Smart Phone Spyware Artifacts:

Product	Artifacts
FlexiSpy	• FSXGAD_2.**.apk (**is version number) located on the MicroSD card in download folder • data/app/com.mobilefonex.mobilebackup-1.apk • data/data/com.google.android.gsf/app_sslcache/android.clients.google.com.443 • bookmark_thumb1 – image from registration page left behind on phone after install • http://djp.cc – located in the browser history on the phone left behind after install • command text messages beginning with <*10> or other numbers especially on CDMA phones • Dialing *#900900900 and send opens the registration screen when FlexiSpy is installed.
MobileSpy	• Files/data/data/com.re=na22ms6/MobileSpyData6.0.xml shows email address that is receiving exfiltrated data • /ms5-a/ms5-2.1-above.apk located on the MicroSD card in the download folder • Dialing #123456789* on the infected device brings up the MobileSpy interface.
MobiStealth	• Mobistealthv2.apk left behind after install in the MicroSD card in the download folder • Folder named "LookOut.secure" in the directory data/data on Android devices • Loggedpictures.ser file contains pictures that MobiStealth captures and uploads • Configuration.xml file contains the FTP information where exfiltrated data is uploaded to.
mSpy	• Dialing #000* and then send brings up mSpy user interface on an infected phone.
Phone Control (Android)	• Phone Control and Phone Control Key applications aren't supposed to show with their true names in the application manager, but show up as "Android System" and Android Service" as if system components. • Dialing 74283 and then send launches the application. • If secure uninstall option is enabled, attempts to uninstall the application will fail, and application must be launched with secret code and option disabled before uninstall is possible.
PhoneSheriff (Android)	• PhoneSheriff.apk located at root/media/download • Root/data/com.studio.sp2 and subfolders • Root/data/com.studio.sp2/databases/StorePS6 stores monitored data • Root/data/com.studio.sp2/databases/psRestrictions stores email address data is sent to and user preferences
SpyBubble	• data/app/com.sbradio-1.apk • radio.apk located at /mnt/sdcard/download • com.radioadv located in data/data • secret.txt containing the PIN number for SpyBubble located in data/data • buddy.txt containing the phone number of the monitoring phone located in data/data • Call log entries showing the default SpyBubble pin of #999999* or similar code beginning with a # and ending with a *
Spyera	• data/app/com.android.support-1.apk • Checkkey.XX.apx located on the MicroSD card in the download folder. • bookmark_thumb1 – image from registration page left behind on phone after install • Check web history for http://spylogs.com/db left behind after installation • Check web history for http://djp.cc left behind after installation • Check for a folder called Logs and a file inside called ownspy.log • http://www.taa.so:8080/services embedded URL beginning
TRacer	• data/app/com.process.system-1.apk • data/data/com.process.system/lib/libnotecallrec.so • data/data/com.process.system/lib/libs2callrec.so • data/data/com.process.system/lib/libkmcallrecorder.so • error message "com.process.system isn't responding"
iPhone Jailbreaking	• Cydia, MBackup, or Absinthe would all indicate jailbreaking which is necessary on an iPhone to install unauthorized applications. • Apple's Xcode can be downloaded and used to check for hidden applications running on an iPhone