NVISO ApkScan malware analysis report
September 17, 2016

General information

File name	**app-debug.apk**
Other known file names	None
Origin	Manually uploaded by anonymous user [2016-09-16 23:15:10]
MD5 hash	74db2ab928f0e69e000b461e72d6009c
SHA256 hash	422b6d6e8f312d8e63ae1423b3d7046fc4dcdf807993cf48a48d73118004c74f
File size	2909.26 KB
Worker	NVISO_API_KALI_01

Static malware analysis

Android manifest (AndroidManifest.xml)

Permissions

ACCESS_NETWORK_STATE	Allows applications to access information about networks
ACCESS_WIFI_STATE	Allows applications to access information about Wi-Fi networks
INTERNET	Allows applications to open network sockets.
READ_EXTERNAL_STORAGE	Allows an application to read from external storage.
READ_PHONE_STATE	Allows read only access to phone state.
WRITE_EXTERNAL_STORAGE	Allows an application to write to external storage.

Services

No services registered.

Virus Total scan results

None of the 55 scanners detected malicious behavior.

Disassembled source code

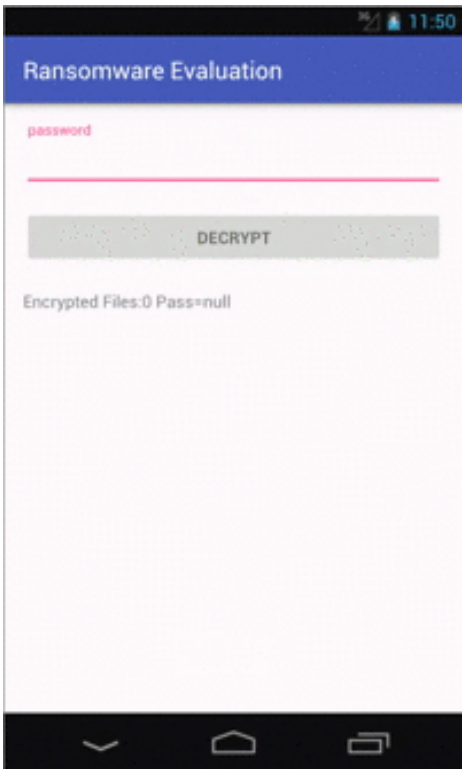
Hardcoded URL's

http://schemas.android.com/apk/res/android

http://schemas.android.com/apk/res-auto

Dynamic malware analysis

Screenshot or animated GIF of the analysed application



Random artificial input is provided to the scanned applications during dynamic analysis, in order to mimic a human being using and interacting with the application. This can result in our report showing a different screen than the one you would see when starting the application.

Disk activity

Accessed files

Filename	/data/data/com.android.vending/shared_prefs/finsky.xml
Filename	/proc/meminfo
Filename	/proc/1258/cmdline
Filename	/proc/1279/cmdline
Filename	/proc/1335/cmdline
Filename	/dev/input/event0
Filename	/proc/1296/cmdline
Filename	/proc/1311/cmdline
Filename	/proc/1313/cmdline
Filename	/proc/1309/cmdline
Filename	/data/data/com.android.gallery3d/shared_prefs/com.android.gallery3d_preferences.xml
Filename	/data/data/com.android.music/shared_prefs/Music.xml
Filename	/proc/1241/cmdline

Network activity

Opened network connections

No network connections were opened.

Automatically placed calls and text messages

Placed phone calls

No phone calls were placed automatically.

Sent SMS messages

No text messages were placed automatically.

Cryptographic activity

Used encryption keys

No cryptographic activity detected.

Encryption operations

No cryptographic activity detected.

Decryption operations

No cryptographic activity detected.

Information leakage

Network information leakage

No network information leakage detected.

SMS information leakage

No SMS information leakage detected.

File information leakage

No file information leakage detected.

Miscellaneous

Started services

Service name com.android.music.MediaPlaybackService

Output generated by ADB logcat

Download ADB logcat file (text format - 302 KB)

report overview | **terms & conditions** | **support & feedback** | **nviso.be**