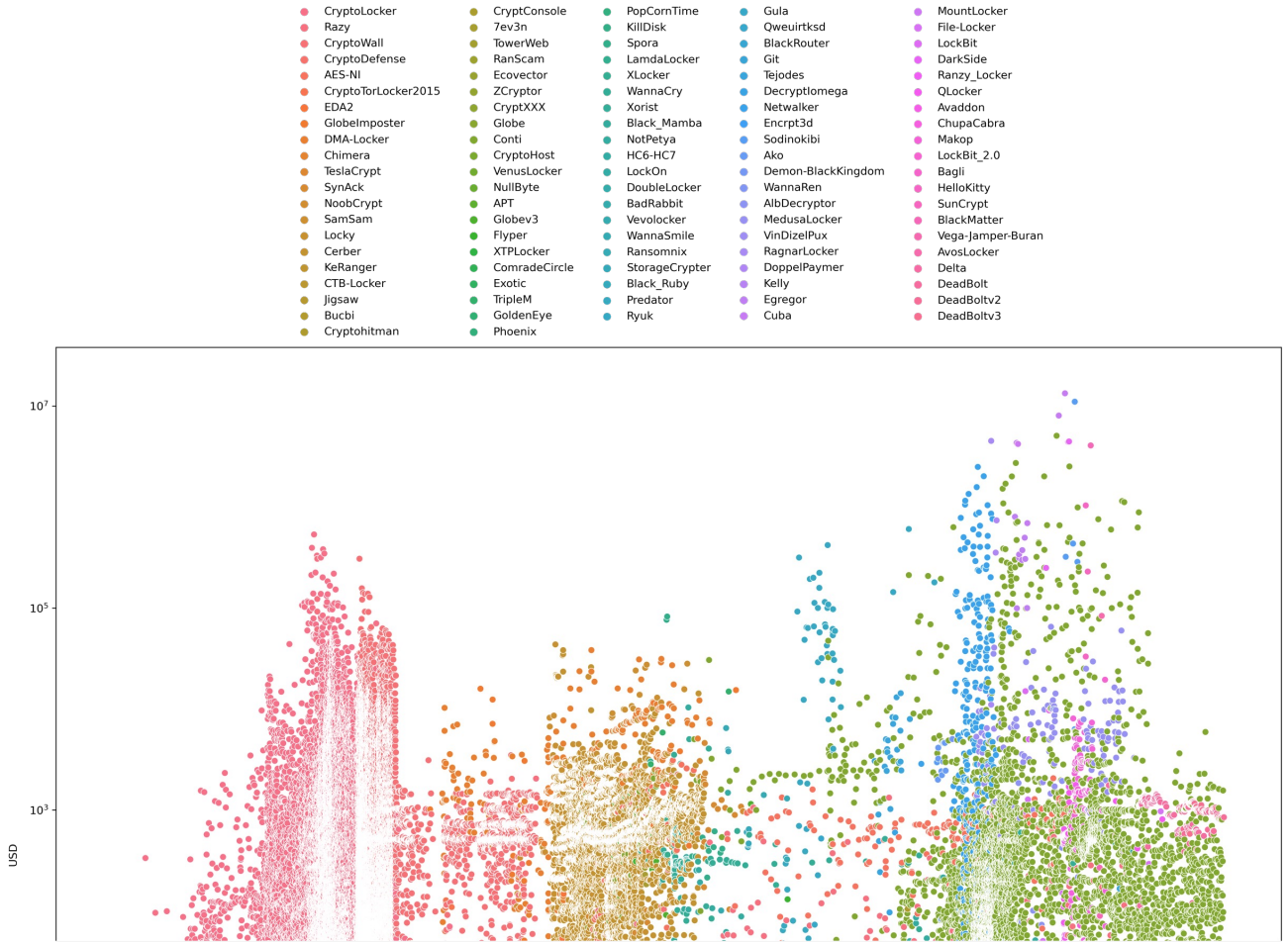
THE CHANGING FACE OF MODELLING CYBER

ÉIREANN LEVERETT, CTO, WARATAH ANALYTICS

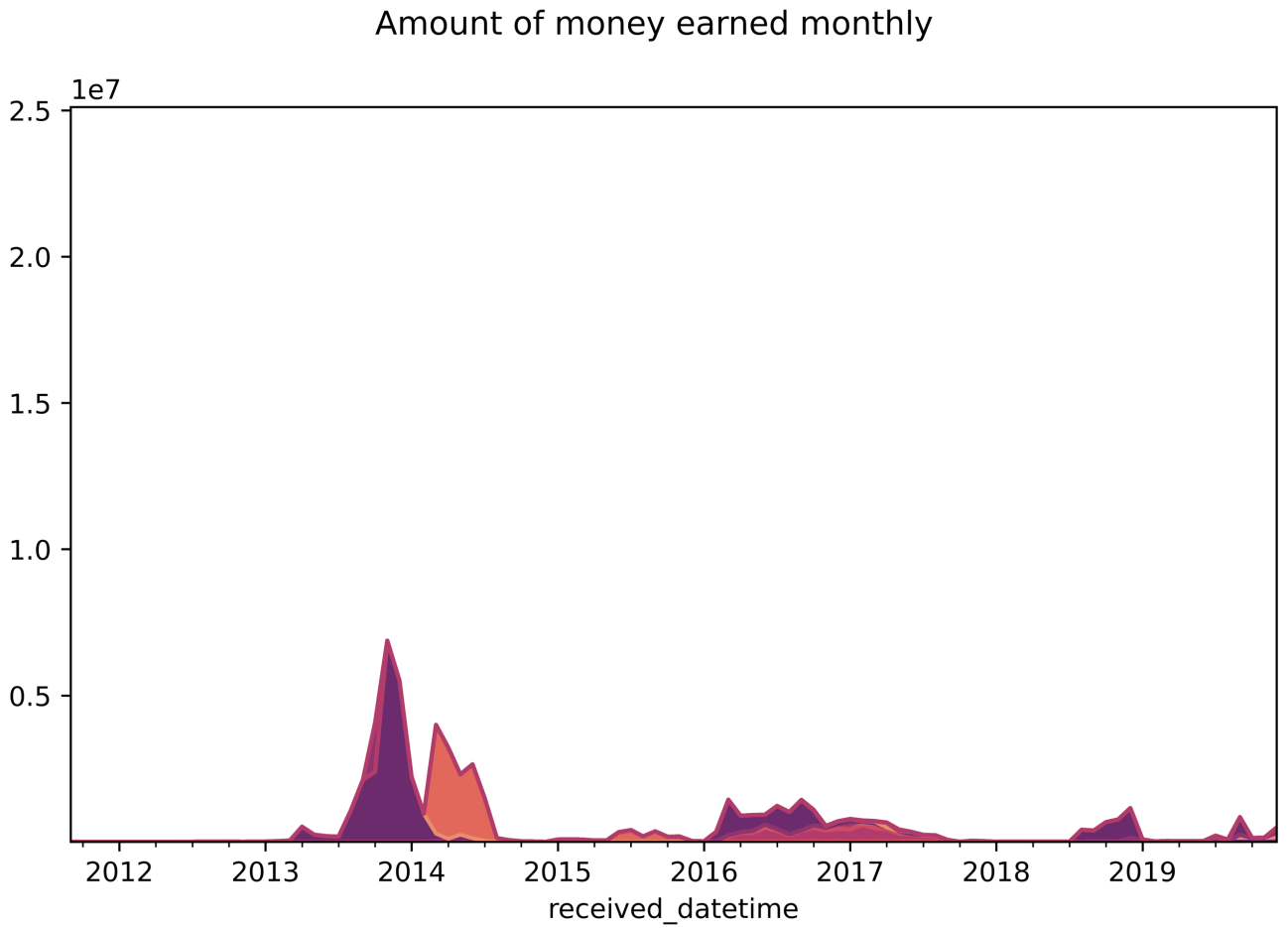
@BLACKSWANBURST

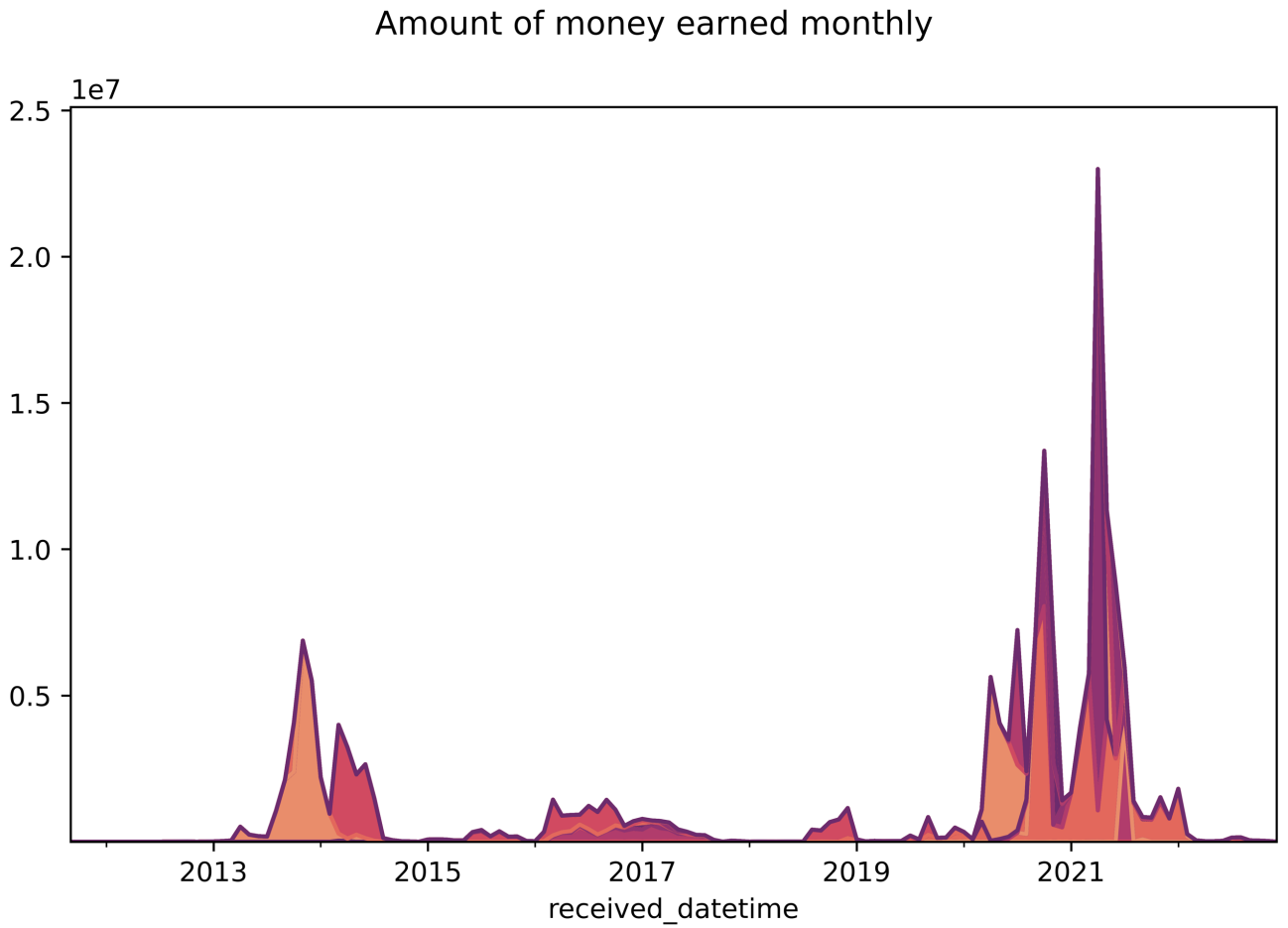


ARE RANSOMS GETTING WORSE OVER TIME?

Spearmans Correlation Coefficient	1.00
P-Value	0.000

IN 2020 WE PUBLISHED THIS


Amount of money earned monthly
1e7
2.5
2.0
1.5
1.0
0.5
2012
2013
2014
2015
2016
2017
2018
2019
received_datetime

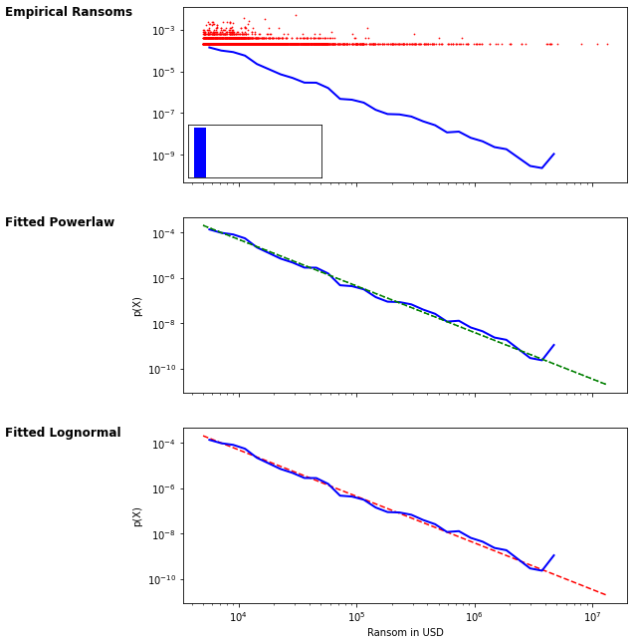

Amount of money earned monthly
1e7
2.5
2.0
1.5
1.0
0.5
2013
2015
2017
2019
2021
received_datetime

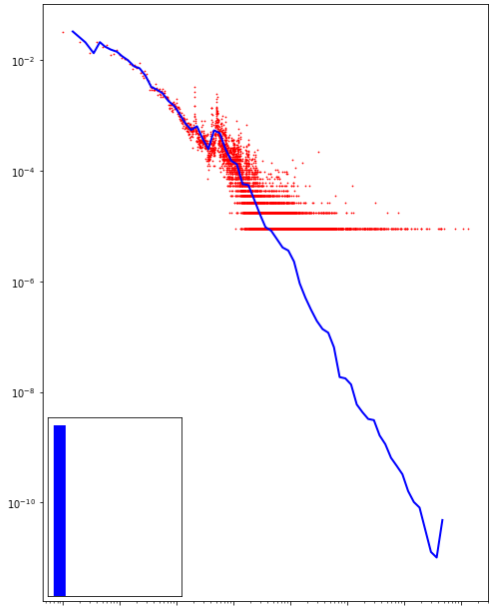
RANSOM TAILS

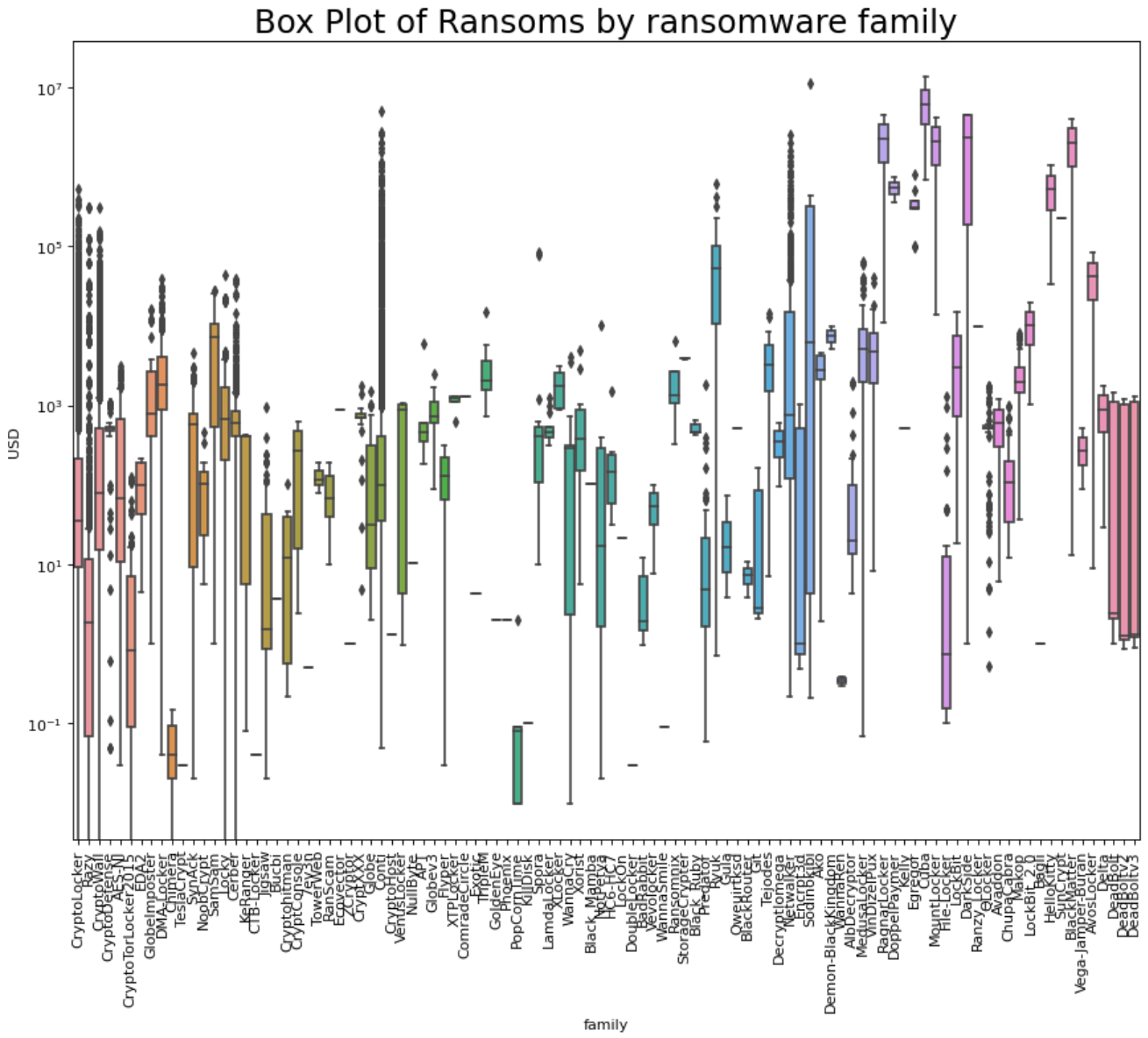
Good fits:

- Lognormal
- Powerlaw

- BUT THERE'S A CATCH…



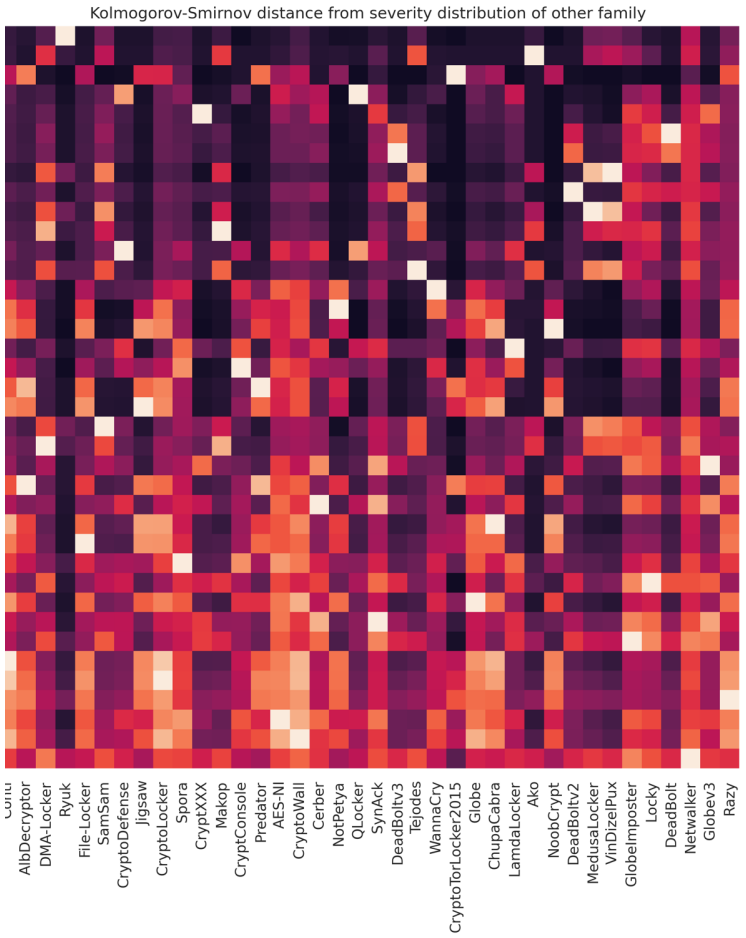


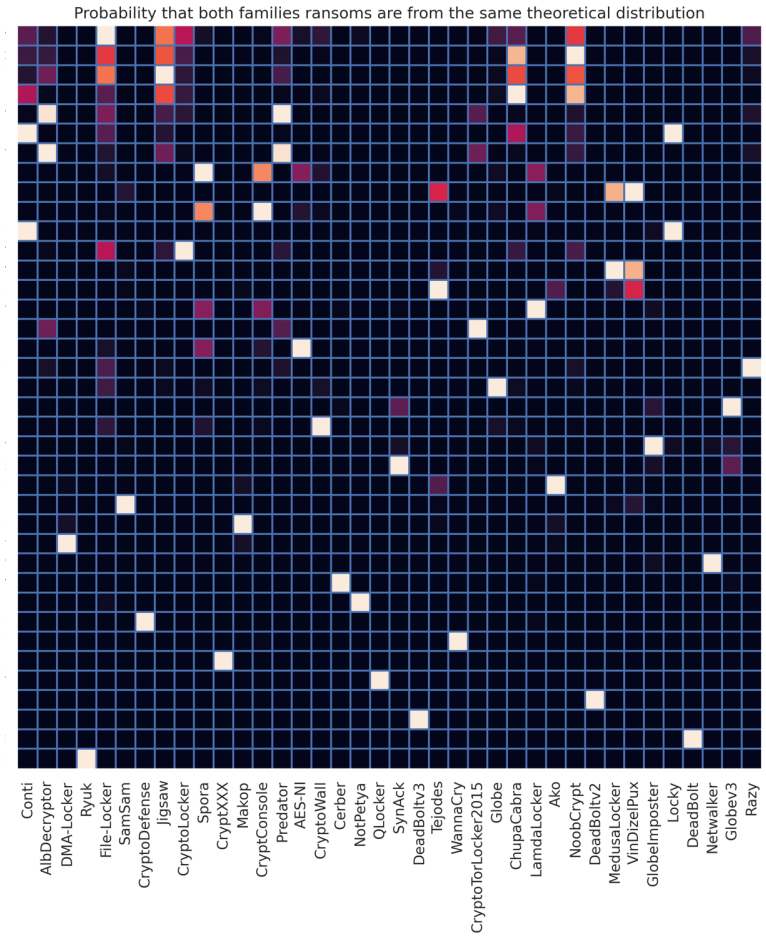


CORRELATION AGAINST GANG IS HIGH;VERY HIGH!

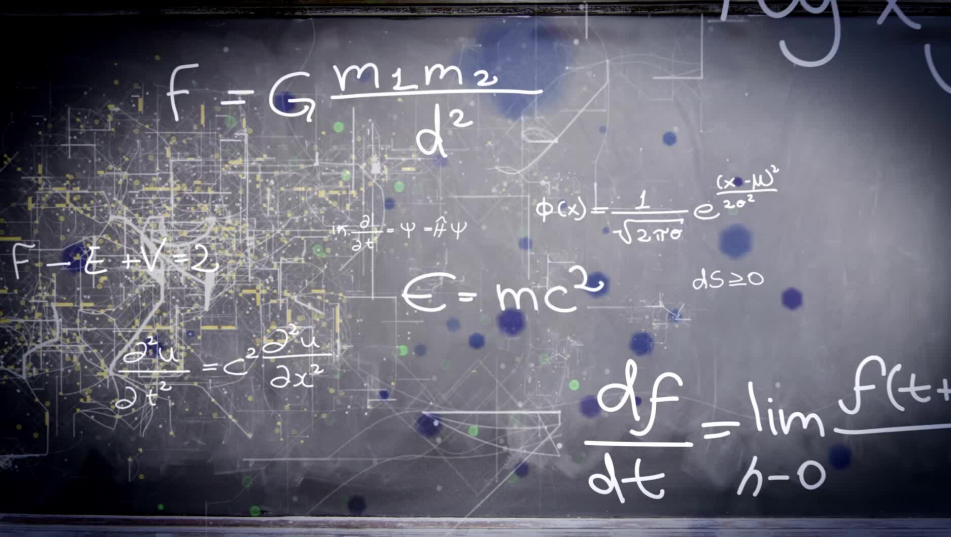
Spearmans Correlation Coefficient	**0.952**
P-Value	0.000

RANSOMWARE LOSSES AREN'T IDENTICALLY DISTRIBUTED!



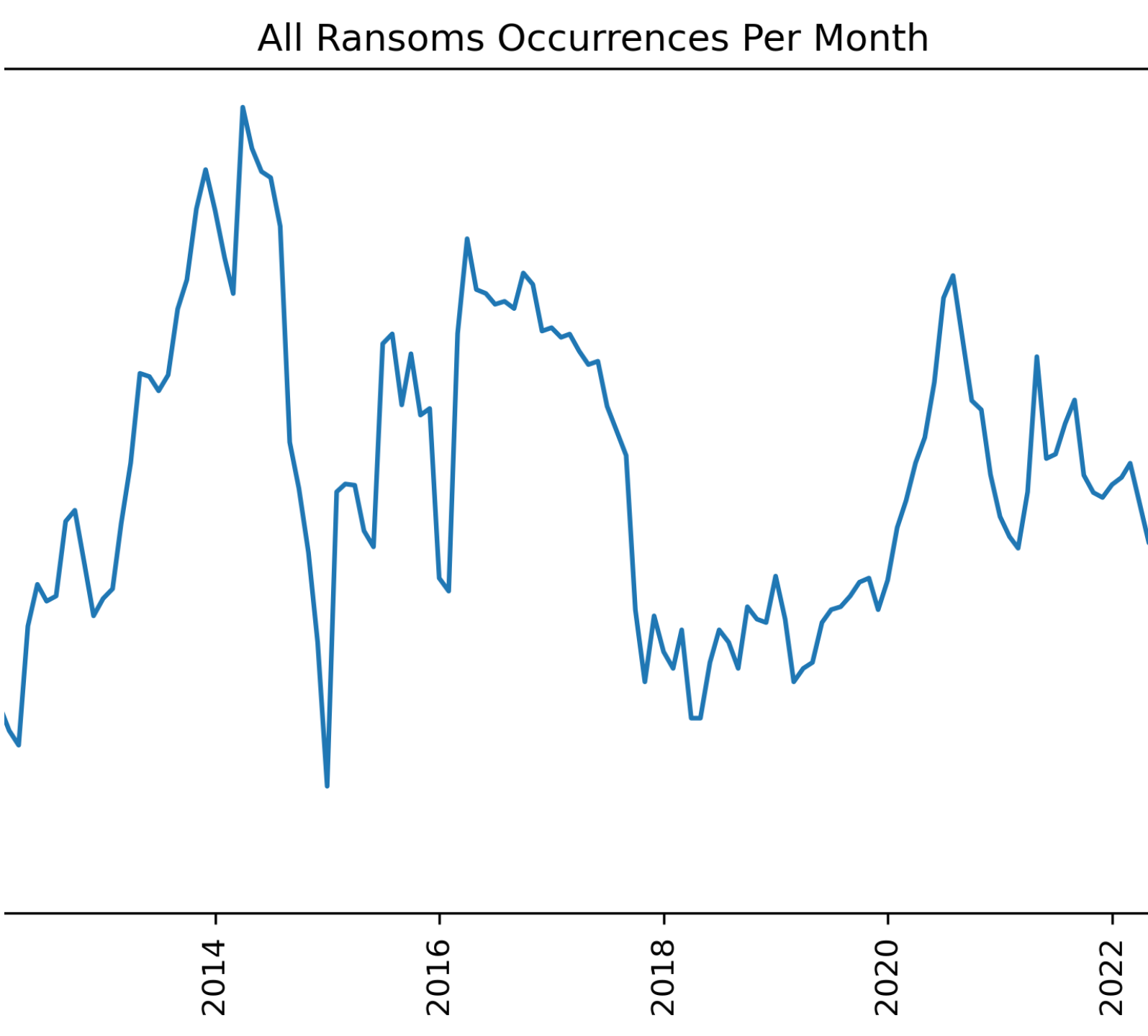


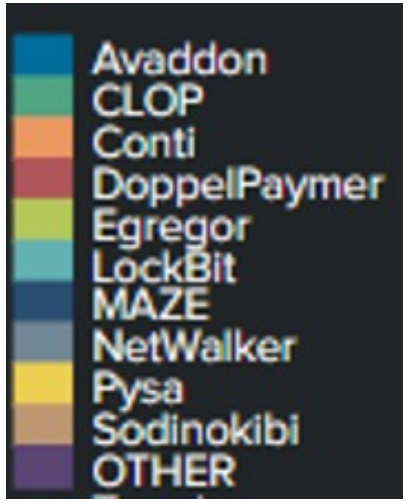
- Left is the KS distance
- Right is the probability (P-Value) that both severities are from the same distribution.
  - White is highly likely to be the same
  - Black is highly unlikely to be the same
- You can also do this for frequency and get similar results.

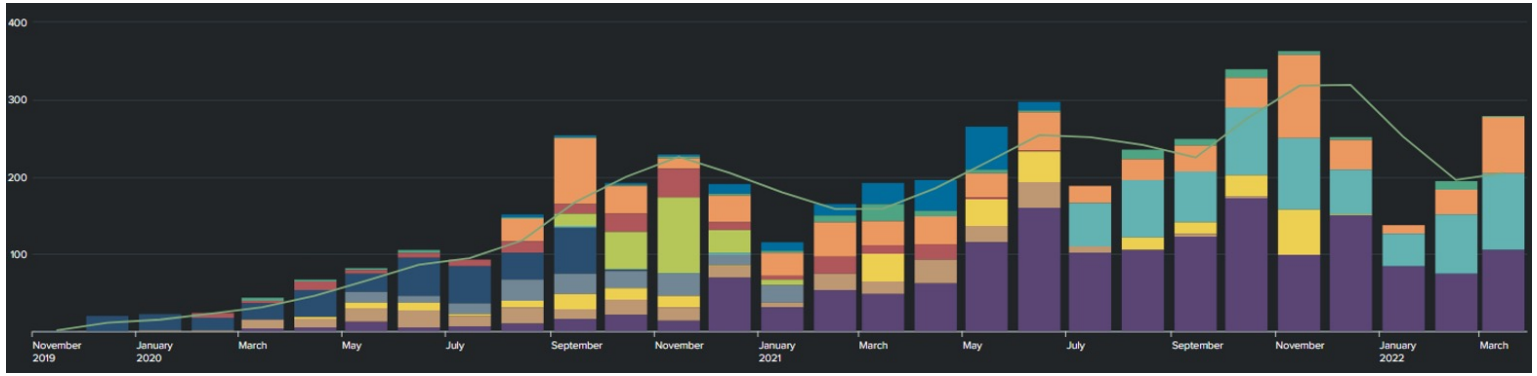


IN OTHER WORDS… RANSOMWARE ISN'T I.I.D. !

- It's definitely not identically distributed.
- It's probably independent.
- We shouldn't be using single distribution fits for the:
  - Frequency
  - Severity
- Powerlaws as mixture models is a well known phenomenon, so the fit makes sense…
- We propose modelling it by mixture model



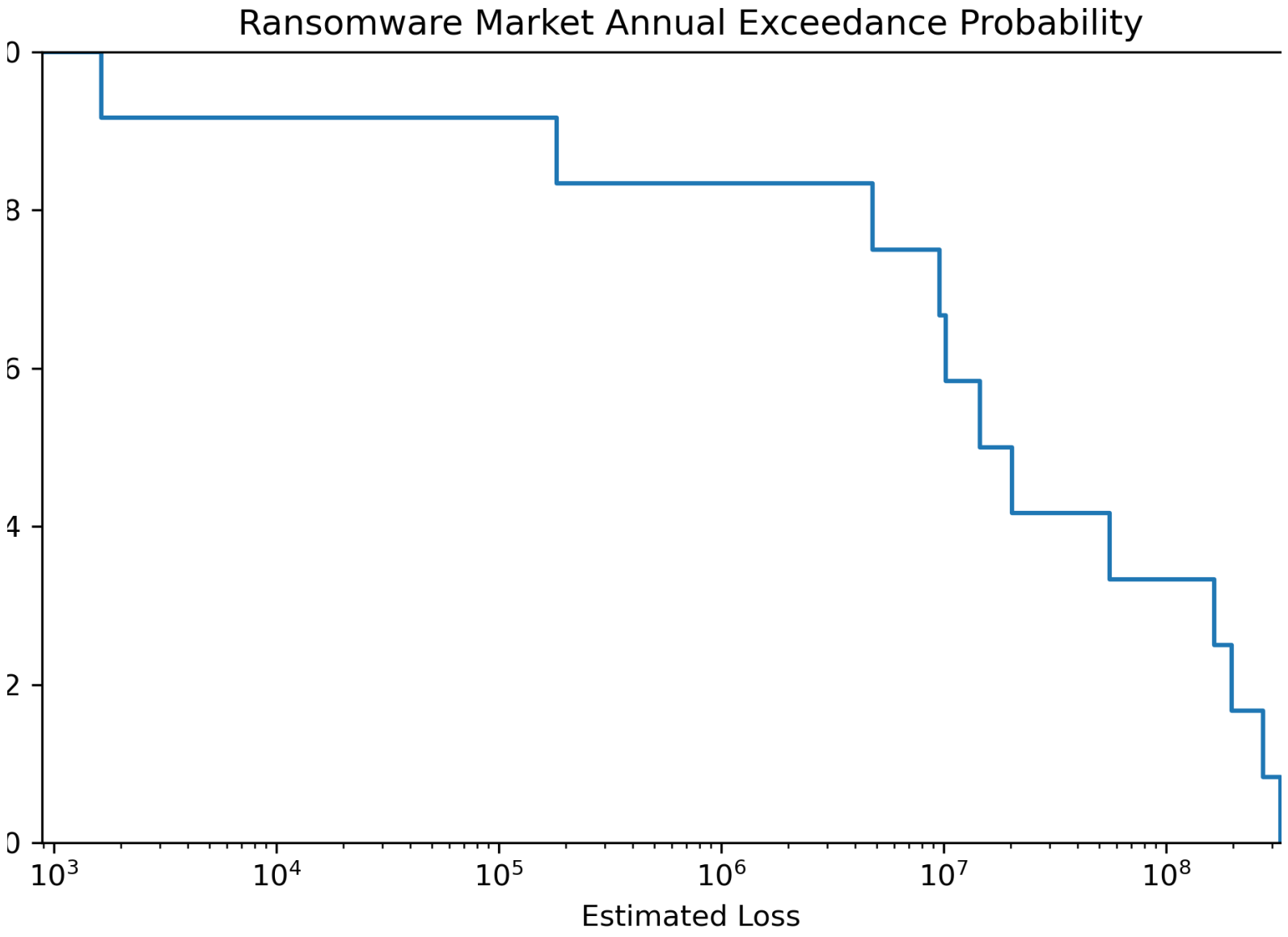




THE FREQUENCY OF RANSOMWARE IS: GROUPS BATTLING OVER "MARKET SHARE"

WHY DOES THIS MATTER?

- The statistics are crisp
- In particular the frequency of event modelling shows wild "regime change"
  - When groups are arrested
  - When their tools are hacked by other groups
  - When they change tools and work practices
- Modelling ransomware losses (or frequency) with a single distribution now presents a:
  - clear,
  - defined,
  - model risk



WE WILL MODEL THIS WITH MULTI-AGENTS IN OASIS LMF

QUESTIONS?

- ELEVERETT@WARATAH.IO
- @BLACKSWANBURST

- WITH THANKS TO LIGHT HILL RISK NETWORKS