

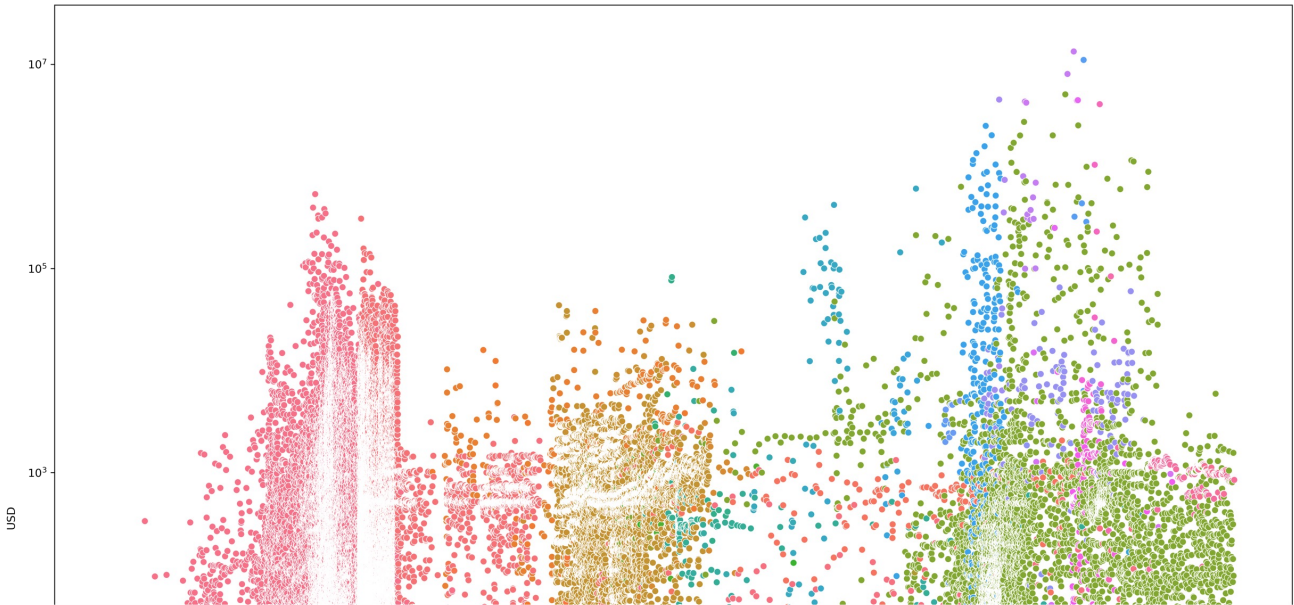


THE CHANGING FACE OF MODELLING CYBER

ÉIREANN LEVERETT, CTO, WARATAH ANALYTICS

@BLACKSWANBURST

- CryptoLocker
- Razy
- CryptoWall
- CryptoDefense
- AES-NI
- CryptoTortLocker2015
- EDA2
- GlobeImposter
- DMA-Locker
- Chimera
- TeslaCrypt
- SynAck
- NoobCrypt
- Samsam
- Locky
- Cerber
- KeRanger
- CTB-Locker
- Jigsaw
- Bucbi
- CryptoHitman
- CryptConsole
- 7ev3n
- TowerWeb
- RanScam
- Ecovector
- ZCryptor
- CryptXXX
- Globe
- Conti
- CryptoHost
- VenusLocker
- NullByte
- APT
- Globev3
- Flyper
- XTPLocker
- ComradeCircle
- Exotic
- TripleM
- GoldenEye
- Phoenix
- PopCornTime
- KillDisk
- Spora
- LamdaLocker
- XLocker
- WannaCry
- Xorist
- Black_Mamba
- NotPetya
- HC6-HC7
- LockOn
- DoubleLocker
- BadRabbit
- Vevolocker
- WannaSmile
- Ransomnix
- StorageCrypter
- Black_Ruby
- Predator
- Ryuk
- Gula
- Qweirtksd
- BlackRouter
- Git
- Tejodes
- Decryptlomega
- Netwalker
- Encript3d
- Sodinokibi
- Ako
- Demon-BlackKingdom
- WannaRen
- AlbDecryptor
- MedusaLocker
- VinDizelPux
- RagnarLocker
- DoppelPaymer
- Kelly
- Egregor
- Cuba
- MountLocker
- File-Locker
- LockBit
- DarkSide
- Ranzy_Locker
- QLocker
- Avaddon
- ChupaCabra
- Makop
- LockBit_2.0
- Bagli
- HelloKitty
- SunCrypt
- BlackMatter
- Vega-Jammer-Buran
- AvosLocker
- Delta
- DeadBolt
- DeadBoltv2
- DeadBoltv3



ARE RANSOMS GETTING WORSE OVER TIME?

**Spearman's
Correlation
Coefficient**

1.00

P-Value

0.000

Conferences > 2020 APWG Symposium on Electr... ?

Averages don't characterise the heavy tails of ransoms

Publisher: IEEE

Cite This

PDF

Éireann Leverett ; Eric Jardine ; Erin Burns ; Ankit Gangwal ; Dan Geer [All Authors](#)

17
Full
Text Views



Abstract

Document Sections

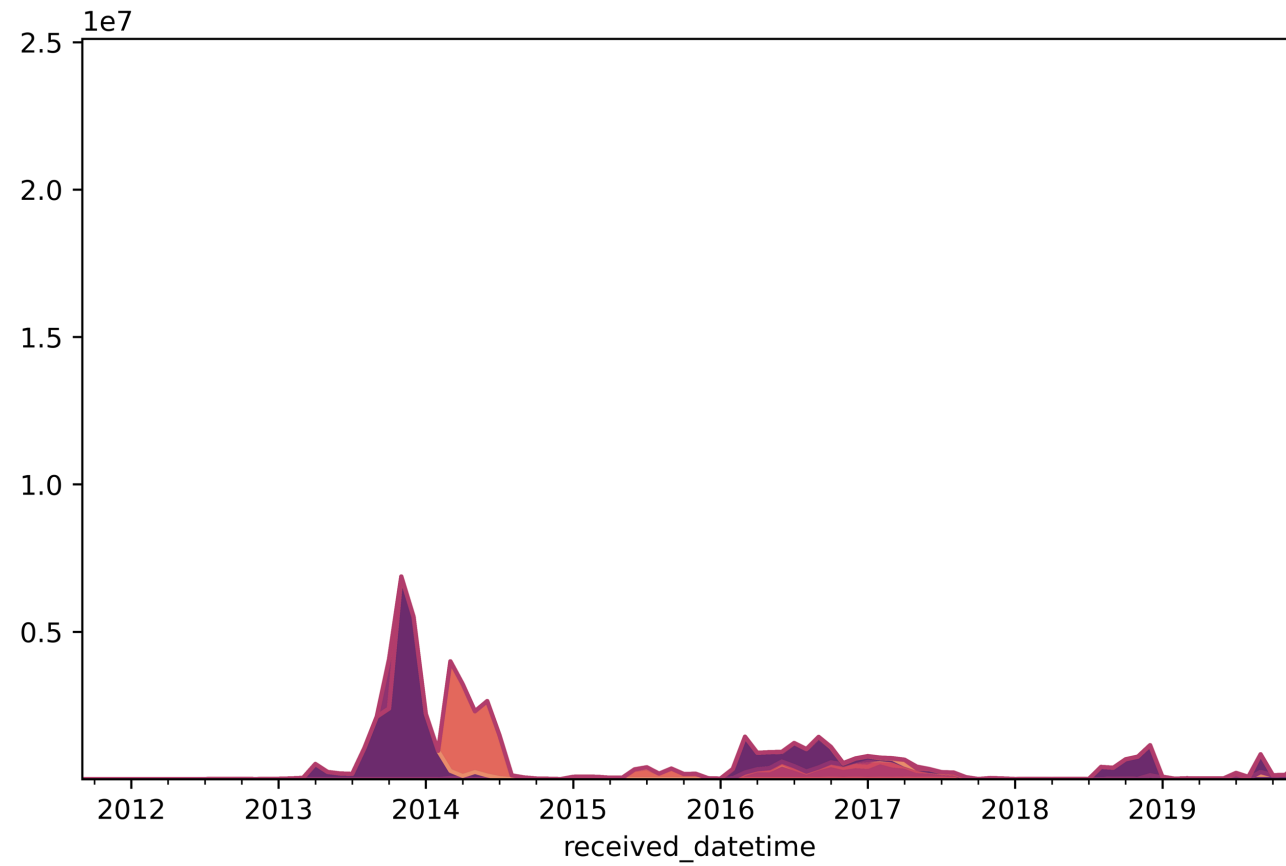
I. Introduction

Abstract:

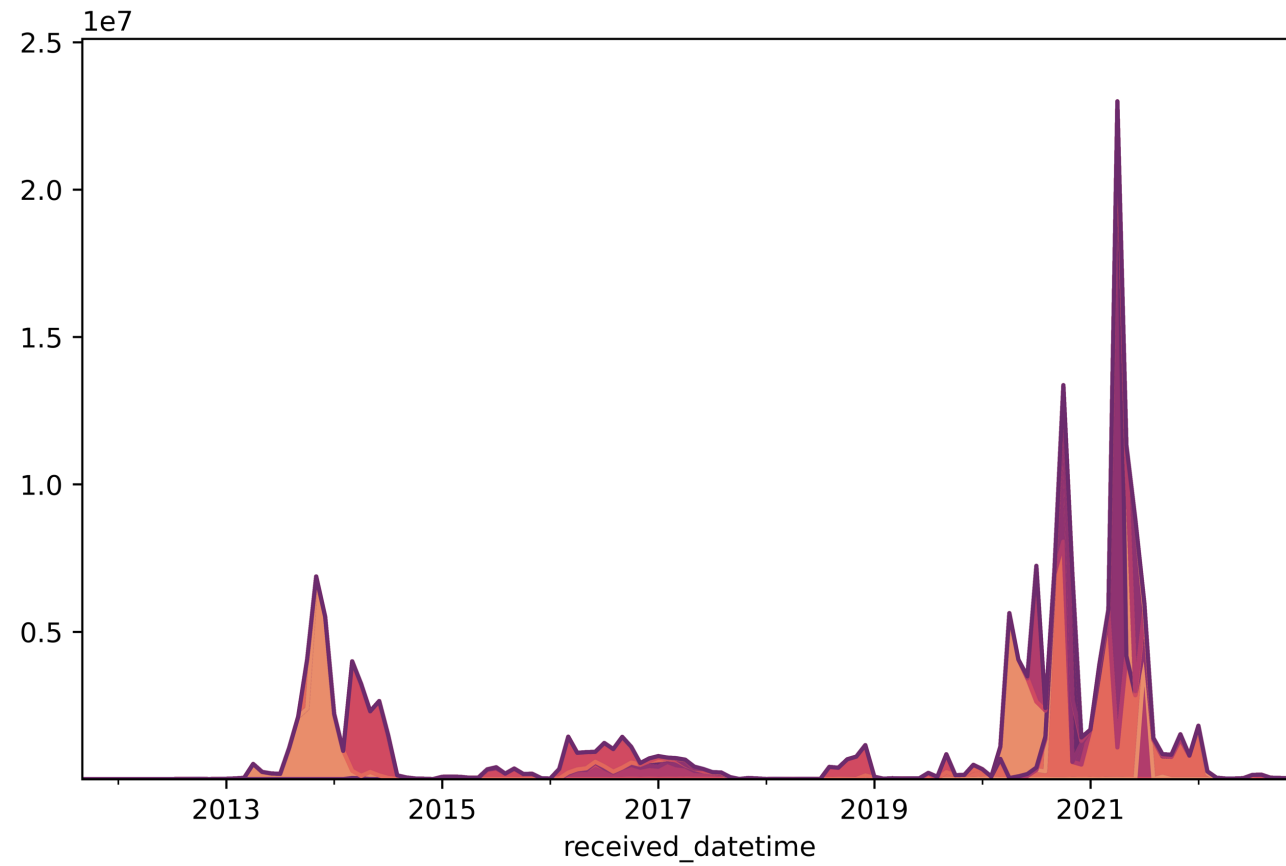
The Bitcoin block-chain is the scoreboard of Ransomware. By mining the data in it and within the malware itself, we can understand the distribution of ransoms and characterise ransomware risk. Ransoms follow the power-law distribution in their amounts. The alpha parameter (α) of those power laws suggest they do not have a well defined average for most years in our study. Indeed, there has not been an α above 2

IN 2020 WE
PUBLISHED
THIS

Amount of money earned monthly



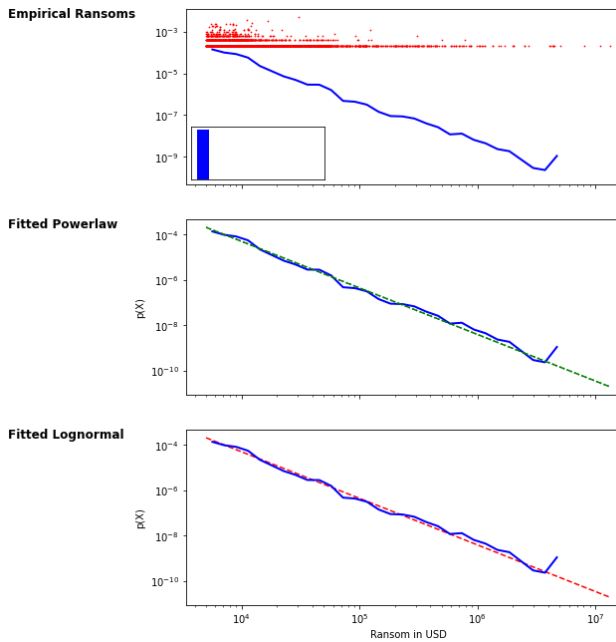
Amount of money earned monthly



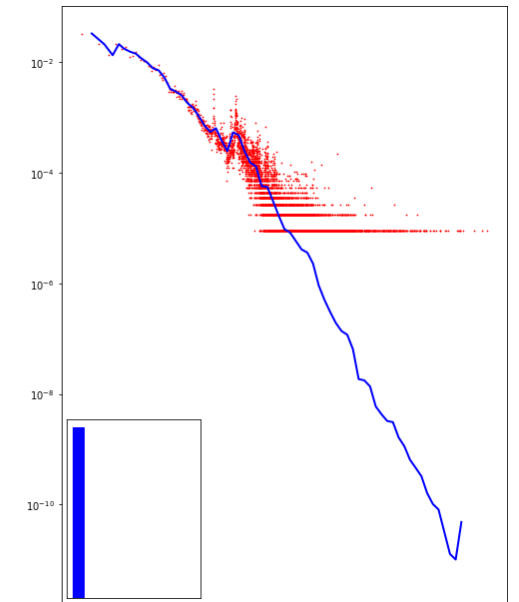
RANSOM TAILS

Good fits:

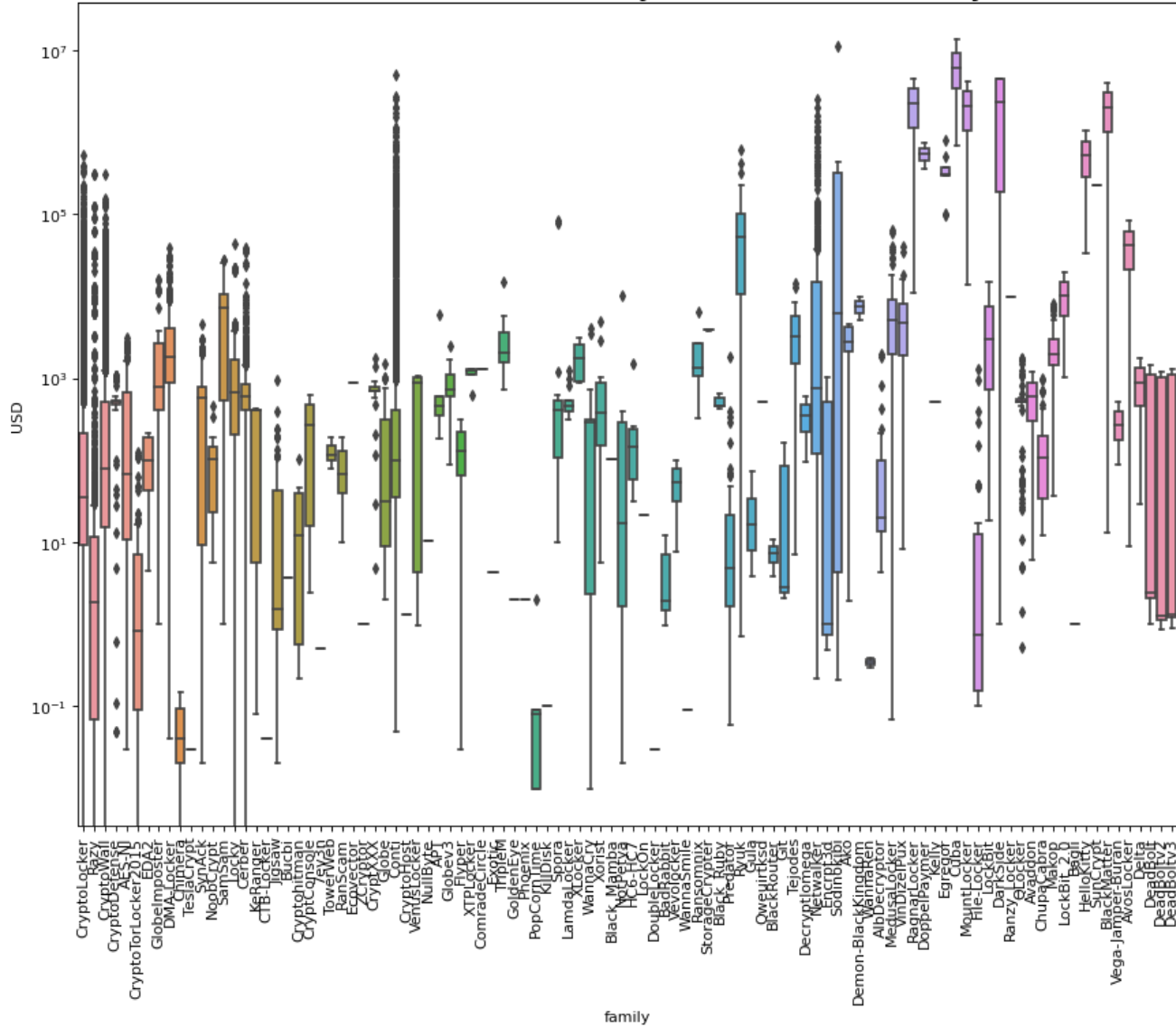
- Lognormal
- Powerlaw
- BUT THERE'S A CATCH...



A



Box Plot of Ransoms by ransomware family



**CORRELATION
AGAINST GANG IS
HIGH; VERY HIGH!**

**Spearman's
Correlation
Coefficient**

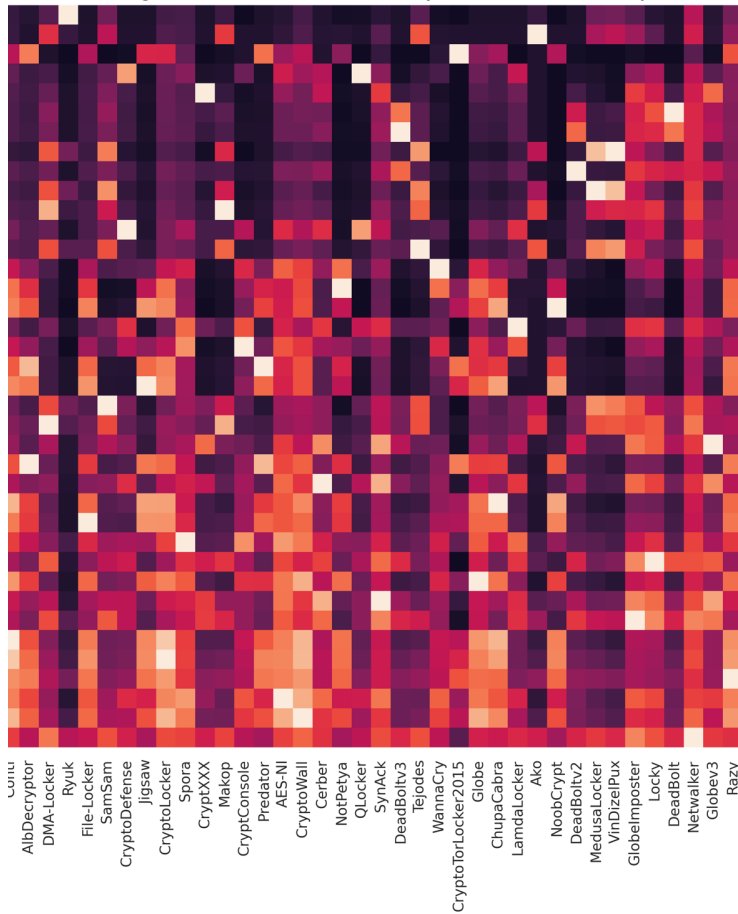
0.952

P-Value

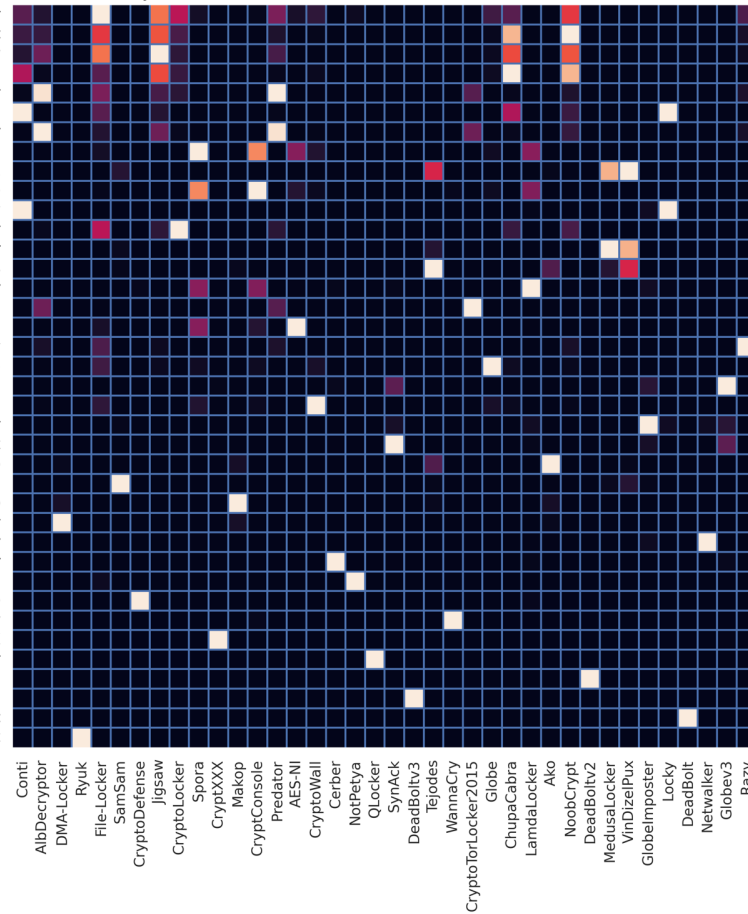
0.000

RANSOMWARE LOSSES AREN'T IDENTICALLY DISTRIBUTED!

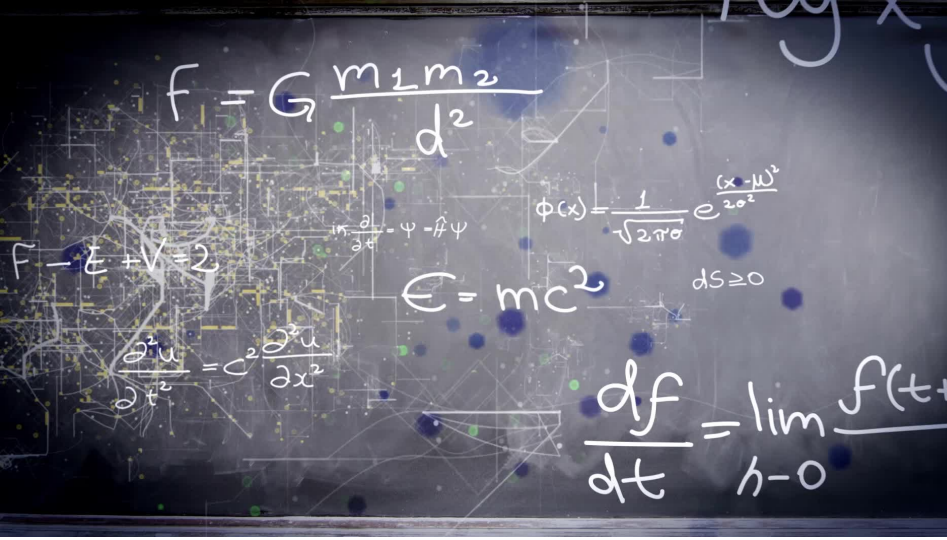
Kolmogorov-Smirnov distance from severity distribution of other family



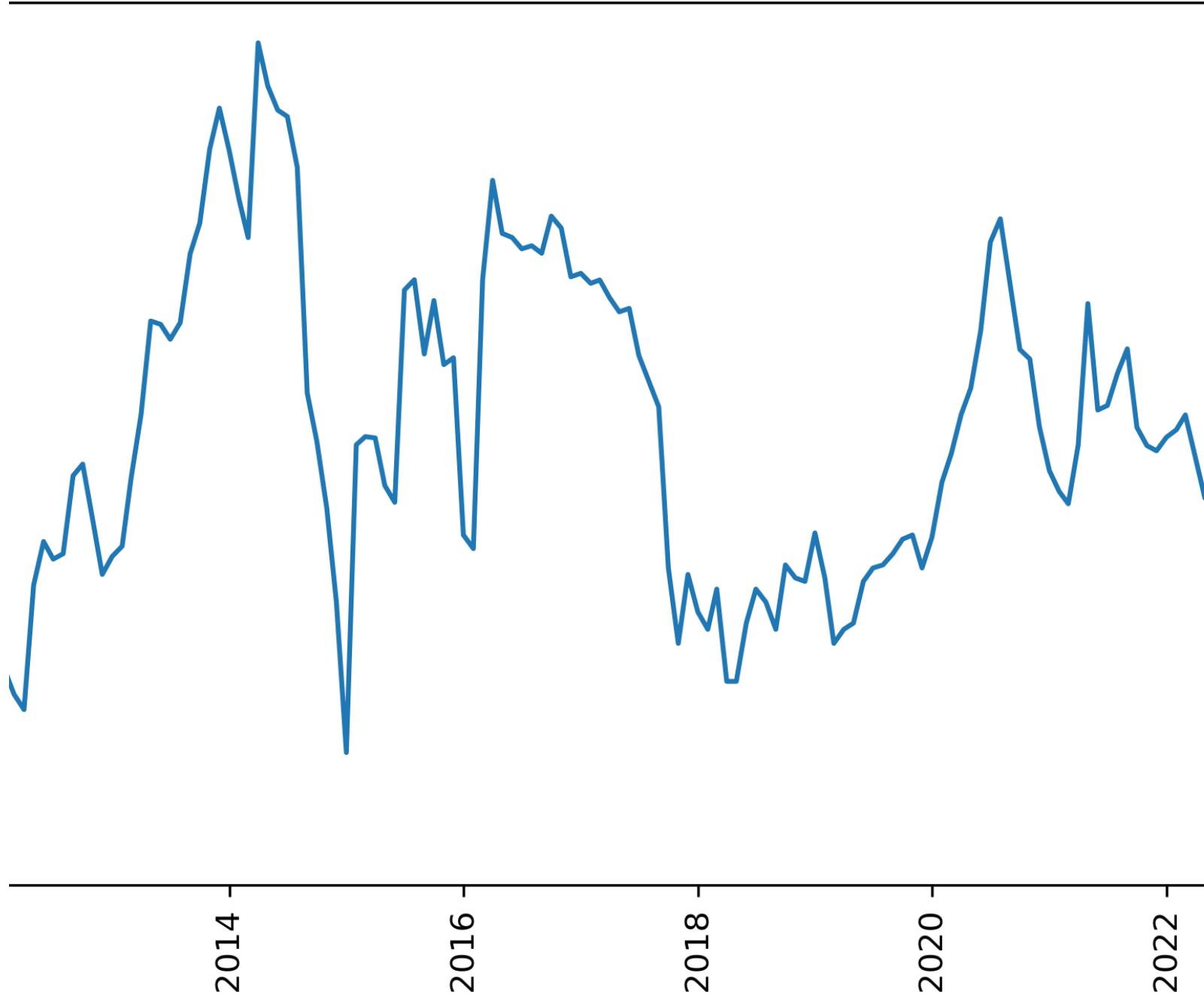
Probability that both families ransoms are from the same theoretical distribution



- 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.

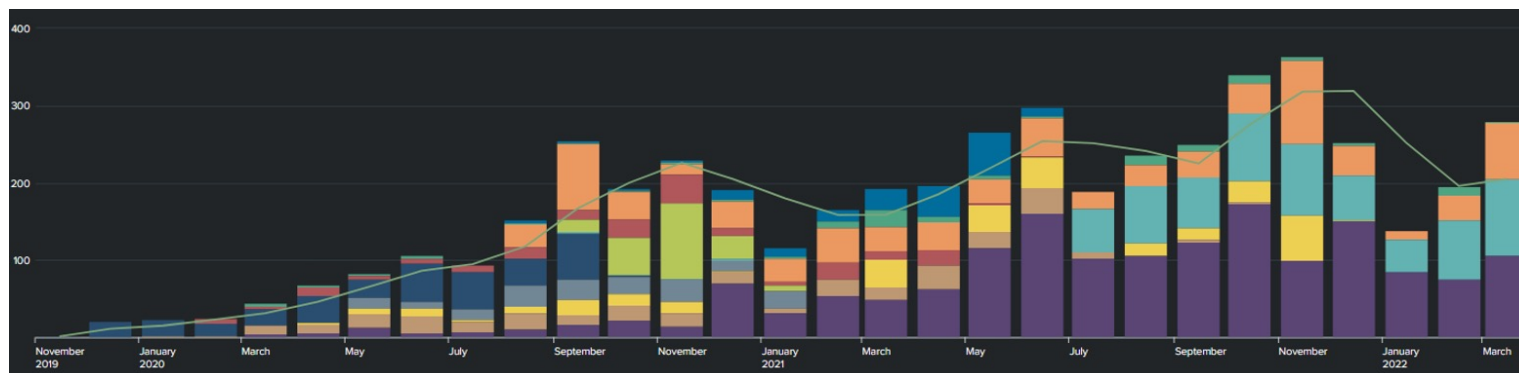


All Ransoms Occurrences Per Month



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



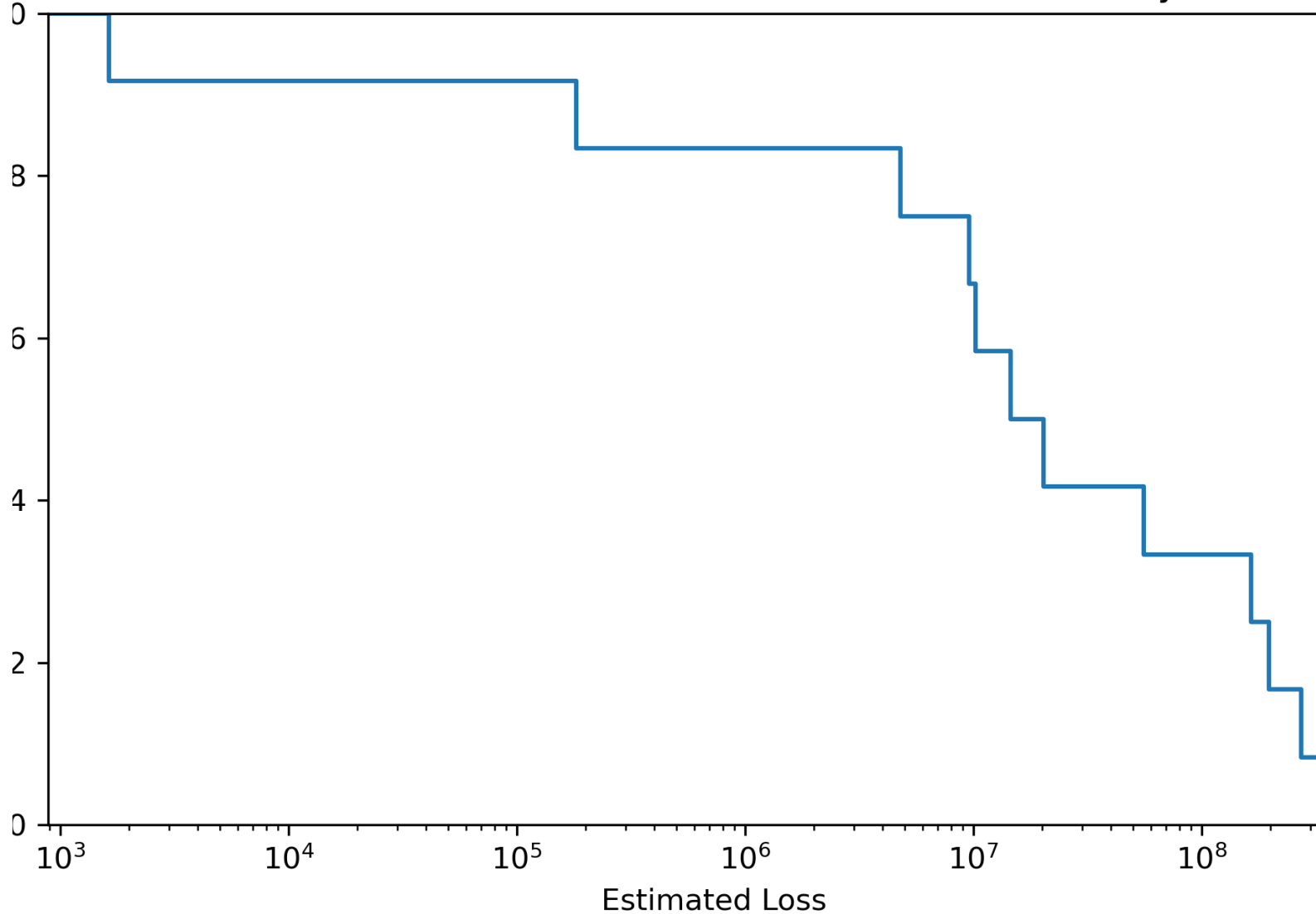
THE FREQUENCY OF RANSOMWARE IS:
 GROUPS BATTLING OVER “MARKET SHARE”

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



Ransomware Market Annual Exceedance Probability



WE WILL
MODEL THIS
WITH MULTI-
AGENTS IN
OASIS LMF

QUESTIONS?

- ELEVERETT@WARATAH.IO
- @BLACKSWANBURST

- WITH THANKS TO LIGHT HILL
RISK NETWORKS

