

Android Undercover: Native Code Translation for AV Stealth

LaurieWired



whoami

- ▶ Reverse Engineer
- ▶ Specialize in cross-platform malware with a focus on mobile malware
- ▶ Run YouTube channel @lauriewired
 - ▶ Explores mobile reverse engineering
- ▶ Representing myself as an individual security researcher today



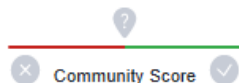
@lauriewired

Follow Along with GitHub

- ▶ https://github.com/LaurieWired/AndroidNativeObfuscation_defcon615

The only difference between this app...

6aaa73a0c642d4ec945e8af438d5a2eaf93ddb5162edda0ad675ba459cf93a83



❗ 5 security vendors and no sandboxes flagged this file as malicious



6aaa73a0c642d4ec945e8af438d5a2eaf93ddb5162edda0ad675ba459cf93a83

5.11 MB
Size

2023-04-23 22:36:06 UTC
1 minute ago



utils5.apk

android apk

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY

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

Popular threat label ❗ trojan.smsspy/anubis

Threat categories trojan banker

Family labels smsspy anubis

Security vendors' analysis ⓘ

Do you want to automate checks?

Avira (no cloud)	❗ ANDROID/Spy.SmsSpy.GAG.Gen	Cynet	❗ Malicious (score: 99)
F-Secure	❗ Malware.ANDROID/Spy.SmsSpy.GAG.Gen	Kaspersky	❗ HEUR:Trojan-Banker.AndroidOS.Anubis.n
ZoneAlarm by Check Point	❗ HEUR:Trojan-Banker.AndroidOS.Anubis.n	Acronis (Static ML)	✓ Undetected
AVAST	✓ Undetected	AVP	✓ Undetected

... and this app

c679fa2522276e1101e7062cfaea21ac35a08d38026878244dc715b8079a9f06

0

/ 65

Community Score

✔ No security vendors and no sandboxes flagged this file as malicious

c679fa2522276e1101e7062cfaea21ac35a08d38026878244dc715b8079a9f06

stringsinnative.apk

android

apk

contains-elf

5.89 MB

Size

2023-04-23 23:27:41 UTC

a moment ago

APK

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY

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?

Acronis (Static ML)	✔ Undetected	AhnLab-V3	✔ Undetected
Alibaba	✔ Undetected	ALYac	✔ Undetected
Antiy-AVL	✔ Undetected	Arcabit	✔ Undetected
Avast	✔ Undetected	Avast-Mobile	✔ Undetected
AVG	✔ Undetected	Avira (no cloud)	✔ Undetected

is partial native code
implementation.

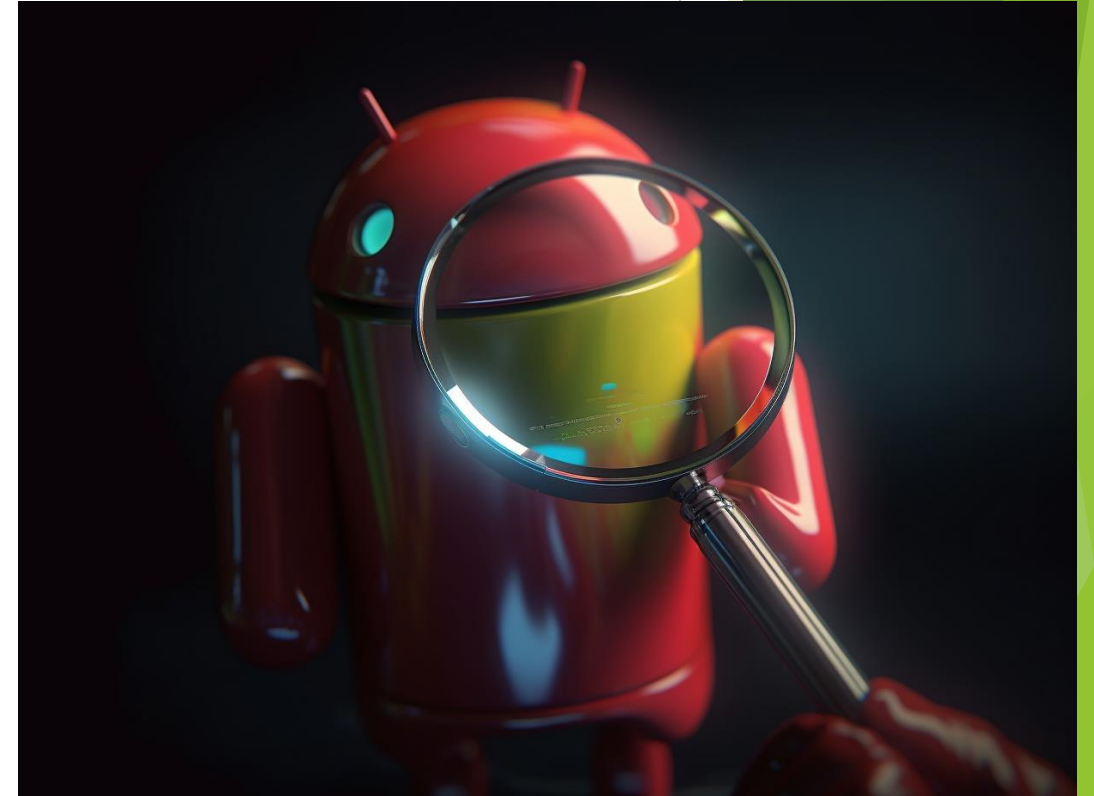
Quick background: let's define obfuscation

- ▶ Obfuscation obscures app data and functionality
- ▶ Common among all platforms
- ▶ Offensive and defensive motivations for obfuscation
- ▶ Essential for Android
 - ▶ Decompiled into pretty Java code



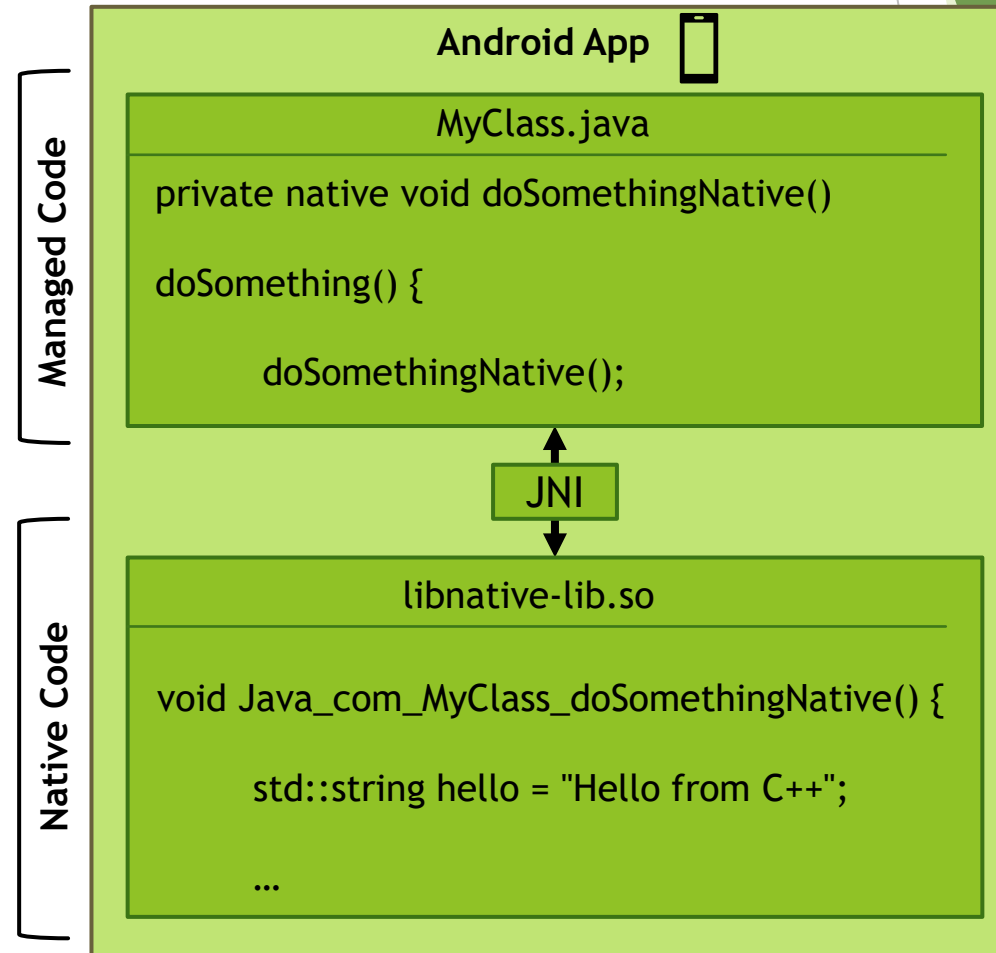
Native as an Obfuscation Technique

- ▶ Native code can hide malicious code
- ▶ More challenging to reverse engineer
 - ▶ Read assembly instead of Java
 - ▶ Understand JNI invocations
- ▶ Limit support for particular instruction set architectures
 - ▶ Remove x86 support



Android Native Code

- ▶ Android apps are written in Java / Kotlin
- ▶ Apps can also include native code
 - ▶ C/C++ code
- ▶ Communicate via the JNI



Hands-on time: Let's dive in!

1. Put on our black hat to understand native code authoring
 - a) Using Android Studio
2. Upload to VirusTotal to check detections (or lack thereof)
3. Put back on our blue hat to reverse engineer the native code
 - a) Using JADX and Ghidra



Funnily, just the presence of native code removes some smaller AV detections

3927b4868b18203de6e5b2eb208096999ee72c35d0f7d5f7f8cbb7eafc4385d0

2 / 65

Community Score

2 security vendors and no sandboxes flagged this file as malicious

3927b4868b18203de6e5b2eb208096999ee72c35d0f7d5f7f8cbb7eafc4385d0
utilsnative1.apk

android apk contains-elf

5.87 MB
Size

2023-04-23 23:08:11 UTC
a moment ago

APK

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

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

Popular threat label trojan.anubis Threat categories trojan banker Family labels anubis

Security vendors' analysis Do you want to automate checks?

Kaspersky	HEUR:Trojan-Banker.AndroidOS.Anubis.n	ZoneAlarm by Check Point	HEUR:Trojan-Banker.AndroidOS.Anubis.n
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
Alihaha	Undetected	AI Yar	Undetected

Real-World Use-Cases

- ▶ Commonly used in custom packers
 - ▶ Use native code to decrypt additional DEX file
 - ▶ Hide additional Java code invocations
- ▶ Not generally used by script kiddies
 - ▶ Too complex to implement





Next Steps

If you want more, try taking another Anubis method and converting it to native code.

Thank you!



Bonus Section



Original Java Detections Full Sample

18

/ 64

Community Score

18 security vendors and no sandboxes flagged this file as malicious

a0ae907ed93da7f6c92160f0d0218856fb7eae58cca4041b24e02882c435bb20

app-debug.apk

android apk

5.30 MB

Size

2023-04-23 20:02:22 UTC

a moment ago

APK

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY

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

Popular threat label

banker.anubis/smsspy

Threat categories

banker trojan

Family labels

anubis smsspy andr

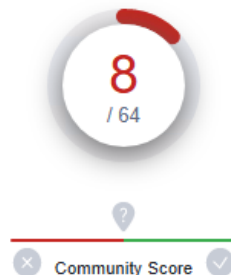
Security vendors' analysis

Do you want to automate checks?

Avast	Android:Banker-SZ [Trj]	Avast-Mobile	Android:Banker-SZ [Trj]
AVG	Android:Banker-SZ [Trj]	Avira (no cloud)	ANDROID/Spy.SmsSpy.GAG.Gen
ClamAV	Andr.Trojan.Anubis-6692604-3	Cynet	Malicious (score: 99)
Cyren	AndroidOS/Banker.AA.gen!Eldorado	ESET-NOD32	Multiple Detections
F-Secure	Malware.ANDROID/Spy.SmsSpy.GAG.Gen	Fortinet	Android/Agent.AOV!tr.spy
Google	Detected	Ikarus	Trojan-Banker.AndroidOS.Anubis
K7GW	Trojan (0056edb51)	Kaspersky	HEUR:Trojan-Banker.AndroidOS.Anubis.n
Microsoft	TrojanSpy:AndroidOS/Anubis.AIMTB	QuickHeal	Android.Anubis.GEN34618
Sophos	Andr/Dropr-HO	ZoneAlarm by Check Point	HEUR:Trojan-Banker.AndroidOS.Anubis.n

First step removing partial codebase

fdcb53f9f26414e61da6776a0c6f1bb1f3c74fe0231cc63cf031e87bf7361506



⚠ 8 security vendors and no sandboxes flagged this file as malicious

fdcb53f9f26414e61da6776a0c6f1bb1f3c74fe0231cc63cf031e87bf7361506

app-debug.apk

android apk

5.12 MB
Size

2023-04-23 21:14:39 UTC
a moment ago



DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY

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

Popular threat label ⚠ **banker.anubis/smsspy**

Threat categories **banker** **trojan**

Family labels **anubis** **smsspy**

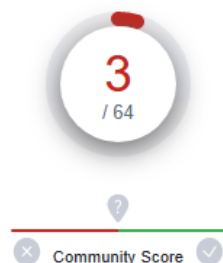
Security vendors' analysis ⓘ

Do you want to automate checks?

Avira (no cloud)	⚠ ANDROID/Spy.SmsSpy.GAG.Gen	Cynet	⚠ Malicious (score: 99)
ESET-NOD32	⚠ A Variant Of Android/Spy.Banker.AMC	F-Secure	⚠ Malware.ANDROID/Spy.SmsSpy.GAG.Gen
Fortinet	⚠ Android/Agent.AOV!tr.spy	Kaspersky	⚠ HEUR:Trojan-Banker.AndroidOS.Anubis.n
QuickHeal	⚠ Android.Anubis.GEN30551	ZoneAlarm by Check Point	⚠ HEUR:Trojan-Banker.AndroidOS.Anubis.n
Acronis (Static ML)	✅ Undetected	AhnLab-V3	✅ Undetected

Anubis-specific detections gone when removing target method

20fe8f748048ca2aef7856a7032f2a99253014ee49ab2ebac94d04f5acf359f5



❗ 3 security vendors and no sandboxes flagged this file as malicious

20fe8f748048ca2aef7856a7032f2a99253014ee49ab2ebac94d04f5acf359f5

utils6.apk

android apk

5.11 MB
Size

2023-04-23 22:38:19 UTC
a moment ago



DETECTION

DETAILS

RELATIONS

BEHAVIOR C

COMMUNITY

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

Popular threat label ❗ smsspy

Family labels smsspy

Security vendors' analysis ⓘ

Do you want to automate checks?

Avira (no cloud)	❗ ANDROID/Spy.SmsSpy.GAG.Gen	Cynet	❗ Malicious (score: 99)
F-Secure	❗ Malware.ANDROID/Spy.SmsSpy.GAG.Gen	Acronis (Static ML)	✓ Undetected
AhnLab-V3	✓ Undetected	Alibaba	✓ Undetected
ALYac	✓ Undetected	Antiy-AVL	✓ Undetected
Arcabit	✓ Undetected	Avast	✓ Undetected