

Reverse Engineering Android Malware



whoami

- ▶ Laurie Kirk
- ▶ Reverse Engineer
- ▶ Specialize in cross-platform malware with a focus on mobile threats
- ▶ Run YouTube channel @lauriewired



@lauriewired

Agenda

- ▶ Introduction to malware analysis
 - ▶ Why mobile RE?
- ▶ Reverse Engineering malicious Android applications
- ▶ Case study reversing SpyNote Android malware
 - ▶ Get our hands on some real malware!
- ▶ Android RE challenge

Malware Detection Flow



Threat hunter discovers potential malware



Malware sent to Reverse Engineers



RE decides malicious or clean



Writes detection to block malware

Platforms Targeted by Malware

Windows

Linux

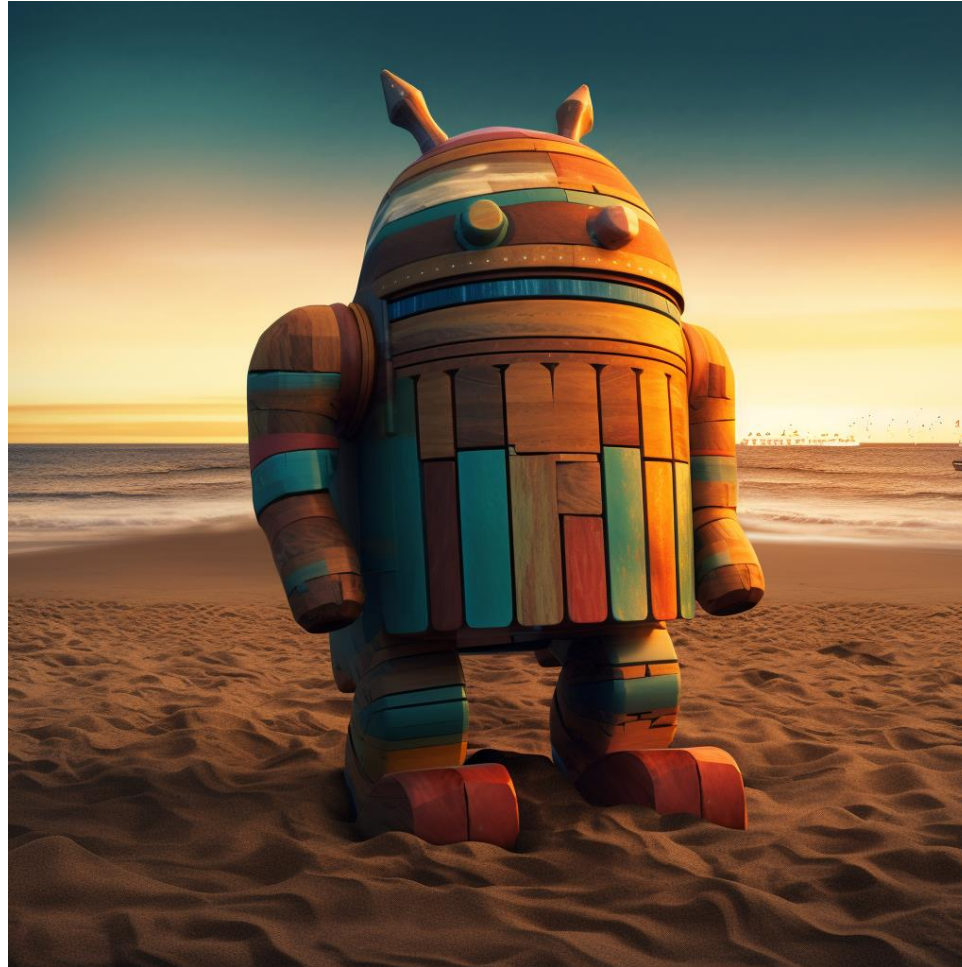
Mac

Android

iOS

Common Malware Types

- ▶ Trojan
- ▶ Ransomware
- ▶ Keylogger
- ▶ Spyware

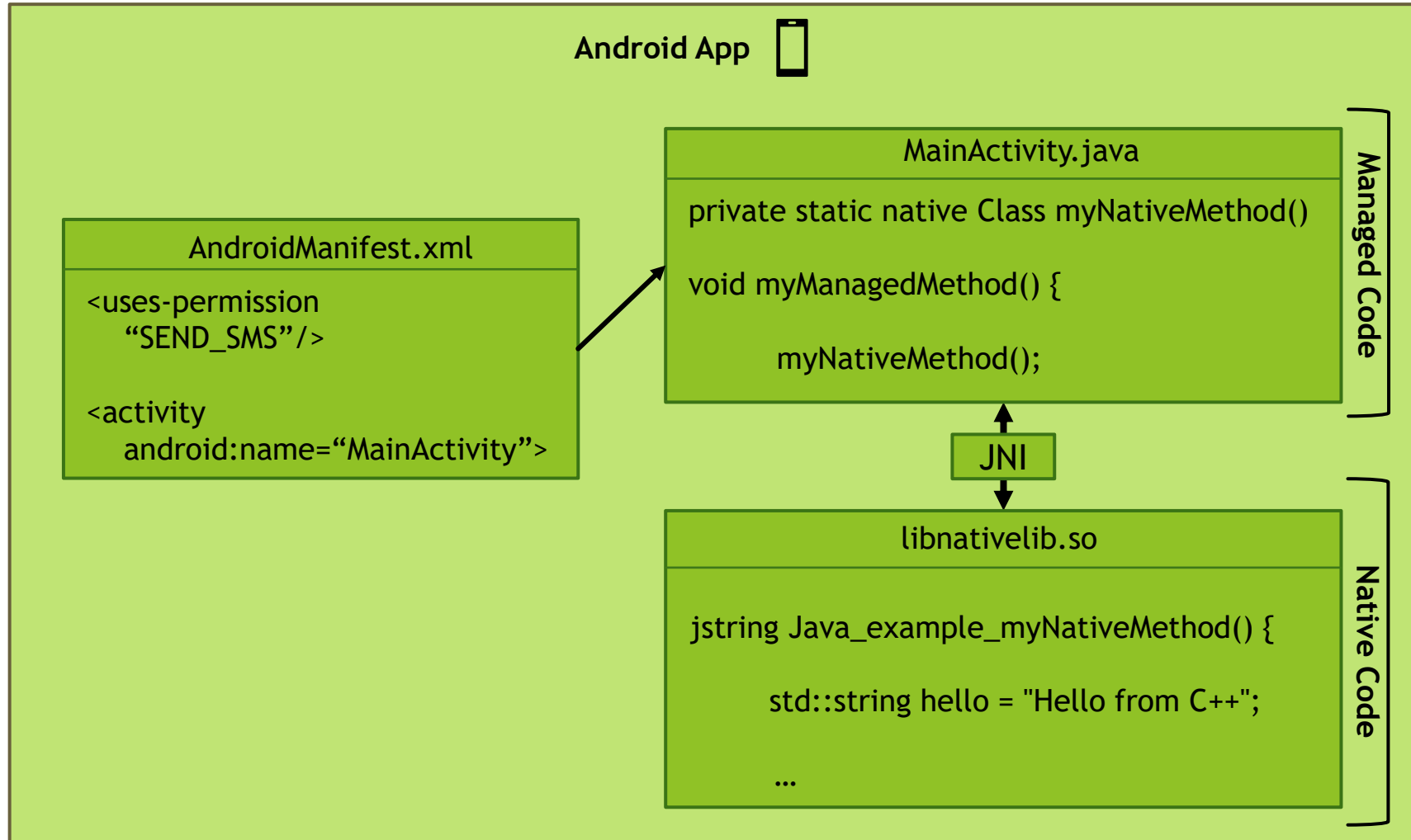


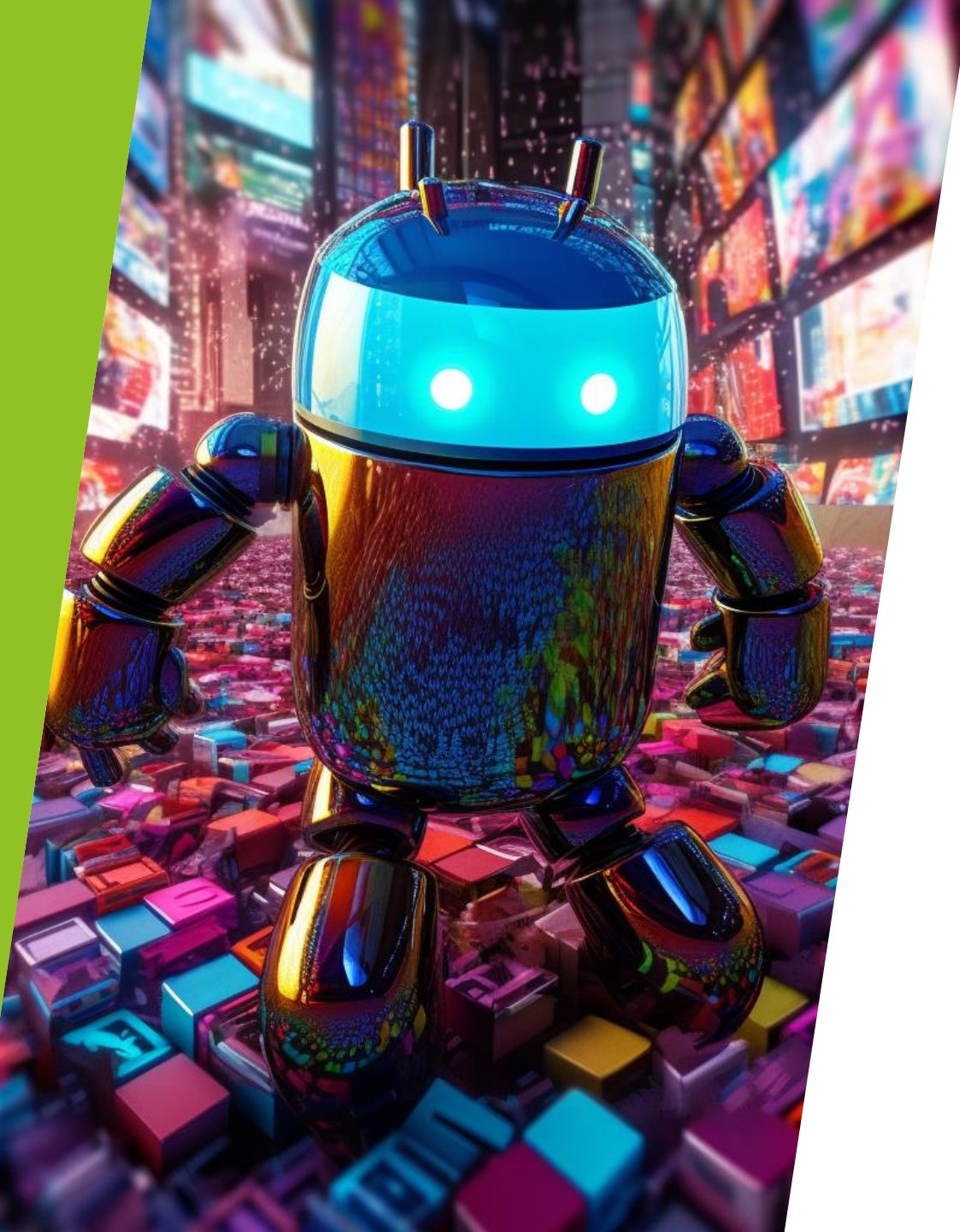
Mobile devices are a prime target for spyware.

Reversing Android Samples

The background of the slide features abstract, overlapping green geometric shapes, primarily triangles and polygons, in various shades of green, creating a modern and dynamic visual effect.

Android App Structure





Android App Components

Activities

Services

Receivers

Content
Providers

Common Tools for Android Analysis



Finding Entrypoints in the Manifest

com

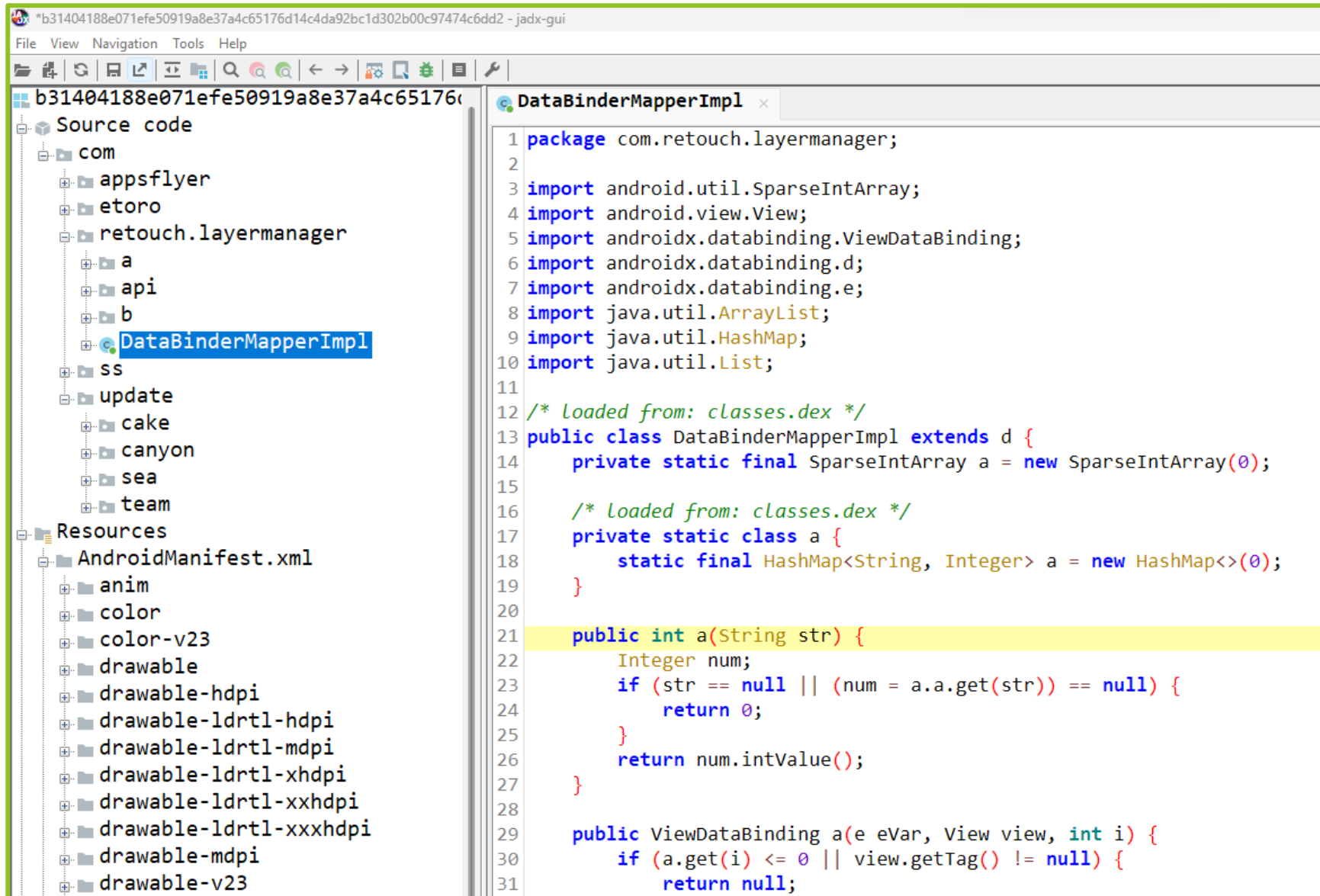
- > apireflectionmanager
- > decryptassetmanager
- > google
- > jcraft.jsch
- ▼ thenextbiggeek.squidgamewallpaper
 - > Activitys
 - > Network
 - ▼ Receivers
 - > ethnographernucleonics
 - > MyrmicidaeAlabamian
 - > stonyjointednonretrenchment
 - > unfelehotdogger
 - > Services
 - > Allobrogesqueller
 - > BuildConfig
 - > consulsalpingoscope
 - > gripeyjetsom
 - > jiltpitifulness
 - > midsentenceprefecundatory
 - > nonrecuperativesoulfostered
 - > Pimpinellarerecorded
 - > R
 - > telomiticLaputan
 - > virilizationmisinformants
 - > visonvehiculatory

AndroidManifest.xml

```
21 <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
22 <uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW"/>
23 <uses-permission android:name="android.permission.QUERY_ALL_PACKAGES"/>
24 <application android:theme="@style/Theme.AppCompat.NoActionBar" android:label="@string/app_name"
25     <activity android:name="com.thenextbiggeek.squidgamewallpaper.Activitys.sleweyedfifish" and
26     <activity android:name="com.thenextbiggeek.squidgamewallpaper.telomiticLaputan">
27         <intent-filter>
28             <action android:name="android.intent.action.MAIN"/>
29             <category android:name="android.intent.category.LAUNCHER"/>
30         </intent-filter>
31     </activity>
32     <service android:name="com.thenextbiggeek.squidgamewallpaper.Services.exophasiaenlistment"
33     <activity android:theme="@style/Theme.AppCompat.NoActionBar" android:label="" android:icon=
34     <receiver android:name="com.thenextbiggeek.squidgamewallpaper.Receivers.unfelehotdogger" and
35     <service android:name="com.thenextbiggeek.squidgamewallpaper.midsentenceprefecundatory"/>
36     <service android:name="com.thenextbiggeek.squidgamewallpaper.Services.VivaColleen"/>
37     <receiver android:name="com.thenextbiggeek.squidgamewallpaper.Receivers.ethnographernucleon
38     <service android:name="com.thenextbiggeek.squidgamewallpaper.Services.Wienckeenervator"/>
39     <service android:name="com.thenextbiggeek.squidgamewallpaper.Services.Amerosteamerload"/>
40     <activity android:name="com.thenextbiggeek.squidgamewallpaper.Activitys.uncommanderlikeFea
41     <activity android:name="com.thenextbiggeek.squidgamewallpaper.Activitys.anociationnumen"/>
42     <activity android:name="com.thenextbiggeek.squidgamewallpaper.Activitys.unshakeableearthgo
43     <activity android:name="com.thenextbiggeek.squidgamewallpaper.Activitys.Swayderwiesenboden
44     <activity android:name="com.thenextbiggeek.squidgamewallpaper.Activitys.solvsbergiteowse"/>
45     <activity android:name="com.thenextbiggeek.squidgamewallpaper.Activitys.Penningtonflatling
46     <service android:label="@string/app_name" android:name="net.godfather.thegodfather.InputSe
47         <intent-filter>
```

Main activity

Decompiling Managed Code



Case Study: SpyNote Malware

- ▶ Prevalent spyware family
- ▶ Distributed via SMS phishing campaigns
- ▶ Logs calls, SMS messages, keystrokes
- ▶ Records audio, screen, and calls
- ▶ SHA256:
eec5096dfca6824317863f9225c29f6c4b3442c48fefa62dc382e3569bca5a60

Hands On: SpyNote Malware

Common Obfuscation Techniques in Android

String Encoding / Encryption

```
TWVzc2FnZXM  
ZGV2aWNlIGFkbWluIGFwCA  
bm90aWZpY2F0aW9ucw  
UGhvbmUgYWRTaW5pc3RyYXRvcg  
U3RhcncQgcm93  
U3RhcncQgcm93  
U3RhcncQgcm93  
ZGV2aWNlIGFkbWlu  
ZGV2aWNlIGFkbWlu  
VXNlIHNlcnZpY2U  
asadadad  
asadadad  
QXBwZWZyIG9uIHRvcA  
b3ZlciBvdGhlciBhcHBz
```



| Recipe | Input |
|---|----------------------------|
| From Base64 | UGhvbmUgYWRTaW5pc3RyYXRvcg |
| Alphabet A-Za-z0-9+/= | |
| <input checked="" type="checkbox"/> Remove non-alphabet chars | |
| <input type="checkbox"/> Strict mode | |
| | REC 26 1 |
| | Output |
| | Phone administrator |

Anti-Emulation

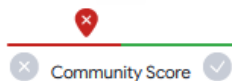
```
String locate = Resources.getSystem().getConfiguration()
if (ArrayUtils.contains(this.mw_countriesExcludeList, locate)) {
    finish();
} else if (this.mw_mainWorkClass.isEmulator()) {
} else {
    if (this.mw_mainWorkClass.PRead(this, "key") ==
```



Open-Source Detections and Rules

VirusTotal

0.tcp.ngrok.io



12 security vendors flagged this domain as malicious

Similar Graph API

0.tcp.ngrok.io

ngrok.io

Registrar
NAMECHEAP INC

Creation Date
9 years ago

Last Analysis Date
16 hours ago



Phishing and Other Frauds software-hardware spyware and malware top-1M

DETECTION

DETAILS

RELATIONS

COMMUNITY 16 +

[Join the VT Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Security vendors' analysis ⓘ

Do you want to automate checks?

| | | | |
|-------------|-----------|---------|-----------|
| Antiy-AVL | Malicious | Avira | Malware |
| BitDefender | Phishing | Certego | Malicious |
| CyRadar | Malicious | Dr.Web | Malicious |
| G-Data | Phishing | Lionic | Malicious |
| Segasec | Phishing | Sophos | Malware |
| VIPRE | Phishing | Webroot | Malicious |
| Abusix | Clean | Acronis | Clean |

Yara Rules

```
rule android_rat_androidTester : Android RAT {
  meta:
    author      = "@_lubiedo"
    date        = "2020-12-02"
    description = "Android Tester"
    malver      = "v.6.4.6"
    version     = "1.0"
  strings:
    $str00      = "Android Tester" fullword
    $str01      = "6.4.4" fullword
    $str02      = "device_admin" fullword
    $res03      = "res/drawable/abc_"
    $res04      = "res/layout/abc_"
  condition:
    uint32be(0) == 0x504B0304 // APK file signature
    and filesize < 1MB and (
      all of ($str*) and any of ($res*)
    )
}
```

Slides and Android RE Challenge



- ▶ Github repo with slides
- ▶ Android RE challenge!
 - ▶ Can you find the C2 in this SpyNote sample?
 - ▶ SHA256:
5c01f7727c78dea9c89dccf92b01b4c45e69406e
6462340779401497bf4d4589

<https://github.com/LaurieWired/ReverseEngineeringAndroidMalware>

Thank you!

Questions?

