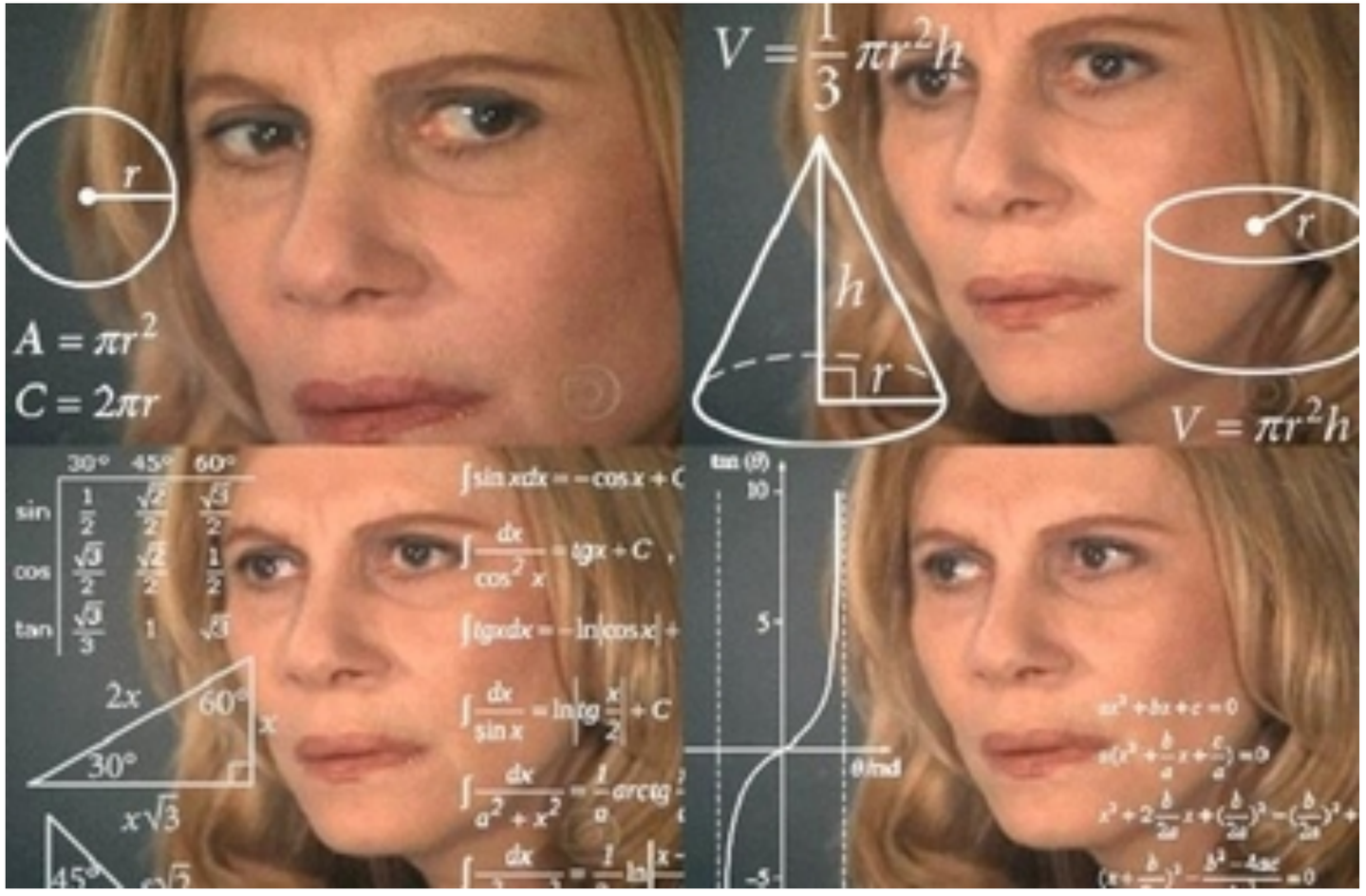
Detecting command and control on MacOS



Whoami

- Anje Knottnerus
- Background in Data Science and Engineering
- Detection Engineer at Adyen

adyen

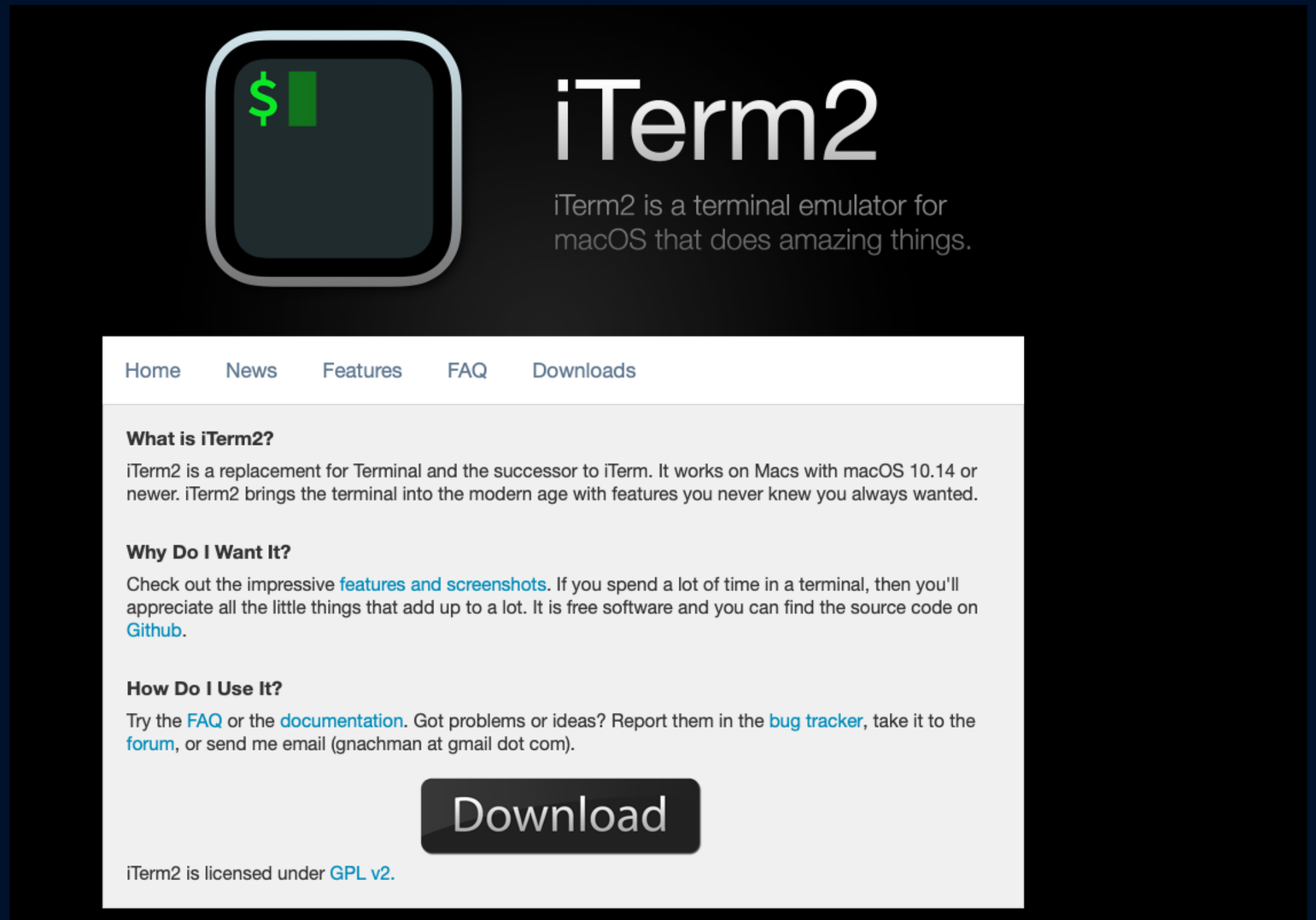

r
$A = \pi r^2$
$C = 2\pi r$
$V = \frac{1}{3}\pi r^2 h$
h
r
r
$V = \pi r^2 h$
30° 45° 60°
sin
cos
tan
2x
60°
30°
x
$x\sqrt{3}$
45°
$\int \sin x dx = -\cos x + C$
$\int \frac{dx}{\cos^2 x} = \operatorname{tg} x + C$
$\int \operatorname{tg} x dx = -\ln|\cos x| +$
$\int \frac{dx}{\sin x} = \ln\left|\operatorname{tg}\frac{x}{2}\right| + C$
$\int \frac{dx}{a^2 + x^2} = \frac{1}{a}\operatorname{arctg}$
tan (θ)
10
5
-5
θ rad
$ax^2 + bx + c = 0$

Universal | Simple

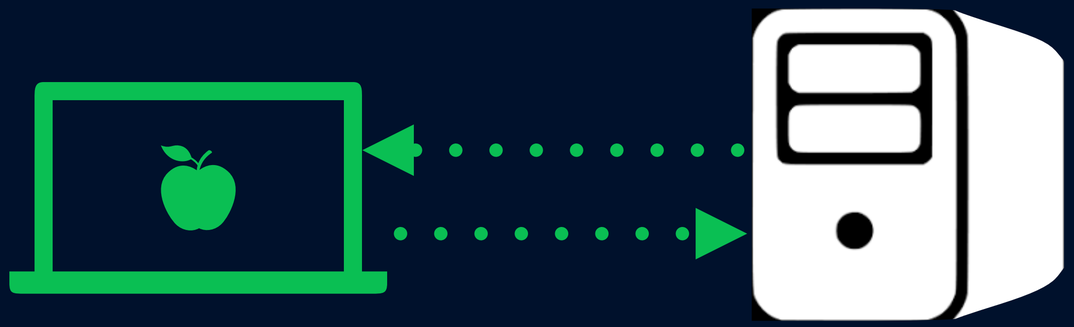
What is command and control?



ZuRu


iTerm2
iTerm2 is a terminal emulator for macOS that does amazing things.
Home
News
Features
FAQ
Downloads
What is iTerm2?
iTerm2 is a replacement for Terminal and the successor to iTerm. It works on Macs with macOS 10.14 or newer. iTerm2 brings the terminal into the modern age with features you never knew you always wanted.
Why Do I Want It?
Check out the impressive features and screenshots. If you spend a lot of time in a terminal, then you'll appreciate all the little things that add up to a lot. It is free software and you can find the source code on Github.
How Do I Use It?
Try the FAQ or the documentation. Got problems or ideas? Report them in the bug tracker, take it to the forum, or send me email (gnachman at gmail dot com).
Download
iTerm2 is licensed under GPL v2.

ZuRu ft. Kephri

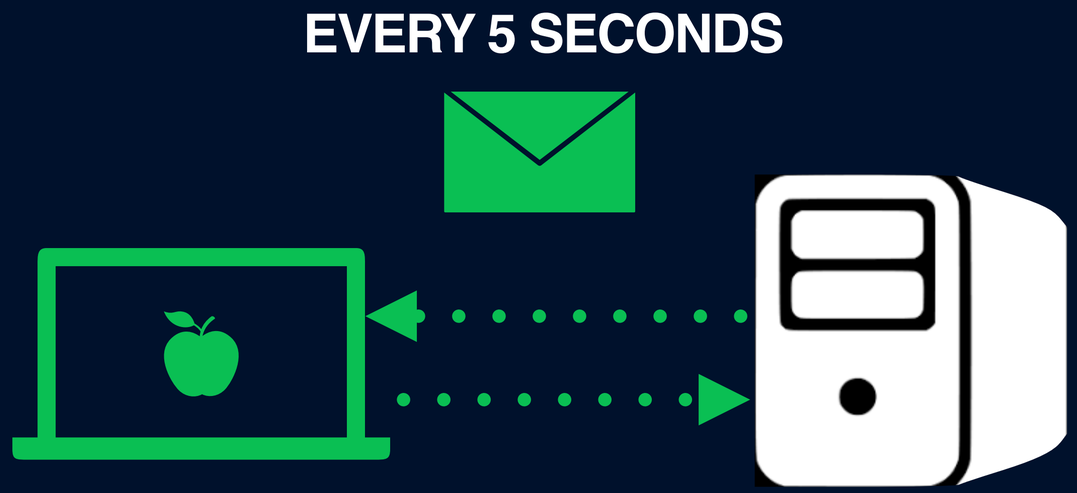


Address	Entry
0x1000192a1	exec::task_get_host_info
0x100019319	exec::task_kill_process
0x1000193f4	exec::task_get_process_list
0x1000193fc	exec::task_get_disk_list
0x1000194c7	exec::task_get_file_list
0x1000198ce	exec::task_get_cmd_rsp
0x100019abb	exec::task_download_file
0x10001a026	exec::task_upload_file
0x10001a45e	exec::task_delete_file
0x10001a54d	exec::task_exec_file

Thec2matrix.com

30	P	Python	R	S	HTTP	U	V	W	X	Y	Z	AA	AB
			Channel										
Name	macOS	Implementation	TCP	HTTP	HTTP2	HTTP3	DNS	DoH	ICMP	FTP	IMAP	MAPI	SMB
AdaptixC2	Yes	golang/C++ QT	Yes	Yes	No	No	No	No	No	No	No	No	Yes
Alchimist	Yes												
Ares	Yes	Python	No	Yes	No	No	No	No	No	No	No	No	No
CALDERA	Yes	pip3	No	Yes	No	No	No	No	No	No	No	No	No
CHAOS	Yes	Go	Yes	No	No	No	No	No	No	No	No	No	No
Core Impact	Yes	binary	Yes	Yes	No	No	Yes	No	No	No	No	No	Yes
DeimosC2	Yes	Golang	Yes	Yes	No	No	No	Yes	No	No	No	No	No
Empire	Yes	install.sh	No	Yes	No	No	No	No	No	No	No	No	No
EvilOSX	Yes	pip3	No	Yes	No	No	No	No	No	No	No	No	No
godoh	Yes	binary	No	No	No	No	Yes	Yes	No	No	No	No	No
ibombshell	Yes	pip3	No	Yes	No	No	No	No	No	No	No	No	No
INNUENDO	Yes	install.sh	No	Yes	No	No	Yes	No	Yes	Yes	Yes	Yes	Yes
MacShellSwift	Yes	python	No	Yes	No	No	No	No	No	No	No	No	No
Merlin	Yes	Binary	No	Yes	Yes	Yes	No	No	No	No	No	No	No

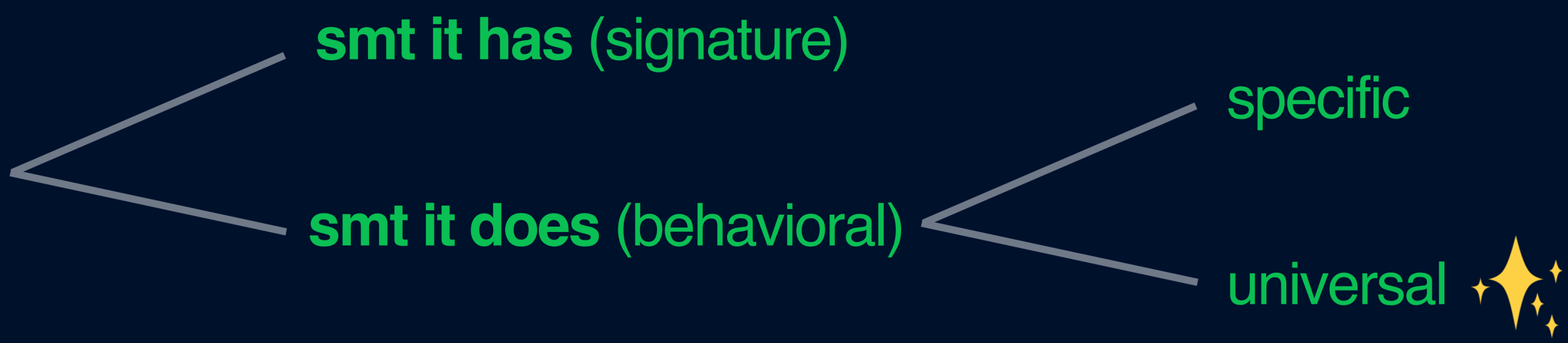
Kephri agent





How to C2 detect in a universal way?

adyen


smt it has (signature)
smt it does (behavioral)
specific
universal

adyen

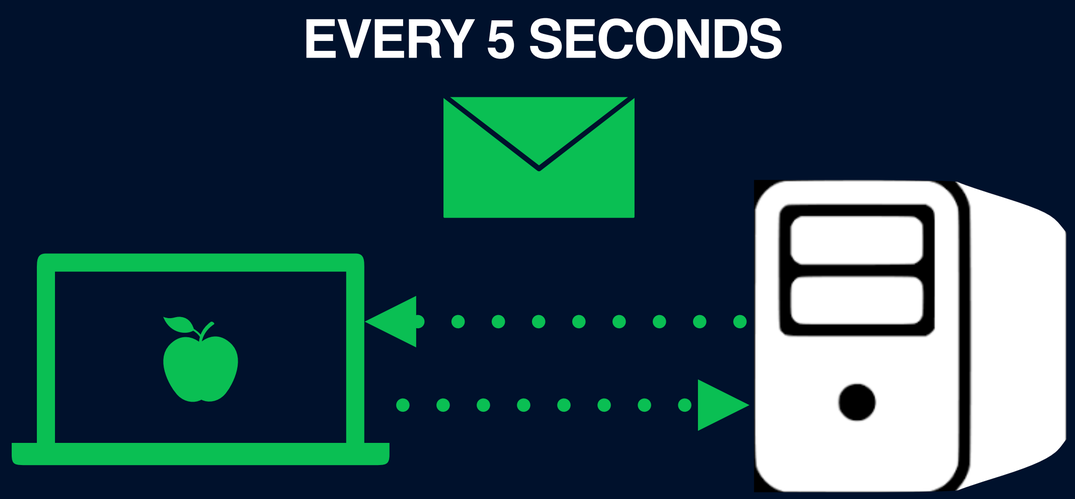

WHACK THE HACKER!
HIGH SCORE:
404
PLAYER 1
0



How to C2 detect in a universal way?

adyen

Beaconing





How to C2 detect in a simple way?

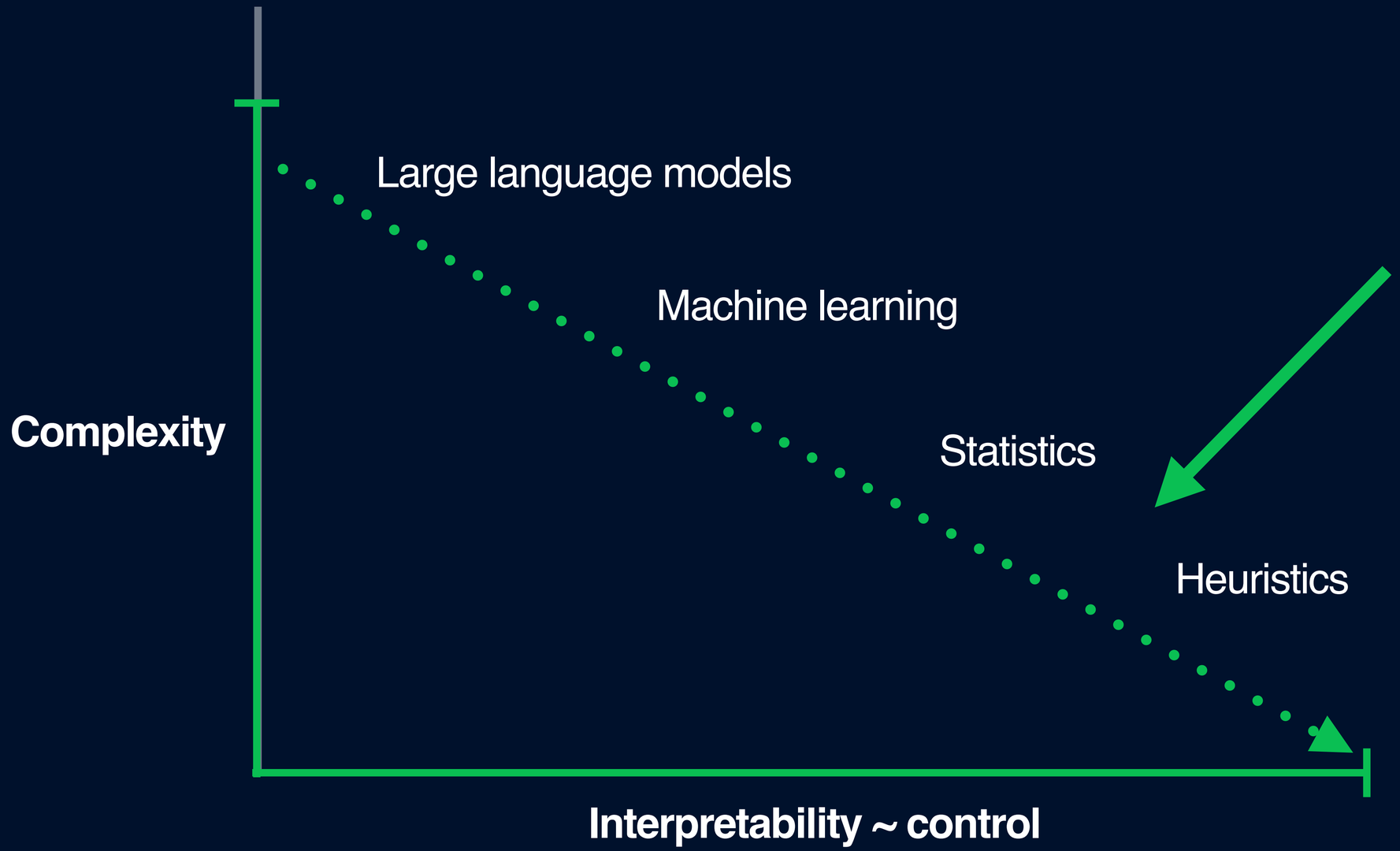




AI






Large language models
Machine learning
Statistics
Heuristics
Complexity
Interpretability ~ control



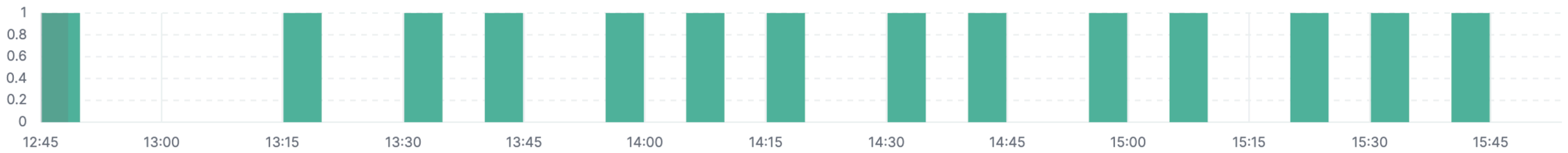
How to detect C2 in a simple way?

adyen

Beaconing

14 hits

Chart options



Jun 20, 2025 @ 12:48:23.773 - Jun 20, 2025 @ 15:53:49.811

Time	host.name	dnsmasq.qname	destination.ip
Jun 20, 2025 @ 15:44:38.000	mb-anje	totallynotac2.belastinqdienst.com	
Jun 20, 2025 @ 15:32:20.000	mb-anje	totallynotac2.belastinqdienst.com	
Jun 20, 2025 @ 15:20:13.000	mb-anje	totallynotac2.belastinqdienst.com	
Jun 20, 2025 @ 15:07:55.000	mb-anje	totallynotac2.belastinqdienst.com	

Beaconing configuration

Parameter	Value
Callback Host Modified	https:/ [redacted] izureedge.net
Callback Interval in seconds	10
Callback Jitter in percent	23



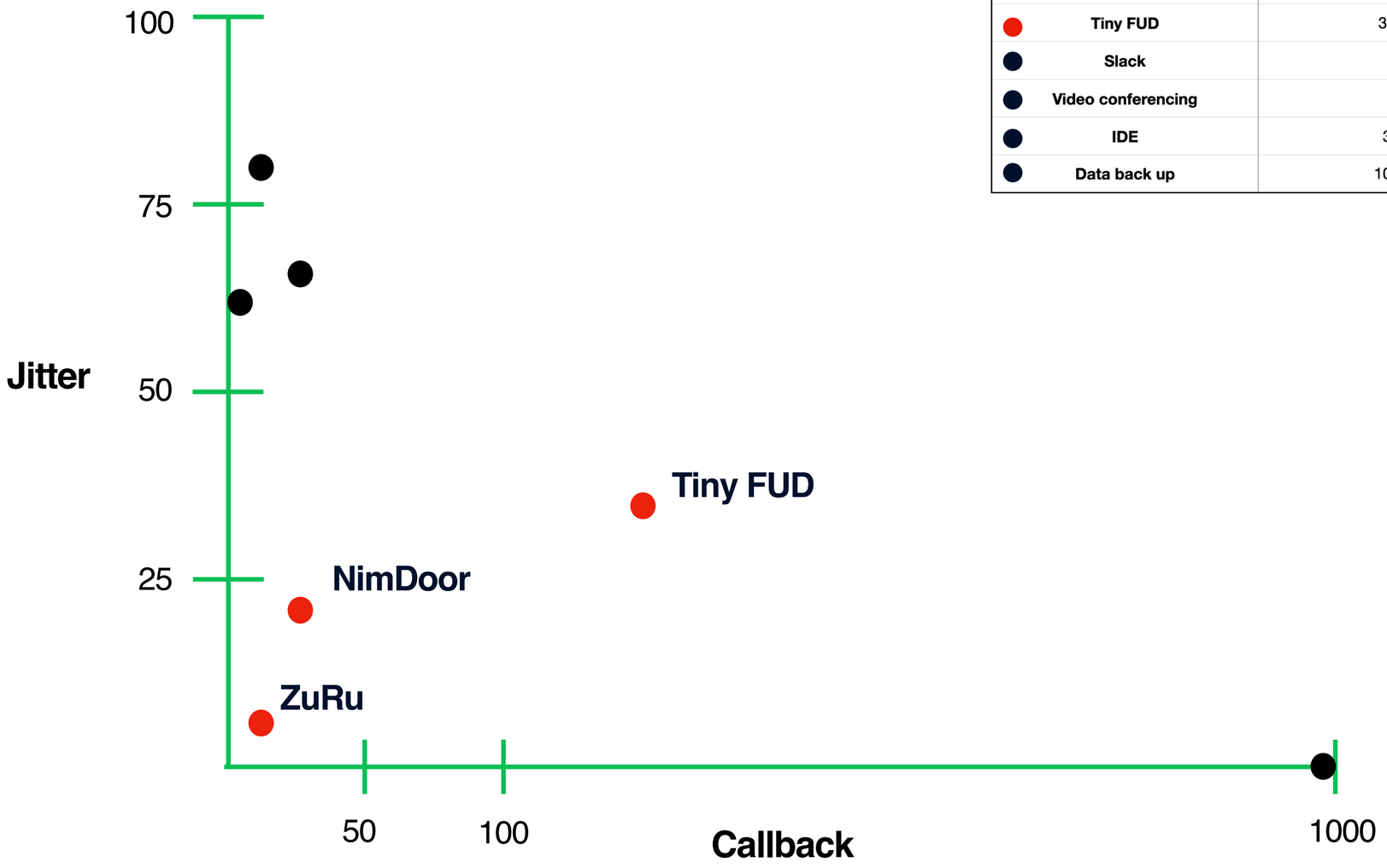
Callback and jitter estimate

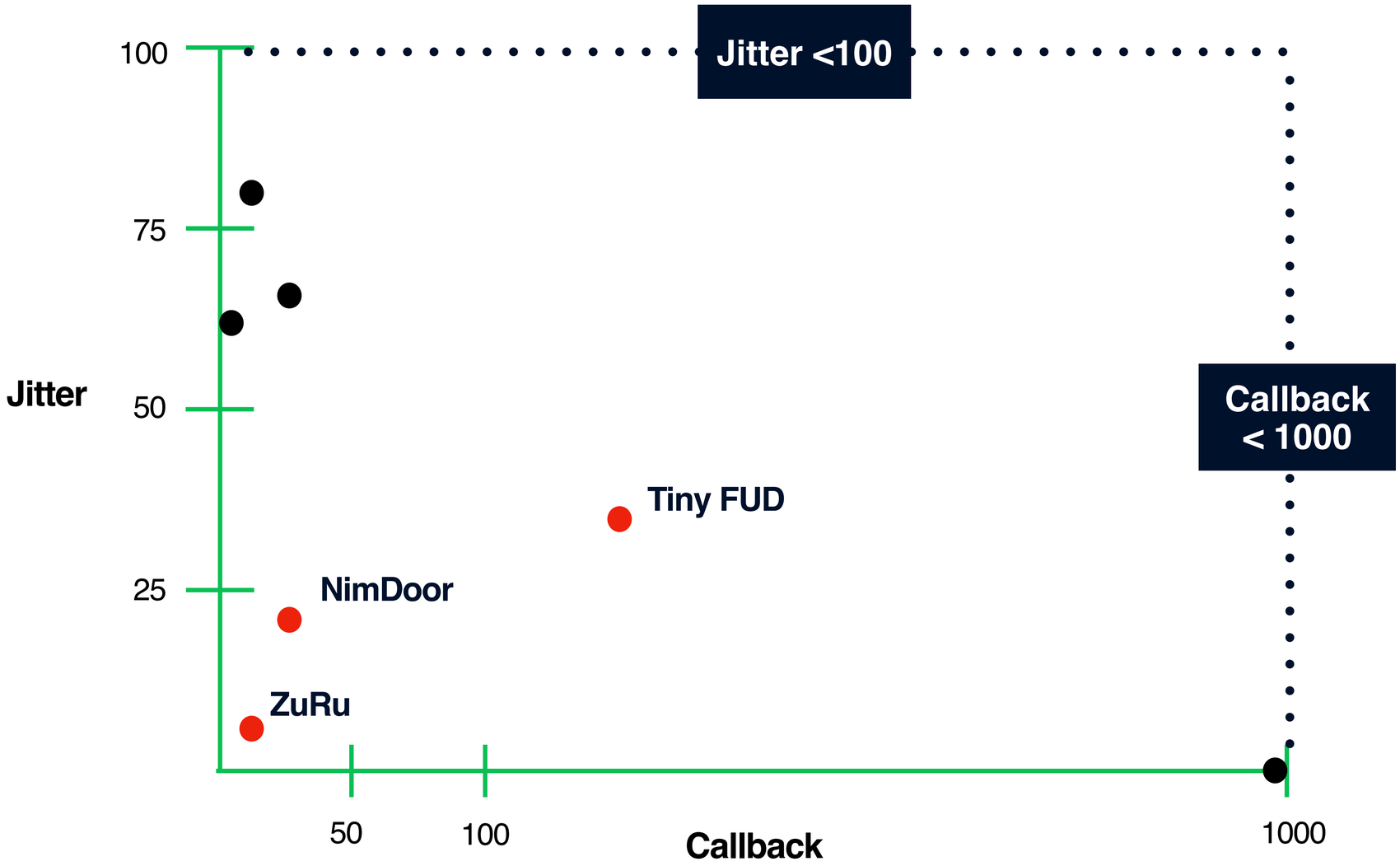
	Time	host.name	dnsmasq.qname
>	Jun 20, 2025 @ 15:44:38.000	mb-anje	totallynotac2.belastinqdienst.com
>	Jun 20, 2025 @ 15:32:20.000	mb-anje	totallynotac2.belastinqdienst.com
>	Jun 20, 2025 @ 15:20:13.000	mb-anje	totallynotac2.belastinqdienst.com
>	Jun 20, 2025 @ 15:07:55.000	mb-anje	totallynotac2.belastinqdienst.com

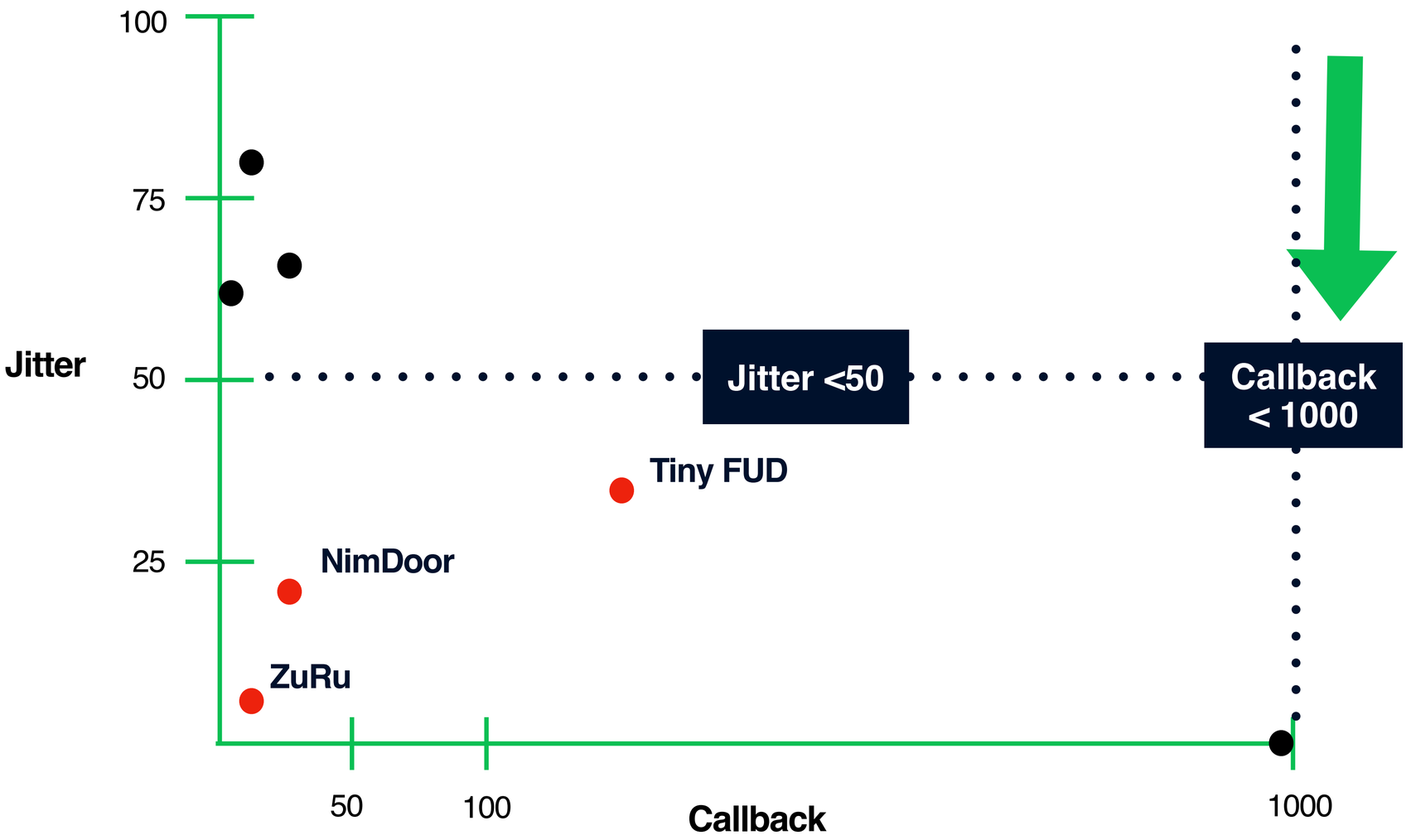
- callback = count of requests / time unit
- jitter = second order difference time / count of requests

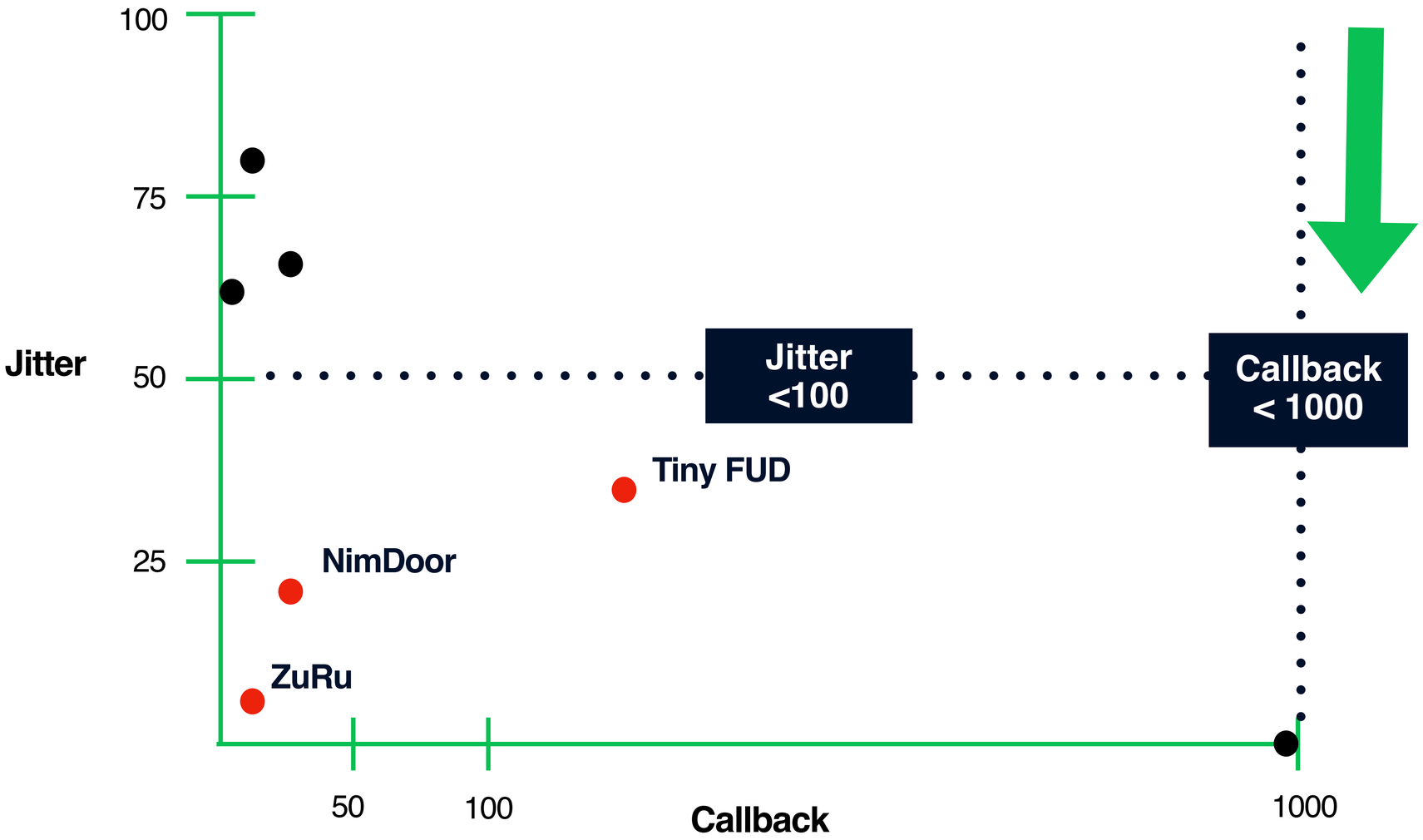
	Callback (seconds)	Jitter (seconds)
MacOS.ZuRu	5	10
NimDoor	30	20
Tiny FUD	300	30
Slack	1	65
Video conferencing	5	78
IDE	30	60
Data back up	1000	0

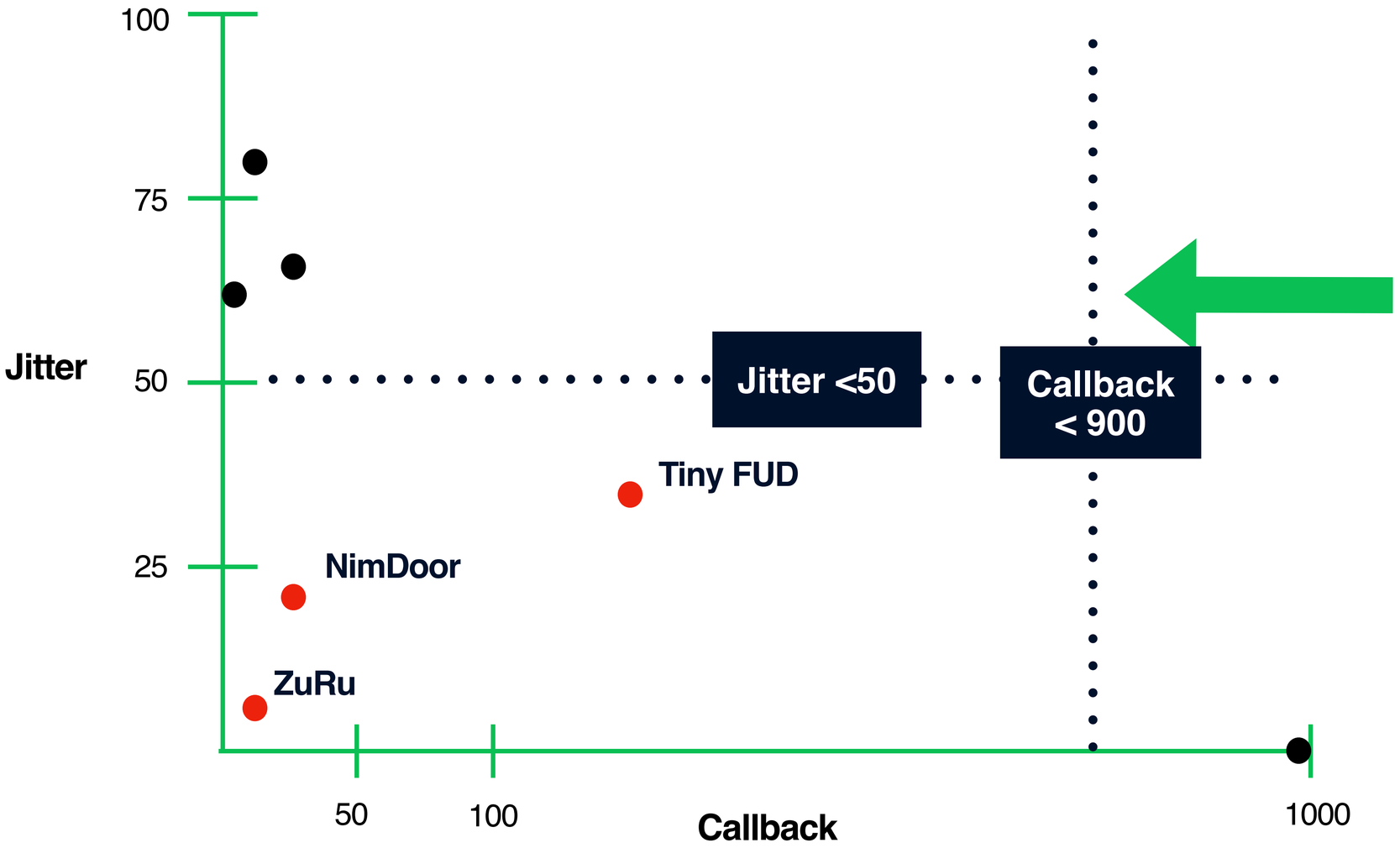
	Callback (seconds)	Jitter (seconds)
MacOS.ZuRu	5	10
NimDoor	30	20
Tiny FUD	300	30
Slack	1	65
Video conferencing	5	78
IDE	30	60
Data back up	1000	0




Jitter <100
Callback
< 1000
100
75
50
25
Jitter
Tiny FUD
NimDoor
ZuRu
50
100
Callback
1000


100
75
Jitter
50
25
Jitter <50
Callback
< 1000
Tiny FUD
NimDoor
ZuRu
50
100
Callback
1000


100
75
Jitter
50
25
Jitter
<100
Callback
< 1000
Tiny FUD
NimDoor
ZuRu
50
100
Callback
1000


100
75
50
25
Jitter
Jitter <50
Callback
< 900
Tiny FUD
NimDoor
ZuRu
50
100
Callback
1000



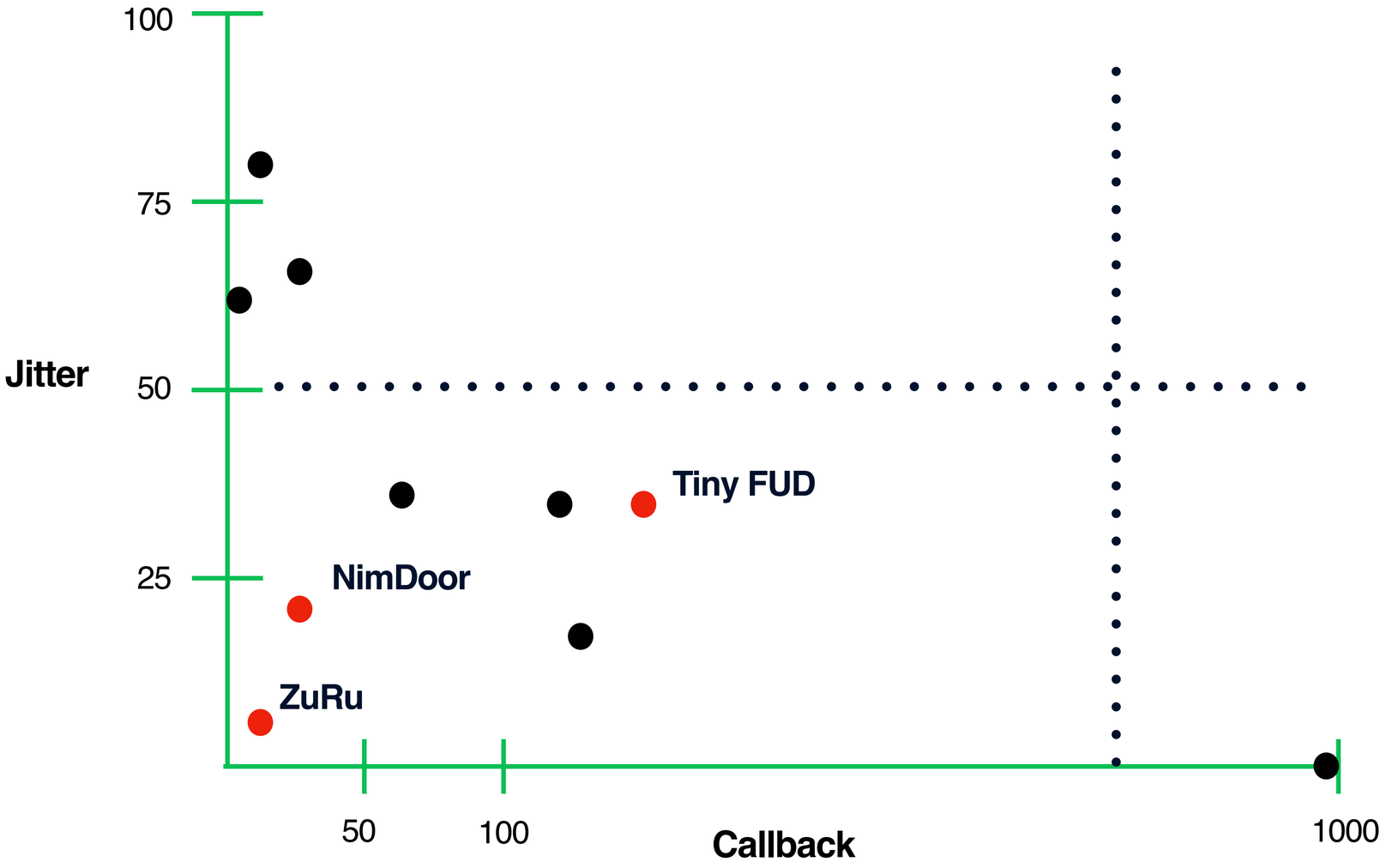


REALITY

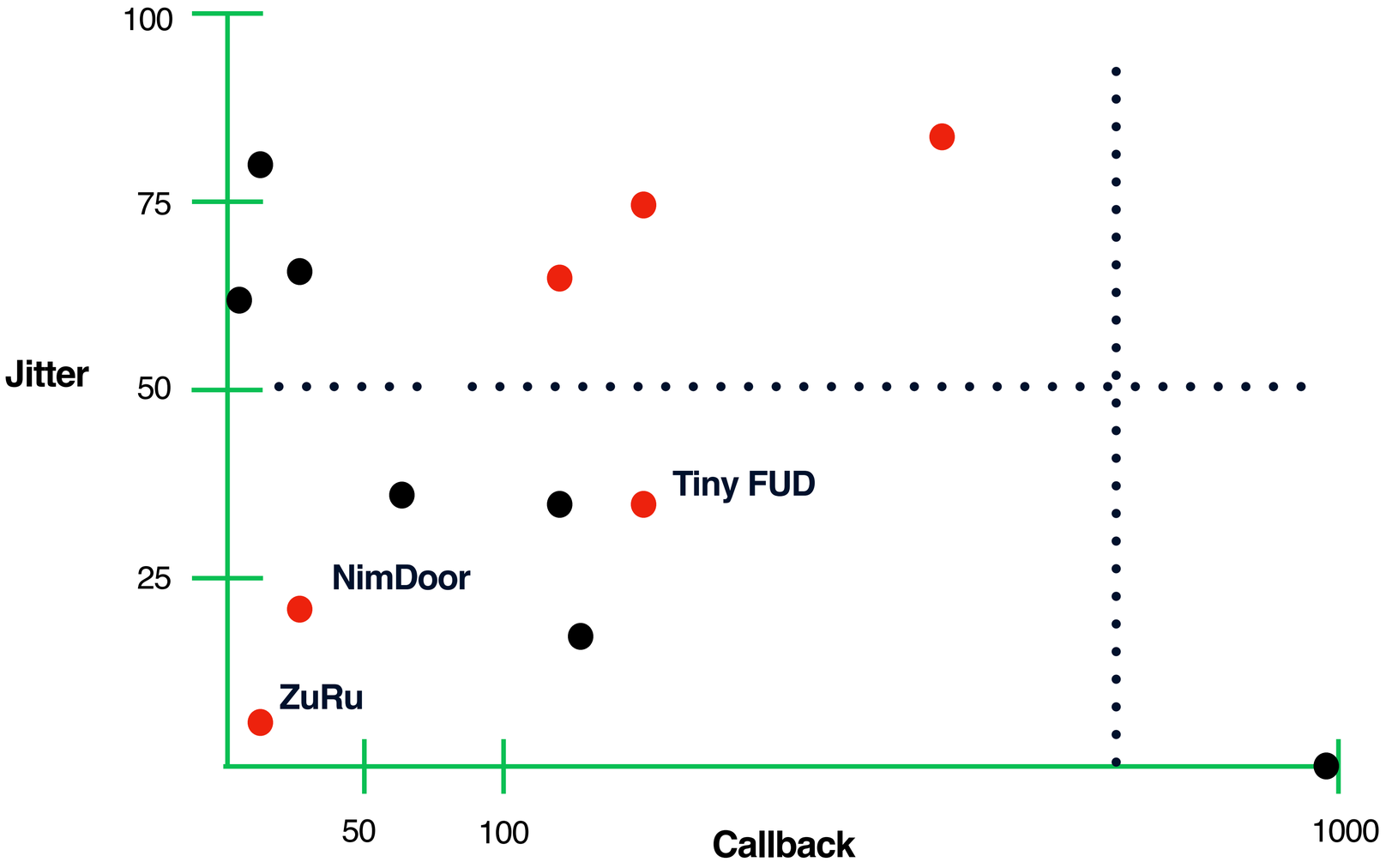




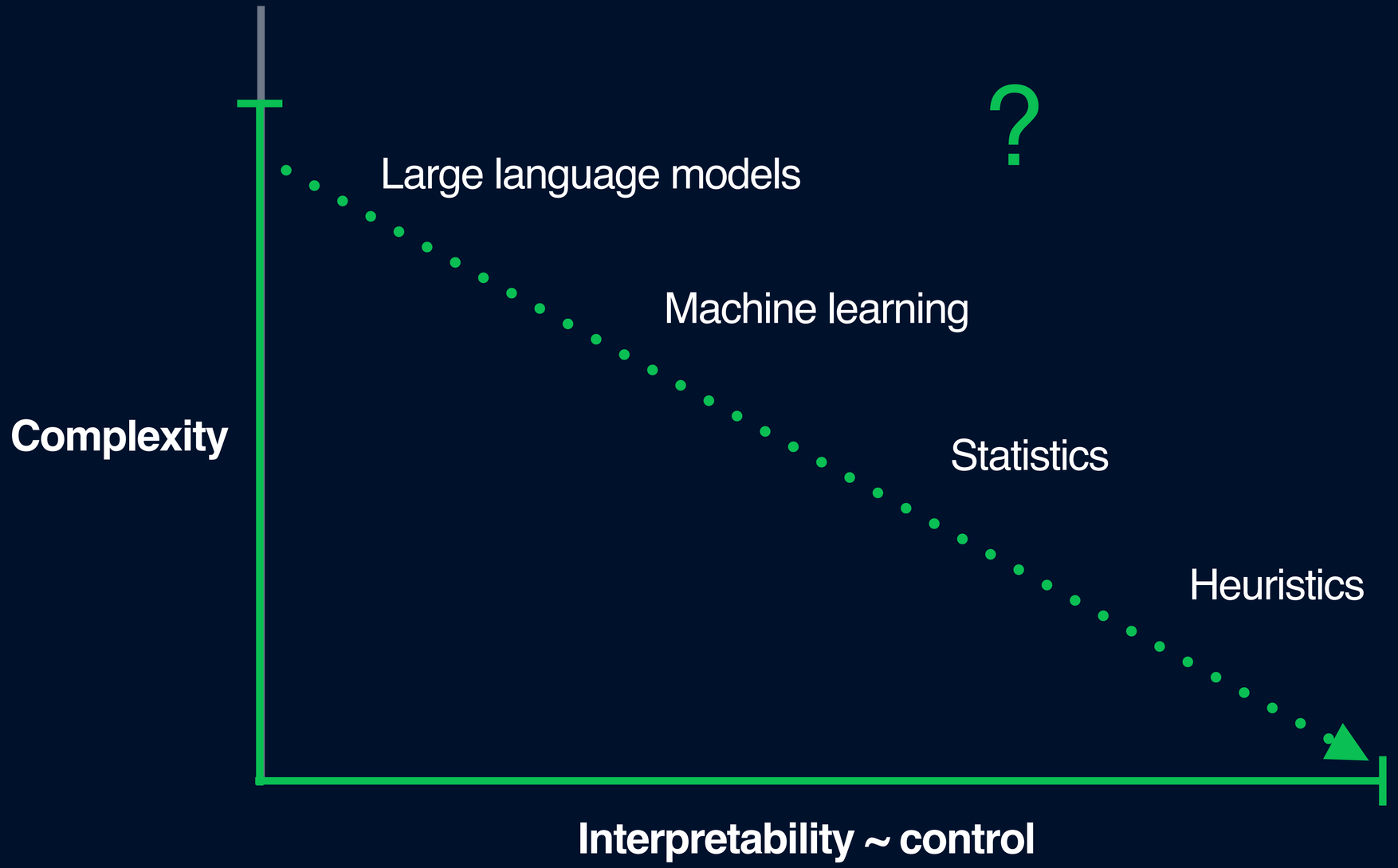
False positives



True negatives



Time to increase complexity?



LOLC2

collection of C2 frameworks that leverage legitimate services to evade detection

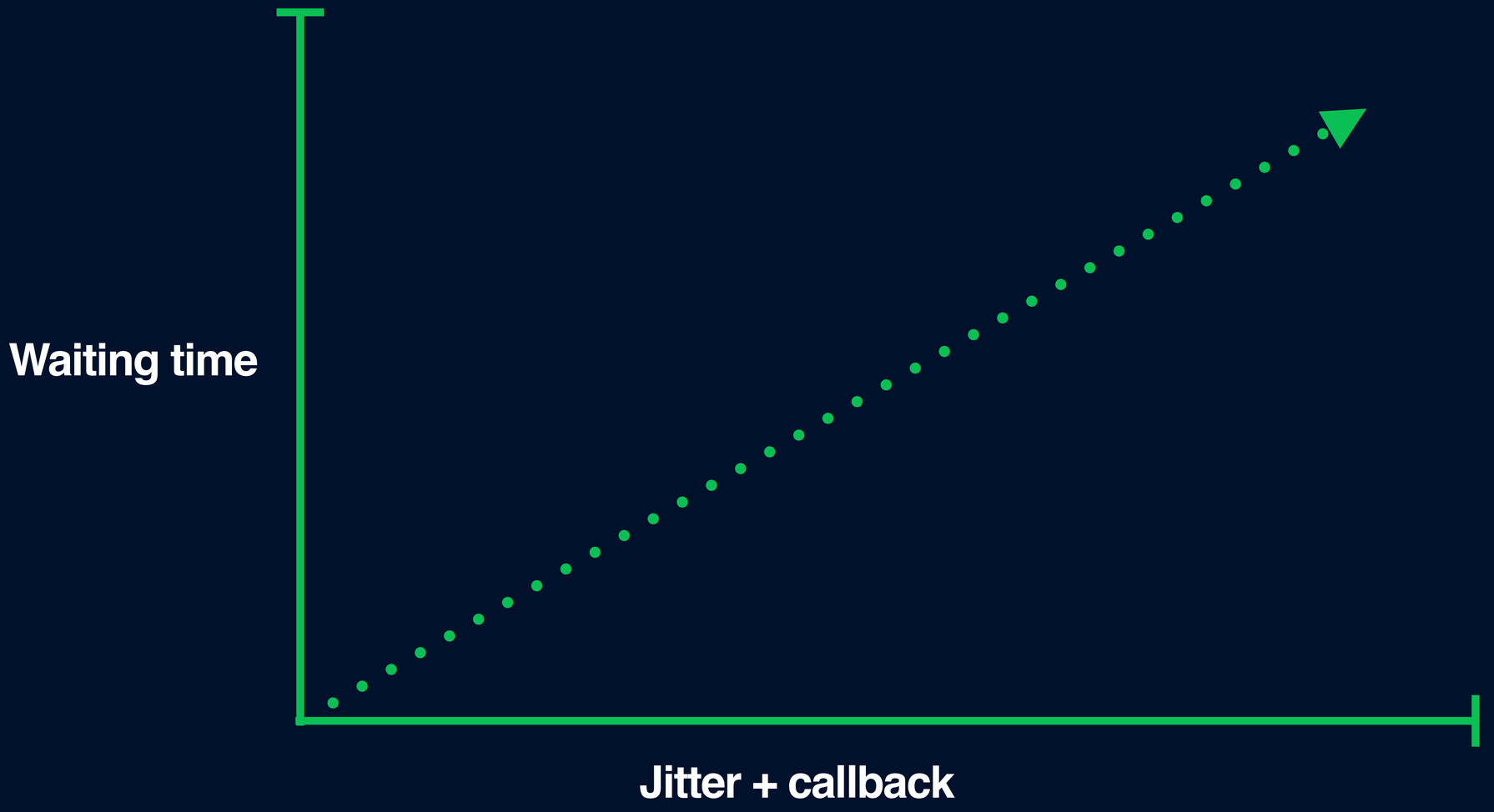
Telegram	CounterStrike 1.6	Cloudflare	Strava	Google Translate
Mastodon	Whatsapp	Microsoft Printer	Microsoft Azure Application Proxy	Asana
X	Onedrive	Microsoft Tasks	Jira	Twitter

The simple approach: heuristics

	Callback (seconds)	Jitter (seconds)
MacOS.ZuRu	5	10
NimDoor	30	20
Tiny FUD	300	30
Slack	1	65
Video conferencing	5	78
IDE	30	60
Data back up	1000	0

Exclude expected combinations
processes + commands + ports + ..

Why stealth comes at a cost




TIME IS MONEY
SO DON'T WASTE IT
meme-arsenal.ru



The detection

adyen

The data pipeline



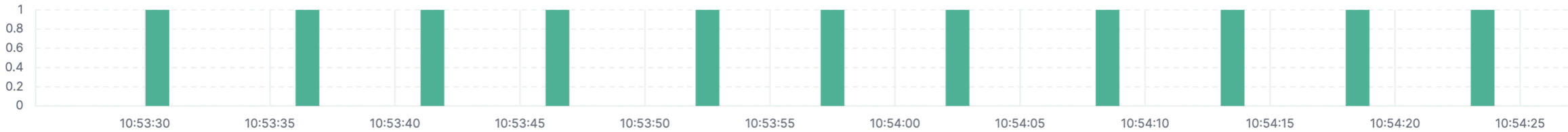
Socket events and processes

```
osquery> select p.pid, p.name, s.remote_port, s.remote_address
ERE s.remote_port=443 LIMIT 1;
+-----+---------+-------------+----------------+
| pid | name    | remote_port | remote_address |
+-----+---------+-------------+----------------+
| 948 | zoom.us | 443         | 52.84.151.36   |
+-----+---------+-------------+----------------+
```

- opensource
- flexible: sql
- manage the volume of socket data



Osquery logs in elastic



Jun 18, 2025 @ 10:53:25.626 - Jun 18, 2025 @ 10:54:26.917

	Time	action	columns.path	columns.name	columns.cmdline	columns.remote_address	columns.remote_port
›	Jun 18, 2025 @ 10:54:23.000	added	/private/var/folders/l4/5tpmdz3d00v8w1k7jkg2y1_r0000gn/T/tmp.OlwCuJRTdv	tmp.OlwCuJRTdv	/var/folders/l4/5tpmdz3d00v8w1k7jkg2y1_r0000gn/T/tmp.OlwCuJRTdv	[redacted]	443

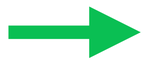
osquery → Filebeat → elastic

Python logic

mac_c2_in_osquery.py

```
93      def hypothesis(  Anje Knottnerus +1 *
160
161             jitter = estimate_jitter(timestamps)
162             if jitter > MAX_JITTER:
163                 continue
164
```















MAC_C2_IN_OSQUERY (id: 1245899)

Status: Open | Priority: High | Assignee | Outcome

Identifiers

- hostname mb-anje
- remote_address 146.190.17.255

Data

- command
  - /Users/anje/Downloads/client
- domain
  - totallynotac2.belastinqdienst.com
- duty_groups
  - security_duty
- estimated_callback 7
- estimated_jitter 1 seconds
- full_name Anje Knottnerus
- number_of_requests 87
- parent_process
- path
  - /Users/anje/Downloads/client
- remote_port
  - 50051

Advantages	Disadvantages
One detection to cover C2 beacons	Baselining
Control of what is detected and what is not	Maintenance
Understandable	
Tailored to your environment	

Universal | Simple





Anje Knottnerus
Security Engineer

adyen