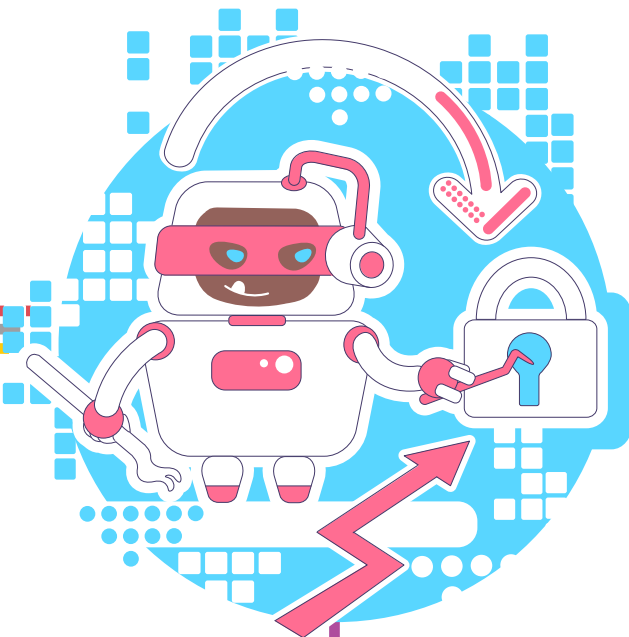


# Android Malware Features



## MetaData

### Hash

악성앱의 지문이라고 할 수 있는 Hash 정보

File Hash	
MD5	175ea3ece22844f8a17e6ca48a8449f0
SHA1	170eee655e7eef2aec705fb3ff8f3eb378fbc69e
SHA256	1d000fa9f60604d9d663ac411aed08e81b9012905696aa87a8a14c2520c4c7d4
Full Fuzzyhash	393216:reeDA+nkYzjoIV56lojiFiocDGgsO/pQHD0Mi:qIAEk7iV5EjrppTf0
DEX Fuzzyhash	49152:WxxqkGTti/CfTdicS11v6zMd7Ud0dUdPUdVdVv3wKCj9:W45Te7UdqUdPUdPVv3wKC5
SO Fuzzyhash	24576:5f5n1n5773pwd+OPuN3FvdrMmI8oQT4tTGRizkQoZQP7ZPNva4:B5BVQoQTW7P7ZPNy

### APK Information

악성앱의 기본 정보

Basic				
	FileSize	Entropy	Entropy Rate	Modify Time
Info	13370975	7.956	0.9	1980-00-00 00:00:00

앱 패키지 및 버전 정보

Package and Version			
	Package Name	Android Version	Version Code
Info	com.pancou.cli	1.1.0	1

앱 실행을 위한 API 레벨 정보

API Level			
	Minimum SDK	Target SDK	Maximum SDK
Info	18	22	-

악용 혹은 변조된 인증서에 대한 정보 확인

Certificate		
	Certificate Name	Certificate S/N
Info	kb	2105370718

콘텐츠 제공자 정보

[Provider](#)

androidx.core.content.FileProvider  
com.google.firebase.provider.FirebaseInitProvider

앱 권한 요청 정보

[Permission Requested](#)

android.permission.ACCESS\_COARSE\_LOCATION  
android.permission.ACCESS\_FINE\_LOCATION  
android.permission.ACCESS\_NETWORK\_STATE  
android.permission.ACCESS\_WIFI\_STATE  
android.permission.ANSWER\_PHONE\_CALLS  
android.permission.AUTHENTICATE\_ACCOUNTS  
android.permission.BIND\_ACCESSIBILITY\_SERVICE  
(이하 생략)

## Network

네트워크 연결 정보

[IP\(Contacted\)](#)

192.168.1.118

[URL\(Contacted\)](#)

https://kisa.or.kr

[URL\(from Memory and Binaries\)](#)

https://boho.or.kr

## Dynamic Info

### Files Activities

악성앱 실행시 주요 파일 행위 정보

FilesActivities	
<b>Files Opened</b>	/data/misc/keychain/pins /data/app/com.pancou.cli-1.apk /data/data/com.pancou.cli/shared_prefs/value.xml /data/data/com.pancou.cli/shared_prefs/is_first_time.xml
<b>Files Written</b>	/data/data/com.pancou.cli/shared_prefs/is_first_time.xml /data/data/com.pancou.cli/shared_prefs/value.xml
<b>Files Deleted</b>	/data/data/com.pancou.cli/shared_prefs/is_first_time.xml.bak /data/data/com.pancou.cli/shared_prefs/value.xml.bak

## ATT&CK Matrix

MITRE ATT&CK Matrix 기반 악성앱 전술 및 기술 분류

Android ATT&CK Matrix	
Initial Access	4 Techniques
Execution	3 Techniques
Persistence	7 Techniques
Privilege Escalation	3 Techniques
Defense Evasion	14 Techniques
Credential Access	4 Techniques
Discovery	8 Techniques
Lateral Movement	2 Techniques
Collection	13 Techniques
Command and Control	8 Techniques
Exfiltration	2 Techniques
Impact	9 Techniques

## ETC

악성앱의 ByteCode 정보

[APK Bytecode](#)

6465780a30333500a5a650d3af0a1b376a9a14db0be137310(이하 생략)

주요 이미지 파일의 Hash

[Image File MD5](#)

72e01aba74b37728d79646d7c43cb1b7

악성앱의 이미지 변환 정보

[APK Bytecode Image](#)

2054x2054 8bit black and white

악성앱 분류 정보

[Classification](#)

Spyware, Evader

아이콘 파일의 ByteCode 정보

[Icon File Bytecode](#)

89504E470D0A1A0A0000000D49484452000000E1000000(이하 생략)

악성앱 공격 조직 정보

[Attacker Group](#)

VoicePhishing-A

## Static Info

악성앱의 시작 함수 정보

[EntryPoint Function](#)

com.pancou.clicom.pancou.cli.activity.LoginActivity

악성앱의 액티비티 함수 정보

[Activities Function](#)

com.pancou.clicom.pancou.cli.activity.LoginActivity  
com.pancou.clicom.pancou.cli.activity.MainActivity

악성앱의 API 함수 정보

[Android API](#)

setMessage  
nativeSendStreamMessage  
nativePushExternalAudioFrameRawData  
encodeFormFields  
(이하 생략)

악성앱의 서비스 정보

[Services](#)

com.google.android.gms.measurement.AppMeasurementJobService  
com.google.android.gms.measurement.AppMeasurementService  
com.google.firebase.components.ComponentDiscoveryService  
com.pancou.cli.service.AppService  
(이하 생략)

악성앱의 브로드캐스트 수신자 정보

[Receivers](#)

com.google.android.gms.measurement.AppMeasurementReceiver  
com.pancou.cli.receiver.BootReceiver  
com.pancou.cli.receiver.CallReceiver  
com.pancou.cli.receiver.HeartBeatReceiver  
(이하 생략)

악성앱에서 확인되는 문자열 정보

[String](#)

문자열

악성앱에 적용된 난독화 정보

[Obfuscation](#)

Flag(0 or 1)

악성앱 내 DB 파일 존재 유무

[Database](#)

Flag(0 or 1)

SO 파일의 컴파일러 정보

[SO Compiler](#)

GCC: (GNU) 4.9.x 20150123 (prerelease)

오픈소스 및 자체 생성 YARA Rule을 통해 악성앱 특징 및 그룹 파악

[YARA Rule](#)

VoicePhishing

한국인터넷진흥원은 안드로이드 악성코드(악성앱)이 가지는 세부적인 정보 유형을 6개 카테고리 총 43가지 특징정보로 분류하여 관리하고 있다.

- 메타데이터(Metadata)  
기본적인 애플리케이션 정보
- 정적정보(Static Info)  
함수, API, 서비스 정보, 문자열 등 코드 내에서 확인 가능한 정보
- 동적정보(Dynamic Info)  
파일 접근/삭제 등 악성앱 실행 시 동작하는 주요 행위 정보
- 네트워크(Network)  
악성앱 실행 시 접속 시도 및 파일/메모리내 포함된 URL/IP 정보
- ATT&CK Matrix  
악성앱을 전략, 전술별(TTPs) 행위를 기술단위별로 추출한 정보
- 기타 정보(ETC)  
악성앱의 Bytecode, 분류 정보 등 기타 정보