Apkscan malware analysis report

February 22, 2013

Static malware analysis

General information

File name	SlideIT_v3.0_-_13_.01_.11_Keyboard_FLIPMODE_.apk
MD5 hash	c065e0bb82d80ea5c16f8b4b692fe4a4
SHA256 hash	c92dd9cf84e8f04f4067d7d5ca44dab2923e6205679c8c71d4a9d78e90b5d29d
File size	1006.93 KB

Android manifest (AndroidManifest.xml)

Requested permissions

Unknown permission: PERMISSION_SLIDEIT_DICTIONARY

Unknown permission: SpeechRecognition

VIBRATE: Allows access to the vibrator

WRITE_SETTINGS: Allows an application to read or write the system settings.

WAKE_LOCK: Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming

READ_PHONE_STATE: Allows read only access to phone state.

Unknown permission: CHECK_LICENSE

INTERNET: Allows applications to open network sockets.

ACCESS_NETWORK_STATE: Allows applications to access information about networks

WRITE_EXTERNAL_STORAGE: Allows an application to write to external storage.

Services

com.dasur.slideit.SlideITIME

com.dasur.slideit.rest.ServiceClientRest

com.dasur.slideit.LanguagePackInstall

com.dasur.slideit.rest.ServiceUpdate

Virus Total scan results

None of the 43 scanners detected malicious behavior.

Disassembled source code

URL's

✓ http://dasur01.com/ws/getBasePath.php?output=json

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

✓ http://secureserver.mobiletextinput.com/Licenser/

✓ http://www.mobiletextinput.com/links/watch.php?v=newfeatures

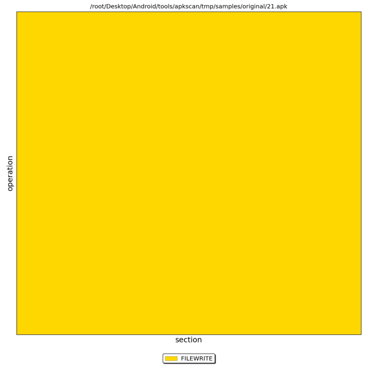
✓ http://www.mobiletextinput.com/links/watch.php?v=slideitonandroid

✓ http://www.mobiletextinput.com/Product/SlideIT/Android/Changelog.php?show

✓ http://www.mobiletextinput.com/Product/SlideIT/Manual/Manual.php?show

✓ https://www.mobiletextinput.com/paypal/buynow.php?os=ANDROID

Dynamic malware analysis



Placed phone calls

No phone calls were placed automatically.

Sent SMS messages

No text messages were placed automatically.

Cryptographic activity

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.