PRE-INSTALLED APPLICATIONS IN ANDROID DEVICES

Abdullah ÖZBAY

TÜBİTAK BİLGEM Cyber Security Institute

Outline

- Problem
    - Supply Chain
    - Case Studies
- Research
    - Data Set
    - Ecosystem
    - Trackers
    - Exported Components
- Ongoing / Future Work
- Conclusion

Problem

- The open-source nature of the Android OS makes it possible for manufacturers to ship custom versions of the OS.
- Some vendors put pre-installed apps on devices that threaten users' privacy and security.
- Out of the box, a device often has 100-500 pre-installed apps.
- No publicly available dataset.

Supply Chain

- Android Certified Partners Program
    - Come pre-loaded with Google’s suite of apps (Play Store, YouTube, Maps, Gmail etc.)
    - Tested by Google in terms of Privacy and Security.
    - Ex. Pixel, Samsung
- Android Compatibility Program
    - Device built on AOSP
    - CDD (Compatibility Definition Document)
    - CTS (Compatibility Test Suite)
    - Doesn’t include Google Apps

Supply Chain-Approval Process

- Compatibility Test Suite (CTS)
- GMS Requirement Test Suite (GTS)
- Vendor Test Suite (VTS)
- Build Test Suite (BTS)
- Security Test Suite (STS)

Case Studies-1

- Tecno
  - Samples of Triada and xHelper Malware Families
  - Chinese Manufacturer
  - Mostly sold in Africa
  - Model W2
  - Detected by Secure-D Lab
- Blu
  - Adups FOTA
  - Model R1
  - Chinese Manufacturer
  - com.adups.fota, com.adups.fota.sysoper, com.data.acquisition, com.fw.upgrade, com.fw.upgrade.sysoper
  - Detected by KryotoWire

Case Studies-2

- OnePlus
  - PII collection
  - Backdoor that allows remote access to user’s device
  - Privilege Escalation
- Facebook
  - 2-way collaboration with vendors
- Huawei
  - Possible backdoors

Data Set

- Firmware files (system, /odm, /oem, /vendor, /product)
- 22 Vendor
- 76 Model
- 10 Different Countries
- 126.418 firmware files
  - 11.814 application files
  - 416 certificates
  - 53.895 libraries
- Only %10 of the applications found in Google Play

Ecosystem

- Vendors
  - Samsung (5477)
  - Xiaomi (1024)
  - Oppo (760)
  - Google (734)
  - OnePlus (506)
  - Huawei (478)
  - Realme (249)
  - Nokia (217)

Ecosystem – Third Parties

- Third Parties – 583 apps
- Facebook – 50
- Digital Turbine
  - com.LogiaGroup.LogiaDeck
- IronSource
  - com.ironsource.appcloud.oobe.hutchison
  - com.orange.aura.oobe"
- Buzzebees – CRM

Ecosystem – Third Parties

- id.co.babe
- Adups
- OnePlus
  - OPDeviceManager
  - EngineerMode
- Caller Identification
  - com.hiya.star
  - com.recognize.number

Trackers-1

- Google Firebase Analytics - 476
- Google AdMob – 315
- Google CrashLytics - 153
- Google Tag Manager – 107
- Facebook Login – 99
- Facebook Share – 87
- AutoNavi / Amap - 80

Trackers-2

- Google AdMob – 315
- AutoNavi / Amap - 80
- Facebook Ads – 67
- Inmobi - 36
- Flurry - 30
- Baidu Location - 15

Trackers-3

- Adjust - 13
- Amazon Advertisement - 12
- Moat - 12
- Yandex Ad - 10
- ironSource - 5

Trackers-Apps

- Deezer – 23
- Upday – 20
- Picmix Photo Editor – 17
- FlipBoard – 17
- BACA PLUS News – 15

Exported Components

- Used for inner or inter app communication
  - exported=“true” or
  - <intent-filter></intent-filter>
- Exported component can cause adversaries to access app resources
- Some apps have enormous number of exported components
- Future work

Ongoing / Future Work

- TPL analysis
- TaintFlow Analysis
- Exported Components
- Root certificates

References

- https://source.android.com/compatibility/cdd?hl=en
- https://source.android.com/compatibility/cts/downloads?hl=en
- https://source.android.com/compatibility/overview?hl=en
- https://www.android.com/certified
- https://www.android.com/certified/partners/
- https://lab.secure-d.io/triada/
- https://www.kryptowire.com/kryptowire-discovers-mobile-phone-firmware-transmitted-personally-identifiable-information-pii-without-user-consent-disclosure/
- https://www.theregister.com/2017/11/14/oneplus_backdoor/
- https://www.chrisdcmoore.co.uk/post/oneplus-analytics/
- https://www.nytimes.com/interactive/2018/06/03/technology/facebook-device-partners-users-friends-data.html
- https://www.reuters.com/article/us-eu-china-huawei-idUSKBN1O611X

Thank you for listening!
To support;
Please scan QR Code and
Install My Application