

2018년 한국정보보호학회 하계학술대회

CISC-S'18

Conference on Information Security
and Cryptography 2018 Summer

2018. 6. 21일(목) ~ 6. 22일(금)
동신대학교 중앙도서관 1층 동강홀(전남 나주시)

- > 주 최 : 한국정보보호학회
- > 주 관 : 동신대학교
- > 후 원 : 국가정보원, 네이버, 교육부, 한국연구재단,
한국전력공사, 전력거래소,
한국인터넷진흥원, 국가보안기술연구소,
한전KPS(주), 한전KDN(주),
한국방송통신전파진흥원



한국정보보호학회

Korea Institute of Information Security & Cryptology

프로그램 일정표

날짜	시간	행사내용								비고	
6월 21일 (목)	11:30 ~ 13:00	등록 및 리셉션 (중앙도서관 1층)									
		세션 A - 정보전산센터									
	13:00 ~ 14:20	암호화폐/ 블록체인1 좌장:허준범 (고려대학교)	네트워크1 좌장:최대선 (공주대학교)	암호이론1 좌장:한동국 (국민대학교)	IoT보안1 좌장:강승호 (동신대학교)	관리정책 교육1 좌장:김태희 (동신대학교)	컴퓨터보안1 좌장:이만희 (한남대학교)	개인정보보호 좌장:신상욱 (부경대학교)	CPS보안 좌장:서정택 (순천향대학교)		
	14:20 ~ 14:30	Break Time									
		세션 B - 정보전산센터									
	14:30 ~ 16:10	암호화폐/ 블록체인2 좌장:임을규 (한양대학교)	네트워크2 좌장:김광조 (카이스트)	암호이론2 좌장:이동훈 (고려대학교)	IoT보안2 좌장:이임영 (순천향대학교)	관리정책 교육2 좌장:이경현 (부경대학교)	취약점분석 좌장:박창섭 (단국대학교)	산업보안 좌장:오희국 (한양대학교)	악성코드 좌장:하재철 (호서대학교)		
	16:10 ~ 16:20	Break Time									
	16:20 ~ 16:50	중 앙 도서관 1층 동강홀	초청강연 : Post Quantum Crypto 표준화 추진 현황 및 KISA의 역할(한국인터넷진흥원)								
	16:50 ~ 17:00		특별강연 : 연구 윤리 및 출판								
	17:00 ~ 17:30		개회식 / 사회 : 운영위원장 이동휘 교수				행안부 장관상, 한국인터넷진흥원장상, 한국전력공사사장상, 한국전자통신연구원장상, 국가보안연구소장상, 학회장상(암호분야 특별상), 학회장상, 여성과학자상				
			개회사 동신대학교 김필식 총장 환영사 한국정보보호학회 홍만표 학회장 축사 한국인터넷진흥원 김석환 원장 국가보안기술연구소 조현숙 소장 한국전력공사 김종갑 사장	우수논문 시상식							
			경품추천								
	17:30 ~ 18:00	이동									
	18:00 ~ 20:00	만찬 : 빚가람 호텔 만찬홀 (구:M-STAY Hotel) : 사회 서정택 교수									
6월 22일 (금)	10:00 ~ 10:30	등록 (정보전산센터 1층)									
		세션 C - 정보전산센터									
	10:30 ~ 11:50	암호화폐/ 블록체인3 좌장:유일선 (순천향대학교)	암호화폐/ 블록체인4 좌장:현상원 (조선대학교)	관리정책 교육3 좌장:김인석 (고려대학교)	관리정책 교육4 좌장:장항배 (중앙대학교)	컴퓨터보안2 좌장:서승현 (한양대학교)	여성과학자 + invited talk 좌장:심미나 (성결대학교)	기타 좌장:이옥연 (국민대학교)	26개 논문 한국전력 공사 견학		
	12:00 ~ 13:00	중식(교직원식당)								중식 (한전구내식당)	
	13:00 ~ 14:30									한국전력거래소 견학	
	14:30 ~ 16:00									한국인터넷 진흥원 견학	
	16:00 ~ 16:30	KTX, SRT 나주역 이동 후 종료									

306호	발표 논문
관리정책 교육 1	악성코드 감염 예방을 위한 보안정책 수립사례 분석 이준희
	4차 산업혁명 환경에서 Trust Service 제공을 위한 사회과학적 정보보호 기반조성 연구 박상호, 나원철, 장항배
	VR과 IoT를 활용한 전공탐색 기반의 대학 홍보전략 최경호, 김병석, 전영재, 진용기, 이동휘
좌장: 김태희 교수 (동신대학교)	

307호	발표 논문
컴퓨터보안 1	안드로이드 클립보드를 활용한 악의적 e-mail 탐지 기술 이효진, 장수인
	기호실행을 이용한 바이너리 난독화 해제 기술 연구 주하중, 김민재, 엄홍열
	Shannon 엔트로피 값 분석을 통한 파일 암호화 판별에 관한 연구 고주성, 곽진
	모바일에서의 애플리케이션 접근 제어 메커니즘 분석 김이진, 최형기
좌장: 이만희 교수 (한남대학교)	

B01-B호	발표 논문
개인정보보호	모바일 앱 개인정보 유출과 최신 TLS 적용 필요성 연구 김성진, 허준범
	양자 컴퓨팅 환경에 안전한 생체 인증 우주, 이동
	개인정보의 비식별 처리 시 발생가능한 문제점 분석 및 대응방안 제시 한경수, 류지민, 서정택
	Mixnet 적용을 통한 자율주행차 운영환경 프라이버시 보호방안 연구 강기완, 서정택
좌장: 신상욱 교수 (부경대학교)	

B06-B호	발표 논문
CPS보안	스마트 가로등 환경에서의 보안 설계 및 실험 오진혁, 한주홍, 양광열, 이옥연
	스마트시티 서비스에 대한 사이버공격 피해사례 및 파급효과 분석 김호, 박영, 백인홍, 신바야르, 서정택
	안전한 스마트공장 연계를 위한 크로스 도메인 보안 방법 김기현, 박해용, 안혜선, 김일용, 하재철
	국내 스마트시티 인프라 사이버보안 취약점 분석 및 대응방안 제시 이성원, 송진우, 서정택
좌장: 서정택 교수 (순천향대학교)	

2018 한국정보보호학회 하계학술대회

A6 컴퓨터보안 1

Ⅱ 이 만 희 (한남대학교) Ⅱ

- 안드로이드 클립보드를 활용한 악의적 e-mail 탐지 기술
이효진, 장수인
- 기호실행을 이용한 바이너리 난독화 해제 기술 연구
주하중, 김민재, 염흥열
- Shannon 엔트로피 값 분석을 통한 파일 암호화 판별에 관한 연구
고주성, 곽 진
- 모바일에서의 애플리케이션 접근 제어 메커니즘 분석
김이진, 최형기

Shannon 엔트로피 값 분석을 통한 파일 암호화 판별에 관한 연구

고주성*, 박진**

*아주대학교 컴퓨터공학과 정보보호응용및보증연구실

**아주대학교 사이버보안학과

Determining File Encryption Status through Shannon Entropy Criteria Analysis

Ju-Seong Ko*, Jin Kwak**

*ISAA Lab., Department of Computer Engineering, Ajou University.

**Department of Cyber Security, Ajou University.

요 약

최근 안드로이드 환경에서 랜섬웨어로 인한 피해를 방지하기 위해 악의적인 앱의 암호화 동작을 실시간으로 탐지할 수 있는 방안에 대한 연구가 진행되고 있다. 암호화 동작을 실시간으로 탐지하기 위한 방안 중 하나는 파일의 암호화 여부를 실시간 모니터링하는 것으로 암호화 여부 판단을 위해 Shannon 엔트로피 값을 이용할 수 있다. 하지만 Shannon 엔트로피를 이용한 기존 연구에서는 엔트로피 값의 기준을 명확히 하지 않아 실제 환경에서 적용은 어려운 실정이다. 따라서 본 논문에서는 다양한 파일 종류 별 Shannon 엔트로피 값 기준을 제시하여 파일 암호화 여부 판별의 정확성을 높이하고자 한다.

I. 서론

사용자의 중요 데이터를 암호화한 후 이를 이용해 이득을 취하는 랜섬웨어는 2015년 4월 광범위하게 유포되기 시작하였고, 전 세계적으로 많은 피해를 발생시켰다[1]. 한국인터넷진흥원은 2017년 분기별 악성코드들 중 랜섬웨어가 모든 분기에서 가장 높은 발생 수를 기록했다고 분석하였으며, 해당 수치에는 안드로이드 기기를 대상으로 한 공격도 포함되었다[2].

랜섬웨어에 감염되어 데이터가 암호화된 경우 이를 복구하기 어렵기 때문에 사전에 예방할 수 있는 방안이 필요하다. 이를 위해 안드로이드 환경에서 랜섬웨어 앱을 실시간 탐지해낼 수 있는 방안에 대한 연구가 활발히 진행 중이다[1].

Jing Chen 등의 연구[3]에서는 특정 앱이 기기 내의 데이터를 암호화할 때 사용자가 암호

화 행동을 인지하고 있는지, 그리고 암호화로 인해 발생하는 결과를 파악하고 있는지의 여부로 랜섬웨어 앱과 정상 암호화 기능 앱을 구분하고 있다.

해당 논문에서 제시한 과정 중 첫 단계에서는 보호되어야 할 파일들을 모니터링 대상으로 정의하고, 파일의 엔트로피 값을 측정하여 해당 파일이 암호화되었는지의 여부를 판단한다[4]. 하지만 안드로이드 기기 내에 보호되어야 할 파일의 종류는 다양하기 때문에 암호화 여부의 기준이 될 엔트로피 값을 파일의 종류에 따라 다르게 설정해야 할 필요가 있다.

본 논문의 2장에서는 랜섬웨어 앱 실시간 탐지 방안, 랜섬웨어와 관련된 정보, 그리고 엔트로피 값 측정을 위한 관련 연구를 다룬다. 3장에서는 측정을 위해 구현한 시스템에 대해 설명하며, 4장에서는 측정 결과 분석을 통해 파일 종류별 기준 값을 제시한다. 마지막으로 5장에서는 향후 연구에 대해 언급하며 결론을 맺는다.

이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2017R1E1A1A01075110).

II. 관련 연구

2.1 랜섬웨어 앱 실시간 탐지 방안

Jing Chen 등의 연구[3]에서는 정상 암호화 기능 앱과 랜섬웨어 앱을 구분하기 위해 현재 수행 중인 암호화 과정을 사용자가 인지하고 있는지 판단한다. 이 판단을 위해 3단계의 분석 과정을 거치는데, 3단계의 내용은 [표 1]과 같다.

[표 1] 랜섬웨어 앱 실시간 탐지 방안 단계

단계	분석 내용
1	모니터링 대상 데이터의 암호화 여부
2	사용자의 암호화 기능 인지 여부
3	사용자와 암호화 앱의 상호작용 여부

단계 1에서는 모니터링 중인 데이터가 암호화된 파일인지를 판단한다. 이를 위해 shannon 엔트로피를 이용하는데, 데이터의 엔트로피 값이 높아질 경우 암호화된 것으로 판단하고 다음 단계를 시작하게 된다[3].

2.2 shannon 엔트로피

shannon 엔트로피는 데이터 파일 내 값들의 분포를 이용해 암호화 여부를 판단한다. 암호문 내의 값들은 평문에 비해 균등한 분포를 가진다는 점을 이용해 특정 파일이 암호화되었는지 판단한다. 이는 암호화 과정에서 발생하는 혼돈 효과를 이용한 것이다. 엔트로피 값 e 는 다음과 같이 계산할 수 있다[4].

$$e = \sum_{i=0}^{255} P_{B_i} \log_2 \frac{1}{P_{B_i}}, \quad P_{B_i} = \frac{F_i}{totalbytes}$$

(F_i 는 파일 내 값 i 의 개수, total bytes는 파일의 크기)

파일 내의 값 분포가 0x00부터 0xFF까지 모두 균등한 경우, e 는 최대값인 8이 된다.

2.3 랜섬웨어에서 사용되는 암호 알고리즘

2017년 1월, 기존 윈도우용 킬디스크 악성코드의 변종인 리눅스용 킬디스크가 발견되었다. 파일 암호화 방식은 윈도우에서 AES와 RSA를

이용했던 점과 달리 리눅스에서는 Triple-DES 방식을 이용하였다[5].

2017년 5월, 전 세계에서 워너크립터 랜섬웨어의 감염 사례가 보고되었다. 랜덤으로 생성한 AES 키를 이용해 AES_128 CBC 방식으로 데이터를 암호화한 후 RSA 공개키로 AES 키를 암호화하는 방식을 이용하였다[6]. AES_128 CBC 방식은 인코더 랜섬웨어에서도 사용되었다[5].

2017년 5월, 제프 랜섬웨어가 네커스 봇넷을 이용한 스팸 메일을 통해 국내에 급속도로 유포되고 있는 정황이 포착되었다. API를 이용해 랜덤한 키를 생성하였고, AES_256 CBC 방식으로 암호화하였다.

[표 2]는 주요 랜섬웨어 별로 사용한 암호 알고리즘을 정리한 것이다.

[표 2] 주요 랜섬웨어 별 암호 알고리즘

No	랜섬웨어 명	암호 알고리즘
1	킬디스크	Triple-DES CBC
2	워너크립터, 인코더	AES_128 CBC
3	제프	AES_256 CBC

2.4 랜섬웨어의 주요 타겟 파일

SOMANSA는 랜섬웨어가 문서 파일과 DB 파일이 존재하는 폴더를 암호화 대상으로 삼고 있으며, 시스템 폴더와 결제 유도에 사용되는 Tor 폴더들은 제외 대상으로 포함되었다고 분석하였다[8]. 또한 Nolen Scaife 등의 연구[4]에서는 랜섬웨어 앱들이 pdf, docx, pptx 등 문서 파일에 가장 많은 접근을 수행했다는 결과를 도출하였다.

2.5 CrypTool

CrypTool은 다양한 암호 알고리즘들을 직접 시연해볼 수 있는 오픈소스 프로젝트로 다양한 해시함수, 키 교환 프로토콜, 그리고 블록 및 공개키 암호 등 400개 이상의 알고리즘을 지원하고 있다. 알고리즘의 입력과 출력으로 문자열, 바이트 값, 파일 등 형태의 제한 없이 이용할 수 있다[9].

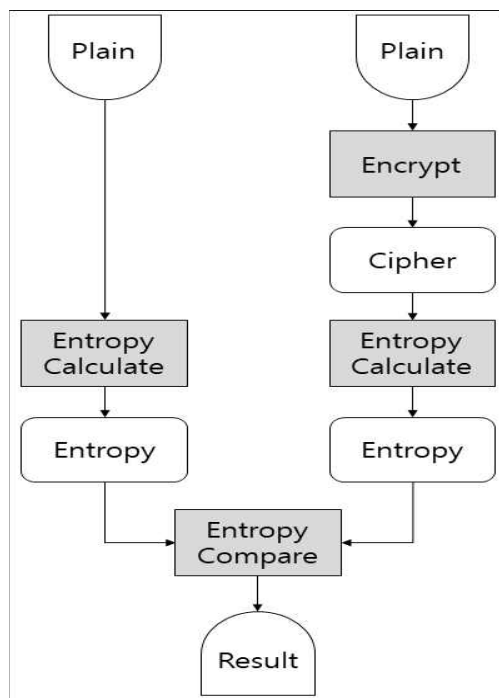
III. 측정 방안 및 구현

3.1 엔트로피 값 종류 별 기준의 필요성

Jing Chen 등의 연구[3] 중 단계 1에서는 모니터링 중인 데이터의 shannon 엔트로피 값이 높을 경우 암호화된 파일로 간주하였다. 하지만 엔트로피 값이 높다는 기준이 명확하지 않아 이에 대한 기준 설정이 필요하다. 또한 Nolen Scaife 등의 연구[4]에서는 파일들의 특성이 다르기 때문에, 파일 종류 별로 shannon 엔트로피 값을 형성하는 범위가 다르다는 것을 언급하였다.

따라서 파일 종류 별 암호화 전·후의 엔트로피 값 비교를 통해 암호화 여부를 판단할 수 있는 파일 종류 별 기준을 제시해야 한다.

3.2 측정 방안



(그림 1) 엔트로피 값 비교과정

랜섬웨어 앱이 많이 접근하는 문서 파일들을 대상으로 암호화 전·후의 엔트로피 값 비교를 수행한다. (그림 1)은 평문과 암호문의 엔트로피 값 비교를 위한 순서도를 나타낸 것이다. Encrypt와 Entropy Calculate에 관한 내용은 각각 3.3, 3.4절에서 구체적으로 다룬다.

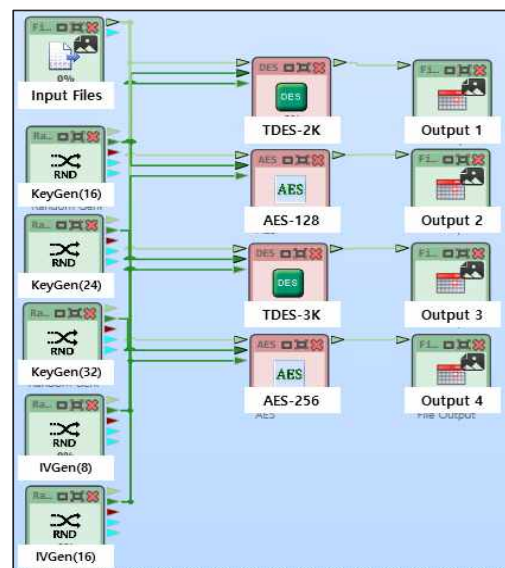
분석 대상 파일 종류는 pdf, pptx, docx, xlsx 총 4가지이며, 각 종류 별로 50개의 평문 데이터를 수집하였다. 비교에 이용할 암호 알고리즘은 랜섬웨어에서 주로 이용되었던 알고리즘들인 TDES-2K(Triple DES 2key), TDES-3K(Triple DES 3key), AES_128, AES_256 총 4가지로 수행하며 모두 CBC 모드를 이용한다.

[표 3]은 분석에 이용될 문서 파일, 암호 알고리즘 종류를 정리한 것이다.

[표 3] 분석 대상 파일 및 암호 알고리즘

항목	분석 대상
문서 파일	pdf, pptx, docx, xlsx
암호 알고리즘	TDES-2K, TDES-3K, AES-128, AES-256

3.3 암호화 수행



(그림 2) CrypTool을 이용한 암호화 구현

(그림 2)는 (그림 1)의 Encrypt 단계를 구체화한 것이다. CrypTool 2.1(stable)을 이용하였으며, 파일 종류 별 구분을 위해 (그림 2)와 같은 워크스페이스를 4개 만들었으며, 각 워크스페이스는 Input Files와 Output 외에 모두 동일한 조건을 가진다.

각 워크스페이스는 암호 알고리즘으로 TDES-2K, TDES-3K, AES-128, AES-256을 포함하고 있다. 암호 알고리즘의 입력으로는 Input Files, KeyGen(N), IVGen(N)을 가지는데

Input Files는 각 종류 별 50개의 파일, KeyGen(N)은 N-byte 크기의 키 생성, IVGen(N)은 N-byte 크기의 Initial Vector 생성을 의미한다. 암호 알고리즘의 출력으로는 Output이 있는데, 이는 각 대응되는 암호 알고리즘의 수행 결과인 암호문이다. [표 4]는 각 위크스페이스에 포함된 항목에 대한 설명을 정리한 것이다.

[표 4] 구현 항목 설명

구현 항목	수행 내용
Input Files	특정 종류에 속하는 파일 50개
Output N	대응되는 알고리즘의 암호문
KeyGen(N)	N-byte 크기의 키 생성
IVGen(N)	N-byte 크기의 IV 생성

3.4 엔트로피 계산 및 비교

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00000000	37	2E	39	39	39	34	37	0D	0A	37	2E	39	39	39	39	7.999947..7.9999
00000010	32	39	0D	0A	37	2E	39	39	39	37	32	0D	0A	37	2E	29..7.999972..7.
00000020	39	39	39	39	39	33	0D	0A	37	2E	39	39	39	35	37	38
00000030	0D	0A	37	2E	39	39	39	35	33	30	0D	0A	37	2E	39	39
00000040	39	39	37	39	0D	0A	37	2E	39	39	39	31	32	0D	0A	9979..7.999912..
00000050	37	2E	39	39	39	36	37	0D	0A	37	2E	39	39	39	37	7.999967..7.9997
00000060	38	35	0D	0A	37	2E	39	39	39	32	33	0D	0A	37	2E	85..7.999923..7.
00000070	39	39	39	39	33	33	0D	0A	37	2E	39	39	39	31	33	999933..7.999913
00000080	0D	0A	37	2E	39	39	37	37	33	0D	0A	37	2E	39	39	..7.999773..7.99
00000090	36	38	31	38	0D	0A	37	2E	39	39	36	34	37	35	0D	0A
000000A0	37	2E	39	39	36	39	39	35	0D	0A	37	2E	39	39	39	7.999995..7.9999
000000B0	32	31	0D	0A	37	2E	39	39	39	30	37	0D	0A	37	2E	21..7.999907..7.
000000C0	39	39	36	32	33	0D	0A	37	2E	39	39	39	35	30		999923..7.999950
000000D0	0D	0A	37	2E	39	39	37	34	31	0D	0A	37	2E	39	39	..7.999741..7.99
000000E0	38	35	33	30	0D	0A	37	2E	39	39	38	34	39	36	0D	0A
000000F0	37	2E	39	39	39	30	38	31	0D	0A	37	2E	39	39	38	39
00000100	35	36	0D	0A	37	2E	39	39	39	34	31	32	0D	0A	37	2E
00000110	39	39	39	36	36	39	0D	0A	37	2E	39	39	39	33	34	999969..7.999934
00000120	0D	0A	37	2E	39	39	39	36	38	39	0D	0A	37	2E	39	39
00000130	39	37	30	31	0D	0A	37	2E	39	39	39	30	38	0D	0A	9701..7.999908..
00000140	37	2E	39	39	39	37	31	33	0D	0A	37	2E	39	39	39	7.999713..7.9999
00000150	31	34	0D	0A	37	2E	39	39	39	33	33	39	0D	0A	37	2E
00000160	39	39	39	39	32	38	0D	0A	37	2E	39	39	39	32	32	999928..7.999282
00000170	0D	0A	37	2E	39	39	39	39	30	31	0D	0A	37	2E	39	39
00000180	39	38	35	35	0D	0A	37	2E	39	39	38	31	34	0D	0A	9855..7.999814..
00000190	37	2E	39	39	39	30	32	0D	0A	37	2E	39	39	39	38	7.999902..7.9999
000001A0	36	30	0D	0A	37	2E	39	39	39	37	38	39	0D	0A	37	2E
000001B0	39	39	39	38	33	39	0D	0A	37	2E	39	39	39	36	30	34
000001C0	0D	0A	37	2E	39	39	39	35	35	0D	0A	37	2E	39	39	..7.999955..7.99
000001D0	39	37	39	31	0D	0A	37	2E	39	39	38	32	31	0D	0A	9791..7.999921..
000001E0	37	2E	39	39	39	38	30	38	0D	0A	37	2E	39	39	39	38
000001F0	35	33	0D	0A												53..

(그림 3) 엔트로피 계산 결과

(그림 3)은 (그림 1)의 Entropy Calculate를 수행한 예이다. Entropy Calculate는 2.2절의 수식을 구현함으로써 구체화할 수 있다. 각 파일 종류 별로 (그림 2)의 Input Files, Output 1-4에 해당하는 파일에 엔트로피 계산을 수행하기 때문에 총 5개의 엔트로피 값 결과 파일이 나오게 되며, 각 결과 파일에는 50개의 엔트로피 값이 포함된다.

엔트로피 값 비교는 각 파일 종류 별로 평균 엔트로피 값과 4개의 암호문 엔트로피 값을 비교하여 수행한다.

IV. 수행 결과 및 기준 제시

4.1 수행 결과 및 분석



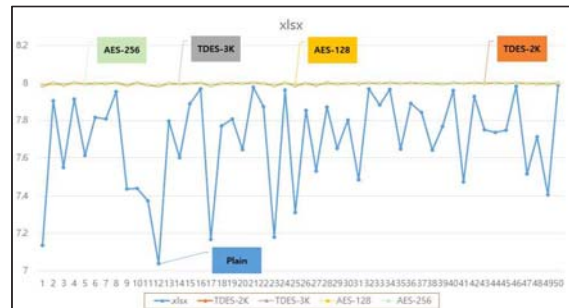
(그림 4) pdf 대상 수행 결과



(그림 5) pptx 대상 수행 결과



(그림 6) docx 대상 수행 결과



(그림 7) xlsx 대상 수행 결과

(그림 4)-(그림 7)은 각각 pdf, pptx, docx,.xlsx에 대한 엔트로피 값 비교 결과를 그래프로 나타낸 것으로 x축은 파일 번호, y축은 엔트로피 값이다. 위 결과를 분석한 정보는 다음 두 가지이다.

① 평문 - 평문 간 엔트로피 값 비교

4가지 수행 결과 모두 개별 파일에 따라 상이한 엔트로피 값을 가지지만, pdf와 pptx 파일은 대체적으로 높은 엔트로피 값을 가지는 것을 알 수 있다. 따라서 각 파일 종류 별로 개별적인 엔트로피 값 기준을 제시해야 한다.

② 평문 - 암호문 간 엔트로피 값 비교

4가지의 암호 알고리즘에서 모든 암호문의 엔트로피 값이 8에 근접하였음을 알 수 있다.

[표 5]는 파일 종류 별 엔트로피 최소/최대값을 정리한 것이다.

[표 5] 파일 종류 별 엔트로피 최소/최대값

분석 대상		최소값	최대값
pdf	Plain	7.557820	7.988754
	TDES-2K	7.995848	7.999979
	TDES-3K	7.996367	7.999981
	AES-128	7.996475	7.999979
pptx	AES-256	7.996759	7.999977
	Plain	7.489538	7.993521
	TDES-2K	7.997166	7.999985
	TDES-3K	7.996879	7.999985
docx	AES-128	7.997184	7.999984
	AES-256	7.997032	7.999985
	Plain	7.133540	7.911868
	TDES-2K	7.927723	7.999979
xlsx	TDES-3K	7.922660	7.999978
	AES-128	7.923519	7.999979
	AES-256	7.926397	7.999979
	Plain	7.038296	7.968575
	TDES-2K	7.983629	7.999924
	TDES-3K	7.981825	7.999927
	AES-128	7.981290	7.999928
	AES-256	7.982834	7.999934

4.2 엔트로피 값 기준 제시

실제 환경에서 암호화된 파일에 대해 어떤 암호 알고리즘으로 암호화되었는지는 알 수 없다. 따라서 평문 엔트로피의 최대값과 전체 암호문 엔트로피의 최소값을 비교하여 엔트로피 값 기준을 제시한다. [표 6]은 파일 별로 평문 엔트로피의 최대값, 암호문 엔트로피의 최소값

을 비교하여 기준 값을 제시한 것이다.

[표 6] 엔트로피 값 비교 및 기준 제시

종류	평문 최대	암호문 최소	기준
pdf	7.988754	7.995848	7.99
pptx	7.993521	7.996879	7.996
docx	7.911868	7.922660	7.92
xlsx	7.968575	7.981290	7.98

위 기준을 적용한 예로, 한 pdf 파일의 엔트로피 값이 기준 값인 7.99보다 큰 경우에는 해당 파일이 암호화된 것으로 간주한다.

V. 결론

본 논문에서는 랜섬웨어 앱 실시간 탐지 방안에서 파일의 암호화 여부를 파악하기 위한 암호화 전·후의 shannon 엔트로피 값을 분석하였다. 파일 종류 별로 형성하고 있는 엔트로피 값이 다르기 때문에 종류 별로 기준이 주어져야 함을 확인하였고, 그에 따라 종류 별 기준을 제시하였다.

하지만 종류 별 수집 데이터 수는 50개씩으로 기준에 대한 정확성이 미흡할 수 있다. 또한 특정 파일들의 경우 암호화되지 않았음에도 기준 엔트로피보다 높은 엔트로피 값을 가질 수 있다.

따라서 향후 연구에서는 많은 수의 데이터 집합을 가지고, 특정 조건의 파일에 대해서도 적용할 수 있는 더 정확한 기준을 마련하고, 이를 랜섬웨어 앱 실시간 탐지에 적용할 수 있도록 해야 한다.

[참고문헌]

- [1] 한국인터넷진흥원, “'16년 랜섬웨어 동향 및 '17년 전망”, 2017.01.
- [2] 한국인터넷진흥원, “2017년 4분기 사이버 위협 동향 보고서”, 2018.01.
- [3] Jing Chen, Chiheng Wang, Ziming Zhao, Kai Chen, Ruiying Du, Gail-Joon Ahn, “Uncovering the Face of Android Ransomware: Characterization and Real-Time Detection”, IEEE Transaction on Information

Forensics and Security, Vol.13 No.5, 2017.12.

- [4] Nolen Scaife, Henry Carter, Patrick Traynor, Kevin R.B. Butler, “CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data”, 2016 IEEE 36th International Conference on Distributed Computing Systems, 2016.06.
- [5] 안랩 시큐리티대응센터(ASEC) 분석팀, “‘리눅스 랜섬웨어’ 본격화되나”, AhnLab 보안 이슈게시판 “http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&seq=26564”, 2017.07.
- [6] 안랩 시큐리티대응센터(ASEC) 분석팀, “위너크립터 랜섬웨어 분석 보고서”, Analysis Report, 2017.05.
- [7] 안랩 시큐리티대응센터(ASEC) 분석팀, “[VOL.87] 2017년 2분기 주요 보안 이슈”, ASEC 리포트, 2017.07.
- [8] SOMANSA, “MALWARE ANALYSIS REPORT No.7 Cerber 랜섬웨어 분석보고서(Rig EK)”, 악성코드 리포트, 2016.12.
- [9] <https://www.cryptool.org/de/cryptool2>