

2018 춘계학술발표대회 논문집

일시 2018년 4월 27일(금) ~ 28일(토)

장소 제주대학교 아라캠퍼스 아라컨벤션홀

주최 사단법인 한국인터넷정보학회

주관 제주대학교

후원 네이버(주), (주)아이티센, (주)LGCNS,
(주)큐브시스템, LG히다씨(주), (주)워드바이스에세이리뷰



B-2-3	본질적 속성값을 이용한 한국어 감성사전 구축에 관한 실증연구	79
	류재관, 이건창(성균관대)	
B-2-4	스파크 분산 환경 기반 프라이버시 보호 빅 데이터 배포 시스템 개발	81
	김대호, 김태수, 유훈, 김종욱(상명대)	
B-2-5	Wasserstein CNN을 이용한 3D 물체 분류	83
	지명근, 전준철(경기대)	
B-2-6	★ 컨볼루션 신경망을 통한 2차원 키포인트 탐지 기반 3차원 인간 자세 추정 방법	85
	박서희, 지명근, 전준철(경기대)	
B-2-7	HMD를 활용한 가상현실 FPS게임 콘텐츠 개발	87
	이성진, 김민상, 홍민(순천향대)	
B-2-8	거리 정규화 레벨셋을 이용한 의료영상 분할	89
	윤희진, 지명근, 전준철(경기대)	

C-1. 인터넷보안 1 (좌장: 김문성 박사(특허청))

C-1-1	안드로이드 랜섬웨어 동향 분석	95
	서승희, 김역, 이창훈(서울과학기술대)	
C-1-2	CyberSecurity Framework와 ISO27001을 비교한 보안 통제 연구	97
	최중우, 원동호(성균관대)	
C-1-3	☆ 차세대 ITS 환경에서 익명성을 보장하기 위한 블록체인 활용 방안	99
	최석준, 곽진(아주대)	
C-1-4	최신 인증 암호화 기술의 안전성 분석	101
	조민정, 공성현, 이창훈(서울과기대)	
C-1-5	안드로이드 환경에서의 랜섬웨어 실시간 탐지 개선 방안에 관한 연구	103
	고주성, 곽진(아주대)	
C-1-6	사이버 레인지 훈련 지원 방안 연구	105
	김대식, 김용현(국방과학연구소)	

안드로이드 환경에서의 랜섬웨어 실시간 탐지 개선 방안에 관한 연구

고주성*, 궤 진**

*아주대학교 컴퓨터공학과 정보보호응용및보증연구실

**아주대학교 사이버보안학과

e-mail : *jsko.isaa@gmail.com, **security@ajou.ac.kr

A Study on the Enhancement of the Real-Time Detection for Android Ransomware

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 위한 연구가 활발히 진행되고 있다. 랜섬웨어로 인한 피해를 사전에 방지하기 위해서는 실행 중인 악의적인 앱의 암호화 동작을 실시간으로 탐지할 수 있어야 한다. 기존 연구에서는 암호화 동작 여부를 판단한 후 정상 암호화 기능 앱과 랜섬웨어를 구분하는 단계를 가지고 있다. 하지만 탐지 대상으로 하는 Application Set에 따라 정상 암호화 기능 앱과 랜섬웨어를 구분한 결과의 정확성이 달라질 수 있다. 따라서 본 논문에서는 정상 암호화 기능 앱과 랜섬웨어를 더 정확하게 구분할 수 있는 개선 방안을 제안한다.

1. 서 론

전 세계적으로 많은 피해를 일으킨 랜섬웨어는 2015년 4월 광범위하게 유포되기 시작하였다. 2016년에는 전년대비 86.8% 증가한 수치를 기록하였으며 모바일환경을 대상으로 한 랜섬웨어 유포 방식 등을 통해 랜섬웨어 피해 영역의 확대를 예상하였다[1]. 실제로 2017년 분기별 악성코드 종류에서는 모든 분기에서 랜섬웨어가 1위를 차지하였으며 안드로이드 기기를 암호화한 후 금전을 요구하는 등의 공격들이 포함되었다. 로키봇, NotPetya의 경우 본래 목적이었던 데이터 파괴가 아닌 랜섬웨어 기능으로 큰 피해를 발생시켰다[2].

랜섬웨어로 인해 데이터가 암호화된 경우 복구하기 어렵기 때문에 사전 예방이 무엇보다 중요하며 이를 위해 안드로이드 환경에서의 랜섬웨어 앱 실시간 탐지에 대한 연구가 활발히 진행 중이다[1]. 실시간 탐지 방안의 경우 탐지 대상이 랜섬웨어 앱인지 또는 정상 암호화 기능 앱인지의 여부를 판별할 수 있어야 한다. 기존 연구에서는 특정 앱이 암호화 기능을 수행할 때 사용자가 이를 인지하고 있는지의 여부로 랜섬웨어 앱과 정상 암호화 기능 앱을 구분하고 있다. 랜섬웨어 앱으로 간주될 경우, 앱을 중지하고 사용자에게 경고 메시지를 전달한다[3].

하지만 해당 논문에서 제시한 탐지 방안은 특정 Application Set에서의 분석을 다루고 있으며 다른 Set을 분석할 경우 구분 결과의 정확성이 달라질 수 있다. 본 논문의 2장에서는 랜섬웨어 앱 실시간 탐지 방안과 관련된 기존 연구를 다루며 3장에서는 기존 연구의 문제점을 분석하고 그에 대한 개선 방안을 제시한다. 마지막으로 4장에서는 향후 진행되어야 할 연구에 대해 언급하며 결론을 맺는다.

2. 관련 연구

2.1 기존 안드로이드 환경에서의 랜섬웨어 실시간 탐지 방안

정상 암호화 기능 앱은 사용자가 암호화할 대상을 선택하는 등 앱과 사용자 간 상호작용을 통해 기능을 수행하지만 랜섬웨어 앱은 사용자의 의지와 관계없이 중요 정보를 암호화한다. 기존 연구에서는 이러한 차이를 통해 정상 암호화 기능 앱과 랜섬웨어 앱을 구분하기 위한 세 가지 단계를 제시하였다[3].

Step 1. Encryption Analysis

이 단계에서는 기기 내에 중요 정보가 담긴 파일을 사전에 정의한 후 해당 파일의 암호화 여부를 모니터링한다. 모니터링 중인 파일의 엔트로피 값 측정을 통해 암호화 여부를 판별하며 해당 파일이 암호화된 경우 다음 단계가 시작된다. 엔트로피 값 측정은 2.2절에서 언급한다.

Step 2. Foreground Analysis

이 단계에서는 현재 사용자가 암호화 기능 앱이 실행되고 있음을 인지하고 있는지의 여부를 판단한다. 암호화 기능을 수행한 앱의 액티비티가 액티비티 매니저 스택의 최상위가 아닐 경우 랜섬웨어 앱으로 간주한다. 스택의 최상위일 경우, 다음 단계가 시작된다.

Step 3. Layout Analysis

이 단계에서는 암호화 기능 앱과 사용자가 상호작용중인지를 판단한다. 랜섬웨어 앱은 사용자에게 암호화 과정을 보여주지 않는다는 점을 이용하며 File List, Hint Text, Button 분석을 수행한다. File List 분석은 파일들의 목록을 보여주는지, Hint Text 분석은 어떤 문자들이 포함되어있는지, Button 분석은 사용자와의 상호작용을 위한 버튼을 분석한다.

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

2.2 shanon 엔트로피

shanon 엔트로피는 암호화 과정에서 발생하는 혼돈 효과를 이용한다. 평문이 암호화될 경우 암호문의 값들은 분포가 균등해진다는 점을 이용해 특정 파일이 암호화되었는지 판단한다. 특정 파일의 값 분포가 0x00부터 0xFF까지 모두 균등한 경우 엔트로피 값은 8이 된다. 엔트로피 값 e 는 다음과 같이 계산할 수 있다[4].

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

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

3. 문제점 및 개선 방안

이 장에서는 기존 연구에서 제시한 탐지 방안 중 Step3. Layout Analysis를 분석하며, 해당 단계에서 발생할 수 있는 문제점과 그에 대한 개선 방안을 제시한다.

3.1 기존 연구의 문제점 분석

File List 분석에서는 정상 암호화 기능 앱의 경우 사용자가 암호화할 파일을 선택할 수 있도록 파일 목록을 보여주지만, 랜섬웨어 앱은 보여주지 않는다는 점을 이용하였다. 하지만 분석 과정에서 앱이 보여준 파일 목록이 기기 내에 실제로 존재하는 파일들의 목록인지는 검사하지 않는다. 따라서 레이아웃에 기본 상태의 리스트를 추가하는 것으로 이를 우회할 수 있다.

Hint Text 분석에서는 정상 암호화 기능 앱들에서 추출한 문자열들을 기반으로 whitelist 형태의 검사를 진행하고 있다. 하지만 분석 과정에서 제시한 “privacy”, “encryption”과 같은 문자열들은 랜섬웨어 앱에서도 나타날 수 있으며, 다른 문자열들 또한 랜섬웨어 앱의 xml 파일에 해당 문자열들을 추가하여 우회할 수 있다.

Button 분석에서는 암호화 기능 앱과 사용자 간의 상호작용을 위해 버튼이 필요하다는 점을 이용하였다. 하지만 분석 과정에서 각 버튼과 대응되는 메소드가 있는지에 대한 여부는 검사하지 않는다. 이는 레이아웃에 버튼을 추가하여 우회할 수 있다.

문제점에 대한 분석은 표 1과 같다.

(표 1) 기존 연구의 문제점

분석 과정	문 제 점
File List	레이아웃에 보여지는 파일 목록의 실제 존재 여부를 검사하지 않음
Hint Text	whitelist 형태 검사를 위한 문자열들이 랜섬웨어 앱에서도 나타날 수 있음
Button	각 버튼이 실제 적절한 메소드와 매핑되고 있는지에 대해 검사하지 않음

3.2 개선 방안 제시

File List 분석에서는 파일 목록에 있는 파일들이 실제로 기기 내의 저장소에 존재하는 파일들인지에 대한 검사가 수행되어야 한다. 정상 암호화 기능 앱의 경우 목록에서 선택한 파일들을 암호화하므로 이 검사 과정이 기능 수행에 영향을 미치지 않는다.

Hint Text 분석에서는 랜섬웨어 앱들로부터 추출한 문자열들을 기반으로 한 blacklist 형태의 검사로 변경한다. 랜섬웨어 앱들이 사용자에게 금전을 요구한다는 점을 이용하면 “pay”, “coin”과 같은 금전 관련 문자열들을 blacklist 문자열로 이용할 수 있다.

Button 분석에서는 각 버튼에 포함된 문자열과 적절한 메소드가 매핑되고 있는지에 대한 검사를 수행해야 한다. 이를 통해 사용자가 버튼을 눌렀을 때 수행 결과를 예측할 수 있도록 보장해야 한다.

표 2에는 위의 개선 방안들을 제시하였다.

(표 2) 개선 방안

분석 과정	개선 방안
File List	목록에 보여지는 파일들이 실제 저장소에 존재하는지에 대해 검사 수행
Hint Text	랜섬웨어 앱들로부터 추출한 문자열들을 기반으로 blacklist 형태의 검사 수행
Button	각 버튼에 포함된 문자열과 적절한 메소드가 매핑되는지에 대해 검사 수행

4. 결론

정상 암호화 기능 앱과 랜섬웨어 앱을 구분하여 랜섬웨어 앱을 실시간 탐지하는 기존 연구의 문제점을 분석하고 그에 대한 개선 방안을 제시하였다. 본 논문에서는 개선 방안에 대한 구체적인 구현 방안은 제시하지 않았으며 구현 방안 제시 및 실제 데이터 셋을 이용한 실증은 향후 연구에서 진행할 예정이다.

참 고 문 헌

- [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.