

Reverse Android malware like a Jedi

Axelle Apvrille, Fortinet

Virus Bulletin Conference, October 2021

① Introduction

② Unpacking

③ Obfuscation

④ CnC

⑤ Static analysis

⑥ Conclusion

Who am I?



Axelle Apvrille, @cryptax

Principal Security Researcher for Mobile Malware and IoT at



Lead organizer of smart devices CTF



Advanced tools for Android reverse engineering



Dexcalibur - 2019

[https://github.com/
FrenchYeti/dexcalibur](https://github.com/FrenchYeti/dexcalibur)

House

House - 2018

[https:
//github.com/nccgroup/house](https://github.com/nccgroup/house)



MobSF - 2015

[https://github.com/MobSF/
Mobile-Security-Framework-MobSF](https://github.com/MobSF/Mobile-Security-Framework-MobSF)

QUARK

Quark - 2019

[https://github.com/
quark-engine/quark-engine](https://github.com/quark-engine/quark-engine)

① Introduction

② Unpacking

③ Obfuscation

④ CnC

⑤ Static analysis

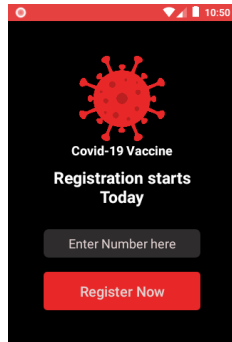
⑥ Conclusion

You need this for Dynamic Analysis



Emulator

FRIDA
Frida server <https://github.com/frida/frida/releases/>
and client!



Sample of Android/Oji.G!worm
Malware (APK)

1 Introduction

2 Unpacking

3 Obfuscation

4 CnC

5 Static analysis

6 Conclusion

1 Introduction

2 Unpacking

3 Obfuscation

4 CnC

5 Static analysis

6 Conclusion

① Introduction

② Unpacking

③ Obfuscation

④ CnC

⑤ Static analysis

⑥ Conclusion

- ① Introduction
- ② Unpacking
- ③ Obfuscation
- ④ CnC
- ⑤ Static analysis
- ⑥ Conclusion**

From user point of view...

	Dexcalibur	House	MobSF	Quark
Setup	★	★ ★	★ ★ ★	★ ★ ★
Use	★ ★ ★	★	★ ★	★ ★ ★

personal opinion - all tools are actually awesome!

Which tool? (preferred choices only)

Unpacking

Dexcalibur

Network monitoring

De-obfuscate

House

File or shared prefs monitoring

General API monitoring

MobSF

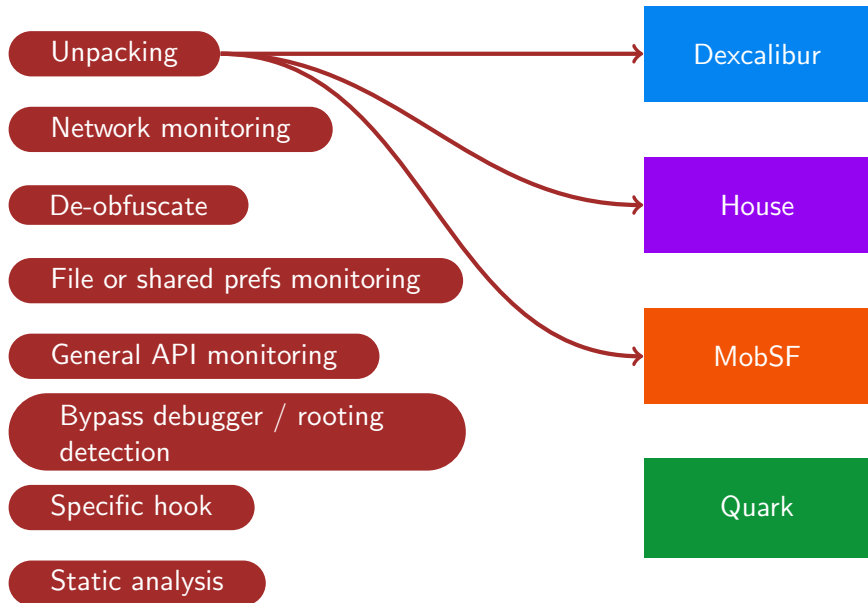
Bypass debugger / rooting
detection

Specific hook

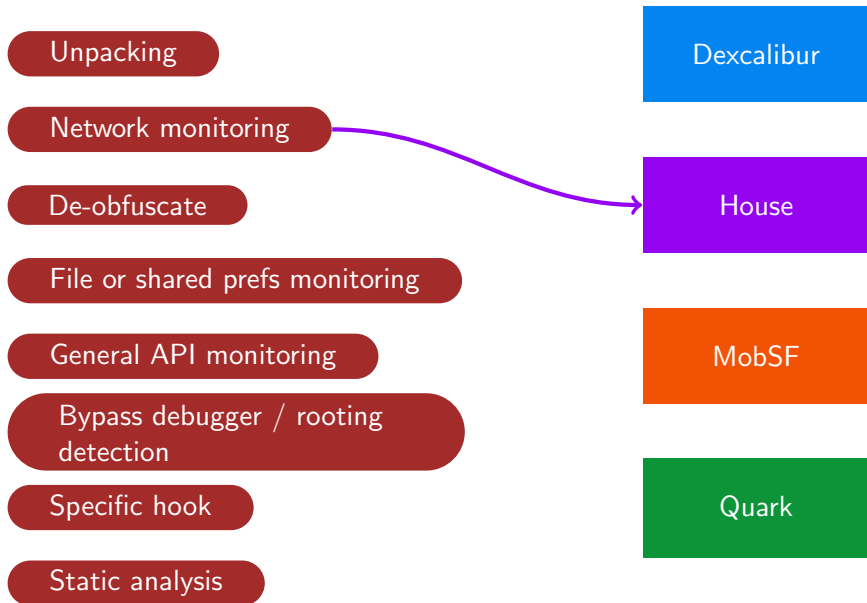
Quark

Static analysis

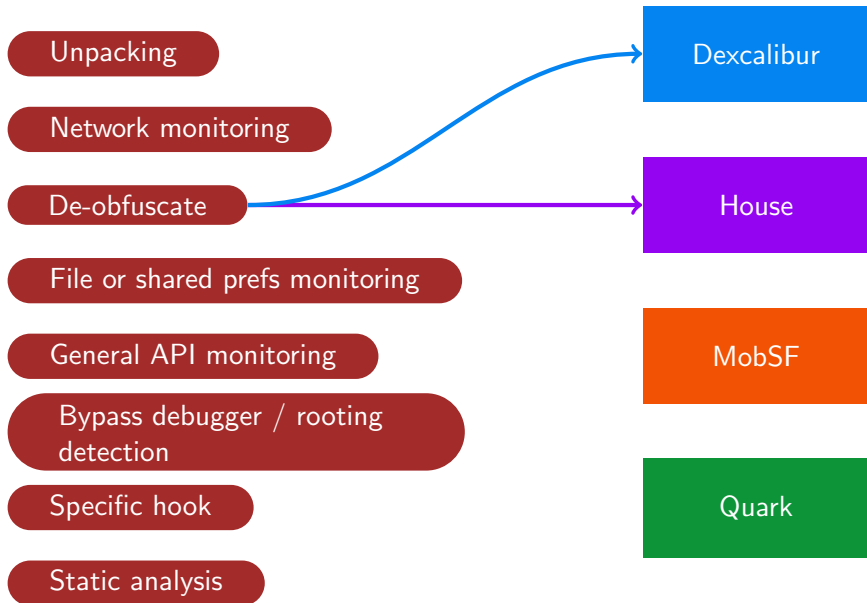
Which tool? (preferred choices only)



Which tool? (preferred choices only)



Which tool? (preferred choices only)



Which tool? (preferred choices only)

Unpacking

Network monitoring

De-obfuscate

File or shared prefs monitoring

General API monitoring

Bypass debugger / rooting
detection

Specific hook

Static analysis

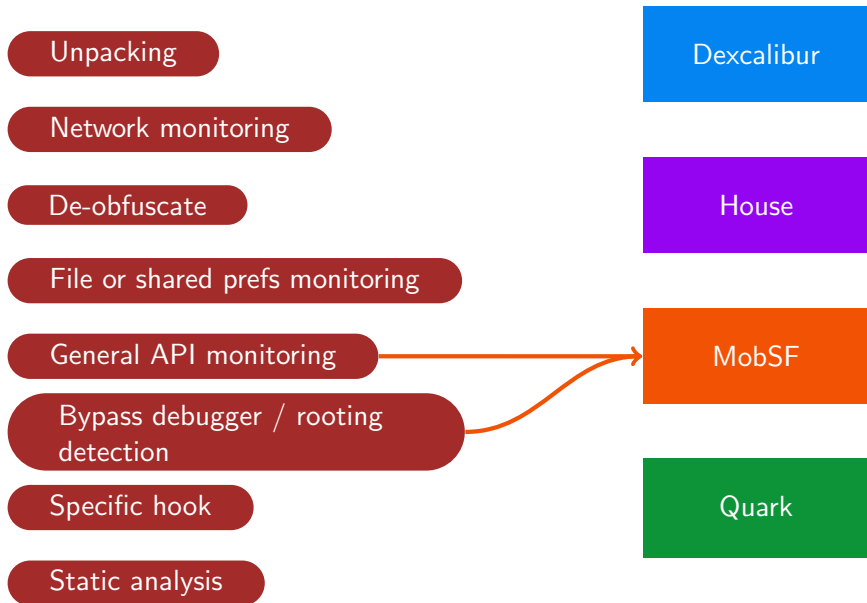
Dexcalibur

House

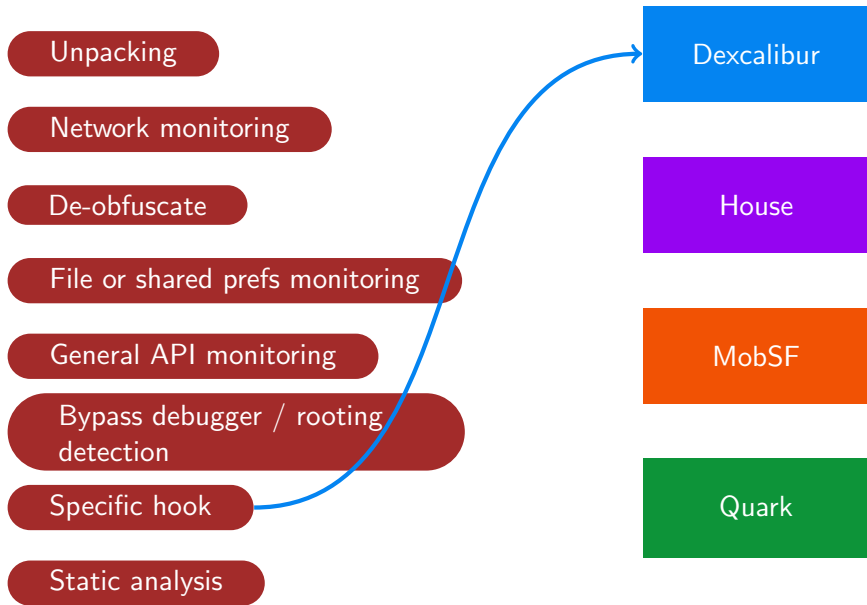
MobSF

Quark

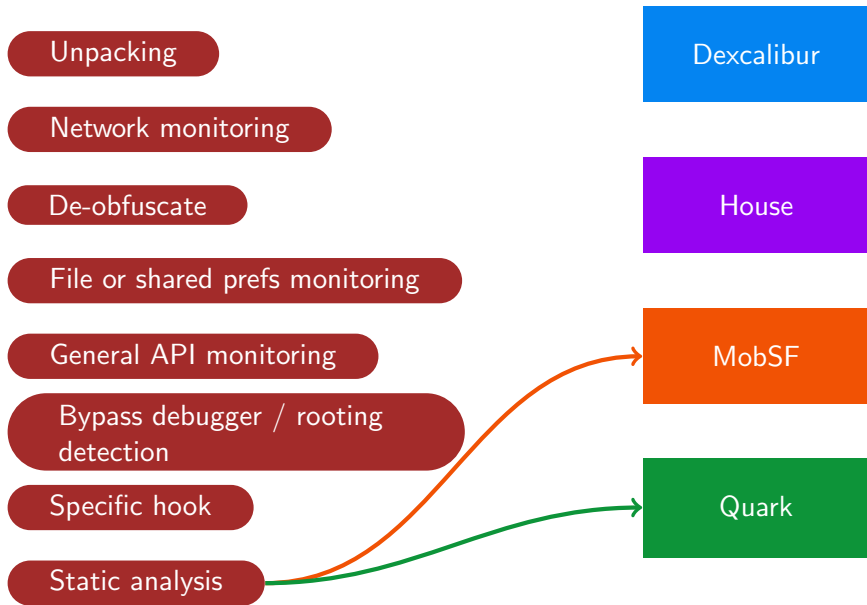
Which tool? (preferred choices only)



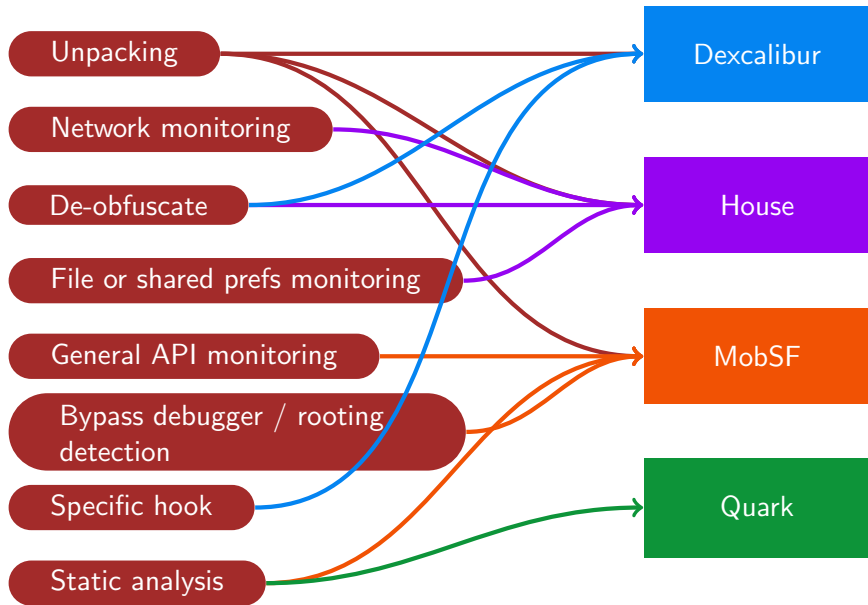
Which tool? (preferred choices only)



Which tool? (preferred choices only)



Which tool? (preferred choices only)



Advanced advanced features?

If you can do it with **Frida**,
you can *probably* do it with [replace]
replace = Dexcalibur/House/MobSF

- In memory DEX loading
- Native unpacking
- Native anti-reversing
- Native de-obfuscation
- ...

but it might be as easy to use Frida *directly*
If you can't do it with Frida.... unlucky!

Thanks for your attention!

Axelle Apvrille

Email: aapvrille (at) fortinet (dot) com

Twitter: @cryptax

The Fortinet logo is displayed within a white rectangular box. It features the word "FORTINET" in a bold, black, sans-serif font. The letter "O" is replaced by a red square icon composed of a 3x3 grid of smaller squares, with the center square missing. A registered trademark symbol (®) is located at the end of the word.

FORTINET®

AxL
2016