DFC 2020 301 Reversing Ransomware 분석 보고서 (각색)

디지털포렌식 김태룡

본문 요약

1. 사건 개요

고객 A의 태블릿 PC가 악성코드에 감염되어 PDF 파일이 암호화되었습니다. A는 악성코드 바이너리와 함께 암호화된 PDF 파일을 분석팀에게 전하였으며, 악성코드는 현재 디렉터리의 모든 PDF 파일을 암호화하고 확장자를 .enc로 변경하는 특징을 가졌다고 덧붙였습니다.

2. 파일 정보

① 파일 정보

순번	파일 명	크기	SHA256
1	dfc_ransom	18.9KB	7DCF40274C80176EF31336267CE39B26B6B2D493DA9C789B03EFAC4B23146615
2	my_secret_file.pdf.enc	1.10MB	9900C142CAE4CE2D30623535D77CC7772FC30C8AB29E3AEA844206D00A8B9E30

3. 분석 결과

① dfc_ransom

√ PDF 대상 랜섬웨어임을 확인하였습니다

② my_secret_file.pdf.enc

√ ARIA 256 알고리즘으로 암호화 된 정황을 확인하였습니다

③ 복원 가능성

- PDF 파일만 대상으로 암호화가 진행되는 정황을 확인하였습니다.
- 암호화 이후 .enc 확장자로 변경되는 정황을 확인하였습니다.
- ARIA 256 알고리즘을 사용하여 IV와 KEY값 입력이 필요 하였습니다.
- IV값으로 "dfc_challenge20" 문자열을 사용한 흔적을 발견하였습니다.
- KEY값으로 암호화 대상 파일 이름의 SHA256 해시 값으로 사용한 흔적을 발견하였습니다.
- ARIA 256 관련 자료가 KISA에 있음을 확인하였습니다.

√ 암호화된 파일의 복호화에 성공하였습니다

4. 결론

- 악성코드는 ARIA 256 알고리즘을 사용하여 "dfc_challenge20" 문자열과 파일 명의 SHA256 해시를 키 값으로 암호화를 진행하는 랜섬웨어이며, PDF만을 암호화하는 특성을 확인하였습니다.
- .enc 확장자로 변경된 암호화된 파일에 대한 복호화 코드 구현에 성공하여 고객 태블릿PC 내 모든 암호화된 PDF 문서를 복원하였습니다.

√ 고객 태블릿 내 암호화된 문서를 모두 복원하였습니다

1. 개요

1-1) 사건 개요

고객 A의 태블릿 PC가 악성코드에 감염되어 PDF 파일이 암호화되었습니다. A는 악성코드 바이너리와 함께 암호화된 PDF 파일을 분석팀에게 전하였으며, 악성코드는 현재 디렉터리의 모든 PDF 파일을 암호화하고 확장자를 .enc로 변경하는 특징을 가졌다고 덧붙였습니다.

1-2) 분석 환경

항목	값	항목	값
OS	Microsoft Windows 10 Home Edition	시스템 종류	64비트 운영 체제
프로세서	Intel(R) Core(TM) i7-1065G7	RAM	16 GB
OS	Ubuntu 20.04 LTS	시스템 종류	64비트 운영 체제
프로세서	가상환경	RAM	4GB

[표 1-1] 분석 환경

1-3) 분석 대상 파일

순번	파일 명	크기	SHA256
1	dfc_ransom	18.9KB	7DCF40274C80176EF31336267CE39B26B6B2D493DA9C789B03EFAC4B23146615
2	my_secret_file.pdf.enc	1.10MB	9900C142CAE4CE2D30623535D77CC7772FC30C8AB29E3AEA844206D00A8B9E30

[표 1-2] 분석 대상

1-4) 분석 도구

도구	버전	용도	제공
HashTab	6.0.0	파일 해시 검증	**Implbits** http://implbits.com/products/hashtab/
HxD	2.4.0.0(x86-64)	파일 Hex 확인 및 편집	**mh-nexus** https://mh-nexus.de/en/hxd/
IDA	7.2.181105	프로그램 디컴파일	**Hex-rays** https://www.hex-rays.com/

1-5) 개발 도구

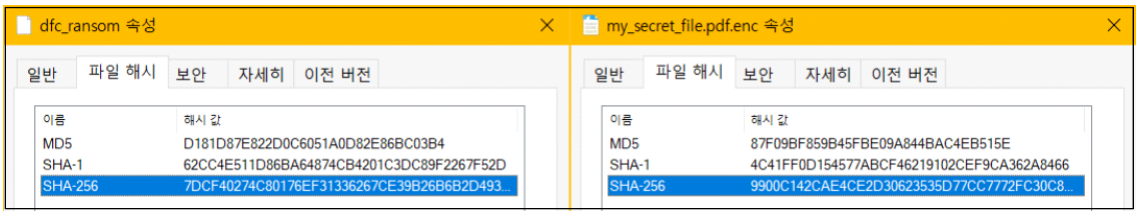
도구	버전	용도	제공
Eclipse	Neon.3 (4.6.3)	IDE	**Eclipse** https://www.eclipse.org/downloads/

2. 분석 내역

2-1) 파일 정보 확인

대상	파일 명	크기	SHA256
현장	dfc_ransom	18.9KB	7DCF40274C80176EF31336267CE39B26B6B2D493DA9C789B03EFAC4B23146615
	my_secret_file.pdf.enc	1.10MB	9900C142CAE4CE2D30623535D77CC7772FC30C8AB29E3AEA844206D00A8B9E30
검증	dfc_ransom	18.9KB	7DCF40274C80176EF31336267CE39B26B6B2D493DA9C789B03EFAC4B23146615
	my_secret_file.pdf.enc	1.10MB	9900C142CAE4CE2D30623535D77CC7772FC30C8AB29E3AEA844206D00A8B9E30

[표 2-1] 채증 당시 현장 기록과 조사 과정에서 추출된 기록 비교자료

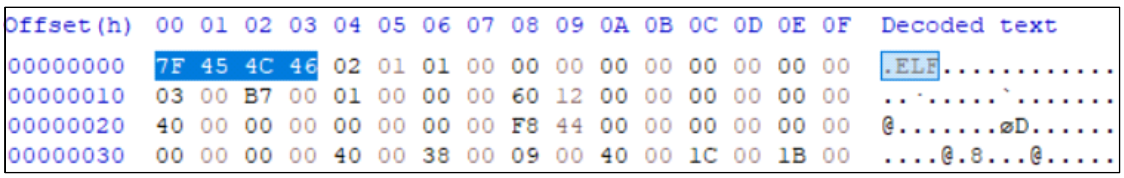


[그림 2-1] Hash Tab을 통한 채증 파일 해시 값 비교 화면

√ 현장 기록과 채증 파일이 동일함을 확인 하였습니다

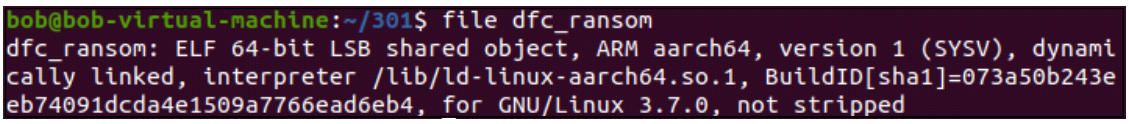
2-2) dfc_ransom 분석

- 대상 멀웨어의 파일 시그니처를 확인한 결과, Linux용 실행파일임을 알 수 있었습니다.



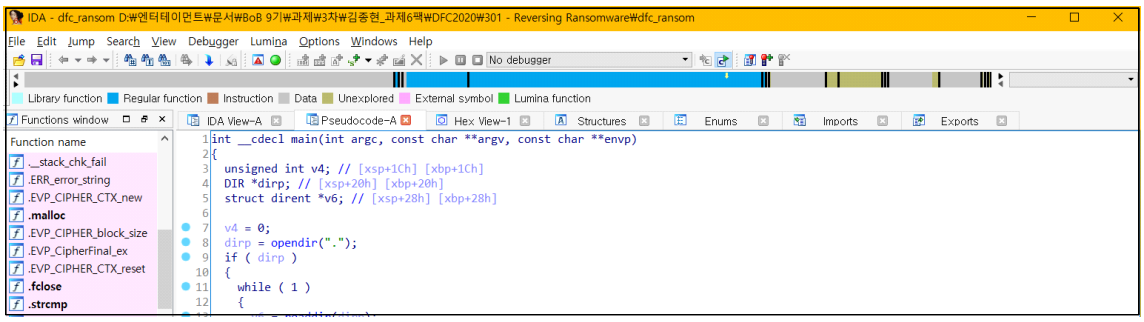
[그림 2-2] ELF 파일임을 확인 한 모습

- Linux 기반 실행파일이므로 멀웨어를 Ubuntu 환경으로 옮겨 세부 정보를 확인하였습니다.



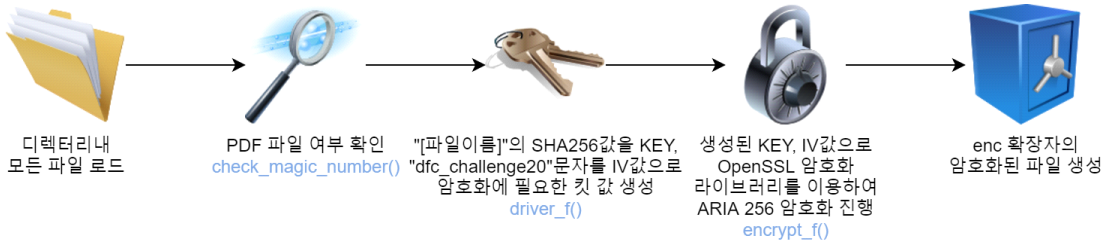
[그림 2-3] 파일에 대한 세부 정보를 확인한 모습

- 64비트 기반 ELF 파일, not stripped 옵션을 통해 디컴파일에 무리가 없음을 확인하였습니다.
- 64비트 기반 ELF이기에 IDAx64를 실행하고, 멀웨어에 대한 디컴파일을 진행하였습니다.



[그림 2-4] 디컴파일 된 멀웨어

- 디컴파일 된 소스코드를 분석한 결과, 아래와 같은 동작 과정을 유추할 수 있었습니다.

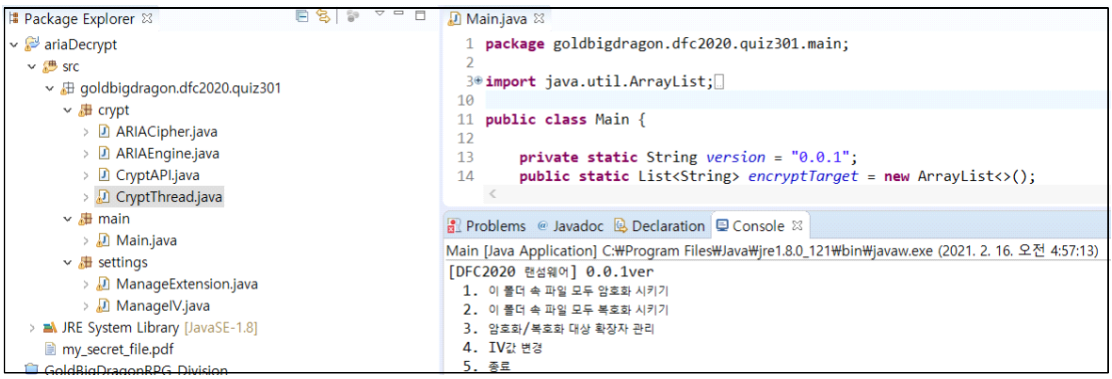


[그림 2-5] dfc_ransom의 암호화 과정

√ dfc_ransom은 ARIA 256 기반 랜섬웨어임을 확인하였습니다

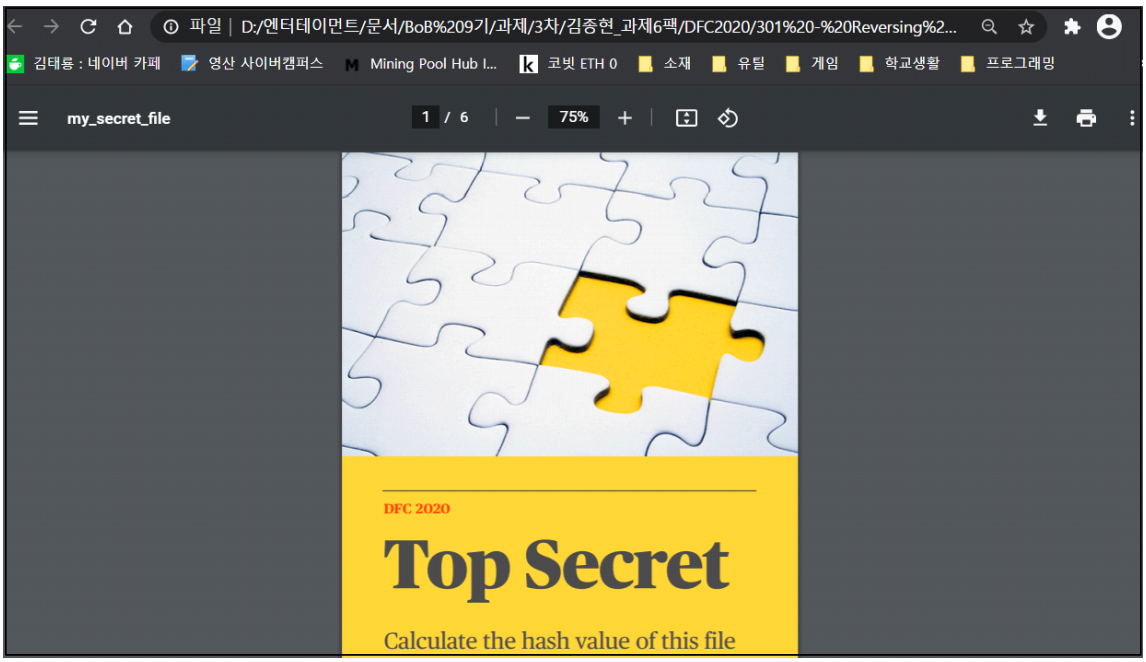
2-3) 복구 코드 작성

- 대상 멀웨어가 사용하는 ARIA 암호 알고리즘은 국내에서 개발 된 알고리즘으로, 관련 정보를 KISA[1]에서 확보할 수 있었습니다.
- 획득한 정보를 토대로 멀웨어의 암호화 기능과 복호화 기능 모두 구현한 Java 코드를 작성하였습니다.
  (소스코드 : https://github.com/GoldBigDragon/DFC2020_301_ARIA_RANSOMWARE)



[그림 2-6] dfc_ransom과 완벽히 동일한 알고리즘으로 암/복호화가 가능한 Java 구문

1) ARIA 암호알고리즘 관련자료 : https://seed.kisa.or.kr/kisa/Board/19/detailView.do



[그림 2-7] 복원된 PDF 문서

- 복원된 PDF 파일의 HASH값
  ① MD5: C5FAD8A98B0969D266378317EA88AA15
  ② SHA-1: B87385897DDE93400620159276BAE46A434A3303
  ③ SHA-256: EBB94106979A9FB2663BC9362F1E16FDFAC612AC5149F25D40668977AB1DC5CD

√ 암호화된 파일의 복호화에 성공하였습니다