



ANDROID STATIC ANALYSIS REPORT

app_icon

 **Spy24 Installer (1.0)**

File Name: installer.apk

Package Name: app.spy24.spy24installer






Scan Date: Aug. 2, 2024, 2:24 a.m.

App Security Score: 35/100 (HIGH RISK)

Grade:



FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
5	6	1	1	1

FILE INFORMATION

File Name: installer.apk

Size: 4.23MB

MD5: 07db1fc8ce64fbdaa4da500940592de5

SHA1: 9c5c2f87ba29fab4a772fc5c6b8d353e6d086264

SHA256: 1f1276f7374dad4e1d89af964c0e505a2d714bbc8c1d9c977c4c4114d7a14af1

APP INFORMATION

App Name: Spy24 Installer

Package Name: app.spy24.spy24installer

Main Activity: app.spy24.spy24installer.MainActivity

Target SDK: 31

Min SDK: 23

Max SDK:

Android Version Name: 1.0

Android Version Code: 1

APP COMPONENTS

Activities: 2

Services: 0

Receivers: 0

Providers: 2

Exported Activities: 0

Exported Services: 0

Exported Receivers: 0

Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed

v1 signature: True

v2 signature: True

v3 signature: False

v4 signature: False

X.509 Subject: CN=Android Debug, O=Android, C=US

Signature Algorithm: rsassa_pkcs1v15

Valid From: 2023-08-29 11:24:23+00:00

Valid To: 2053-08-21 11:24:23+00:00

Issuer: CN=Android Debug, O=Android, C=US

Serial Number: 0x1

Hash Algorithm: sha1

md5: 5d56781a78dcc19deb6a6ee8cddb3aca

sha1: 78b987b07c0192cc0089eac29da39d7b8c4813dc

sha256: ed3e06dcf83bfac1b8e1cbb3a3135d0a42b34a9a3462522c27ba2a1ec14f4c367

sha512: 3335d6f5435a61d0141a06d429c70e94c8bac571ff4d70da81b7f2b7bd88d718af8f1416dbf4265169daf0159122914b7fbf11bf313fc4156a593dd31184a16d

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: cc77a4e370894cd33e572c8002e98e065d311e2511f71234e7e261acc61aca5d

Found 1 unique certificates

☰ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.REQUEST_INSTALL_PACKAGES	dangerous	Allows an application to request installing packages.	Malicious applications can use this to try and trick users into installing additional malicious packages.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

APKID ANALYSIS

FILE	DETAILS
------	---------