

추계학술 발표대회

2019.11.1(금)~2(토)

부경대학교 대연캠퍼스

주최 사단법인 한국인터넷정보학회

주관 부경대학교

후원 (주)카카오, (주)아이티센, LGCNS(주), (주)한스컴정보통신

www.ksii.or.kr



KOREAN SOCIETY FOR INTERNET INFORMATION

사단법인 한국인터넷정보학회

법인등록번호 101-86-11111

논문발표

11월 2일(토) 09:30~11:30(향파관 3층 309호)

세션 B. 인터넷보안

좌장 : 배인한 교수(대구가톨릭대)

- B-1 DLOTA2 기반의 안전한 펌웨어 업데이트 방안
이민경, 최슬기, 광진(아주대)
- B-2 DCV 기반 공격기법 분석 및 대응방안
정해선, 광진(아주대)
- B-3 유전 알고리즘을 이용한 컴파일러 분류
황철훈, 신건윤, 한명목(가천대)
- ☆ B-4 은닉형 안티포렌식 APK 분류기법에 관한 연구
김대규, 김창수(부경대)
- B-5 악성코드 프로파일 기반 유사 악성코드 검색 연구
강홍구, 최보민, 김경한, 박순태(KISA)
- B-6 완전동형암호를 이용한 Metropolis Hastings 샘플링 알고리즘에 관한 연구
유준수, 윤지원(고려대)
- B-7 완전 동형암호를 이용한 베이지안 선형 회귀분석
홍미연, 윤지원(고려대)
- B-8 안드로이드 취약점 기반 변종 랜섬웨어 동향 분석
박소희, 광진(아주대)
- B-9 암호화된 데이터상에서 영상처리를 위한 Gaussian 필터 구현
송백경, 윤지원(고려대)

11월 2일(토) 09:30~11:30(향파관 3층 304호)

세션 C. 인터넷통신

좌장: 김석훈 교수(순천향대)

- ☆ C-1 실시간 얼굴인식을 위한 분산 시스템
장종권, 범정현, 추현승(성균관대)
- C-2 Wi-Fi 기반 그룹 관리 MAC 프로토콜 구현
한명승, 장윤경, 유인태(경희대)
- C-3 무선 센서 네트워크에서 시간 효율적인 지연 제한 데이터 집계를 위한 제한 기법
Vo Van Vi, Dung T. Nguyen(성균관대), 김문성(서울신학대), 추현승(성균관대)
- C-4 듀티 사이클 센서 네트워크에서 구조 기반 데이터 집산 알고리즘에 대한 성능 평가
Dung T. Nguyen(성균관대), 김문성(서울신학대), 추현승(성균관대)
- C-5 WIT-tree 기반의 가중치 빈발패턴 마이닝 기법의 분석
임현근, 윤은일, 남효주, 백윤지, 김종성, 김현호(세종대)
- C-6 STPA 기반 무인기 조작 규정 안전 검증 새로운 방법
Xiaorui Shao, 김창수(부경대), 라일군(Univ. of Colorado Denver)
- C-7 STPA 기반 무인기 시스템상의 컴포넌트 오류 및 불안정한 상호작용에 관한 연구
Palash Sontakke, 김창수(부경대), 라일군(Univ. of Colorado Denver)
- C-8 복수의 SFC 환경에서 모니터링 에이전트 배치 최소화를 통한 시그널링 비용 감소 방안
이도경, 김문성, 사이드무함마드라자, 추현승(성균관대)

안드로이드 취약점 기반 변종 랜섬웨어 동향 분석

박소희*, 궤진**

*아주대학교 컴퓨터공학과 정보보호응용및보증연구실

**아주대학교 사이버보안학과

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

Trend Analysis of Android Vulnerabilities based Variant Ransomware

So-Hee Park*, Jin Kwak**

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

**Department of Cyber Security, Ajou University

요 약

최근 안드로이드 기기의 성능 향상에 따라 사용자가 기기에 저장하는 중요 데이터가 증가하였으며, 이로 인해 안드로이드 환경을 타겟으로 하는 랜섬웨어가 증가하고 있다. 새로 발견된 랜섬웨어의 대부분은 변종 랜섬웨어이며 기존의 방어 기법을 우회하거나 피해를 증가시키는 방식으로 발전하고 있다. 기존 랜섬웨어 공격의 주요 대상이었던 PC 환경에서는 안드로이드보다 다양한 종류의 랜섬웨어가 발생했기 때문에 PC 환경 랜섬웨어의 배포 경로를 이용한 안드로이드 환경의 변종 랜섬웨어가 발생할 수 있다. 따라서 본 논문에서는 PC 및 안드로이드 환경에서 발생한 랜섬웨어의 배포 경로를 분석하고, PC 환경의 재배포 기능을 위한 안드로이드 취약점 및 변종 랜섬웨어에 대해 분석한다.

1. 서 론

랜섬웨어는 시스템을 잠그거나 데이터를 암호화하여 사용할 수 없도록 한 다음 이를 인질로 금전을 요구하는 악성 프로그램이다[1]. 안드로이드 기기의 성능 향상으로 사용자가 저장하는 중요 데이터가 많아졌고, 이로 인해 안드로이드 환경을 타겟으로 하는 랜섬웨어가 지속적으로 증가하고 있다. 새롭게 발견되는 랜섬웨어 중 대부분은 변종 랜섬웨어이며 기존의 방어 기법을 우회하는 방식으로 발전하고 있다[2]. 안드로이드에는 원격 코드 실행, 권한 상승 등의 취약점 항목이 존재하며, 이를 이용한 변종 랜섬웨어가 발생할 수 있다[3]. 따라서 본 논문에서는 PC 및 안드로이드 환경에서 발생하는 랜섬웨어의 특징을 분석하고, 안드로이드 취약점을 이용해 PC 환경의 랜섬웨어와 유사한 배포 경로를 가지는 변종 랜섬웨어에 대해 분석한다.

본 논문의 구성은 다음과 같다. 2절의 관련 연구에서 PC 및 안드로이드 환경의 랜섬웨어를 배포 경로와 BlueBorne을 분석하고, 3절에서 안드로이드 취약점을 이용하여 랜섬웨어 앱을 재배포하는 변종 랜섬웨어를 분석하며, 4절에서 결론을 맺는다.

2. 관련 연구

2.1 변종 악성코드 발생 현황

AV Test에서 수집한 통계 자료에 따르면 2019년 9월 발견된 맬웨어는 약 9억4725만에 달하며, 이 중 신종 맬웨어는 0.97%인 917만 개다[2]. 이를 통해 최근 맬웨어의 대부분은 기존 발생한 맬웨어의 변종임을 알 수 있다. 또한 변종 랜섬웨어는 탐지 회피나 공격 기법을 추가한 형태로 발전하고 있다[4].

2.2 PC 환경 대상 랜섬웨어의 배포 경로

□ WannaCry

2017년 발생한 WannaCry는 스피어 피싱 및 해킹된 웹

사이트를 통해 사용자들을 감염시켰다. 이후 Windows의 SMB 원격 코드 실행 취약점을 통해 네트워크에 연결된 취약한 기기를 추가적으로 감염시켰다. 랜섬웨어가 실행되면 시스템 내에 존재하는 데이터 파일을 암호화한다[5].

□ BadRabbit

2017년 발생한 BadRabbit은 웹 사이트에 조작된 스크립트를 삽입하여 방문자들이 Adobe Flash 업데이트 설치 파일로 위장한 랜섬웨어를 설치하도록 유도했다. 이후 네트워크에 있는 다른 컴퓨터로 감염을 확대시켰으며 디스크를 암호화한다[6].

□ GandCrab

2018년 발생한 GandCrab은 사칭 이메일, 정상으로 위장한 파일, 멀티바이징을 사용하여 사용자들을 감염시켰다. 이후 사용자의 주요 파일을 암호화시키며 감염 사실 및 복구관련 안내 페이지를 생성한다[4].

(표 1) PC 환경 대상 랜섬웨어 및 배포 경로

랜섬웨어	배포 경로
WannaCry	피싱, 웹 사이트 해킹, 재배포
BadRabbit	업데이트 위장, 재배포
GandCrab	사칭, 정상 웹 사이트 위장, 멀티바이징

2.3 안드로이드 환경 대상 랜섬웨어의 배포 경로

□ SimpleLocker

2014년 발생한 SimpleLocker는 가짜 Google Play 사이트에서 정상 앱으로 위장하여 배포되었다. 앱이 설치되면 안드로이드 폰의 SD카드 안에 있는 중요 파일을 암호화하고 기기를 사용할 수 없게 한다[7].

□ DoubleLocker

2017년 발생한 DoubleLocker는 해킹된 웹 사이트에서 가짜 Adobe Flash 업데이트로 위장하여 배포되었다. 앱이 설치되면 데이터를 암호화하고 기기의 PIN을 랜덤하게 변경하여 사용자가 기기에 액세스하지 못하도록 차단한다[8].

□ WannaLocker

2017년 발생한 WannaLocker는 서드파티 앱 스토어에서

정상 앱으로 위장하거나 악성 링크를 사용한 피싱 공격을 통해 배포되었다. 앱이 설치되면 공격자에게 사용자 정보를 보내고 데이터를 암호화한다[9].

(표 2) 안드로이드 환경 대상 랜섬웨어 및 배포 경로

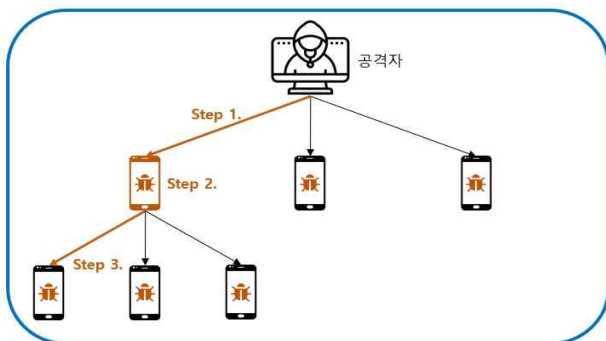
랜섬웨어	배포 경로
SimpleLocker	피싱, 정상 앱 위장
DoubleLocker	업데이트 위장
WannaLocker	피싱, 정상 앱 위장

2.4 BlueBorne

BlueBorne은 블루투스 취약점을 이용한 새로운 공격 벡터로, 블루투스 기능이 켜있는 기기라면 페어링 되어있지 않더라도 제어권을 탈취할 수 있다. Armis는 안드로이드에 BlueBorne을 적용하기 위한 4개의 취약점을 제시하였으며, 인접한 기기들에 맬웨어를 퍼트릴 수 있다고 발표하였다[10].

3. 안드로이드 취약점 기반 변종 랜섬웨어

PC 환경을 대상으로 발생한 랜섬웨어의 배포 경로를 분석한 결과, PC 환경에서는 감염된 기기가 랜섬웨어를 재배포하여 많은 피해를 발생시켰다. 안드로이드 랜섬웨어는 PC 랜섬웨어를 따라 변종 랜섬웨어로 동작할 수 있기 때문에 안드로이드 환경을 대상으로 한 랜섬웨어에서도 재배포 기능을 포함한 변종이 발생할 수 있다. (그림 1)은 변종 랜섬웨어가 안드로이드의 권한 상승 및 Bluetooth 취약점을 이용해 랜섬웨어 앱을 재배포하는 과정에 대해 나타낸 것이다.



(그림 1) 변종 랜섬웨어의 동작과정

Step 1. (표 2)에 정리한 배포 경로를 통해 안드로이드 기기에 랜섬웨어 앱 설치

Step 2. 안드로이드 권한 상승 취약점을 통해 랜섬웨어 앱이 설치된 기기의 권한 탈취

Step 3. 권한을 탈취한 기기에서 BlueBorne을 이용해 주변 기기에 랜섬웨어 앱 재배포

Step 1.은 기존 랜섬웨어가 배포되는 방식과 유사하다. Step 2.에서는 랜섬웨어 앱을 기기에 설치 및 동작시키기 위해 안드로이드의 권한 상승이 필요하다. PC 랜섬웨어와 같이 랜섬웨어가 안드로이드 권한 상승 취약점을 이용하여 기기의 권한을 탈취함으로써 피해 기기를 2차 배포의 숙주로 만들고 랜섬웨어의 재배포를 위해 Bluetooth를 이용할 수 있다. (표 3)은 CVE-Details에 등록된 안드로이드 대상의 권한 상승 취약점들 중 3가지를 정리한 것이다[11].

(표 3) 권한 상승 취약점 및 설명

취약점	설명
CVE-2019-2041	불안정한 기본값을 가진 NFC 모듈의 기기 식별 방해
CVE-2019-2178	경계 검사를 누락하여 범위를 벗어난 write 설정 가능
CVE-2019-9461	VPN 라우팅의 안드로이드 기기 커널에서 정보 노출 발생

Step 3.에서는 주변 기기에 랜섬웨어를 재배포하는 PC 대상 랜섬웨어의 동작을 적용할 수 있다. Step 2.에서 숙주가 된 기기가 BlueBorne을 이용하여 주변 기기의 제어권을 탈취한다. 이후 랜섬웨어 앱을 설치하여 피해를 확산시킬 수 있다. (표 4)는 CVE-Details에 등록된 BlueBorne이 기기의 제어권을 탈취하기 위해 이용하는 취약점 4가지를 정리한 것이다[11].

(표 4) BlueBorne 취약점 및 설명

취약점	설명
CVE-2019-0781	테더링 과정에서 원격코드 실행 가능
CVE-2019-0782	장치 간 네트워크 연결에서 원격코드 실행 가능
CVE-2019-0783	장치 간 네트워크 연결에서 중간자 공격 가능
CVE-2019-0785	주변 장치 식별 시 정보 노출 발생

4. 결론

최근 발견되는 맬웨어 통계에 따르면 새로 발견된 랜섬웨어는 기존 랜섬웨어의 변종일 가능성이 높다. 현재 안드로이드 환경의 랜섬웨어가 위장과 같은 단일된 배포 방식을 사용하고 있더라도 새롭게 등장하는 변종 랜섬웨어는 다양한 배포 방식을 사용할 수 있다.

본 논문에서는 안드로이드 취약점을 이용해 재배포될 수 있는 변종 랜섬웨어를 제시하였다. 재배포로 인해 랜섬웨어가 더 빠르게 확산됨에 따라 피해가 커질 수 있다. 따라서 안드로이드 대상 변종 랜섬웨어 대응을 위한 지속적인 연구가 필요하다.

참고문헌

- [1] 한국인터넷진흥원, “랜섬웨어 정의 및 감염경로”, <https://www.krcert.or.kr/ransomware/information.do>
- [2] AVTEST, “Malware”, <https://www.av-test.org/en/statistics/malware/>, 2019.
- [3] AndroidSource, “Android 보안 게시판”, <https://source.android.com/security/bulletin/2019-09-01>, Sep 2019.
- [4] 한국인터넷진흥원, “끝나지 않는 위협. ‘랜즈크랩’, 랜섬웨어 악성코드 분석 기술 보고서, Feb 2019.
- [5] 사이버침해대응본부 침해사고분석단, “워너크라이 분석 스페셜 리포트”, 한국인터넷진흥원, Oct 2017.
- [6] Avast, “배드래빗(BadRabbit) 랜섬웨어 - 분석 및 예방책 소개”, <https://blog.avastkorea.com/1245>, Oct 2019.
- [7] SymantecConnect, “SimpleLocker: First Confirmed File-Encrypting Ransomware for Android”, <https://www.symantec.com/connect/blogs/simplelocker-first-confirmed-file-encrypting-ransomware-android>, Jun 2014.
- [8] WeliveSecurity, “DoubleLocker: Innovative Android Ransomware”, <https://www.welivesecurity.com/2017/10/13/doublelocker-innovative-android-malware/>, Oct 2017.
- [9] Avast, “New triple-threat mobile version of the malware WannaLocker targets banks in Brazil”, <https://blog.avast.com/wannalocker-targets-banks-in-brazil>, Jul 2019.
- [10] Armis, “The Attack Vector “BlueBorne” Exposes Almost Every Connected Device”, <https://www.armis.com/blueborne/>
- [11] CVEDetails, “<https://www.cvedetails.com/cve/>”