CHES 2019

Capture the Flag Challenge

The WhibOx Contest - Edition 2

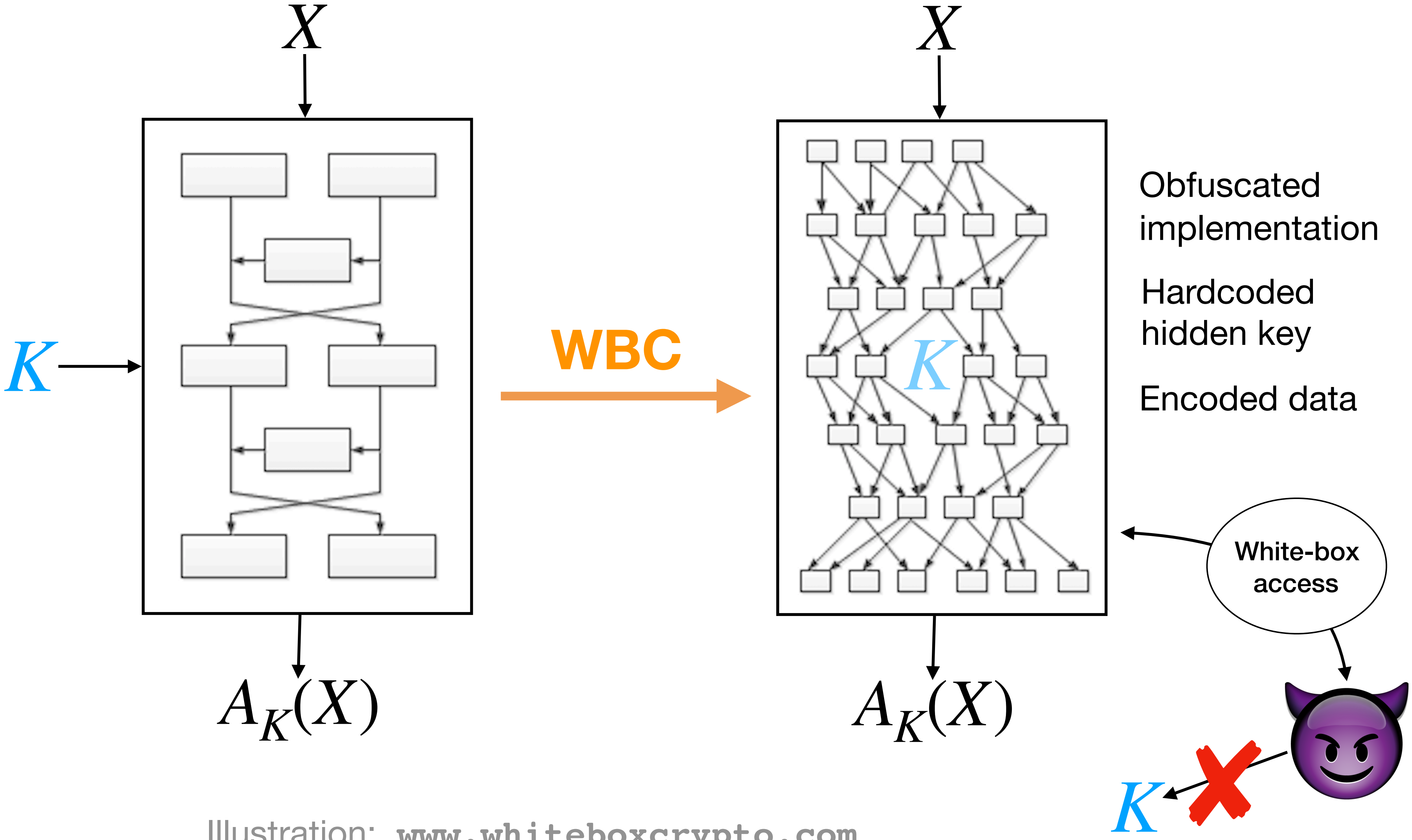
CHES challenge

- This is the **5th edition** of the CHES challenge
- Previous challenges
  - 2015: Crypto-engineering CTF
  - 2016: Power analysis & secure implementations
  - 2017: WhibOx contest - edition 1
  - 2018: Deep-learning based SCA
  - 2019: WhibOx contest - edition 2

CYBERCRYPT. CryptoExperts

- Next year: **looking for candidates**

White-box cryptography



Obfuscated implementation

Hardcoded hidden key

Encoded data

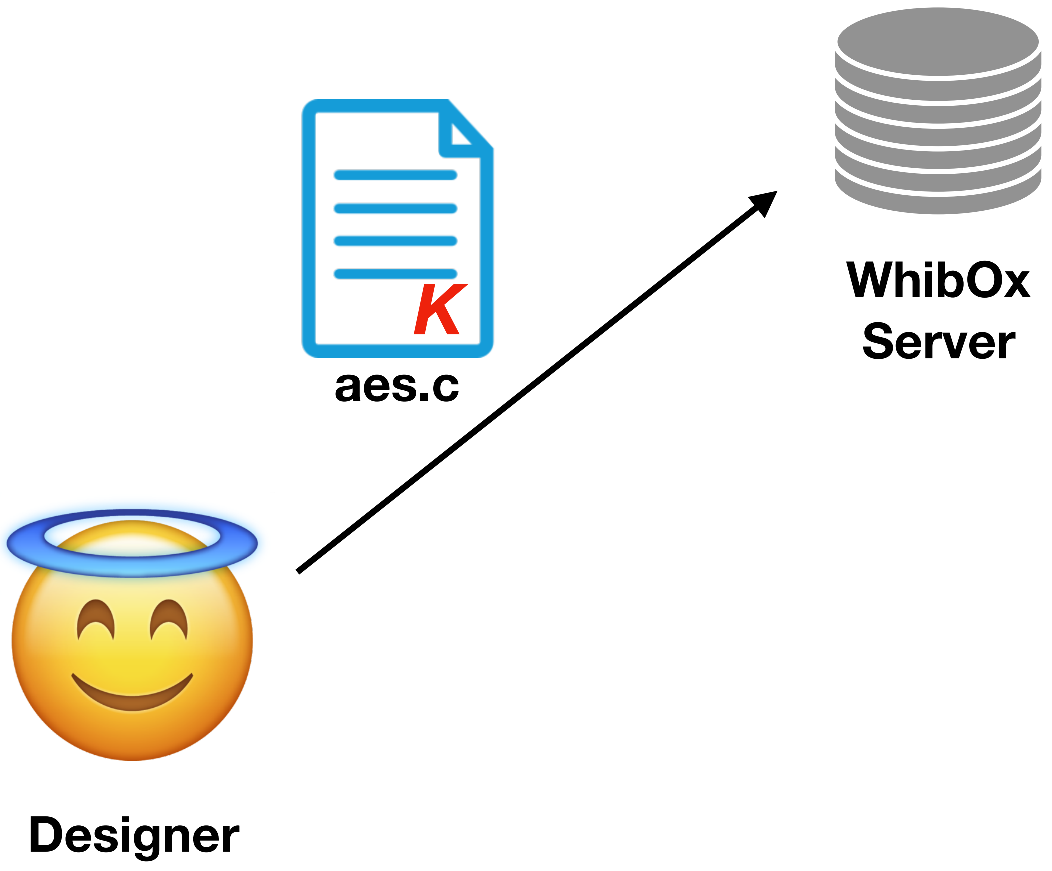
Illustration: **www.whiteboxcrypto.com**

White-box contest

Goal: confront designers and attackers of practical white-box crypto

White-box contest

Goal: confront designers and attackers of practical white-box crypto



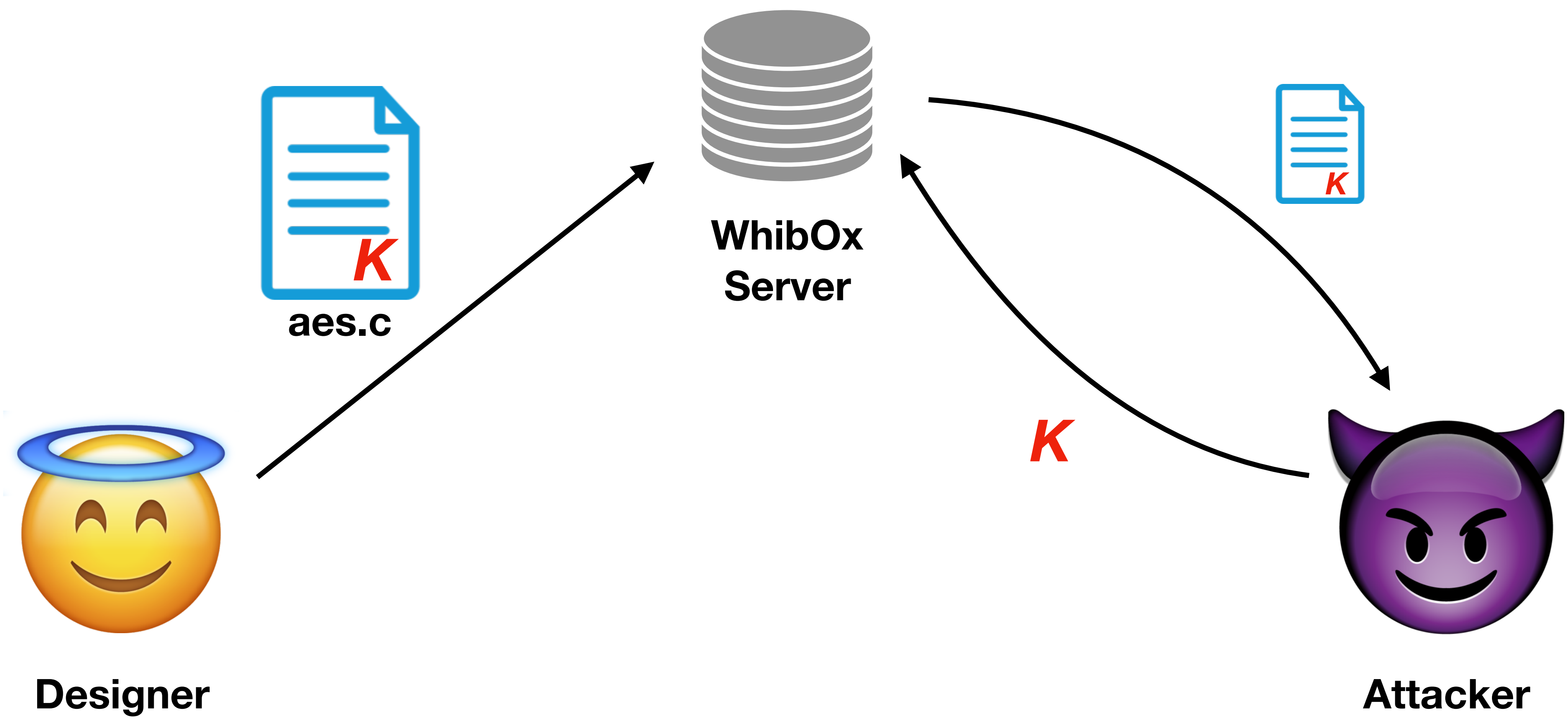
aes.c

WhibOx Server

Designer

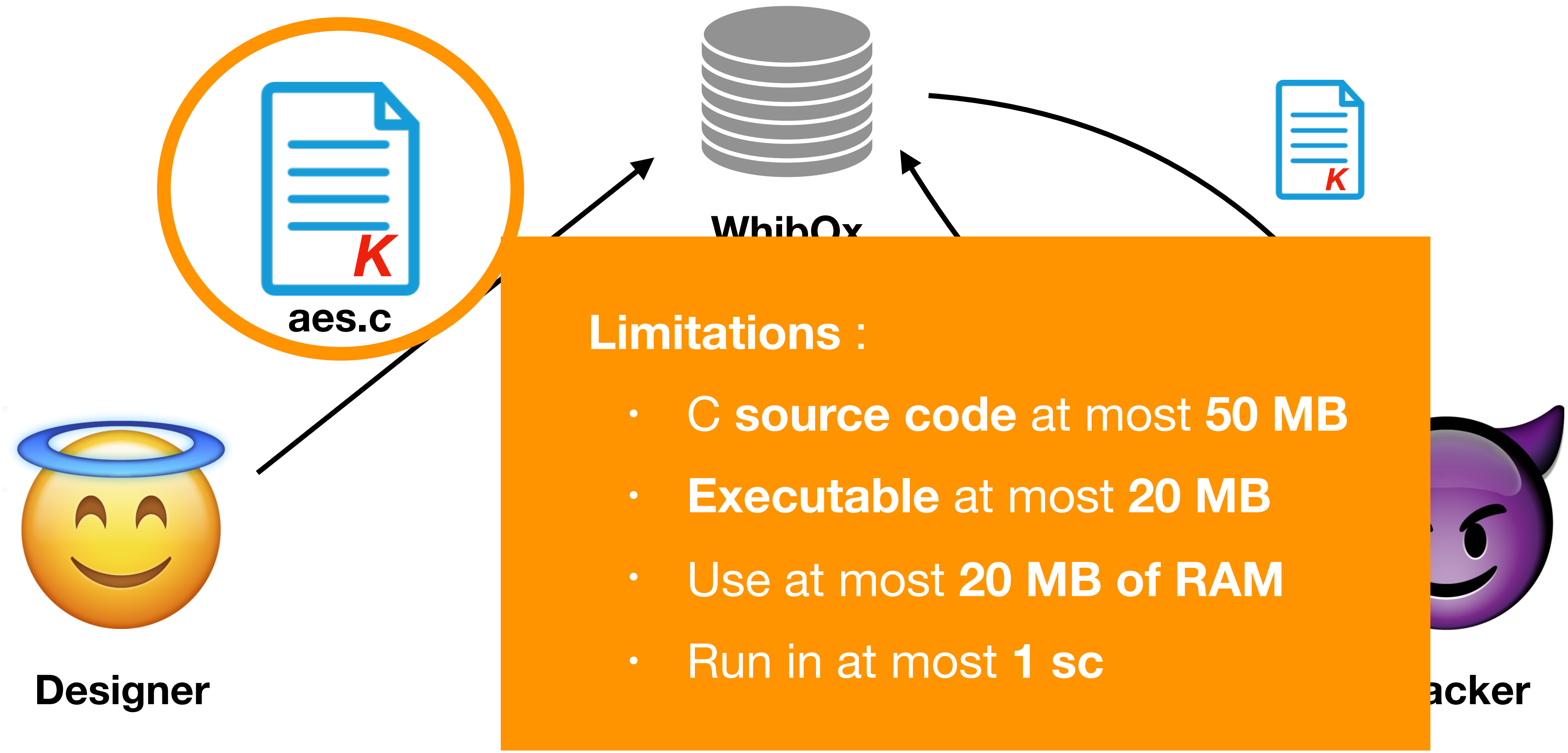
White-box contest

Goal: confront designers and attackers of practical white-box crypto



White-box contest

Goal: confront designers and attackers of practical white-box crypto



Limitations :

- C **source code** at most **50 MB**
- **Executable** at most **20 MB**
- Use at most **20 MB of RAM**
- Run in at most **1 sc**

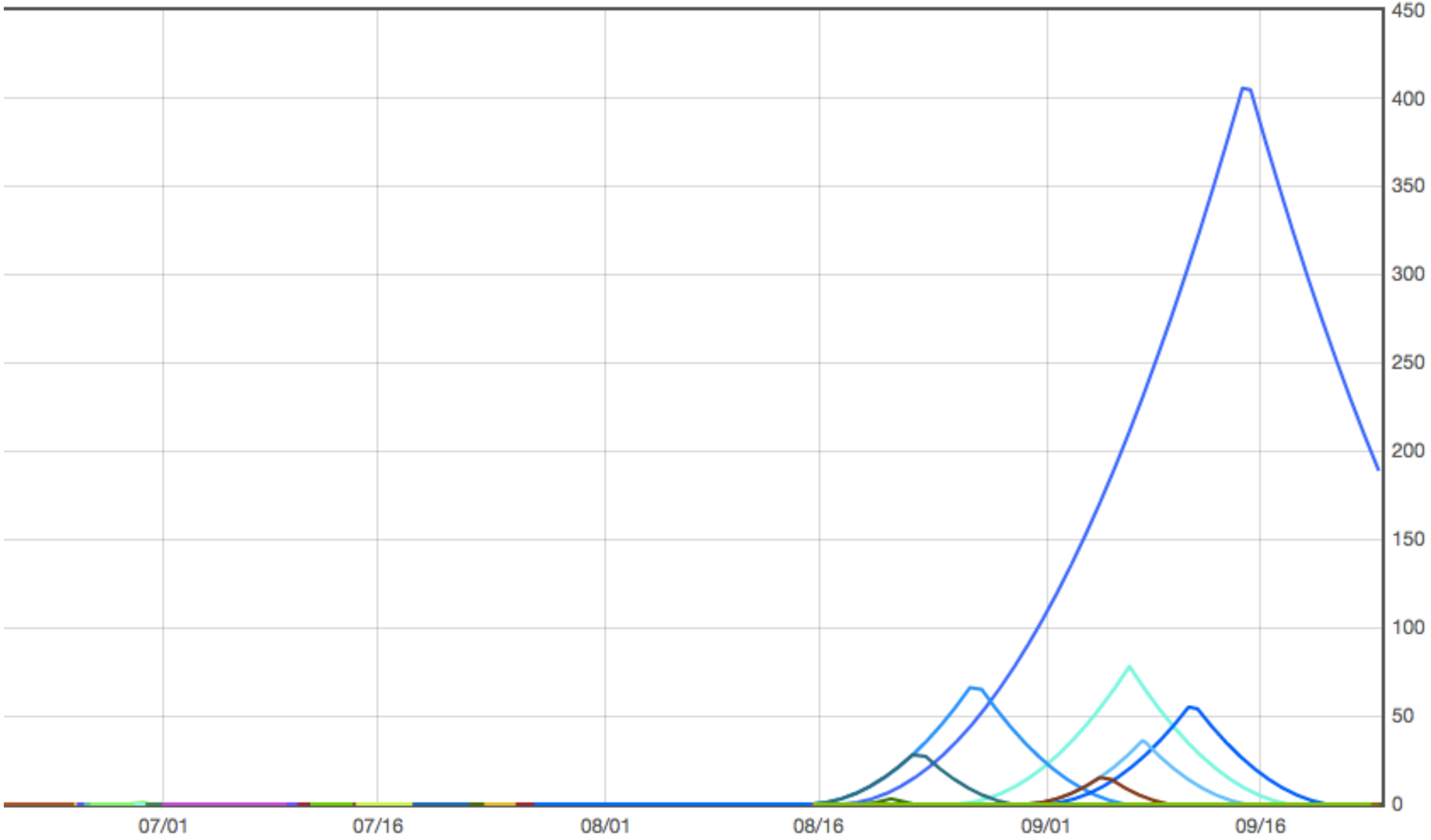
Score system

- A challenge implem gets 🍓 points as long as it stays unbroken
- At time t an implem worth $\alpha \cdot (t - t_0)^2$
  - t_0 is the time of submission
  - α is a constant depending of the performances
- When an implem with n 🍓 gets broken
  - the designer score n 🍓 points (with max rule)
  - the attacker score n 🍌 points (with max rule)
  - the 🍓 score of the implem. starts to decreasing down to 0

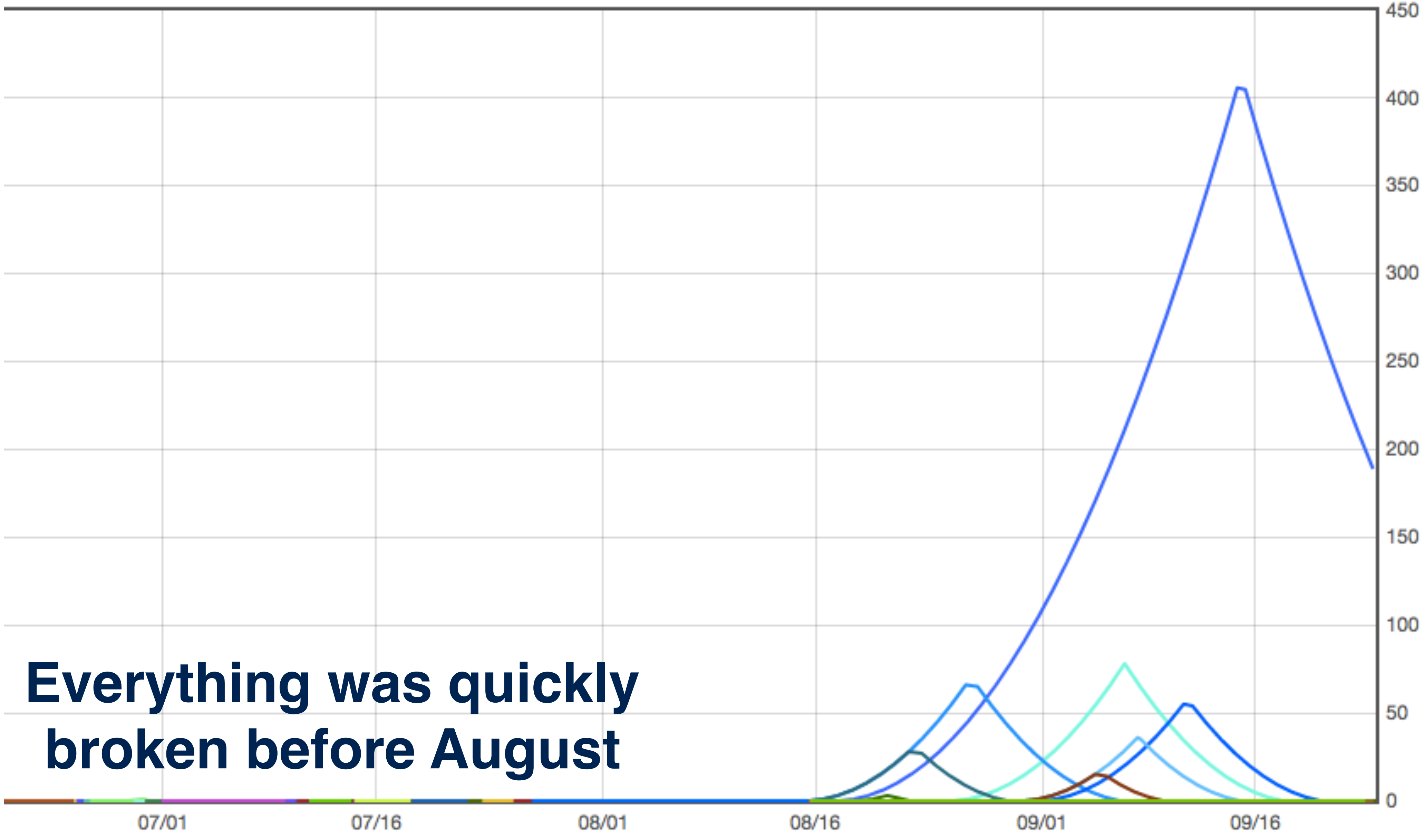
News in edition 2

- Performance factor α (w.r.t. running time, code size, RAM consumption)
- Bonus (🥕) points are introduced for the inversion
- Improved time granularity
- Support of 32-bit and 64-bit instructions
- 2 compiler options: GCC & TCC

Recall: results of edition 1

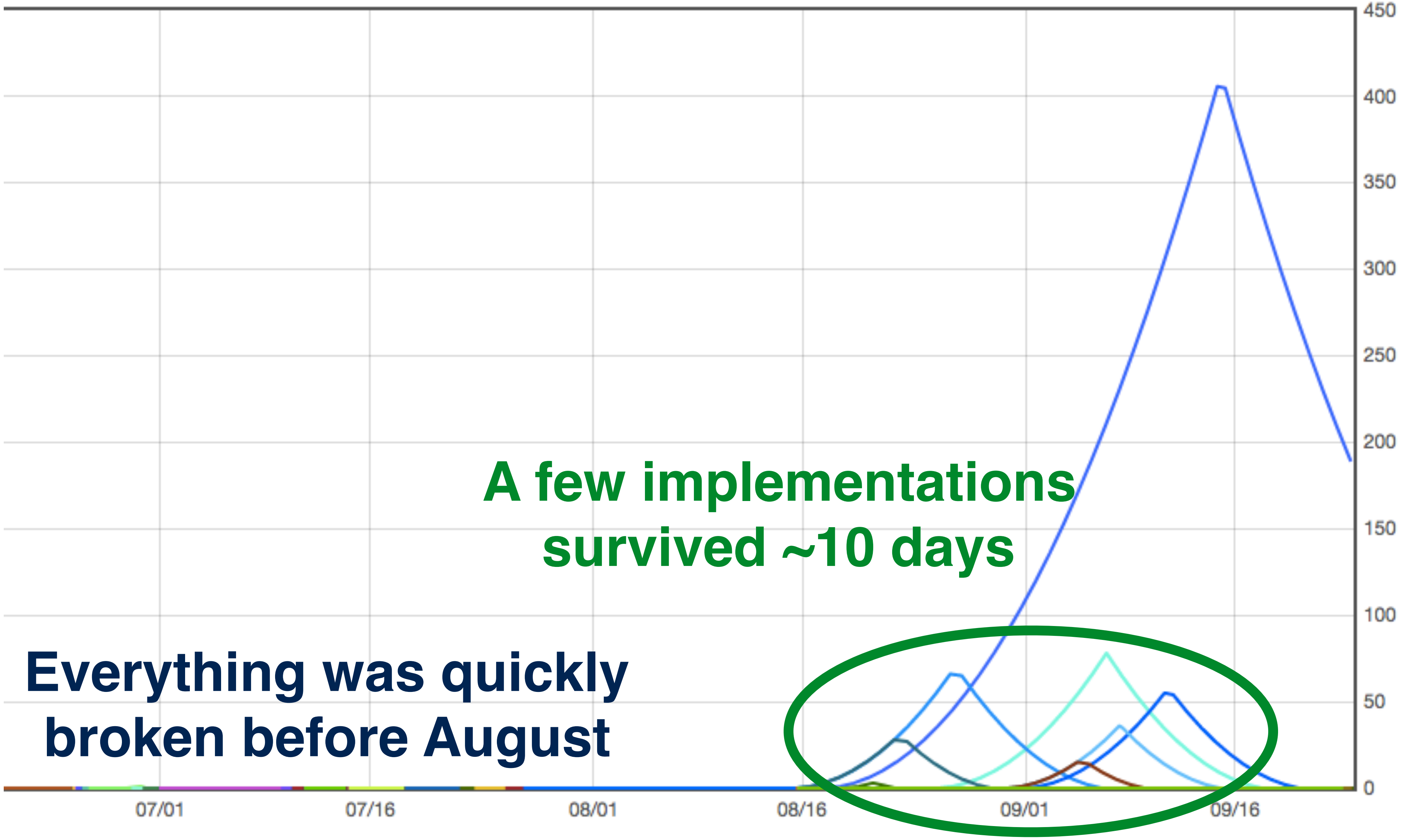


Recall: results of edition 1



Everything was quickly broken before August

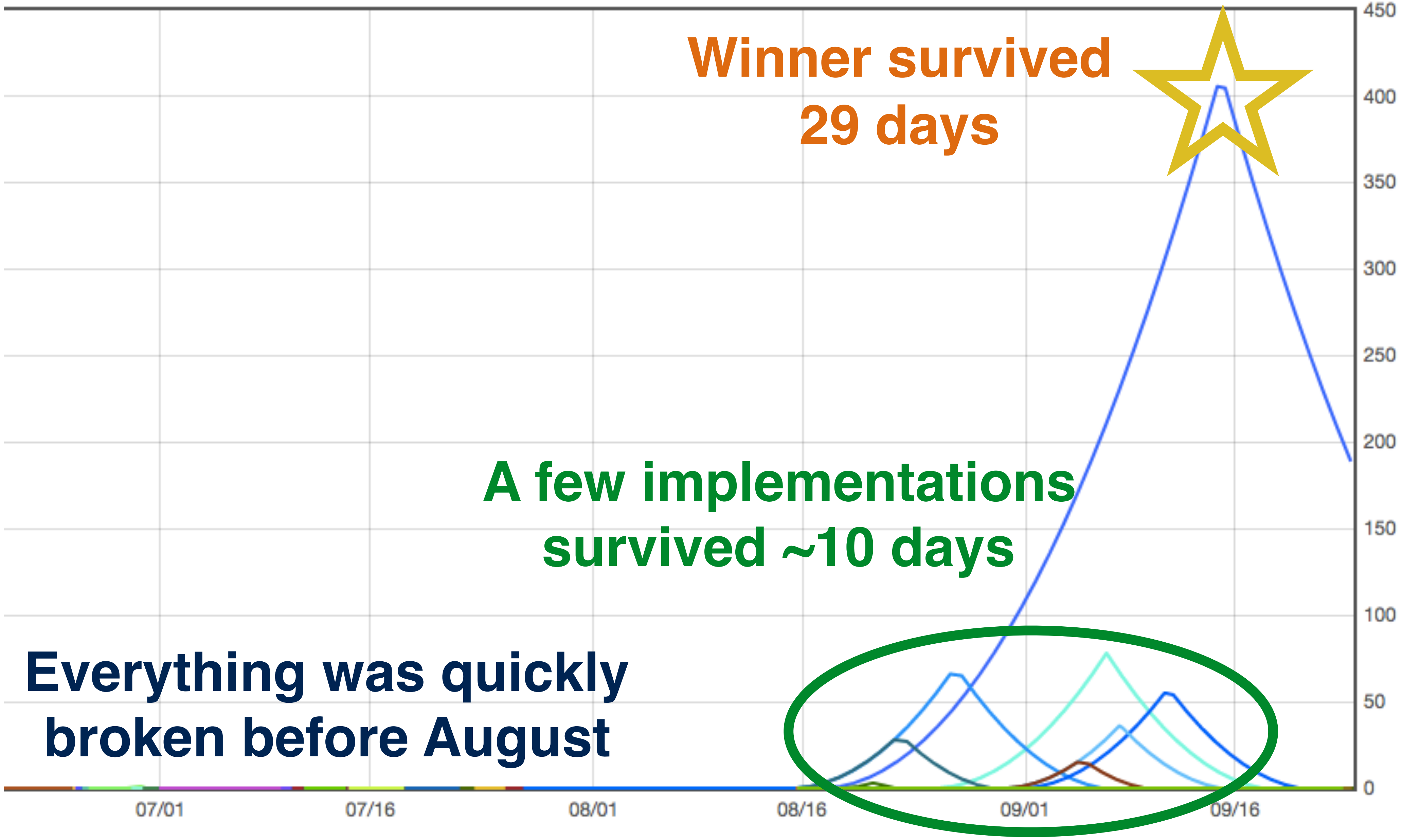
Recall: results of edition 1



A few implementations survived ~10 days

Everything was quickly broken before August

Recall: results of edition 1

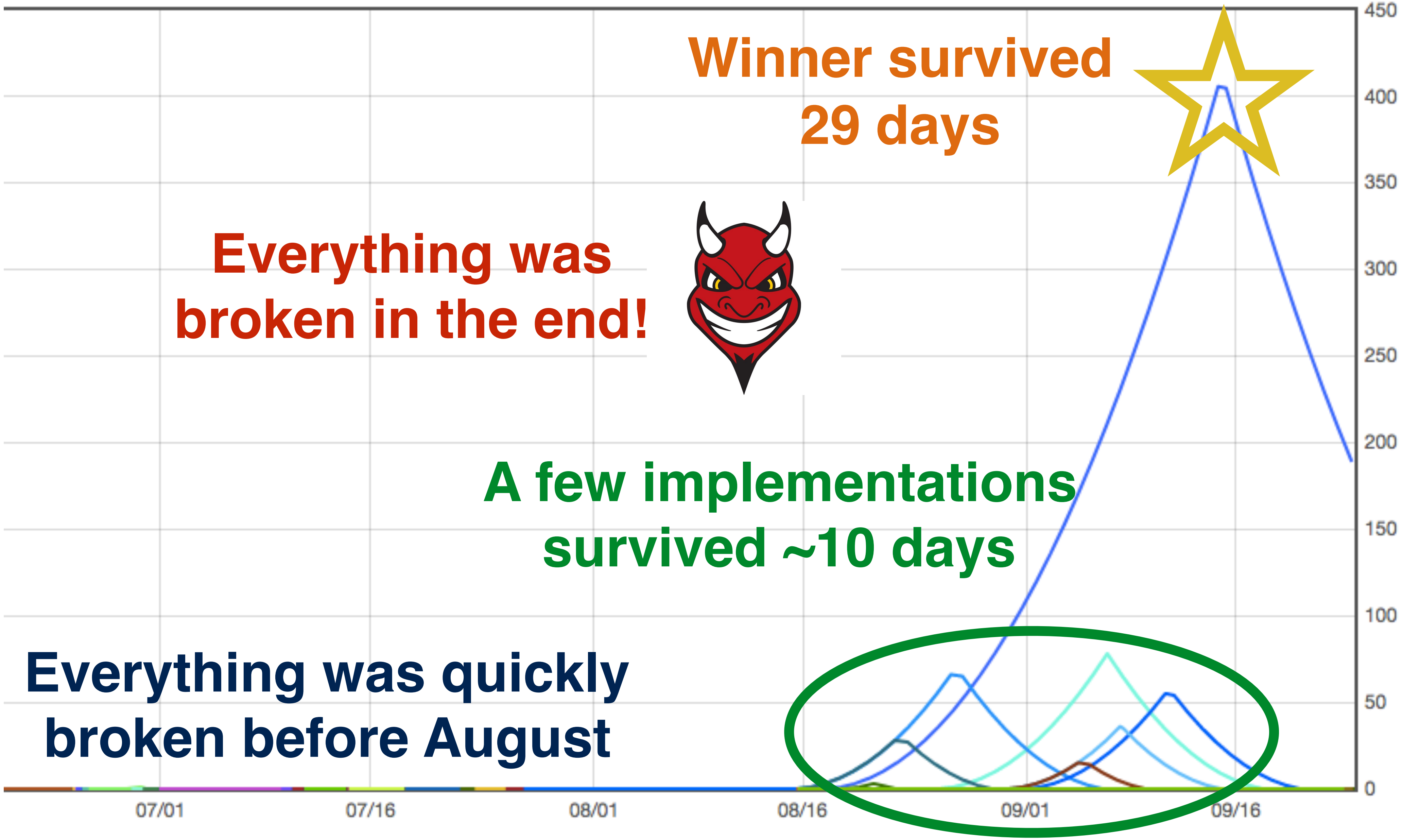


Winner survived 29 days

A few implementations survived ~10 days

Everything was quickly broken before August

Recall: results of edition 1



Winner survived 29 days

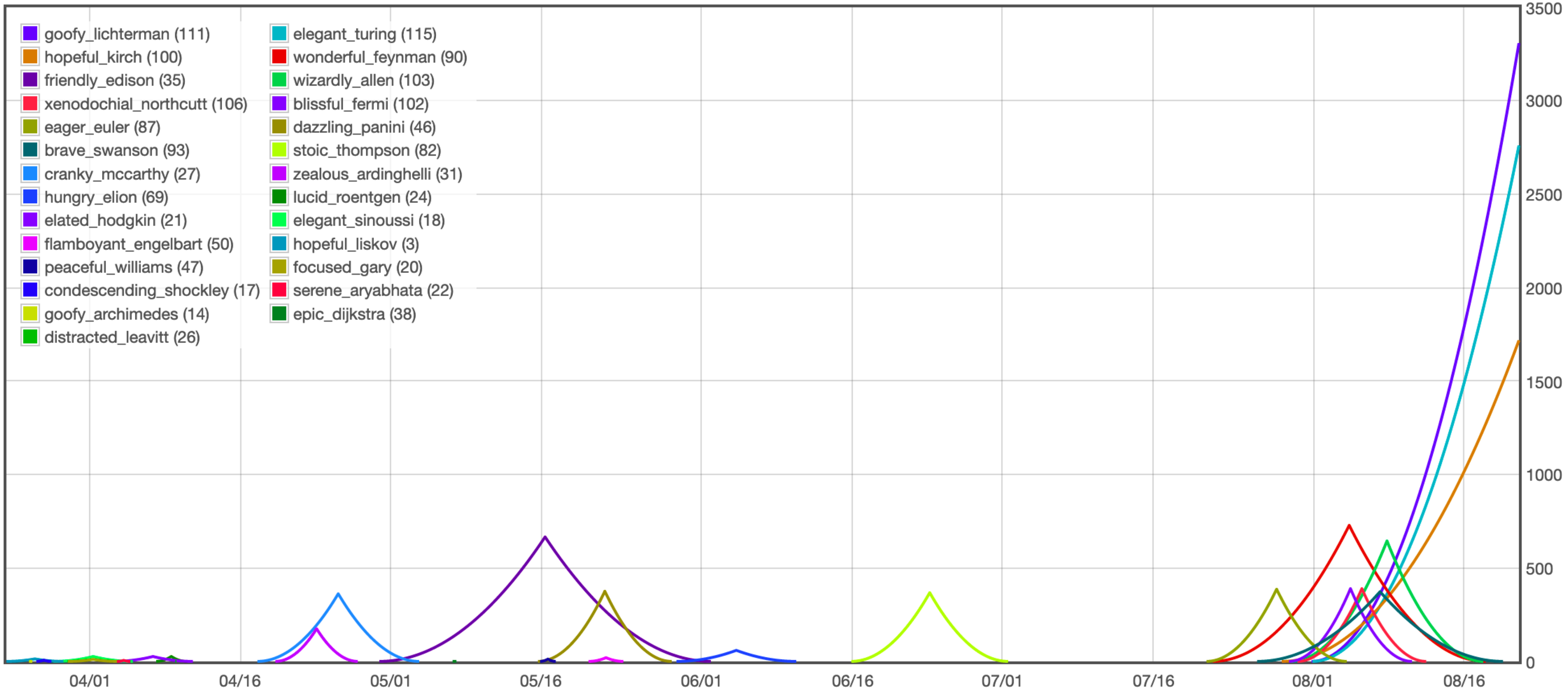
Everything was broken in the end!

A few implementations survived ~10 days

Everything was quickly broken before August

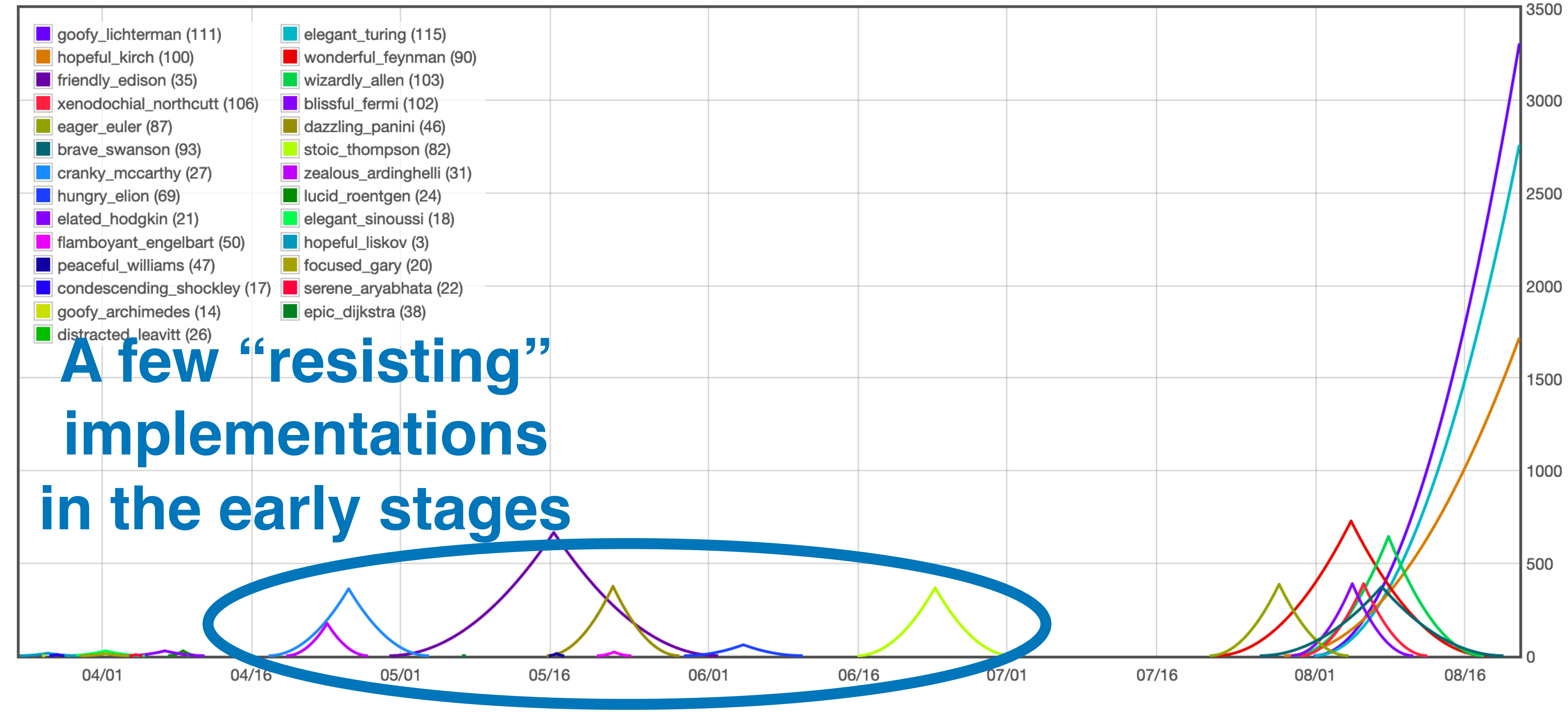
Results of edition 2

Strawberry scores over time



Results of edition 2

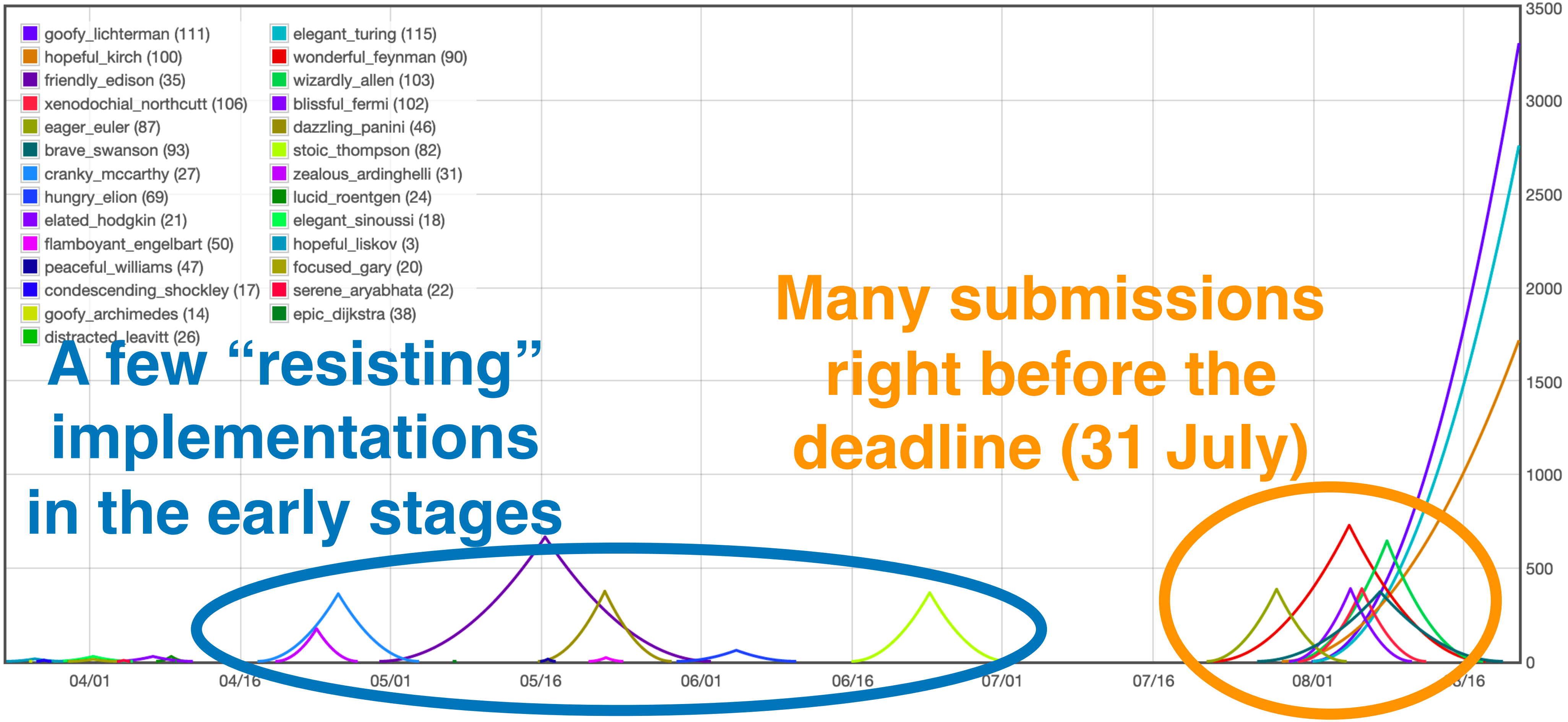
Strawberry scores over time



A few "resisting" implementations in the early stages

Results of edition 2

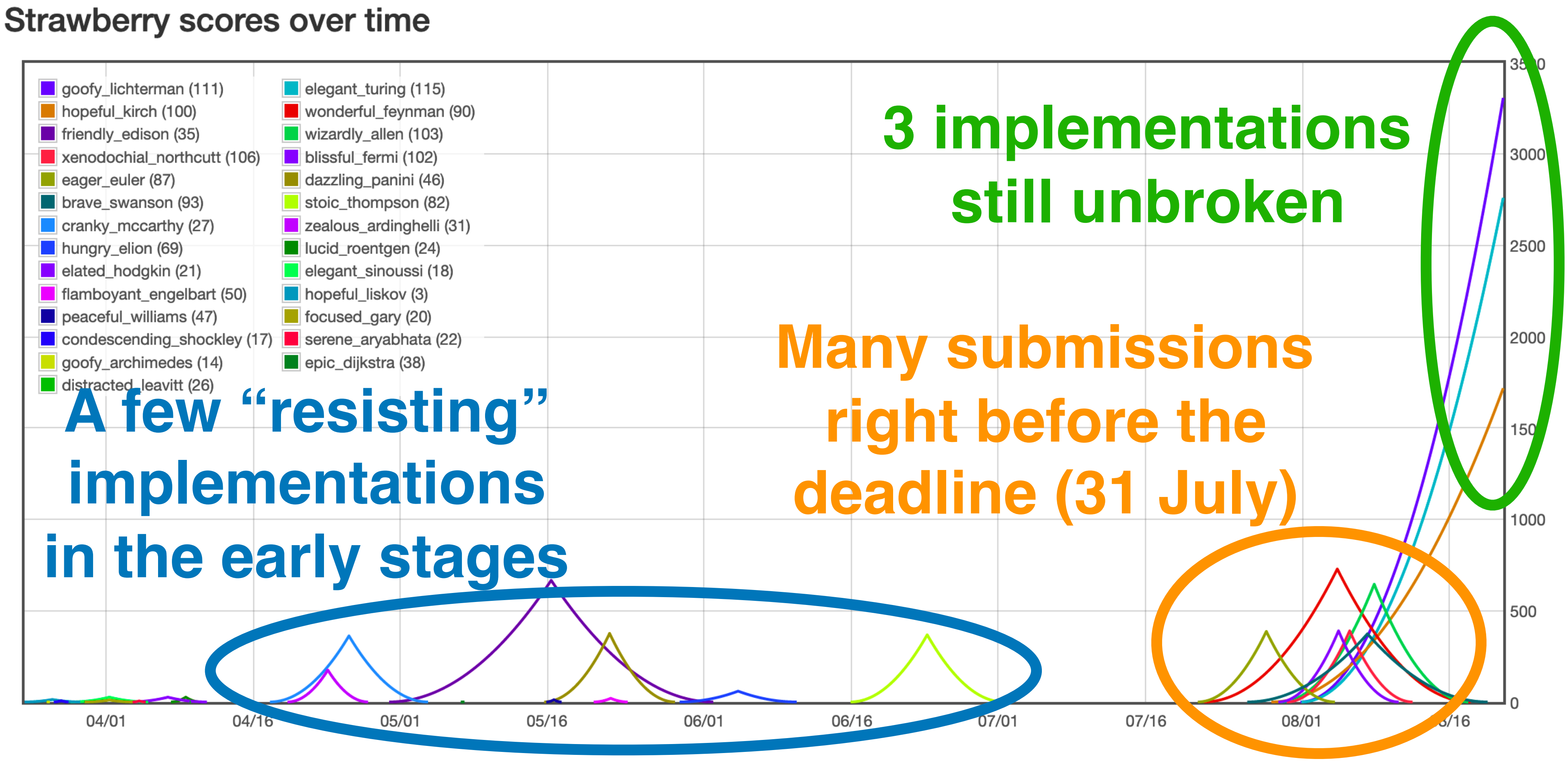
Strawberry scores over time



A few “resisting” implementations in the early stages

Many submissions right before the deadline (31 July)

Results of edition 2

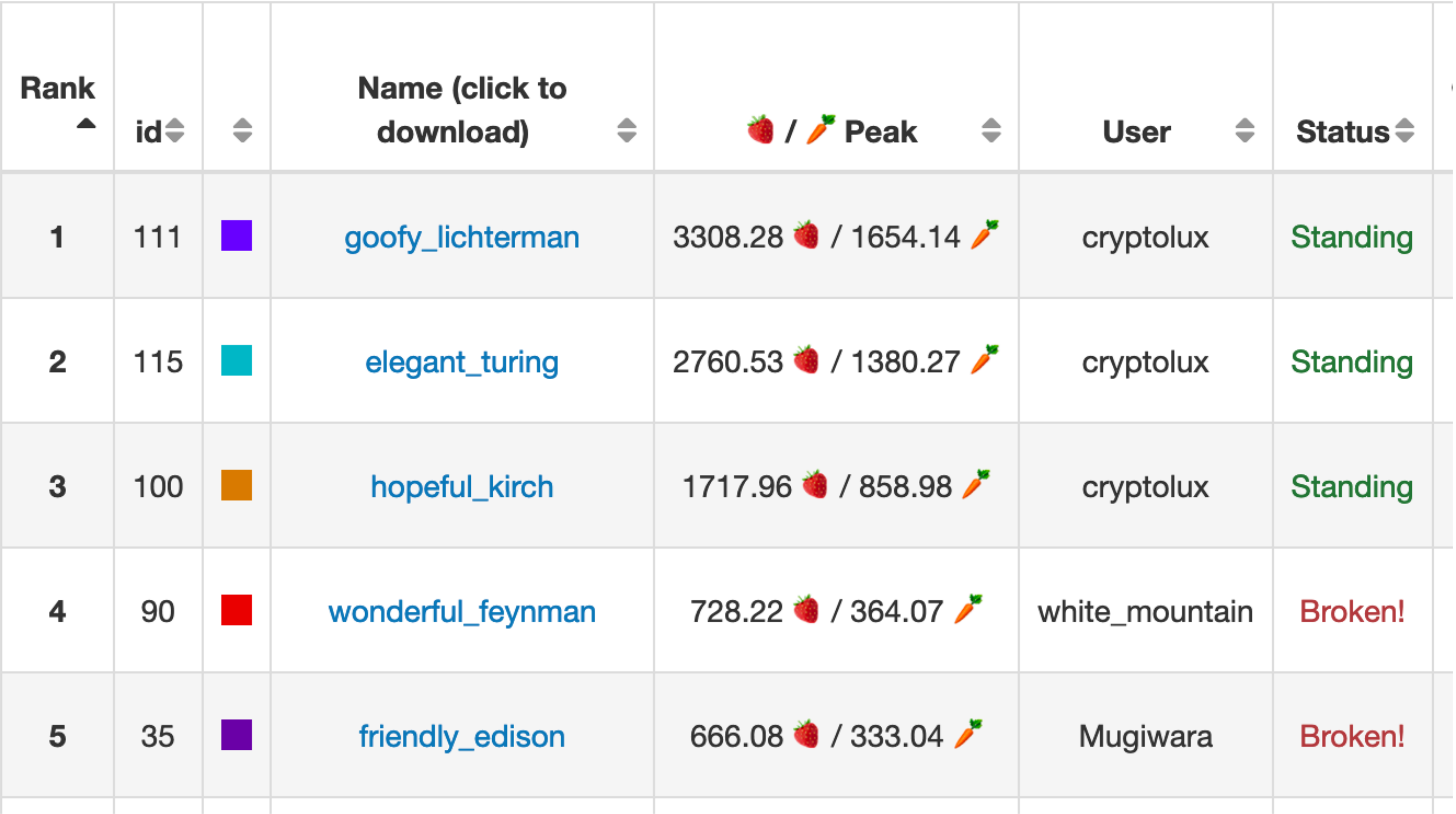


3 implementations still unbroken

Many submissions right before the deadline (31 July)

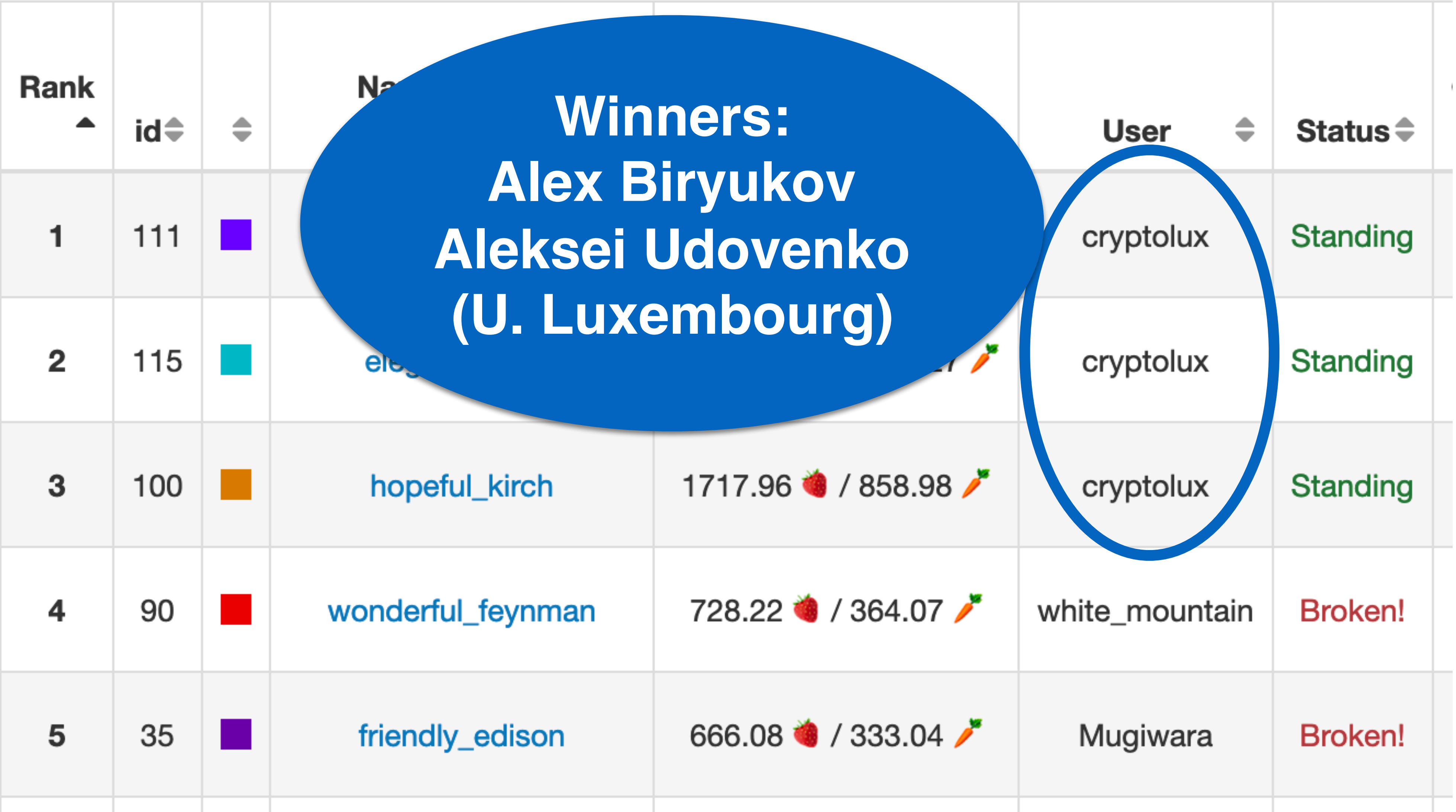
A few "resisting" implementations in the early stages

Strawberry scoreboard



Rank ▲	id ⬍	⬍	Name (click to download) ⬍	🍓 / 🥕 Peak ⬍	User ⬍	Status ⬍
1	111	🟪	goofy_lichterman	3308.28 🍓 / 1654.14 🥕	cryptolux	Standing
2	115	🟦	elegant_turing	2760.53 🍓 / 1380.27 🥕	cryptolux	Standing
3	100	🟧	hopeful_kirch	1717.96 🍓 / 858.98 🥕	cryptolux	Standing
4	90	🟥	wonderful_feynman	728.22 🍓 / 364.07 🥕	white_mountain	Broken!
5	35	🟪	friendly_edison	666.08 🍓 / 333.04 🥕	Mugiwara	Broken!

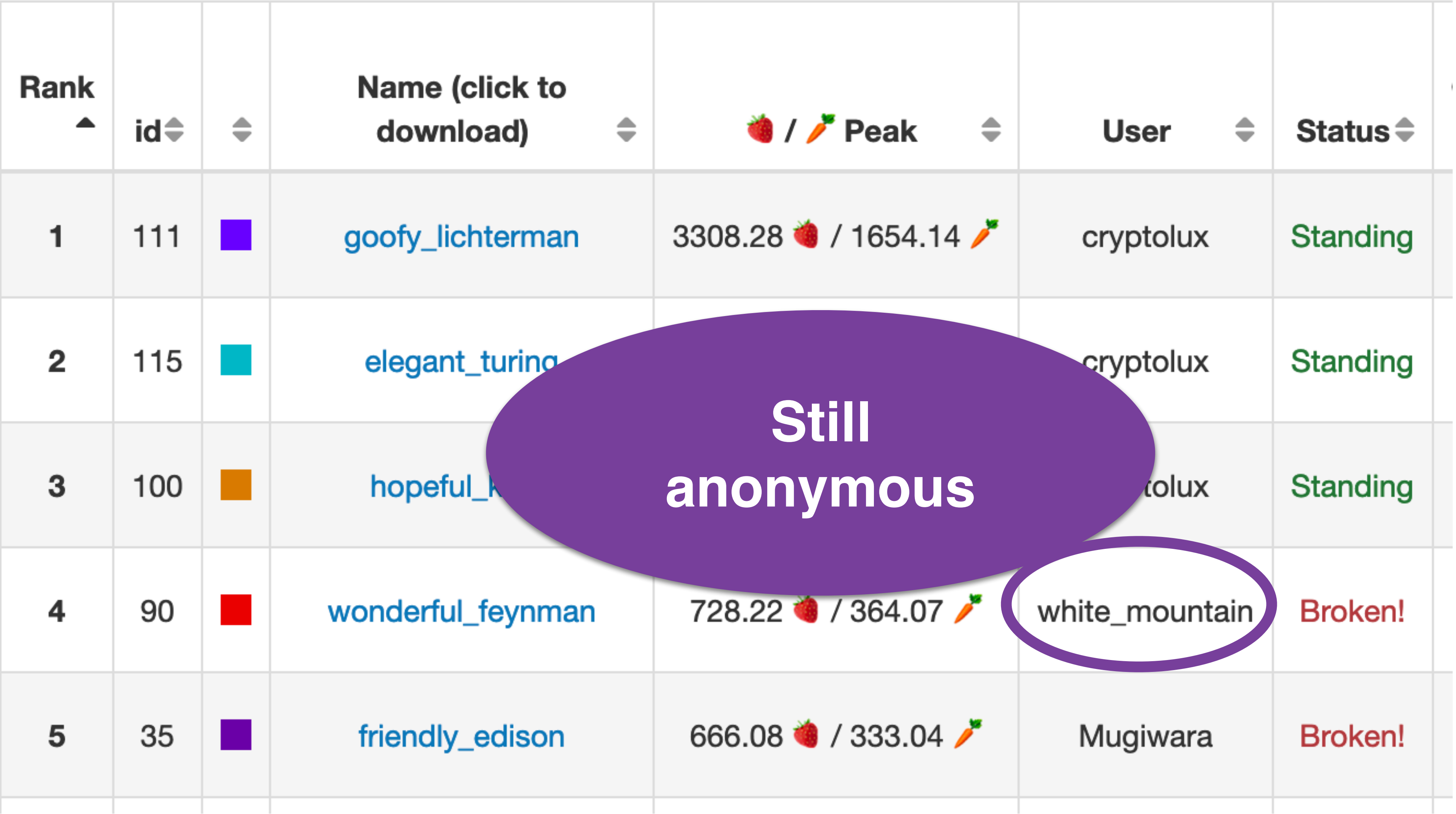
Strawberry scoreboard



Rank ▲	id ⬍	⬍	Na		User ⬍	Status ⬍
1	111	🟪			cryptolux	Standing
2	115	🟦	ele	27 🥕	cryptolux	Standing
3	100	🟧	hopeful_kirch	1717.96 🍓 / 858.98 🥕	cryptolux	Standing
4	90	🟥	wonderful_feynman	728.22 🍓 / 364.07 🥕	white_mountain	Broken!
5	35	🟪	friendly_edison	666.08 🍓 / 333.04 🥕	Mugiwara	Broken!

Winners:
Alex Biryukov
Aleksei Udovenko
(U. Luxembourg)

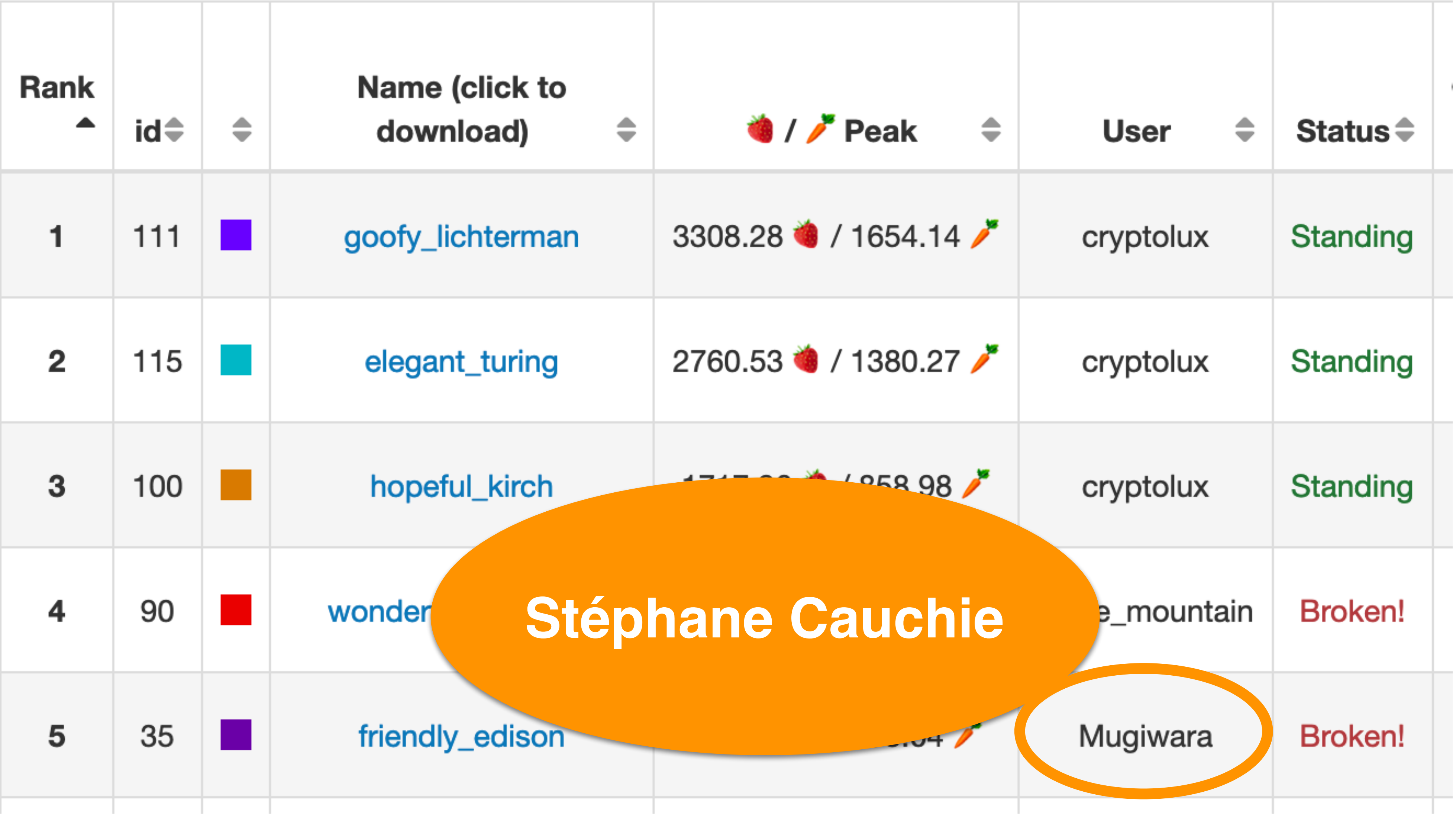
Strawberry scoreboard



Rank	id		Name (click to download)	🍓 / 🥕 Peak	User	Status
1	111	🟪	goofy_lichterman	3308.28 🍓 / 1654.14 🥕	cryptolux	Standing
2	115	🟦	elegant_turing	[illegible]	cryptolux	Standing
3	100	🟧	hopeful_k	[illegible]	tolux	Standing
4	90	🟥	wonderful_feynman	728.22 🍓 / 364.07 🥕	white_mountain	Broken!
5	35	🟪	friendly_edison	666.08 🍓 / 333.04 🥕	Mugiwara	Broken!

Still anonymous

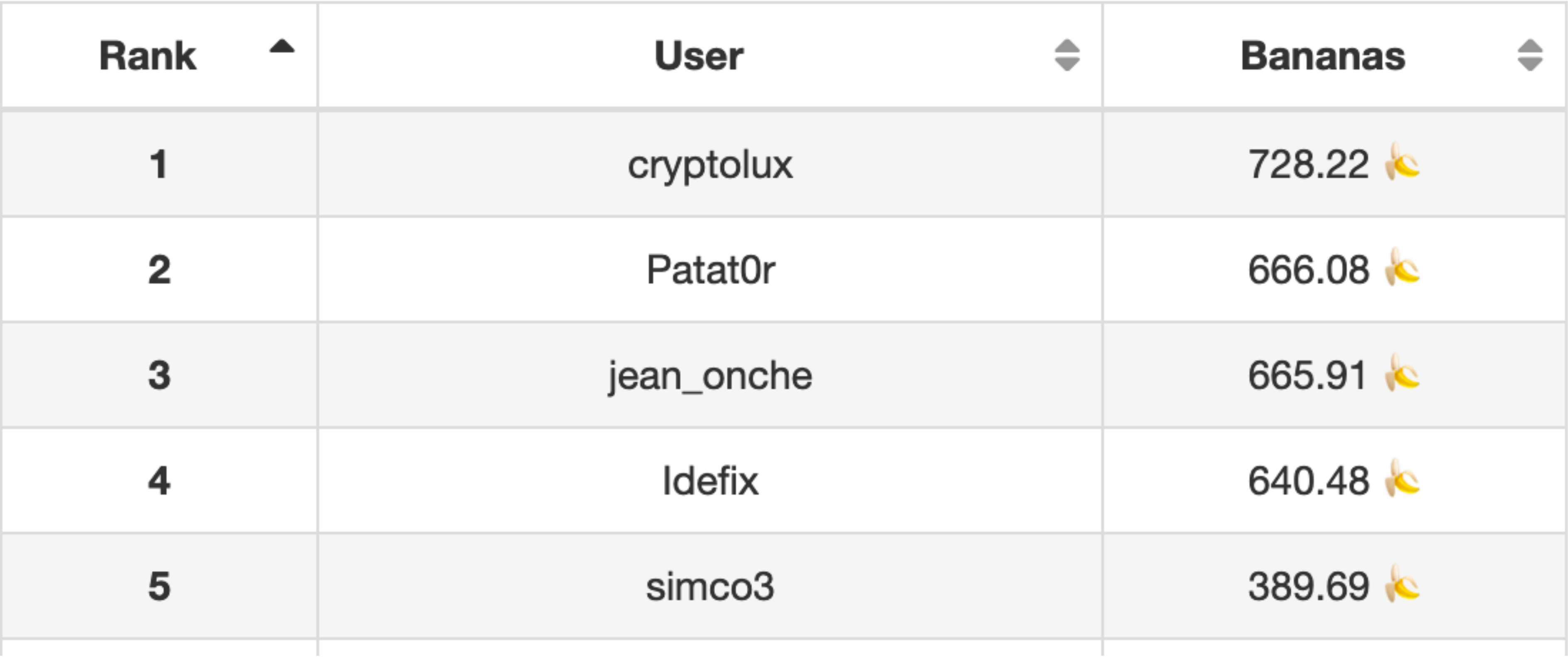
Strawberry scoreboard



Rank	id		Name (click to download)	🍓 / 🥕 Peak	User	Status
1	111	🟪	goofy_lichterman	3308.28 🍓 / 1654.14 🥕	cryptolux	Standing
2	115	🟦	elegant_turing	2760.53 🍓 / 1380.27 🥕	cryptolux	Standing
3	100	🟧	hopeful_kirch	1717.96 🍓 / 858.98 🥕	cryptolux	Standing
4	90	🟥	wonder[illegible]	[illegible]	[illegible]e_mountain	Broken!
5	35	🟪	friendly_edison	[illegible].04 🥕	Mugiwara	Broken!

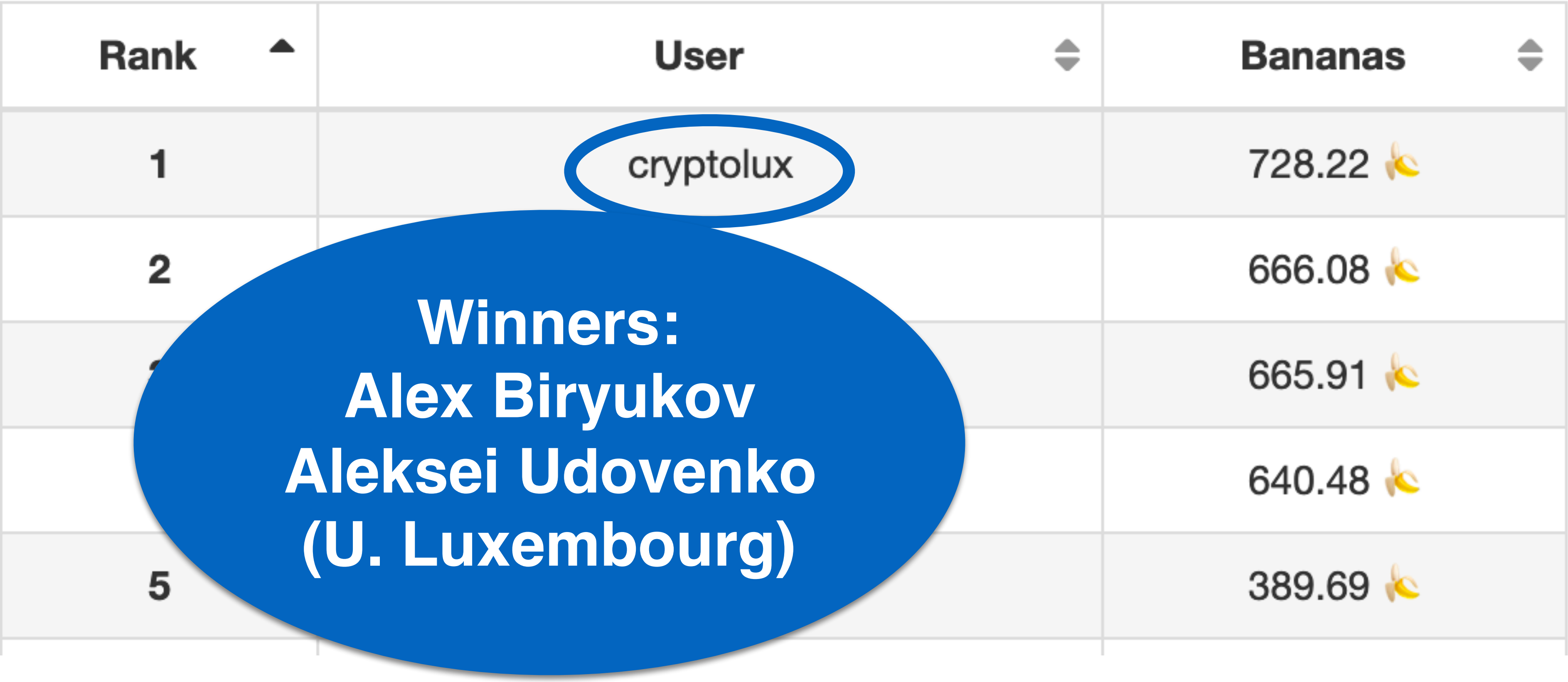
Stéphane Cauchie

Banana scoreboard



Rank ▲	User ⬍	Bananas ⬍
1	cryptolux	728.22 🍌
2	Patat0r	666.08 🍌
3	jean_onche	665.91 🍌
4	Idefix	640.48 🍌
5	simco3	389.69 🍌

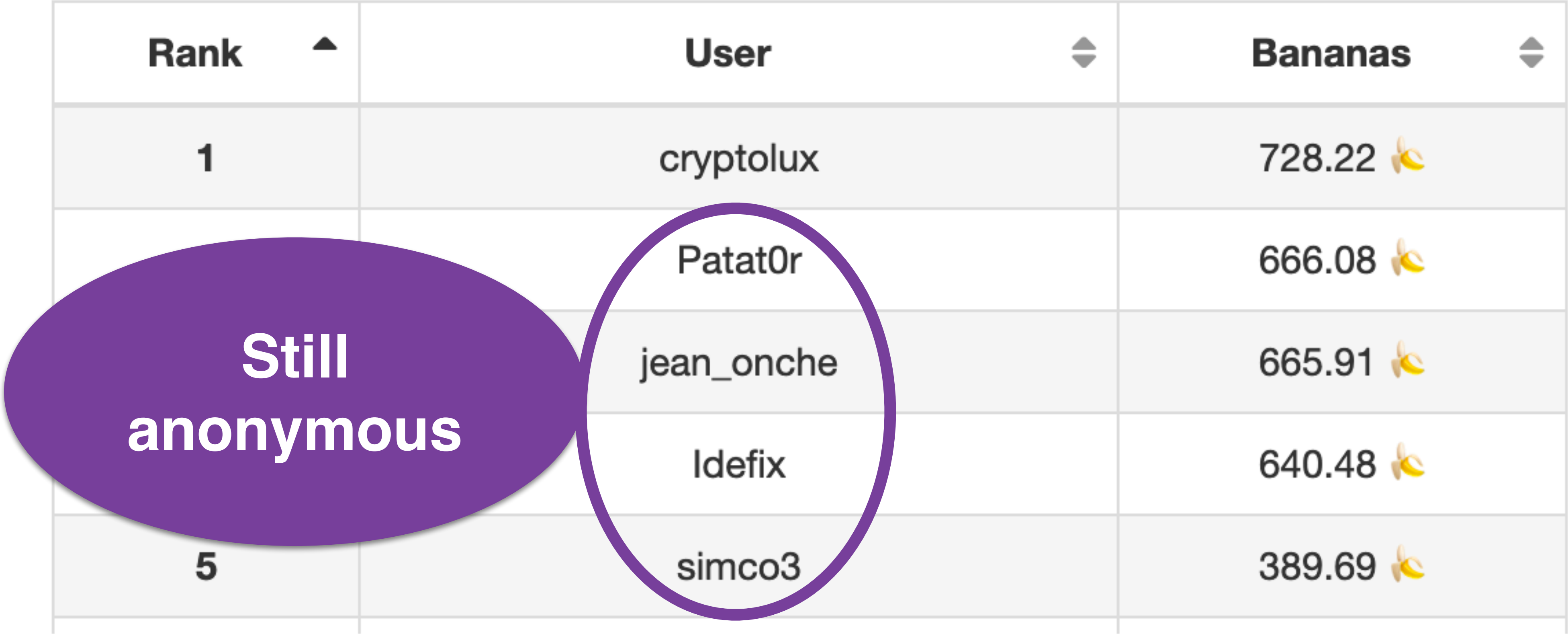
Banana scoreboard



Rank ▲	User	Bananas
1	cryptolux	728.22 🍌
2	[illegible]	666.08 🍌
[illegible]	[illegible]	665.91 🍌
[illegible]	[illegible]	640.48 🍌
5	[illegible]	389.69 🍌

Winners:
Alex Biryukov
Aleksei Udovenko
(U. Luxembourg)

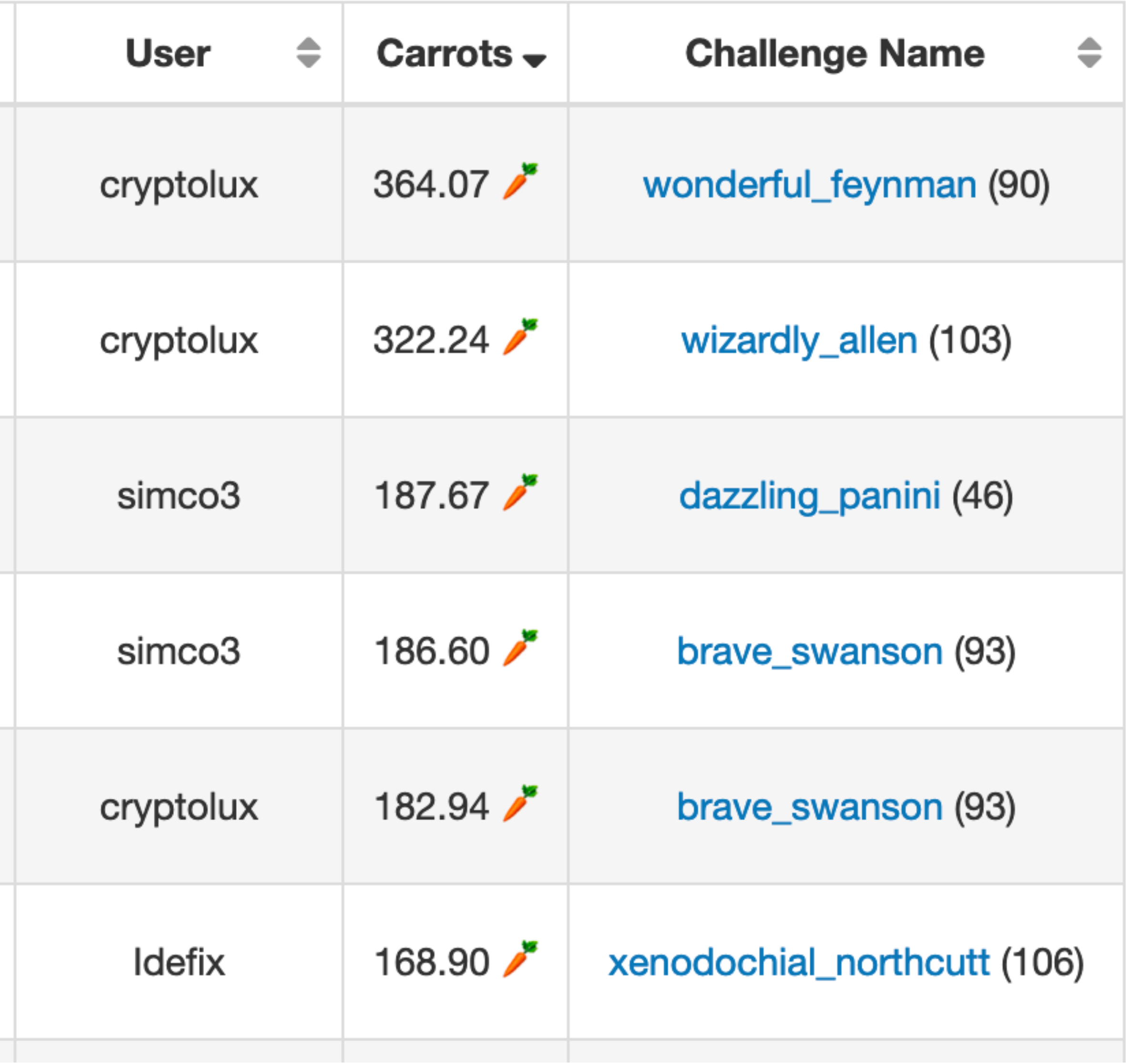
Banana scoreboard



Rank	User	Bananas
1	cryptolux	728.22 🍌
	Patat0r	666.08 🍌
	jean_onche	665.91 🍌
	Idefix	640.48 🍌
5	simco3	389.69 🍌

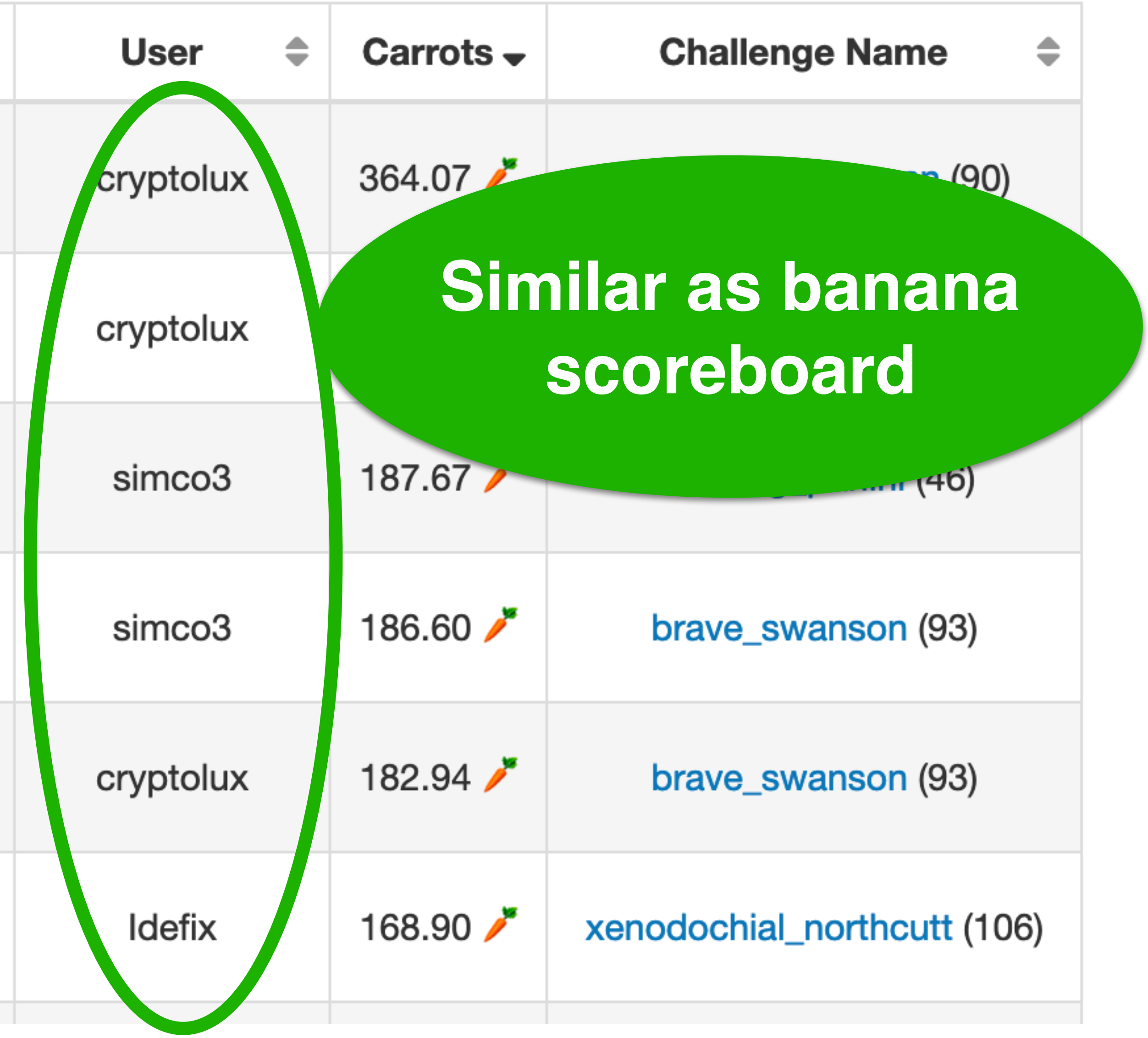
Still anonymous

Carrot scoreboard



User	Carrots	Challenge Name
cryptolux	364.07 🥕	wonderful_feynman (90)
cryptolux	322.24 🥕	wizardly_allen (103)
simco3	187.67 🥕	dazzling_panini (46)
simco3	186.60 🥕	brave_swanson (93)
cryptolux	182.94 🥕	brave_swanson (93)
Idefix	168.90 🥕	xenodochial_northcutt (106)

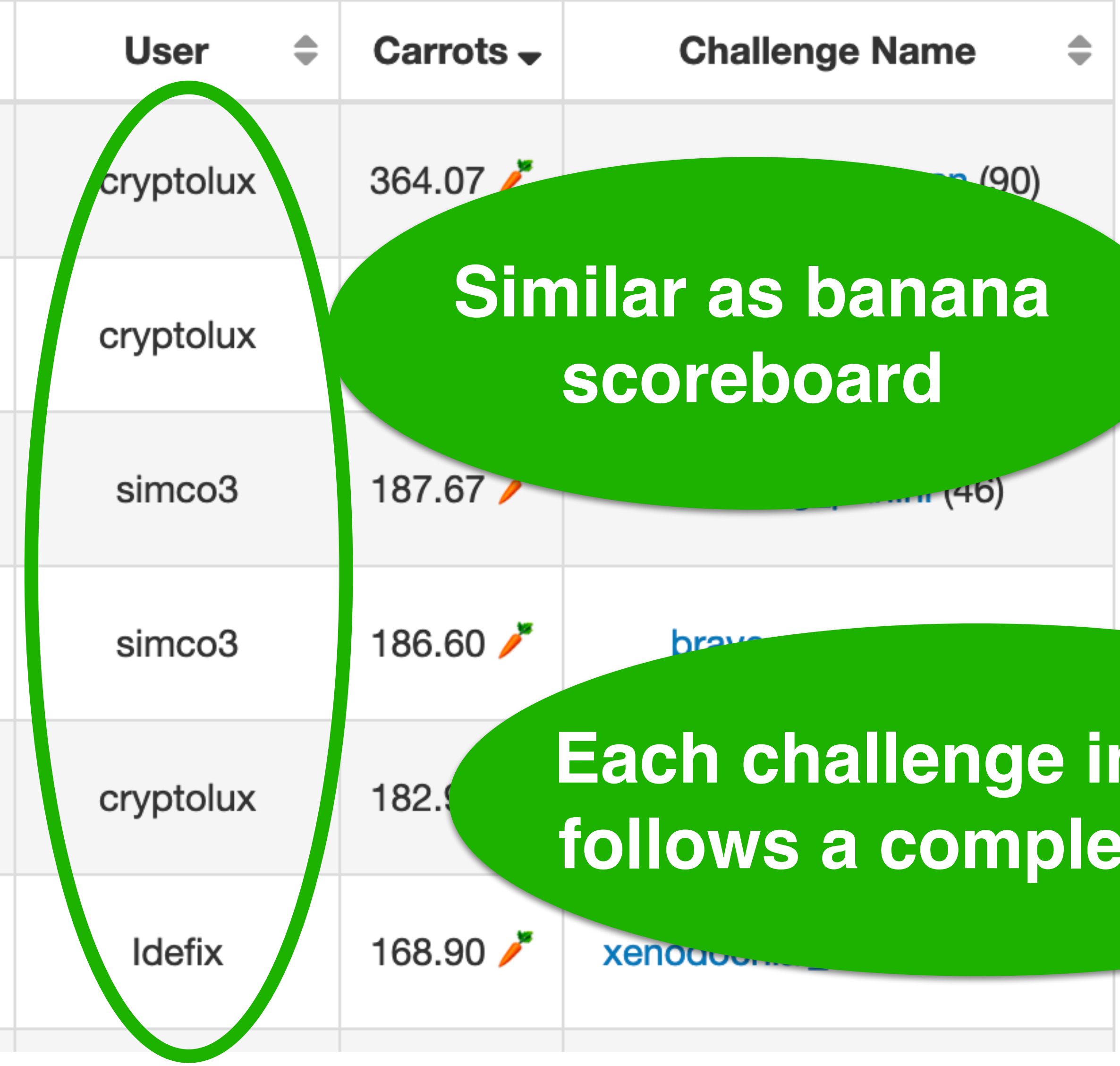
Carrot scoreboard



User	Carrots	Challenge Name
cryptolux	364.07 🥕	[illegible] (90)
cryptolux	[illegible]	[illegible]
simco3	187.67 🥕	[illegible] (46)
simco3	186.60 🥕	brave_swanson (93)
cryptolux	182.94 🥕	brave_swanson (93)
Idefix	168.90 🥕	xenodochial_northcutt (106)

Similar as banana scoreboard

Carrot scoreboard



User	Carrots	Challenge Name
cryptolux	364.07 🥕	(90)
cryptolux		
simco3	187.67 🥕	(46)
simco3	186.60 🥕	brav
cryptolux	182.	
Idefix	168.90 🥕	xenod

Similar as banana scoreboard

Each challenge inversion follows a complete break

Final notes

- Congratulation to the double winners:
  - **Alex Biryukov** (U. Luxembourg)
  - **Aleksei Udovenko** (U. Luxembourg)
- Special thanks to:
  - **Stefan Kölbl** (CYBERCRYPT)
  - **Junwei Wang** (CryptoExperts)
- All the submitted implementations are available:

  https://whibox.cyber-crypt.com/
- Try to break cryptolux standing challenges:

  https://www.cryptolux.org/index.php/Whitebox_cryptography
- Wall of fame to come soon: https://www.cyber-crypt.com/whibox-contest/
- Any suggestion for next edition: https://whibox-contest.slack.com/