Defensive Lab Agency

Pithus: let's open the Android pandora's box

PassTheSalt - 05/07/2021

Esther Onfroy

@U039b

Expert in Android security and reverse engineering, Esther *a.k.a.* U039b is a French hacktivist and speaker.

Co-founder:

- ↗ Defensive Lab Agency > defensive-lab.agency
- ↗ Exodus Privacy > exodus-privacy.eu.org
- ↗ Echap > echap.eu.org
- ↗ Pithus > beta.pithus.org
- ↗ PiRanhaLysis > piranhalysis.github.io

What my days are made of

- Penetration testing
- Regulatory compliance audits
- RE of malware & SDK
- Expert witness
- Craft free software
- Give talks in Froglish
- Awareness & trainings

I work for lawyers, DPO, CISO, NGO, academics, journalists, ...

Wh[at|y] Pithus?

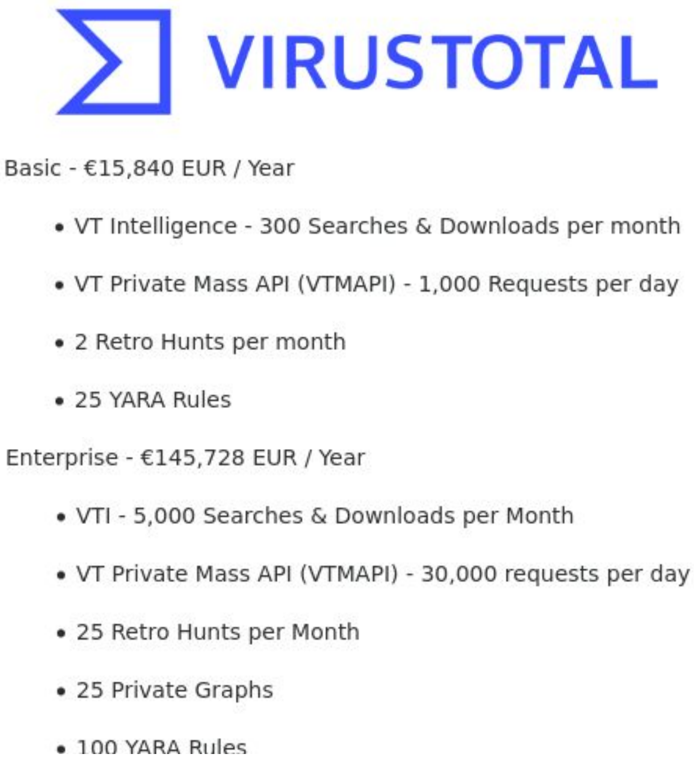
Why?

Candid reason:

Try to answer the lack of open threat intelligence tools for the Android world.

Political reason:

Threat intel. and analysis should be available for all and not the property of a private company.



Basic - €15,840 EUR / Year

- VT Intelligence - 300 Searches & Downloads per month
- VT Private Mass API (VTMAPI) - 1,000 Requests per day
- 2 Retro Hunts per month
- 25 YARA Rules

Enterprise - €145,728 EUR / Year

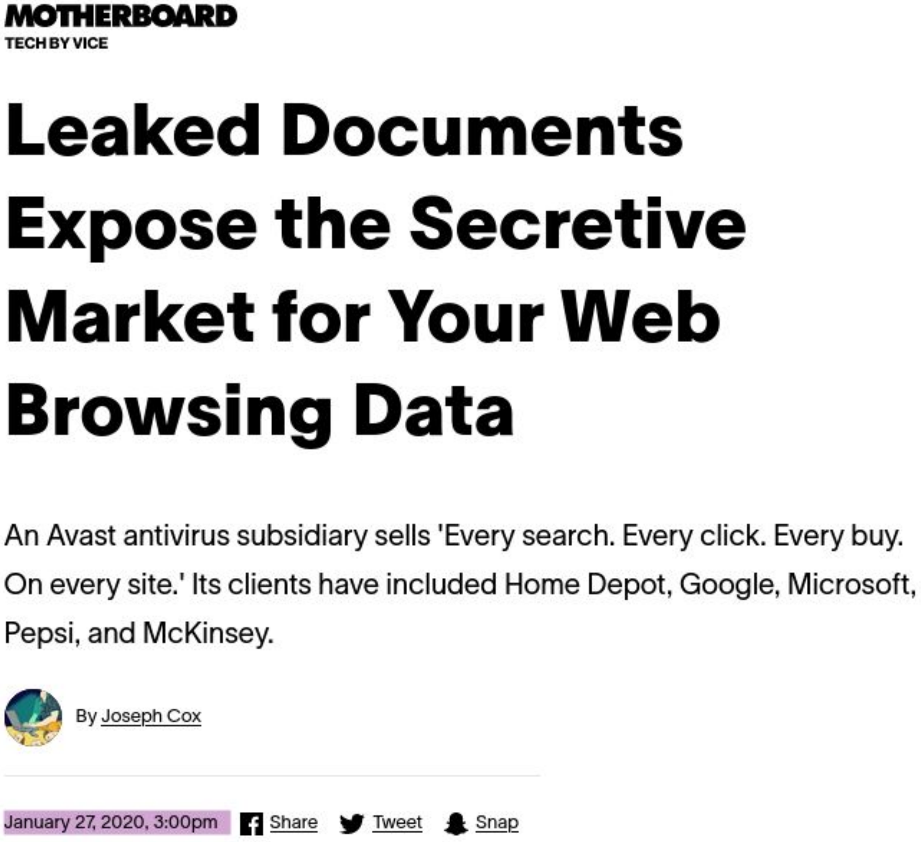
- VTI - 5,000 Searches & Downloads per Month
- VT Private Mass API (VTMAPI) - 30,000 requests per day
- 25 Retro Hunts per Month
- 25 Private Graphs
- 100 YARA Rules

Why!

Long story short.

Privacy activists asked Avast for APKLab increased quotas.

Avast said they want more recognition in the privacy community after the scandal last year and refused.



MOTHERBOARD
TECH BY VICE

Leaked Documents Expose the Secretive Market for Your Web Browsing Data

An Avast antivirus subsidiary sells 'Every search. Every click. Every buy. On every site.' Its clients have included Home Depot, Google, Microsoft, Pepsi, and McKinsey.

By Joseph Cox

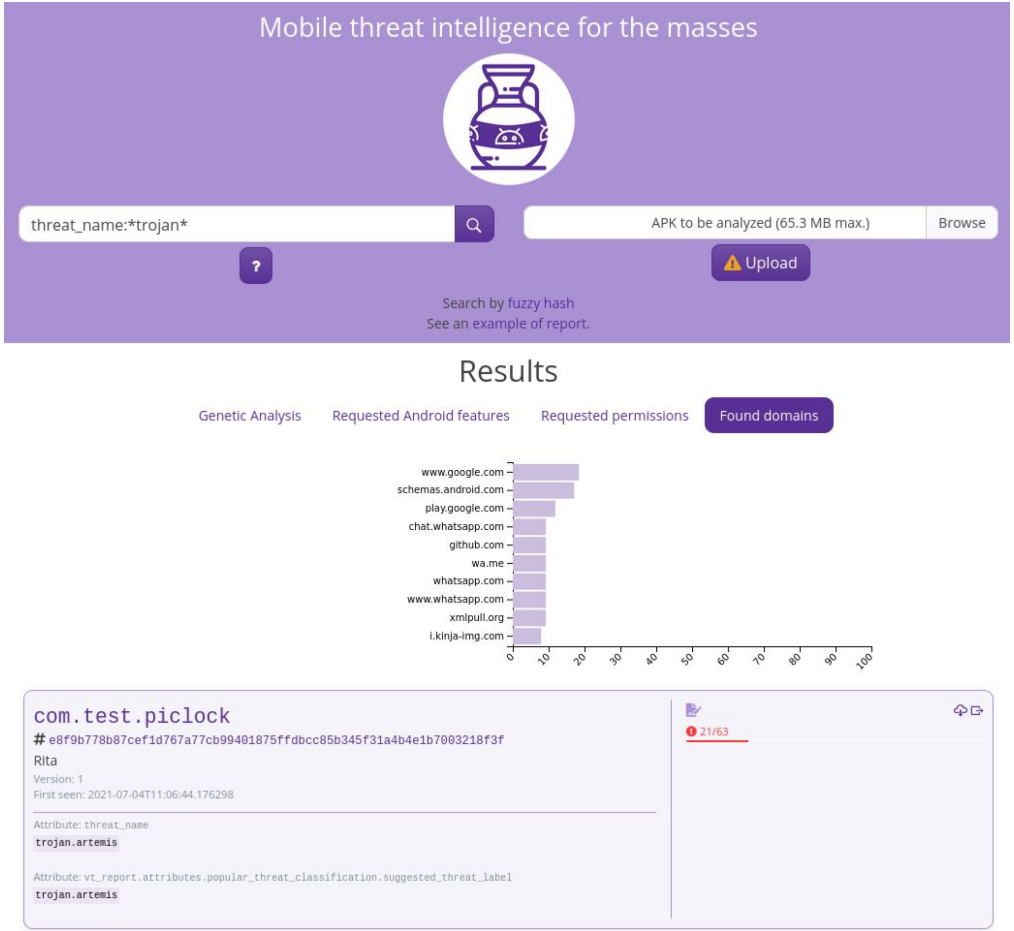
January 27, 2020, 3:00pm

What

Mobile threat intelligence playground for the masses.

- Open source platform
- Driven by its community
- Based on existing FOSS tools
- Self-hostable

https://beta.pithus.org



Mobile threat intelligence for the masses

threat_name:*trojan*

Search by fuzzy hash
See an example of report.

Results

com.test.piclock

e8f9b778b87cef1d767a77cb99401875ffdbcc85b345f31a4b4e1b7003218f3f

Rita

Version: 1

First seen: 2021-07-04T11:06:44.176298

Attribute: threat_name

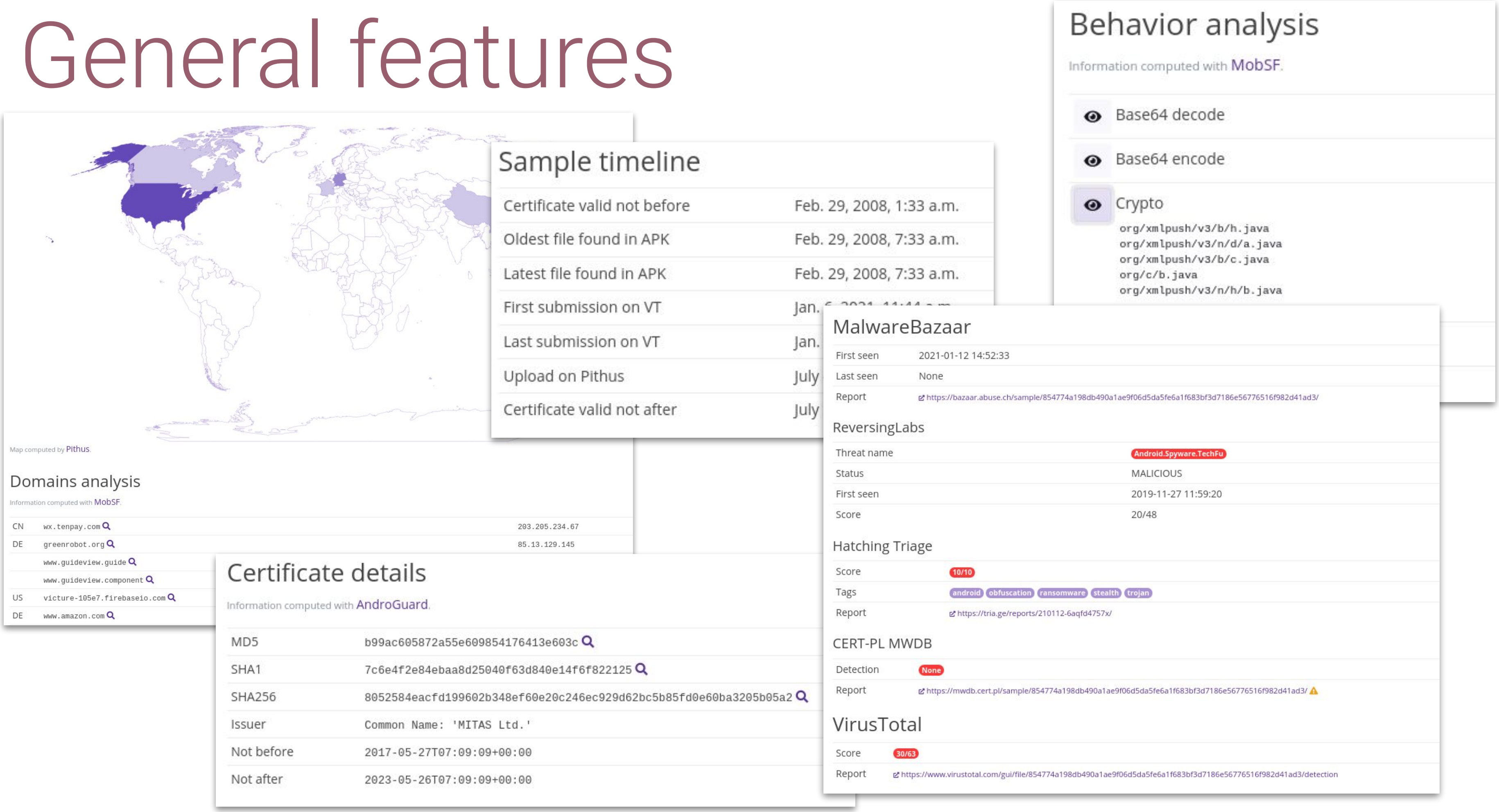
`trojan.artemis`

Attribute: vt_report.attributes.popular_threat_classification.suggested_threat_label

`trojan.artemis`

21/63

General features



Map computed by Pithus.

Domains analysis

Information computed with MobSF.

CN	wx.tenpay.com	203.205.234.67
DE	greenrobot.org	85.13.129.145
	www.guideview.guide	
	www.guideview.component	
US	victure-105e7.firebaseio.com	
DE	www.amazon.com	

Sample timeline

Certificate valid not before	Feb. 29, 2008, 1:33 a.m.
Oldest file found in APK	Feb. 29, 2008, 7:33 a.m.
Latest file found in APK	Feb. 29, 2008, 7:33 a.m.
First submission on VT	Jan. 6, 2021, 11:44 a.m.
Last submission on VT	Jan.
Upload on Pithus	July
Certificate valid not after	July

Certificate details

Information computed with AndroGuard.

MD5	b99ac605872a55e609854176413e603c
SHA1	7c6e4f2e84ebaa8d25040f63d840e14f6f822125
SHA256	8052584eacfd199602b348ef60e20c246ec929d62bc5b85fd0e60ba3205b05a2
Issuer	Common Name: 'MITAS Ltd.'
Not before	2017-05-27T07:09:09+00:00
Not after	2023-05-26T07:09:09+00:00

Behavior analysis

Information computed with MobSF.

- Base64 decode
- Base64 encode
- Crypto

```
org/xmlpush/v3/b/h.java
org/xmlpush/v3/n/d/a.java
org/xmlpush/v3/b/c.java
org/c/b.java
org/xmlpush/v3/n/h/b.java
```

MalwareBazaar

First seen	2021-01-12 14:52:33
Last seen	None
Report	https://bazaar.abuse.ch/sample/854774a198db490a1ae9f06d5da5fe6a1f683bf3d7186e56776516f982d41ad3/

ReversingLabs

Threat name	Android.Spyware.TechFu
Status	MALICIOUS
First seen	2019-11-27 11:59:20
Score	20/48

Hatching Triage

Score	10/10
Tags	android obfuscation ransomware stealth trojan
Report	https://tria.ge/reports/210112-6aqfd4757x/

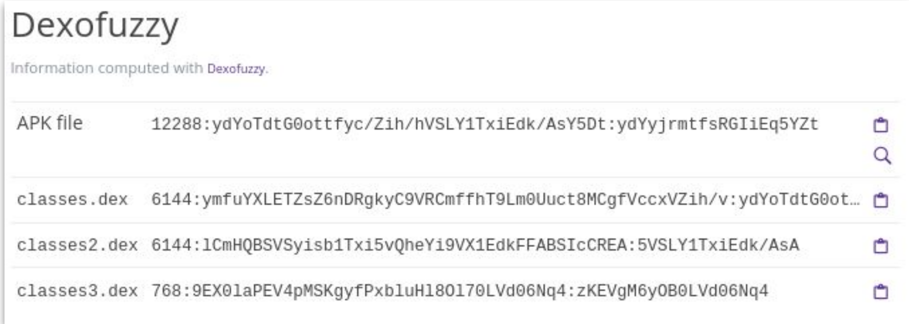
CERT-PL MWDB

Detection	None
Report	https://mwdb.cert.pl/sample/854774a198db490a1ae9f06d5da5fe6a1f683bf3d7186e56776516f982d41ad3/ ⚠

VirusTotal

Score	30/63
Report	https://www.virustotal.com/gui/file/854774a198db490a1ae9f06d5da5fe6a1f683bf3d7186e56776516f982d41ad3/detection

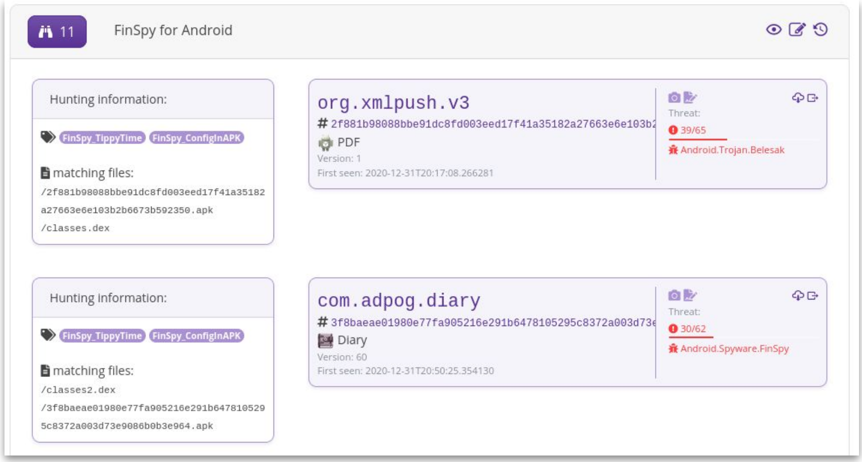
Threat intelligence



Dexofuzzy

Information computed with Dexofuzzy.

APK file	`12288:ydYoTdtG0ottfyc/Zih/hVSLY1TxiEdk/AsY5Dt:ydYyjrmtfsRGIiEq5YZt`
classes.dex	`6144:ymfuYXLETZsZ6nDRgkyC9VRCmffhT9Lm0Uuct8MCgfVccxVZih/v:ydYoTdtG0ot…`
classes2.dex	`6144:lCmHQBSVSyisb1Txi5vQheYi9VX1EdkFFABSIcCREA:5VSLY1TxiEdk/AsA`
classes3.dex	`768:9EX0laPEV4pMSKgyfPxbluHl8Ol70LVd06Nq4:zKEVgM6yOB0LVd06Nq4`



11 FinSpy for Android

Hunting information:

FinSpy_TippyTime FinSpy_ConfigInAPK

matching files:

```
/2f881b98088bbe91dc8fd003eed17f41a35182
a27663e6e103b2b6673b592350.apk
/classes.dex
```

org.xmlpush.v3

2f881b98088bbe91dc8fd003eed17f41a35182a27663e6e103b2

PDF

Version: 1

First seen: 2020-12-31T20:17:08.266281

Threat:

39/65

Android.Trojan.Belesak

Hunting information:

FinSpy_TippyTime FinSpy_ConfigInAPK

matching files:

```
/classes2.dex
/3f8baeae01980e77fa905216e291b647810529
5c8372a003d73e9086b0b3e964.apk
```

com.adpog.diary

3f8baeae01980e77fa905216e291b6478105295c8372a003d73e

Diary

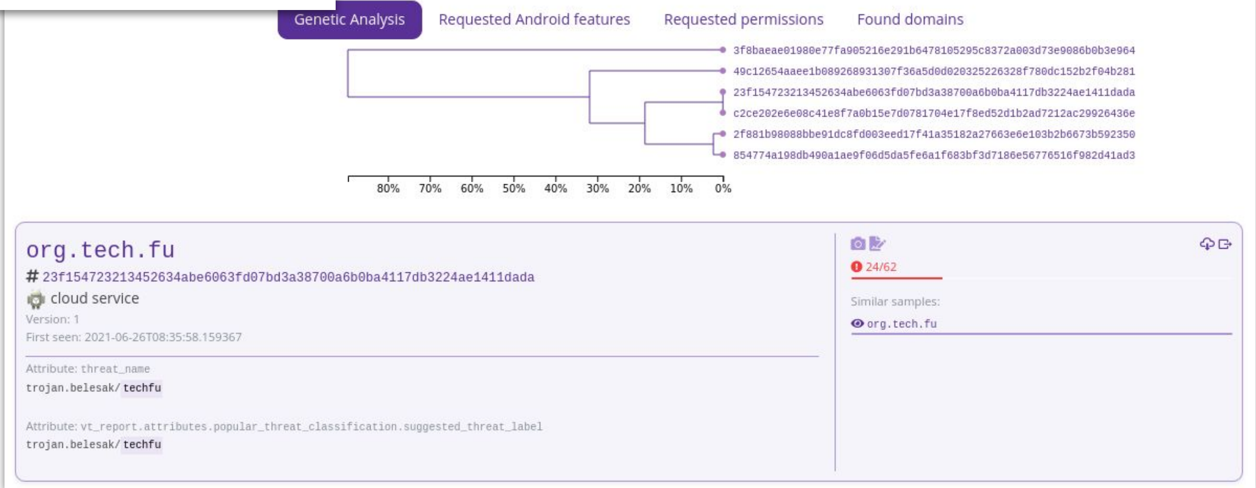
Version: 60

First seen: 2020-12-31T20:50:25.354130

Threat:

30/62

Android.Spyware.FinSpy


Genetic Analysis
Requested Android features
Requested permissions
Found domains
3f8baeae01980e77fa905216e291b6478105295c8372a003d73e9086b0b3e964
49c12654aaee1b089268931307f36a5d0d020325226328f780dc152b2f04b281
23f154723213452634abe6063fd07bd3a38700a6b0ba4117db3224ae1411dada
c2ce202e6e08c41e8f7a0b15e7d0781704e17f8ed52d1b2ad7212ac29926436e
2f881b98088bbe91dc8fd003eed17f41a35182a27663e6e103b2b6673b592350
854774a198db490a1ae9f06d5da5fe6a1f683bf3d7186e56776516f982d41ad3
80%
70%
60%
50%
40%
30%
20%
10%
0%

org.tech.fu

23f154723213452634abe6063fd07bd3a38700a6b0ba4117db3224ae1411dada

cloud service

Version: 1

First seen: 2021-06-26T08:35:58.159367

Attribute: threat_name

trojan.belesak/ techfu

Attribute: vt_report.attributes.popular_threat_classification.suggested_threat_label

trojan.belesak/ techfu

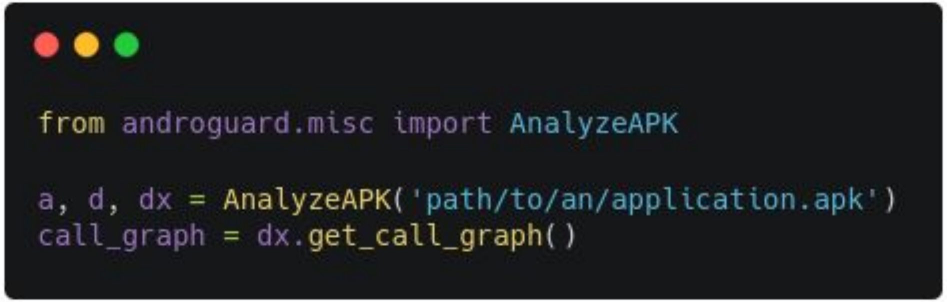
24/62

Similar samples:

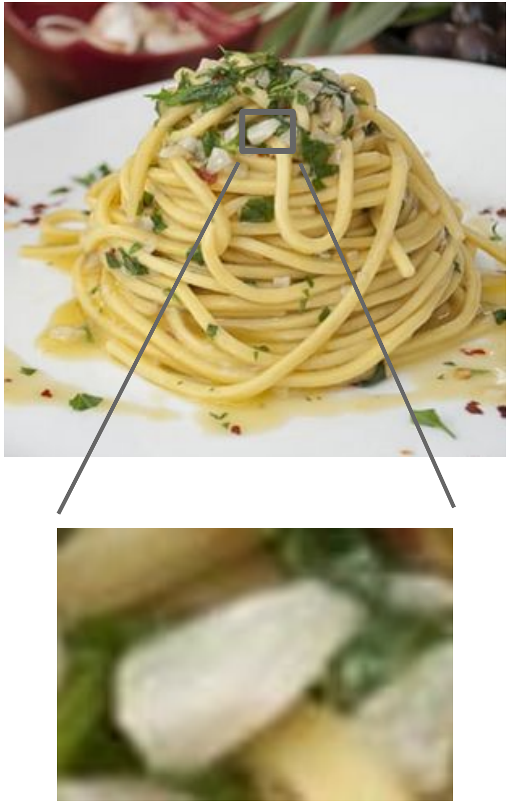
org.tech.fu

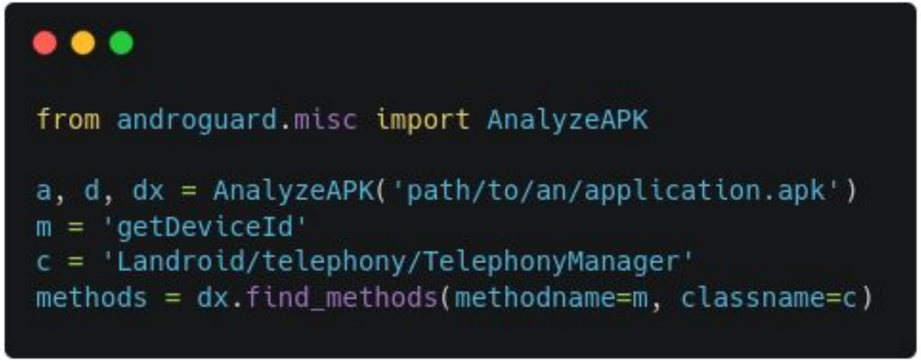
CFG dissection

Extract entire CFG



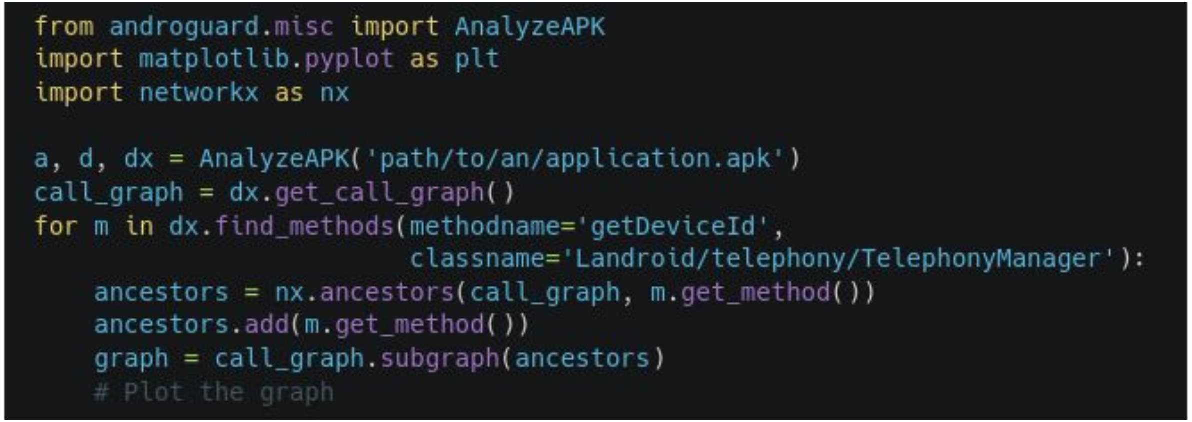
```python
from androguard.misc import AnalyzeAPK

a, d, dx = AnalyzeAPK('path/to/an/application.apk')
call_graph = dx.get_call_graph()
```



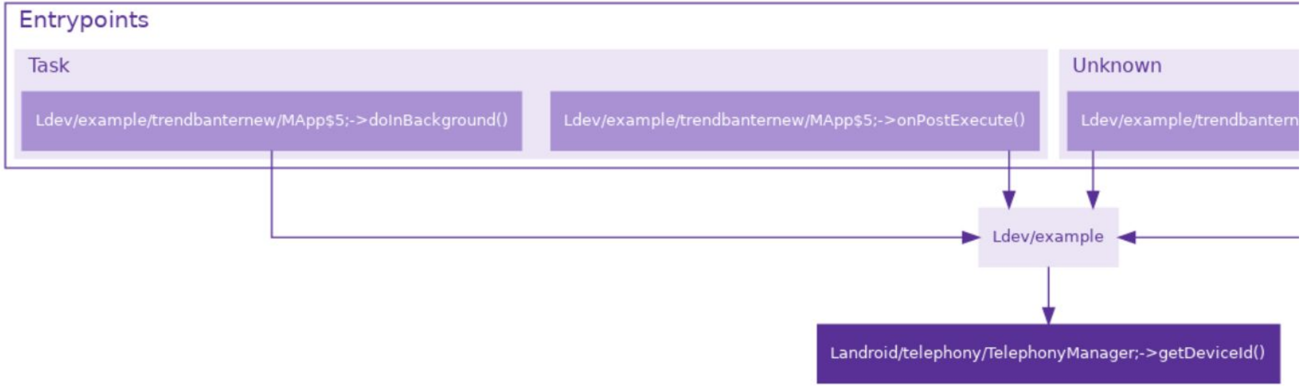


```python
from androguard.misc import AnalyzeAPK

a, d, dx = AnalyzeAPK('path/to/an/application.apk')
m = 'getDeviceId'
c = 'Landroid/telephony/TelephonyManager'
methods = dx.find_methods(methodname=m, classname=c)
```

Extract API CFG



```
from androguard.misc import AnalyzeAPK
import matplotlib.pyplot as plt
import networkx as nx

a, d, dx = AnalyzeAPK('path/to/an/application.apk')
call_graph = dx.get_call_graph()
for m in dx.find_methods(methodname='getDeviceId',
                         classname='Landroid/telephony/TelephonyManager'):
    ancestors = nx.ancestors(call_graph, m.get_method())
    ancestors.add(m.get_method())
    graph = call_graph.subgraph(ancestors)
    # Plot the graph
```


Entrypoints
Task
Ldev/example/trendbanternew/MApp$5;->doInBackground()
Ldev/example/trendbanternew/MApp$5;->onPostExecute()
Unknown
Ldev/example/trendbantern
Ldev/example
Landroid/telephony/TelephonyManager;->getDeviceId()

How to compare CFG?

1. For each sample:
   a. count the number of entrypoints per type for each API
   b. flatten into a vector of *n* dimensions
2. Compute pairwise distances*
3. Normalize with magic**
4. Compute hierarchical clustering
5. Plot dendrogram

$$\left\{\begin{array}{cccc} & EType_1 & EType_2 & EType_j \\ API_1 & 0 & 12 & \ldots \\ API_2 & 0 & 0 & \ldots \\ API_3 & 0 & \ldots & \ldots \\ API_4 & 7 & \ldots & \ldots \\ API_i & \ldots & \ldots & \ldots \end{array}\right\}$$

1521 dimensions in Pithus:
- 117 tracked APIs (*i*)
- 13 entrypoint types (*j*)

* euclidean or Jaccard

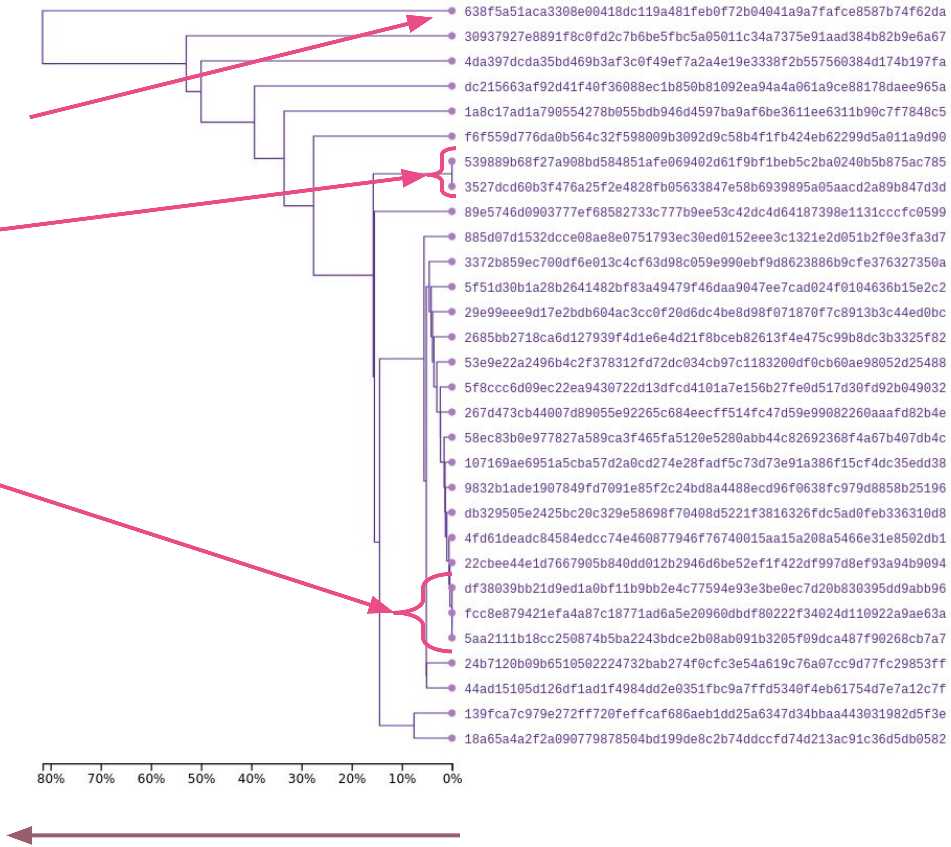
** cross multiplication

The result

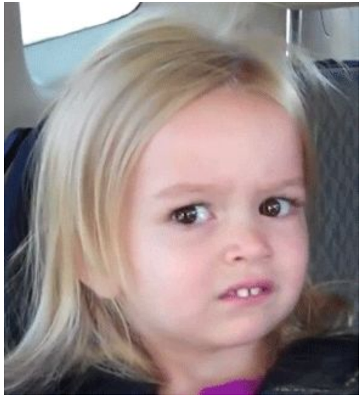
One sample totally different of all the others

Isolated similar samples

Similar samples probably part of a larger cluster



percentage of difference



Conclusion

Conclusion

- Still in *beta*
- 3 active contributors
- Has detected FinSpy hidden in Wire

And

- Need feedbacks
- Need contributions
- Need brain juice
- Need more tests, yes, more!

Come and experiment!

Thank you!

esther@defensive-lab.agency

Q/A