Analysis Report aKixIdZir2.apk

Sample Name: aKixIdZir2.apk
Filesize: 554091
MD5: fccaae0ea4e6a18195ea22ee36526556
SHA1: 74e064d18561b63a9439aa7fa1eef13d70ef6d54
SHA256: 5ffaf48aa6c0bc2efd6671ac8872f287e46f2287160f4249a26dc1c5021c7e58
AIML: 0 **(UNKNOWN)**
Static: **(CLEAN)**
MultiAV: **(CLEAN)**
Dynamic Analysis Using Sandboxing: 0 **(UNKNOWN)**

MITRE ATT&CK MATRIX

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
System Information Discovery 1													
Valid Accounts	Windows Management Instrumentation	Registry Run Keys / Startup Folder	Process Injection	Masquerading	OS Credential Dumping	System Information Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder	Software Packing	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	Carrier Billing	Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Risk Summary

- Networking
- System Summary
- Malware Analysis System Evasion
- Anti Debugging

Static Summary

- Yara
- oletools

AV Engines Scan Summary

- clamav
- comodo
- mcafee
- node32
- sophos
- microsoft (File not scanned. There might be issue in file path or something els)
- cyren
- kaspersky
- avast

BEHAVIOUR ANALYSIS

SYSTEM STARTUP PROCESS

-> **OpenWith.exe** (PID: 4064, CMD: C:\Windows\system32\OpenWith.exe -Embedding, MD5: 5D37A62943F1071FFFFE1DE74B8F2778)

URL ANALYSIS

FOUND URLS IN SOURCE

http://schemas.android.com/apk/res/android
@Source : HS.xml

https://android.googlesource.com/toolchain/llvm-project
@Source : libZZplyOlaR.so

IP ANALYSIS

IP FOUND IN SOURCE

Not Found

DOMAINS ANALYSIS

DOMAIN FOUND IN SOURCE

Not Found

BEHAVIOUR

FOUND INLINED NOP INSTRUCTIONS (LIKELY SHELL OR OBFUSCATED CODE)

Filetype : Zip archive data, at least v0.0 to extract, compression method=deflate

Entropy : 7.99041717601121

Trid :
@arraytag : def
Def : ['Android Package (27504/1) 56.12%', 'Java Archive (13504/1) 27.55%', 'ZIP compressed arch ive (8000/1) 16.32%']

Filename : aKixIdZir2.apk

Submissionpath : C:\Users\user\desktop\

Filesize : 554091

Md5 : fccaae0ea4e6a18195ea22ee36526556

Sha1 : 74e064d18561b63a9439aa7fa1eef13d70ef6d54

Sha256 : 5ffaf48aa6c0bc2efd6671ac8872f287e46f2287160f4249a26dc1c5021c7e58

Sha512 : ad91dbdf54f1f7afb8c30f2e229e89c058c4f0d2deaa2259414aecc4647edd5daa5cf45817ac142923959fb10b 7aad2eaff425e48ef9006eed62e628a790e74c

Ssdeep : 12288:PyVzzedIGnyG8lFGReBo2c5vDbhkKS62K++7:PUKdvD8ILBxK9L

Tlsh : 26C423EB4FAD1D0DD5B9D6F148D3EB0B6364DC8A49BC0F1522A362452708A1DCB278BC

Preview : PK.....!.!.!V..4...8...9...META-INF/com/android/build/gradle/app-metadata.propertiesK,(.M-ILI,I.K-*....5.3.J.K)..Lq/JL.I..)M...I.....p..PK.....!.!.G6.....classes.dex
..kl.....w...?..._.u...A^$.!.?..c'.c.....Y.....*...J..@j.h....B.|..R

Java :