recording의 일부 |
| recording | mp3 | 4.13MB | 분석이 필요함 |

[표 1] 파일 속성 및 주석 리스트

추가적인 조사를 진행하던 도중 Unalloc 파일 내부에서 Unalloc_18_1096187904_2169929728 파일과 Unalloc_18_2169929728_3243671552 파일의 Autopsy의 Text항을 확인해보니 그림2와 같이 하나의 파일 안에 여러가지 파일의 확장자를 확인할 수 있었다.

[WHS-2] .iso



| Name | S | C | O | Modified Time | Access Time | Created Time |
|------------------------------------|---|---|---|---------------------|---------------------|---------------------|
| Unalloc_18_10759864320_11833606144 | | | | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 |
| Unalloc_18_1096187904_2169929728 | | | | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 |
| Unalloc_18_11833606144_12907347968 | | | | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 |
| Unalloc_18_12907347968_13961089792 | | | | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 |
| Unalloc_18_13961089792_15054831616 | | | | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 |
| Unalloc_18_15054831616_16128573440 | | | | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 |
| Unalloc_18_16128573440_17179669184 | | | | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 |
| Unalloc_18_2169929728_3243671552 | | | | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 |
| Unalloc_18_22446080_1096187904 | | | | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 |
| Unalloc_18_3243671552_4317413376 | | | | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 |
| Unalloc_18_4317413376_5391155200 | | | | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 |
| Unalloc_18_5391155200_6464897024 | | | | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 |
| Unalloc_18_6464897024_7538638848 | | | | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 |
| Unalloc_18_7538638848_8612380672 | | | | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 |
| Unalloc_18_8612380672_9686122496 | | | | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 |
| Unalloc_18_9686122496_10759864320 | | | | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 |

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other C

Strings Indexed Text Translation

Page: 1 of 4 Page Matches on page: - of - Match 100% Reset

JFIF
\$dTrs
2cQc
JST7
[c9"
SR(p
KH3h
4lp
zSymF
jk
\$*8T
<To8
4aSX
ts3e
uk^IWZ
[14K
8U-h
xkx
m>n>q
3N>D8+
Jm&Q
1W.O
#1a\$
V{#r
J-
ukz
p.ZW
[vUR
d%78
d41v
jVo/g8
24i)
(oIFO
FCYL
0AoxFhu
U89ws
7WB7W
....

[그림 2] 카빙되어있는 파일 Text부분

파일이 카빙된 것임을 확인하였고, 카빙 툴인 foremost를 이용하여 카빙을 풀어서 숨겨놓은 파일들을 복구했다.

```
HackingLab canary dreamhack foremost myenv pwn_venv
juwan1@DESKTOP-C2MLG4B:~$ cd foremost/
juwan1@DESKTOP-C2MLG4B:~/foremost$ foremost -t all -i 1
Processing: 1
|*****|
juwan1@DESKTOP-C2MLG4B:~/foremost$ foremost -t all -i 2
ERROR: /home/juwan1/foremost/output is not empty
Please specify another directory or run with -T.
juwan1@DESKTOP-C2MLG4B:~/foremost$ foremost -t all -i 2
Processing: 2
|*****|
juwan1@DESKTOP-C2MLG4B:~/foremost$
```

[그림 3] foremost를 사용하여 복구

파일이 2개로 나누어진 것을 1과 2로 나누어 결과값을 output_1과 output_2로 나누어서 복구하였다.

먼저 output_1을 조사해보자. 이 폴더 안에서는 다음과 같은 의심되는 목록들이 발견되었다.



[그림 4] 01776339.png



[그림 5] 01974176.jpg

| 파일명 | 파일 형식 | 파일 용량 | 주석 |
|----------|-------|-------|-------------------|
| 01776339 | png | 52KB | HYDRA |
| 01974176 | jpg | 56KB | HYDRA Rearch Base |

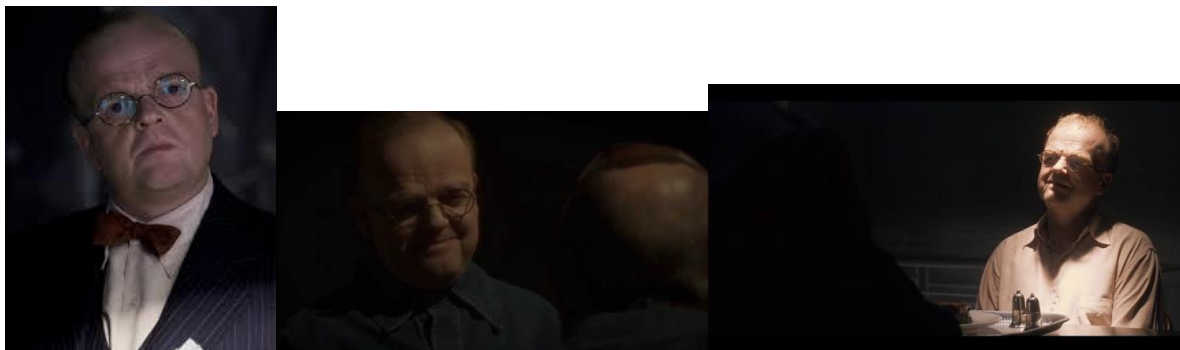
[표 2] 의심되는 파일 리스트

다음과 같은 파일들을 얻을 수 있었는데, 주석은 구글 이미지 검색 기능을 통하여 [HYDRA Research Base | Marvel Cinematic Universe Wiki | Fandom](#) 라는 정보를 얻을 수 있었다. 이를 통하여 문제에서 일어난 범행은 HYDRA에 의하여 이루어졌다고 확신할 수 있다.

다음으로 output_2를 살펴보자.




[그림 6] 00906533.jpg



[그림 7,8,9] (왼쪽부터) 00906667.jpg, 00906675.jpg, 01459906.jpg




[그림 10] 01459779.png


SBB CFF FFS

Ticket-ID 390708058822

| | | | | | | | |
|--|-------|------------------------------|---------|--------------------------------------|-------|---------|---|
| Economy Ticket | | | | Arnim Zola | | | |
| Valid: 2021 | | | | 20.05.1941 | | | |
| 30 | 🕒 | von/de/da/from → nach/a/a/to | | 30 | 🕒 | KL. CL. | |
| 28.03 | 09:21 | Lausanne | → Aosta | 28.03 | 18:23 | 2 | 2 |
| * | * | * | → * | * | * | * | * |
| | | | | | | | |
| Full Price | | | | CHF 26,40 | | | |
| | | | | PCD | | | |
| (L) (SPEZ) (SPEZ) (70) No ordine: 438781486 | | | | No item: 4004 incl. 7.70% IVA/FFS | | | |



[그림 11] 00905815.pdf

| 파일명 | 파일 형식 | 파일 용량 | 주석 |
|----------|-------|-------|-------------------|
| 00906533 | jpg | 67KB | HYDRA Rearch Base |
| 00906667 | jpg | 4KB | HYDRA의 연구원 |
| 00906675 | jpg | 16KB | HYDRA의 연구원 |
| 01459906 | jpg | 30KB | HYDRA의 연구원 |
| 01459779 | png | 64KB | HYDRA의 연구원 |
| 00905815 | pdf | 122KB | 레일패스 티켓 |

[표 3] 얻은 파일 리스트

분석할 정보가 output1에 비하여 많이 보였다. 0090667~01459779의 조금 더 정확한 정보는 구글 이미지 검색을 통하여 https://marvelcinematicuniverse.fandom.com/wiki/Arnim_Zola 를 얻을 수 있었다. 이 인물은 Arnim Zola 라는 사람이었으며 HYDRA의 연구원이라는 사실을 확인할 수 있다. 이를 통하여 이번 사건은 HYDRA의 영향이 있었음을 다시한번 확인할 수 있는 정보가 되었다. 00905815는 범행때 이동수단으로 사용한 티켓으로 예상된다. 이제 얻은 모든 의심되는 파일을 md5로 추출하자.

| Name | In Folder | Current MD5 |
|---------------------|---------------------------------|----------------------------------|
| 00905815.pdf | \\\\wsl.localhost#Ubuntu-20.... | 0DF93F0EAE98A8669AED40C138710E83 |
| 01459779.png | \\\\wsl.localhost#Ubuntu-20.... | 4A442F111021AEA457C8BAACA0E991E9 |
| 01459906.jpg | \\\\wsl.localhost#Ubuntu-20.... | 4A913E0006786D5372BFEBB3A487D878 |
| 00906675.jpg | \\\\wsl.localhost#Ubuntu-20.... | 777695E5F10DD2507D9A6005278678D |
| 00906667.jpg | \\\\wsl.localhost#Ubuntu-20.... | 9FFC15E326EF989DB6D0B08276AF103E |
| 00906533.jpg | \\\\wsl.localhost#Ubuntu-20.... | ADC973854BBE10D17F4B35CE8EC8905 |
| 01974175.jpg | \\\\wsl.localhost#Ubuntu-20.... | 9F96AFD95F63CE272C68C1F83D2748C8 |
| 01776330.png | \\\\wsl.localhost#Ubuntu-20.... | 1DAEFB37062158F450BD1C3AE2CE873D |
| recording.mp3 | C:\\Users\\sim\\OneDrive\\바... | B52421A7547369A770B892026D1B25D0 |
| 2021_04_09T1621.mp3 | C:\\Users\\sim\\OneDrive\\바... | 066C187F3010F62A56C82298116EC3F8 |

[그림 12] 의심되는 파일 md5 추출값

2. 파일 분석

아직 해결하지 못한 recording.mp3를 분석해보자. 먼저 Audacity를 통하여 문제의 파일을 열어보았다.

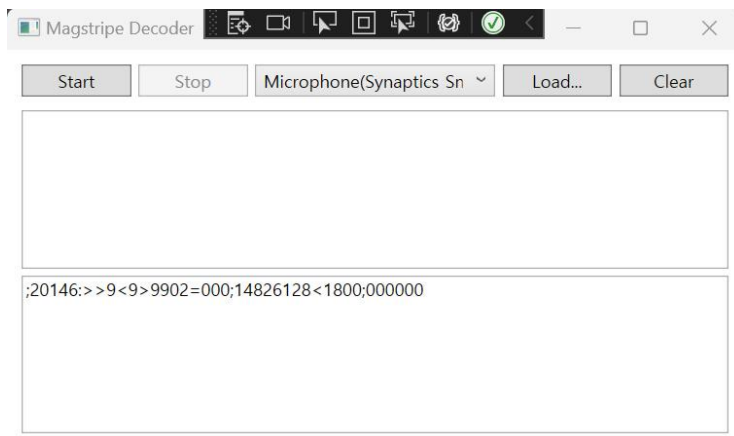


[그림 13] recording.mp3 내부

무언가 기록되어있었다. 이는 자기 스트라이프인데, 다른 장비에서도 신용카드의 정보를 저장하기 위하여 이를 사용한다. 한마디로, **신용카드의 정보를 자기 스트라이프에 저장해서 관리하는 방식을 범인은 사용한 것이다.** 이를 분석하는 magstripe decoder를 사용하기로 하였다. 하지만

System.ArgumentException: 'Unsupported Wave Format'

라는 에러가 계속해서 발생했다. 이는 recording.mp3의 파일 형식의 문제였고 <https://online-audio-converter.com/>를 통하여 wav파일로 형식을 변환하여 진행하였다.

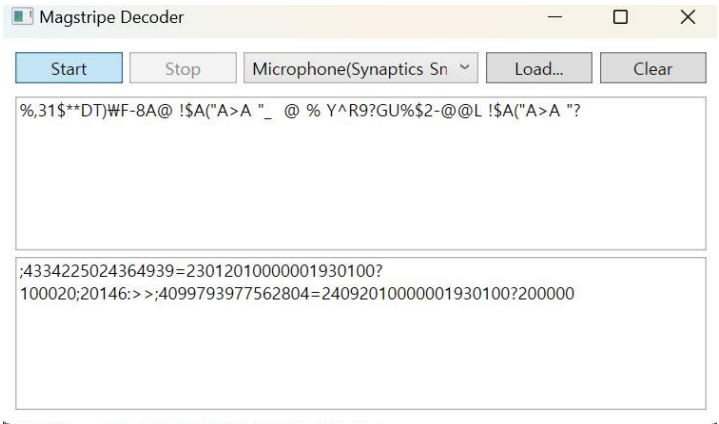


[그림 14] 디코딩 결과

아무런 값도 나오지 않았다. **자기 스트라이프에 신용카드를 저장하는 방식 이외에 다른 방식으로 문제를 접근하는 방법이 떠오르지 않아 스테가노그래피를 의심하였다.**

[WHS-2] .iso

여러 방법으로 오디오를 분석해보다가 **오디오를 뒤집어서** 분석기에 넣었더니 다음과 같은 정보를 확인할 수 있었다.



[그림 15] 오디오를 뒤집어서 실행한 디코딩 결과

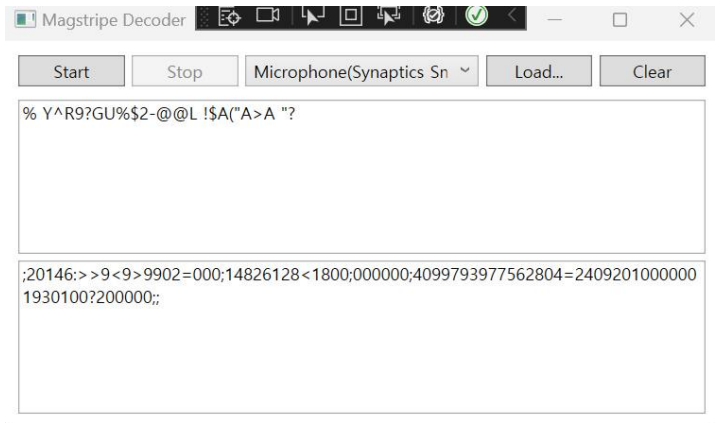
카드 정보 2개를 확인할 수 있었다.

4334 2250 2436 4939 <- 문제에서 주어진 정보가 유출된 카드

4099 7939 7756 2804 <- 정보가 유출됨이 의심되는 새로운 카드

새로운 카드의 정보 또한 확인할 수 있었다.

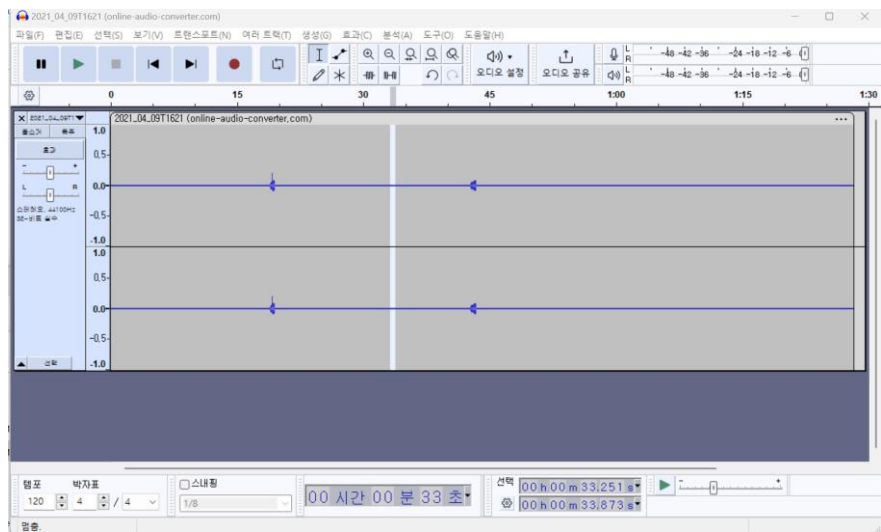
마지막으로 2021_04_09T11621.mp3 또한 분석하여 recording.mp3의 일부임을 확인해보자. 물론 이 파일도 뒤집어서 분석해야 한다.



[그림 16] 2021_04_09T11621 분석 결과

4099 7939 7756 2804만 확인할 수 있다. 이를 통하여 recording.mp3의 일부임을 확인할 수 있다.

Audacity를 통하여 의심을 확신으로 바꾸어보자.



[그림 17] 2021_04_09T1621.mp3 분석

그림 13과 비교하였을 때 이의 일부임을 확인할 수 있다.

5. Flag

1) 파일 수집 단계 md5 값

2021_04_09T1621.mp3 – 066C187F3010F62A56C82298116EC3F8

recording.mp3 – B52421A7547369A770B892026D1B25D0

01776330.png - 1DAEFB3706215BF450BD1C3AE2CE873D

01974175.jpg - 9F96AFD95F63CE272C68C1F83D2748C8

00906533.jpg - ADCD973854BBE10D17F4B35CE8EC8905

00906667.jpg - 9FFC15E326EF989DB6D0B08276AF103E

00906675.jpg - 777695E55F10DD2507D9A6005278678D

01459906.jpg - 4A913E0006786D5372BFEBB3A4B7DB78

01459779.jpg - 4A442F111021AEA457C8BAACA0E991E9

00905815.jpg - 0DF93F0EAE98A8669AED40C138710E83

2) 파일 분석 단계 발견한 CC

4334 2250 2436 4939

4099 7939 7756 2804

6. 별도 첨부

문제 :

On April 9th, 2021, at 16:25, a "Skimming" device was discovered on the ATM of the Swiss Post location in Avenue Piccard, 1015 Lausanne, Switzerland.

The device was discovered when it malfunctioned and detached as a customer withdrew his credit card (CC) from the machine. According to security cameras, it was possible to establish that the device was placed shortly before at 16:20.

The digital forensic unit of the police collected the device and created a physical image of a micro-SD card found inside. The image is provided for download here:

Filename: 1_Skimmer_mSD.zip

SHA2-256: 1c5ad394daa49573f4088a31fb7f6a3f537dbcd092fd5abc8b572ebedbc262

We suspect that data from the CC are recorded in the files present on the memory card.

For reference, the CC number of the client is also provided:

CC Number: 4334 2250 2436 4939

번역 :

2021년 4월 9일 16시 25분 스위스 로잔 1015 애비뉴 피카르에 있는 스위스 포스트 지점 ATM에서 '스키밍' 장치가 발견되었습니다.

고객이 그의 신용카드(CC)를 기계에서 인출하면서 기기가 오작동하고 분리되었을 때 발견되었습니다. 보안 카메라에 따르면, 16시 20분에 기기가 그 직전에 놓여진 것을 확인할 수 있었습니다.

경찰의 디지털 포렌식 부서는 이 장치를 수집하여 내부에서 발견된 마이크로 SD 카드의 실제 이미지를 만들었습니다. 이 이미지는 여기에서 다운로드하기 위해 제공됩니다:

파일명 : 1_Skimmer_mSD.zip

SHA2-256: 1c5ad394daa49573f4088a31fb7f6a3f537dbcd092fd5abc8b572ebedbc262

우리는 CC의 데이터가 메모리 카드에 있는 파일에 기록되어 있다고 의심합니다.

참고로 클라이언트의 CC 번호도 제공됩니다:

CC 번호 : 4334 2250 2436 4939

7. Reference

- <https://lemonpoo22.tistory.com/77>
- https://marvelcinematicuniverse.fandom.com/wiki/Arnim_Zola
- https://marvelcinematicuniverse.fandom.com/wiki/HYDRA_Research_Base
- <https://jacobotarrio.org/2014/how-magnetic-stripe-cards-work.html>
- <https://online-audio-converter.com/>
- <https://namu.wiki/w/%EB%A7%88%EA%B7%B8%EB%84%A4%ED%8B%B1%20%EC%8A%A4%ED%8A%B8%EB%9D%BC%EC%9D%B4%ED%94%84>