정 보 보 호 학 회 지
제34권 제5호, 2024. 10

모바일 환경을 대상으로 한 랜섬웨어 공격 동향 및 동작 분석

위 다 빈*, 박 명 서**

요 약

랜섬웨어는 2000년대 중반에 등장한 이후 지속적인 진화를 거치며 전 세계적으로 가장 큰 보안 위협 중 하나로 자리 잡았다. 랜섬웨어는 다양한 운영체제에서 활동하며, 주로 PC 운영체제를 중심으로 활동했으나, 스마트폰 운영체제 또한 점차 공격의 대상이 되고 있다. 모바일 랜섬웨어는 크게 잠금화면 랜섬웨어와 암호화 랜섬웨어로 나눌 수 있다. 잠금화면 랜섬웨어는 기기의 화면을 잠가 사용자가 스마트폰을 정상적으로 사용할 수 없게 하며, 암호화 랜섬웨어는 전통적인 랜섬웨어와 유사하게 파일을 암호화하는 방식으로 작동한다. 그러나 Windows나 Linux와 같은 PC 운영체제에 대한 랜섬웨어 공격은 자주 보도되지만, 모바일 운영체제에 대한 랜섬웨어 공격에 대한 뉴스는 비교적 드문 상황이다. 본 논문에서는 모바일 랜섬웨어의 생성 과정과 침투 방식, 그리고 공격 유형을 다루며, 최신 모바일 랜섬웨어 샘플의 동작을 분석하고, 모바일 랜섬웨어 발생이 저조한 이유를 설명한다.

Ⅰ. 서 론

스마트폰은 10여 년 전 도입된 이후 전 세계적으로 빠르게 확산되었다. 우리나라 성인의 스마트폰 사용률은 2012년 53%에서 시작해 매년 증가하여 2024년에는 98%에 달했다[1]. 또한 지난해에는 일상생활에서 가장 필요한 매체로 ‘스마트폰’을 선택한 비율이 70%에 이르렀다[2]. 스마트폰은 이제 TV를 넘어 필수 매체로 자리 잡았으며, 우리는 그에 크게 의존하고 있다. 스마트폰을 구동시키는 주요 OS는 안드로이드와 iOS 두 가지로 나뉜다. 이 중 안드로이드는 글로벌 스마트폰 OS 시장에서 70.29%의 점유율을 차지하고 있다[3].

안드로이드는 주로 스마트폰, 태블릿, 스마트워치 등 다양한 모바일 장치를 위해 개발된 리눅스 커널 기반의 오픈 소스 운영 체제이다. 2003년에 설립된 안드로이드는 2005년에 구글에 인수되어, 2008년에 첫 상용 버전을 출시했다. 안드로이드는 오픈 소스 특성상 누구나 자유롭게 코드를 수정하고 배포할 수 있어, 다양한 기기 제조사들이 이를 채택하여 맞춤형으로 사용할 수 있다. 또한, 사용자 인터페이스는 다양하게 커스터마이징할 수 있으며, 멀티태스킹 기능으로 여러 앱을 동시에 사용할 수 있다. 그리고, Google Play Store를 통해 수백만 개 이상의 앱을 이용할 수 있다. 안드로이드 아키텍처는 여러 계층으로 구성되어 있다. 가장 아래에는 리눅스 커널이 있어 하드웨어 추상화, 프로세스 및 메모리 관리, 보안 기능 등을 제공한다. 그 위에는 하드웨어 추상화 계층 (HAL)이 위치해 다양한 하드웨어가 안드로이드 운영 체제에서 원활하게 작동할 수 있도록 돕는다. 다음으로는 C와 C++로 작성된 네이티브 라이브러리 계층과 ART 계층이 있으며, 각각 개발자들이 저수준 시스템 자원 및 하드웨어 기능에 접근할 수 있도록 돕고, 앱 실행과 관리에 필요한 바이트코드를 네이티브 코드로 변환한다. 그 위에는 Java API 프레임워크 계층이 있어 개발자들이 앱을 개발할 수 있도록 다양한 라이브러리와 API를 제공한다. 최상위 계층인 애플리케이션 계층에서는 사용자와 시스템 애플리케이션이 실행된다[4]. 안드로이드는 이렇게 다양한 장점과 글로벌 스마트폰 시장에서 큰 점유율을 차지하고 있기 때문에 공격자의 훌륭한 타겟이 될 것 같아 보이지만, 2022년 statusta에서 발표된 랜섬웨어의 주요 타겟이 되는 운영 체제에 대한 통계를

* 한성대학교 융합보안학과 (대학원생, dbwe@hansung.ac.kr)
** 한성대학교 융합보안학과 (조교수, pms91@hansung.ac.kr)

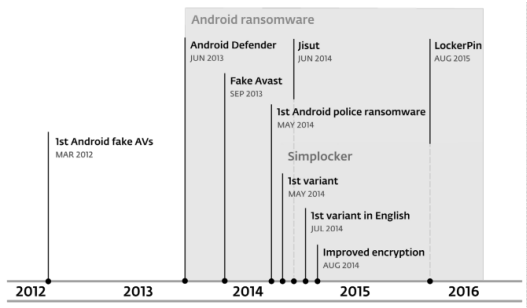
windows os와 관련된 랜섬웨어 공격이 91%로 거의 대부분을 차지한다는 것을 확인할 수 있다[5].

Ⅱ. 배 경

모바일 랜섬웨어는 스마트폰과 같은 모바일 장치를 대상으로 하는 랜섬웨어 형태의 악성 소프트웨어이다. 일반적으로 모바일 랜섬웨어는 사용자로부터 금전을 요구하며, 이를 위해 사용자의 기기에 접근을 제한하거나 기기에 있는 데이터를 암호화한다. 금액을 지불하는 경로는 주로 가상화폐로 지불한다[6]. 본 장에서는 실제 사례를 통해 모바일 랜섬웨어의 등장과 침투 방식 에 대해 설명하고, 두 가지 주요 공격 유형으로 대상 시스템을 공격하는 방식을 분류하였다.

2.1. 모바일 랜섬웨어의 시작과 등장

[그림 1]과 같이 가짜 안티바이러스(Fake AV)는 오래전부터 존재해 온 악성 소프트웨어의 한 유형으로, 안드로이드 환경에서는 2012년부터 활동하기 시작했다. 이 소프트웨어는 가짜 검사 결과를 표시해 사용자가 파일이 감염되었다고 믿게 만들어, 금전적인 대가를 요구하는 특징을 가진다. 이런 유형은 주로 '스케어웨어(Scareware)'로 분류되며, 엄밀히 말하면 일반적인 랜섬웨어로 간주되지는 않는다. 그러나 일부 개발자는 이러한 프로그램에 잠금 화면 랜섬웨어 기능을 추가해 더 공격적인 방식으로 사용자를 위협했다. 그 결과 '경찰 랜섬웨어'라는 새로운 형태의 악성 소프트웨어가 등장하게 되었다. 이 악성코드는 겉으로는 백신 앱처럼 보이지만, 법 집행 기관을 사칭하여 피해자의 장치에서 불법 활동이 탐지되었다고 속이며 금전을 요구한다[7]. 예를 들어, ScarePakage라는 랜섬웨어는 Adobe Flash 또는 유명 백신 앱을 가장해 설치되며, FBI를 사칭해 '당신의 휴대폰이 잠겼으며, 이를 해제하려면 금액을 지불해야 한다'는 협박성 메시지를 표시한다.이 메시지는 다른 화면으로 이동하거나 휴대폰을 재시작해도 계속 나타나며, 범죄자들에게 MoneyPak 바우처로 수백 달러를 지불해야만 기기를 다시 제어할 수 있다[8]. 한편, 모바일 랜섬웨어 중 최초로 실제 파일을 암호화한 사례는 2014년에 등장한 Simplocker로, AES 암호화를 사용하여 이미지, 문서, 비디오 파일을 암호화한다[9].



〔그림 1〕 안드로이드 랜섬웨어의 등장과 발전

2.2. 모바일 랜섬웨어의 침투 방법

모바일 랜섬웨어는 주로 세 가지 경로를 통해 안드로이드 기기에 침투한다. 첫 번째는 가짜 어플리케이션을 통한 침투이다. 이런 가짜 어플리케이션을 배포하는 사이트는 원본 웹사이트와 동일한 인터페이스를 구현한다. 사용자는 이러한 모방된 웹사이트에 속아 가짜 어플리케이션을 다운받게 된다. 두 번째는 스미싱 (Smishing)을 통한 침투이다. 스미싱은 문자(SMS)와 피싱 (Phising)의 합성어로, 악성 앱 주소가 포함된 문자 메시지를 대량으로 무작위 전송 해 악성 앱을 설치하도록 유도하여 다양한 정보를 편취 하는 수법이다. 사용자가 악성 링크가 포함된 문자 메시지를 받고 이를 클릭했을 때 감염이 이루어진다. 세 번째는 감염된 웹사이트 방문을 통한 침투이다. 유의해야 할 점은 유명한 사이트도 악성 코드를 포함할 수 있어 항상 안전하지 않을 수 있다는 것이다[10].

2.3. 모바일 랜섬웨어의 공격유형

모바일 랜섬웨어의 주요 유형은 잠금 화면 랜섬웨어와 암호화 랜섬웨어 두 가지이다. 먼저 잠금 화면 랜섬웨어는 기기의 화면을 잠그는 방식으로 작동한다. 시스템 접근을 차단하여, 사용자가 시스템이 암호화되었다고 믿게 만든다. 이 유형은 중요한 파일을 실제로 암호화하지는 않는다. 반면, 암호화 랜섬웨어는 기기의 기본 기능을 방해하지 않는 동시에 문서, 사진, 동영상 등 시스템의 데이터를 암호화하여 복호화 키 없이는 접근할 수 없게 만든다[11].

Ⅲ. 모바일 랜섬웨어 동작 분석

3.1. 모바일 랜섬웨어 동작 분석 환경

모바일 랜섬웨어를 분석하기 위해 사용한 도구는 [표 1]와 같다. 가상환경에서 안전하게 동작을 확인하기 위해 nox를 사용하였으며, 동적 분석을 위해 jeb를 사용하였다. 다운받은 샘플 파일을 nox에서 실행시키기 위해 adb_nox를 사용하였고, apk의 패킹 여부를 확인하기 위해 APKID를 사용하였다.

〔표 1〕 분석환경 및 도구

분류	종류	버전
분석 환경	데스크탑	windows10
	스마트폰	android12
분석 도구	nox	7.0.6.0005-7.1.2700230529
	jeb	5.0.0.202308071454
	nox_adb	1.0.36
	APKID	2.1.5

또한, 분석한 랜섬웨어는 [표 2]와 같다. 해당 악성코드 샘플은 멀웨어바자 (MalwareBazaar)에서 확보하였으며, 해당 사이트에서 가장 최근에 올라온 랜섬웨어를 대상으로 분석을 진행하였다. 멀웨어바자는 어뷰즈 (abuse.ch)가 제작한 무료 악성코드 샘플 저장소로, 누구나 멀웨어바자에 접속해 원하는 샘플을 무제한으로 다운로드할 수 있으며, 보안 전문가들도 자신이 발견한 샘플을 기여할 수 있다. 제공된 샘플들은 검색 멀웨어 패밀리 이름, 해시, 태그 등으로 분류되어 있어 검색이 용이하다. 또한 자동화를 위한 API도 지원한다 [12].

〔표 2〕 분석 대상 랜섬웨어

이름	sha256 해시값
Sotarmaf.apk	de2ef69a5c7ccae38bf78c537829bc426908defe4331d9959332ce4b89c70054
kawendra.apk	b5ab87692109c072cc277246e957ab32cfce6973f9f06c609ba51b53114cce51
PsiphonAndroid.s.apk	184356d900a545a2d545ab96fa6dd7b46f881a1a80ed134db1c65225e8fa902b

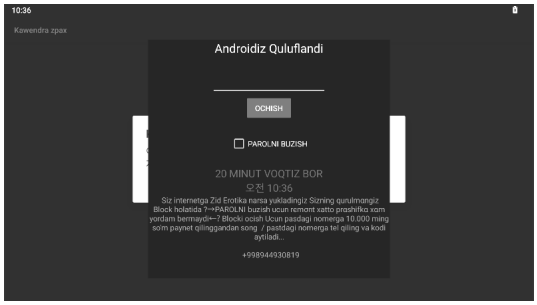
3.2. 잠금화면 랜섬웨어 동작 분석

분석한 잠금화면 랜섬웨어는 총 2가지로Sotarmaf.apk 와 UltraHack_SO2.apk 이다. 두 랜섬웨어 각각 멀웨어바자에 2024년 2월 20일과 21일에 올라온 샘플을 대상으로 분석을 진행하였다. 먼저 Sotarmaf.apk 랜섬웨어의 경우 실행시키면 기기 화면에 휴대전화가 잠겼으며 몇시간 내 포맷될 것이고 바이러스 잠금을 해제하려면 특정 아이디로 문의하라는 이란어로 작성된 글이 들어가 있는 사진이 [그림 2]와 같이 뜨게 된다. 이후 사용자는 스마트폰은 뒤로가기, 홈키 등의 일반적인 동작으로는 해당 화면에서 벗어 날 수 없게 된다.

Sotarmaf.apk 랜섬웨어는 사용자 화면에 Window Manager 클래스를 사용하여 전체 화면을 덮는 뷰를 추가하고, 뷰에 setOnTouchListener를 설정하여, 사용자가 뷰를 4초 이상 길게 누를 시 뷰를 제거 한 뒤 Toast.makeText 매서드로 바이러스가 제거됨을 알리며 서비스를 종료한다. 따라서 Sotarmaf.apk 랜섬웨어는 다음과 같은 방식으로 사용자의 작업을 방해하고, 특정 조건을 만족시킬 시 스스로 제거되는 잠금화면 랜섬웨어이다.

다음으로 kawendra.apk 랜섬웨어는 실행시키면 기기 화면에 비밀번호 입력창과 '20분 남았습니다'라는 메시지가 포함된 경고창이 [그림 3]과 같이 화면 중앙에 나타난다. 경고창 하단에는 '인터넷에 금지된 에로틱한 자료를 업로드한 죄로 장치가 차단되었으며, 차단 해제를 위해 10,000 우즈베크 솜을 특정 번호로 결제한 후 함께 표시된 전화번호로 문의하라'는 안내와 전화번호가 제공된다. 이후 사용자는 스마트폰은 뒤로가기, 홈키 등의 일반적인 동작으로는 해당 화면에서 벗어날 수 없게 된다.

〔그림 2〕 Sotarmaf.apk의 잠금화면



〔그림 3〕 kawendra.apk의 잠금화면

kawendra.apk 랜섬웨어는 사용자 화면에 WindowManager 클래스를 사용하여 전체 화면을 덮는 뷰를 추가하고, 뷰에 EditText를 선언하여 텍스트를 입력받을 수 있는 텍스트 박스를 설치한다. 뷰에는 버튼이 포함되어 있어, 사용자가 버튼을 클릭하면 onClick 메서드가 호출된다. 이때 EditText에 입력된 텍스트가 '77776516'인 경우 뷰를 제거하며 서비스를 종료한다. 따라서 kawendra.apk 랜섬웨어는 다음과 같은 방식으로 사용자의 작업을 방해하고, 특정 조건을 만족시킬 시 스스로 제거되는 잠금화면 랜섬웨어이다.

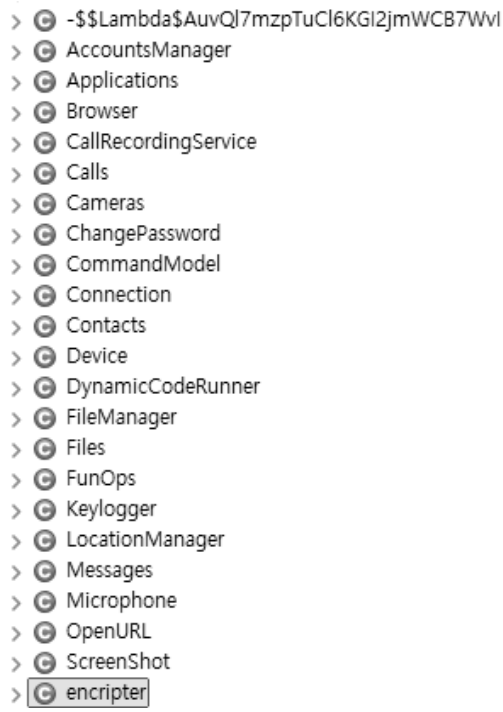
3.3. 암호화 랜섬웨어 동작 분석

분석한 암호화 랜섬웨어는 1가지로 Psiphon Android.s.apk이다. 해당 암호화 랜섬웨어는 앞에 소개된 2개의 잠금화면 랜섬웨어보다 복잡한 형태를 가졌다. 이 랜섬웨어는 [그림 4]와 같이 Psiphon라는 vpn 어플리케이션으로 위장하여 설치 된다.

PsiphonAndroid.s.apk는 모바일 암호화 랜섬웨어라고 소개되지만 사실 파일을 암호화하는 기능을 가진 봇넷에 가깝다. 봇넷이란 악성코드에 감염되어 공격자에 의해 원격으로 기기를 제어 당해 악성 활동을 수행하는 컴퓨터 네트워크를 의미한다. PsiphonAndroid.s.apk는 C&C (Command and Control) 서버와 통신해 명령을 받은 후 [그림 5]와 같이 키로거, 통화녹음, 브라우저 기록수집, 개인정보탈취 등 다양한 악성 행위를 수행한다.

이러한 악성행위 중 하나가 바로 랜섬웨어 행위이다. 2014년에 발견된 최초의 모바일 암호화 랜섬웨어인 simlpock은 암호화 행위만을 수행했지만, 최근의 모바일 암호화 랜섬웨어는 단순히 랜섬웨어 행위만 하는 것이 아닌 일반 앱으로 위장하거나 봇넷과 결합하는 등 다양한 악성 기능이 추가되었다는 것을 알 수 있다. PsiphonAndroid.s.apk의 코드 중 암호화 기능을 수행하는 코드는 다음과 같다. PsiphonAndroid.s.apk는 encripter 클래스를 통해 파일을 암호화하고 복호화한다. 가장 먼저 클래스 로드 시 String으로 선언된 encripter.password 변수가 빈 문자열로 초기화된다. 이후 crypter 메서드는 JSON 형식의 데이터를 가진 객체인 'params'으로부터 "password" 키 값의 벨류 값을 추출하여 encripter.password 변수에 추가한다. 그 후, checkperm을 호출해 안드로이드 버전이 6.0 이상인지 확인하고, 외부 저장소에 쓰기 권한이 있는지 확

〔그림 4〕 Psiphon으로 위장한 PsiphonAndroid.s.apk



〔그림 5〕 PsiphonAndroid.s.apk의 다양한 악성행위

인한 후 “txt”, “jpg”, “doc”를 포함한 13가지의 확장자 중 하나인 경우 FileEncryption메서드를 호출한다. FileEncryption메서드는 파일을 암호화하는 메서드로 8바이트 크기의 salt값을 생성하여 저장한다. 그 후, 솔트 값을 통해 비밀키를 생성하고 Cipher 객체를 AES/CBC/PKCS5Padding 암호화 방식으로 초기화하고, 암호화에 사용된 초기화 벡터(IV)를 파일에 저장한다. 이후, 파일을 64바이트씩 updata 메서드로 암호화한다. 파일 끝에 도달하면 dofinal 메서드로 남은 데이터를 최종 블록으로 암호화하여 저장한다. 암호화된 파일은 원래 파일 이름에 “.enc”가 추가된 형태로 생성된다.

Ⅳ. 모바일 랜섬웨어 활동의 저조 원인

현대인은 스마트폰을 통해 새로운 정보를 접하고, 메신저를 통해 시공간에 구애받지 않고 소통하며, 다양한 상품이나 음식을 주문한다. 이렇게 스마트폰이 우리 삶에 큰 영향을 미치고 있지만, VirusTotal에서 2021년도에 발표한 전년도 랜섬웨어 활동 보고서인 “Ransomware In a Global Context”에 따르면 랜섬웨어로 탐지된 파일의 95%는 윈도우 운영체제에서 동작하는 실행 파일인 “.exe”와 동적 라이브러리 파일 “.dll”이였고 단 2%만 안드로이드 기반이라고 발표했다[13]. 또한 2023년 2분기 카스퍼스키의 통계에 따르면 모바일 랜섬웨어 패키지 수는 2022년 3,821개에서 2023년 1,318개로 줄어들었다고 발표했다[14]. 이렇듯 windows등 다른 운영체제를 타겟한 랜섬웨어는 활발하게 활동하고 있지만 모바일 랜섬웨어가 줄어들고 있는 이유는 몇 가지 이유가 있다.

첫 번째로, 기본적으로 안드로이드와 iOS 사용자는 주로 공식 앱스토어인 Google Play Store 또는 Apple App Store에서 애플리케이션을 다운로드한다. 추가적으로 안드로이드는 Google Play Protect가 내장되어 있어 기기의 어플리케이션을 스캔하여 악성코드를 검사하고, 애플은 샌드박싱 (sandboxing)이라는 기능을 통해 애플리케이션이 기기의 자원과 데이터에 제한된 접근만 가능하게 하고, 공개된 취약점이 부족하며, 애플 생태계 자체에 폐쇄성까지 어우러져 랜섬웨어 공격자들에게 훨씬 더 어려운 대상이 된다. 두 번째로, 엄격하게 통제되는 IOS와 다르게 안드로이드는 여러 기기 제조사들이 자신의 기기에 맞게 안드로이드를 수정하기 때문에 일반적으로 모든 기기에서 작동하는 어플리케이션을 만들기 어렵다. 또한 공격자가 모바일 운영 체제에서 관리자 접근 권한인 ‘루트’권한을 확보하는것은 매우 어렵다[15]. 마지막으로, 최근 랜섬웨어의 전략인 빅게임 헌팅의 등장에서 보았듯이, 공격으로 인해 조직의 운영이 마비되는 등 큰 피해를 입을 가능성이 크고, 고액의 몸값을 지불할 능력과 가능성이 높은 병원, 은행, 학교, 정부 기관 등 중요한 인프라나 기업을 타겟으로 공격하는 것이 효과적이라는 사실이 밝혀졌다. 이러한 조직들은 데이터의 중요성 때문에 몸값을 지불하지 않을 경우 막대한 피해를 입게 된다. 개인이나 작은 조직을 공격하는 것보다 대규모 조직을 대상으로 하는 것이 랜섬웨어 공격자들에게 더 많은 수익을 안겨준다[16].

Ⅴ. 결 론

현재 랜섬웨어는 많은 이들에게 피해를 주고 있는 악성코드이다. 하지만 모바일 환경에서의 피해는 잘 발견되지 않는 상황이다.

본 논문은 이러한 배경 속에서 모바일 환경을 대상으로 한 랜섬웨어의 생성 과정과 침투유형, 그리고 공격유형에 대해 살펴보았다. 또한 멀웨어바자에 올라와 있는 최근의 모바일 랜섬웨어를 모바일 랜섬웨어의 유형별로 분석하였으며. 마지막으로 모바일 랜섬웨어 활동의 저조 원인을 다양한 지표를 바탕으로 서술하였다.

참 고 문 헌

[1] (국민권익신문, “2024년 한국 성인 스마트폰 사용률 98% - 50대 99%, 60대 이상 96%”, https://www.crnews.co.kr/news/articleView.html?idxno=6232, 2024.07.11)

[2] (국민일보, “OTT 이용률 77.0%… 60대 이상 스마트폰 보유 늘어”, https://www.kmib.co.kr/article/view.asp?arcid=0924337280, 2023.12.29)

[3] (조선비즈,“애플 iOS, 스마트폰 OS 점유율 ‘30%’ 눈앞… 구글 안드로이드는 내리막길”, https://biz.chosun.com/it-science/ict/2023/12/28/KDY6QFRQRBDNDIQRSSAM5KZKUM/,2023.12.28)

[4] (spiceworks/Chiradeep BasuMallick, “What Is Android OS? History, Features, Versions, and

Benefits", https://www.spiceworks.com/tech/tech-general/articles/android-os/,2024.03.19)
[5] (statista/Ani Petrosyan,"What systems have you seen infected by ransomware?", https://www.statista.com/statistics/701020/major-operating-systems-targeted-by-ransomware/,2022.10.27)
[6] (Monique Becenti, "Mobile Ransomware - How Handheld and Mobile Devices Leave Organizations Exposed", https://www.zimperium.com/blog/mobile-ransomware-how-mobile-devices-leave-organizations-exposed/, 2023.07.18.)
[7] (eset, "The Rise of Android Ransomware", https://web-assets.esetstatic.com/wls/2016/02/Rise_of_Android_Ransomware.pdf)
[8] (Stu Sjouwerman, "The Evolution of Mobile Ransomware", https://blog.knowbe4.com/evolution-of-mobile-ransomware)
[9] (avast, "The evolution of mobile ransomware", https://blog.avast.com/the-evolution-of-mobile-ransomware)
[10] (Andreea Chebac, "Mobile Ransomware: The Next Step for Cybercriminals", https://heimdalsecurity.com/blog/mobile-ransomware-the-next-step-for-cybercriminals/, 2022.11.17.)
[11] (Amnah Albin Ahmed, Afrah Shaahid, Fatima Alnasser, Shahad Alfaddagh, Shadha Binagag, Deemah Alqahtani, "Android Ransomware Detection Using Supervised Machine Learning Techniques Based on Traffic Analysis", Sensors 2024, 2023.12.28)
[12] (Infosec/David Balaban, "Top 7 Android Ransomware Threats", https://www.infosecinstitute.com/resources/threat-intelligence/top-7-android-ransomware-threats/ , 2016.04.11.)
[13] (VIRUSTOTAL, "Ransomware in a global context", https://blog.virustotal.com/2021/10/ransomware-in-global-context.html, 2021.10.04)
[14] (ANTON KIVVA, "IT threat evolution in Q2 2023. Mobile statistics", https://securelist.com/it-threat-evolution-q2-2023-mobile-statistics/110427/,2023.08.30)
[15] (Lindsay Kaye, "Mobile Phone Ransomware: a Primer", https://ransomware.org/blog/mobile-phone-ransomware-a-primer/, 2022.02.03)
[16] (데일리시큐/길민권, "랜섬웨어 피해액, 2023년 10억 달러 넘어…역대 최고액", https://www.dailysecu.com/news/articleView.html?idxno=153448, 2024.02.08)

〈저자소개〉

위 다 빈 (Dabin We)
학생회원
2024년 2월 : 강남대학교 소프트웨어응용학부 졸업
2024년 3월~현재 : 한성대학교 융합보안학과 석사과정
<관심분야> 정보보호, 디지털포렌식

박 명 서 (Myungseo Park)
종신회원
2013년 2월 : 국민대학교 수학과 이학사
2015년 2월 : 국민대학교 금융정보보안학과 이학석사
2014년 12월~2017년 2월 : 국가보안기술연구소 연구원
2021년 8월 : 국민대학교 금융정보보안학과 이학박사
2021년 9월~2022년 2월 : 국민대학교 금융정보보안학과 박사후연구원
2022년 3월~2023년 8월 : 강남대학교 ICT융합공학부 조교수
2023년 9월~현재 : 한성대학교 융합보안학과 조교수
<관심분야> 정보보호, 디지털 포렌식