AVTOKYO2012

AV TOKYO
no drink, no hack.

Appthority

Surprising behaviors in Japanese mobile apps

contact@appthority.com | +1 (855) 346-SAFE | @GetAppthority | www.appthority.com

関ヶ原演義

関ヶ原演義
開発: D2C, Inc.
トップ デベロッパー

- Popular Android app in Japan
- App version: 1.09
- Leverages DES for encryption
- Hardcodes the private key:
  - 5b42403433653737
- Appthority App ID: 1965901

https://play.google.com/store/apps/details?id=jp.battleofsekigahara.AppSekigahara

拡散性ミリオンアーサー

拡散性ミリオンアーサー
開発: SQUARE ENIX
App を購入、ダウンロードするには iTunes を開いてください。

- Popular iOS app in Japan
- App version: 1.3.1
- App communicates with RFC1918 addresses
  - http://192.168.50.38:3009
- We often see mobile apps looking for hosts on internal networks
- Appthority App ID: 1672342

https://itunes.apple.com/jp/app/kuo-san-xingmirionasa/id497936185?l=ja&mt=8

UNO™ FREE

UNO™ FREE
開発: Gameloft
トップ デベロッパー

- Popular Android app in Japan
- App version: 1.1.1
- Executes /system/bin/chmod 777 (rwx!)
- Executes:
  - which su
  - which busybox
  - su
- Tries to determine if the phone is rooted
- Appthority App ID: 1344769

https://play.google.com/store/apps/details?id=com.gameloft.android.ANMP.GloftUFHM

探検ドリランド by GREE(グリー)

探検ドリランド by GREE(グリー)
開発: GREE, Inc.
App を購入、ダウンロードするには iTunes を開いてください。

- Popular iOS app in Japan
- App version: 1.0.7
- Does *NOT* use 位置独立コード (PIE)
- Path and developer disclosure:
  - /Users/ryosuke.inamori/ws/ios/dig/../GreeSDK/GreeSDK/Vendor/OAuthConsumer/OAMutableURLRequest.m, etc.
  - ryosuke.inamori, shinji.watanabe and xiaofan.dai
- Appthority App ID: 1571797

https://itunes.apple.com/jp/app/tan-jiandorirando-by-gree/id446748892?mt=8

Driland - Trading Card Game

Driland - Trading Card Game
開発: GREE, Inc.
トップ デベロッパー

- Popular Android app in Japan
- App version: 1.0.18
- Sends the user's IMEI and other device information to 107.20.158.229
- Enumerates apps installed on the device
- Hardcoded private keys
- Appthority App ID: 1073282

https://play.google.com/store/apps/details?id=jp.gree.android.pf.greeapp53188&hl=ja

ダークサマナー

ダークサマナー
開発: Ateam Inc.
App を購入、ダウンロードするには iTunes を開いてください。

- Popular iOS app in Japan
- App version: 1.02.00
- Uses OpenFeint API, which can be bruteforced to obtain personal info via their unauthenticated API
  - https://api.openfeint.com/users/for_device.xml?udid=c63e008e6271c3ac128eb6a242a9817528b6baef
- (Just need a list of UDIDs)
- Appthority App ID: 629643

https://itunes.apple.com/jp/app/dark-summoner-jp/id494173613?l=ja&mt=8

Pirates Age - Card Battle Game

Pirates Age - Card Battle Game
開発: GREE, Inc.
トップ デベロッパー

- Popular Android app in Japan
- App version: 1.1.5
- Sends the user's IMEI and other device information to a Amazon Web Service's Ashburn, VA data center
- Appthority App ID: 1968831

https://play.google.com/store/apps/details?id=jp.gree.android.pf.greeapp53185&hl=ja

不良道～ギャングロード～

不良道～ギャングロード～
開発: Applibot Inc.
App を購入、ダウンロードするには iTunes を開いてください。

- Popular iOS app in Japan
- App version: 2.6
- Includes a device's UDID as a query string parameter in a URL that is sent via HTTPS
  - https://ws.kg.vg/?campain_id=%@&udid=%@
- Stores connection info on DropBox!
  - https://dl.dropbox.com/u/99870167/gang_ConnectionList.json
- Appthority App ID: 1205284

https://itunes.apple.com/jp/app/bu-liang-dao-gyangurodo/id463650058?mt=8

ありがとうございます

Appthority

Looking for a job? Introduce yourself!

contact@appthority.com | +1 (855) 346-SAFE | @GetAppthority | www.appthority.com