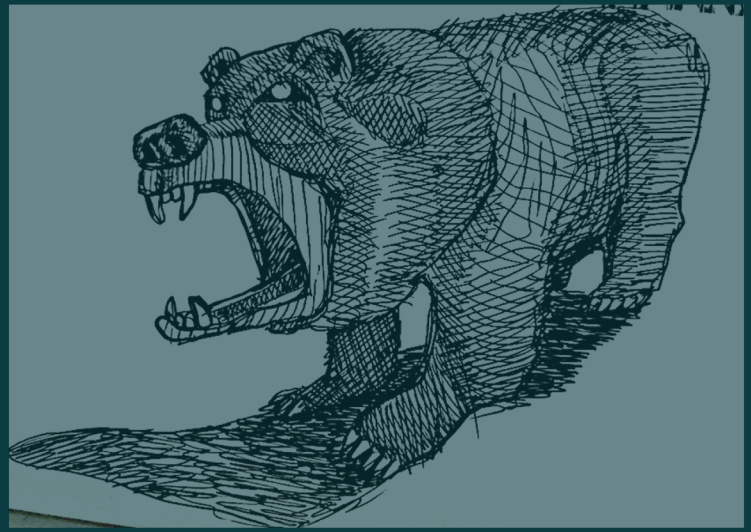
Ransomware as a Science

TLP: Amber

Bakuei Matsukawa (Trend Micro, Researcher),
Vladimir Kropotov (Trend Micro, Researcher),
Fyodor Yarochkin (Trend Micro, Researcher),
Robert McArdle (Trend Micro, Director FTR),
Shingo Matsugaya (Trend Micro, Researcher)
Erin Burns (Concinnity Risks, UK)
Éireann Leverett (Concinnity Risks, UK)

Agenda



Introduction

Sourcing the data

Understanding the data

Data fusion (playing with the data)

Conclusions and QA

Introduction

- We have data, lots of data of different types
- We try to view ransomware holistically, all groups, all types of victims
  - All ransomware actors (profiteers/state actors/noobs)
  - All victims (paying/not paying/blocked by endpoint)
  - Interdisciplinary (Binaries/Networks/Financials/Risk)
- We have some novel techniques for tracking threat actors
- We have some evidence for policy makers to consider
- We are aiming for a theory of change beyond “make backups”

Data sources and knowledge domains

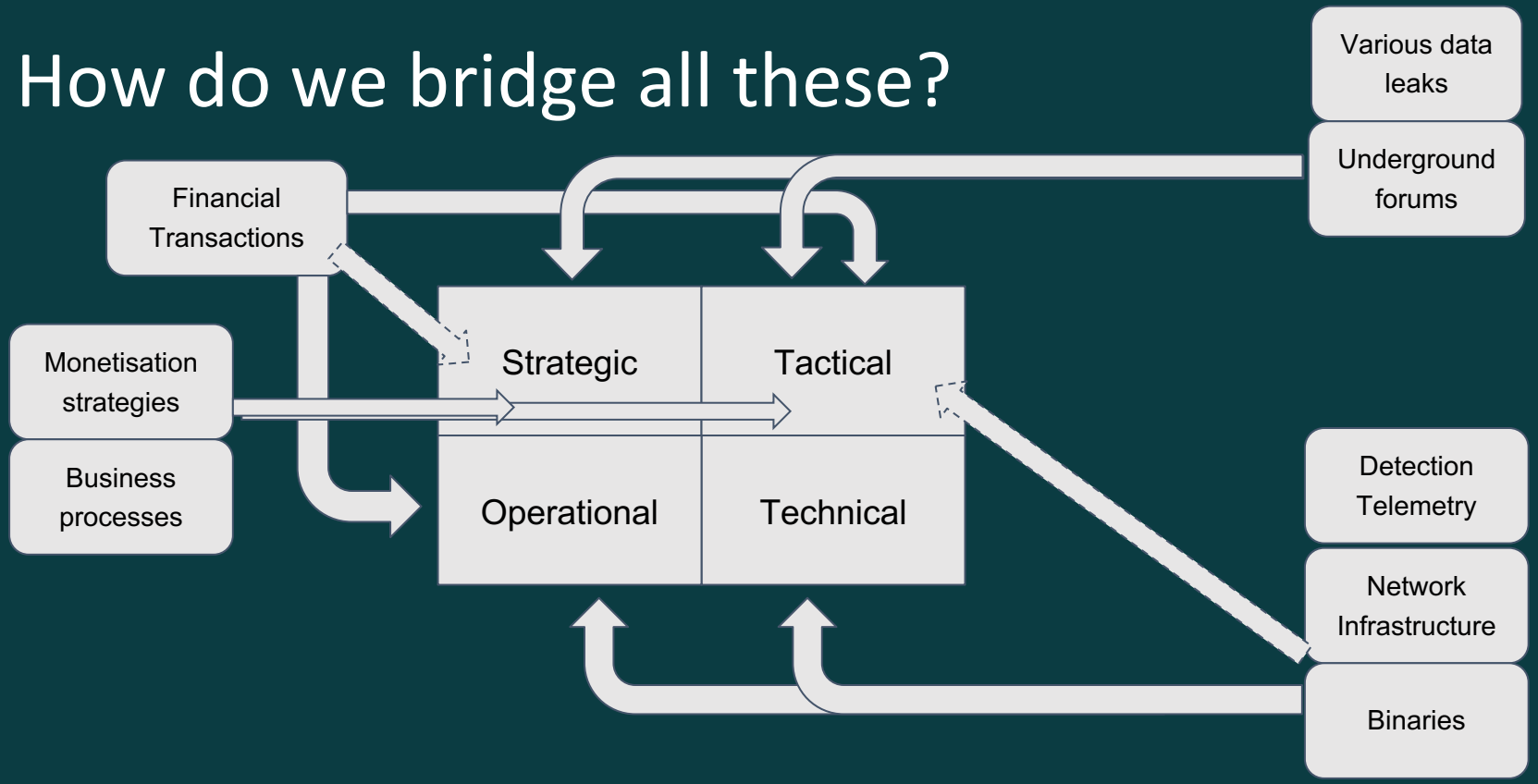
Detection Telemetry
Network Infrastructure

Underground forums
Various data leaks

Blockchain and Financial Transactions
Monetization strategies and Business processes

Time Series analysis
Statistical Methods
(DataSci/AI/ML/Quantum/ZeroTrust/Buzzword Bingo/ J/K)

How do we bridge all these?



How do we bridge all these?

Time Series Analysis!

Sourcing the data

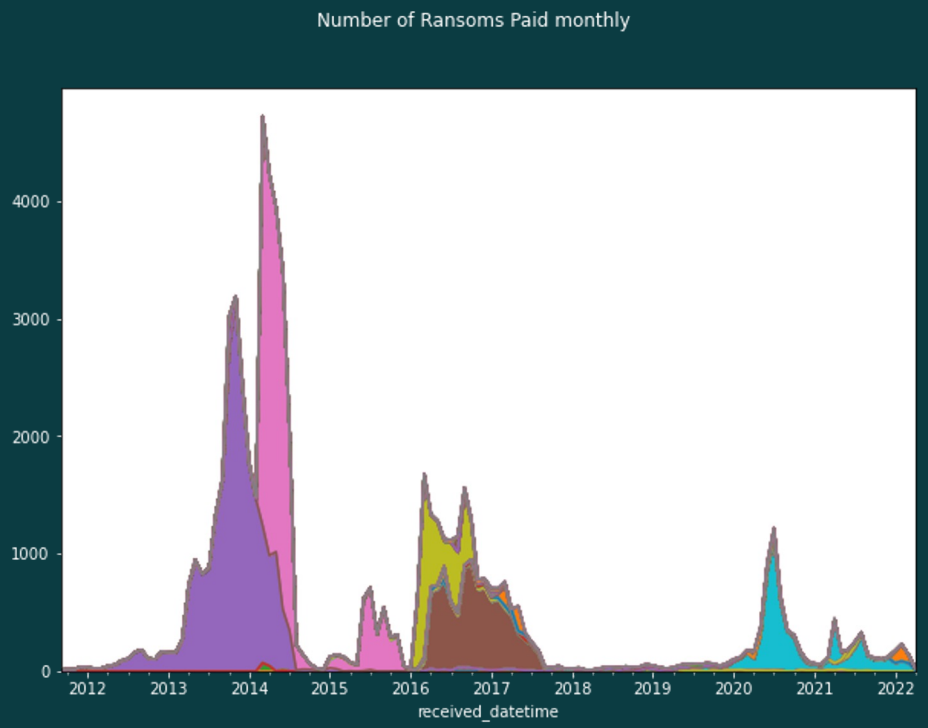
Detections: ransomware over time by geolocation

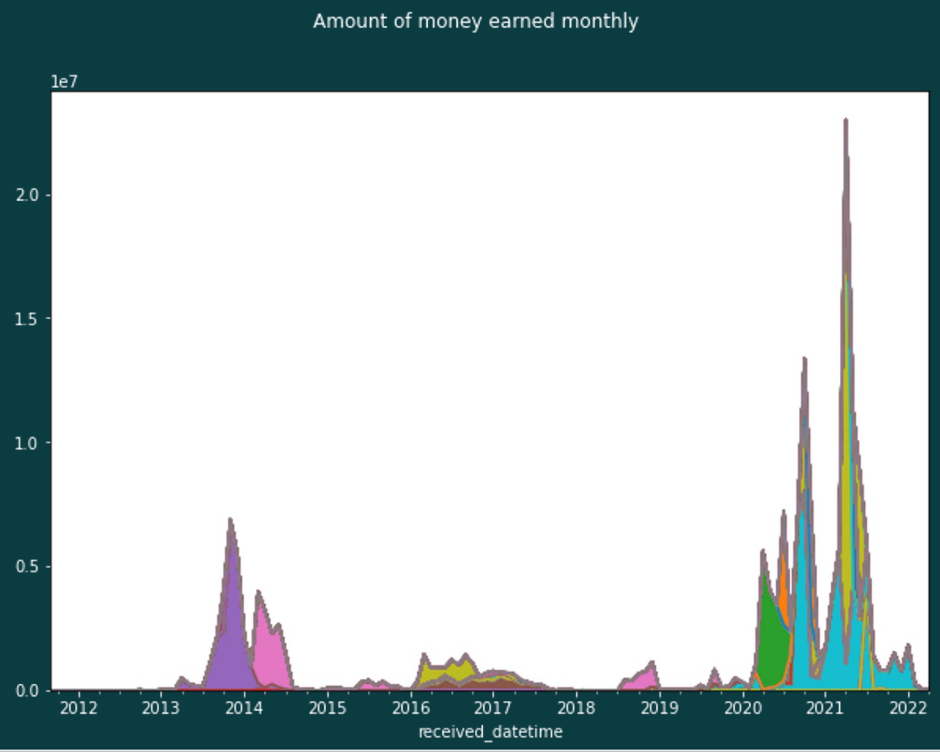
	Jul-21		Aug-21		Sep-21		Oct-21		Nov-21		Dec-21
1	United States	26.5%	United States	20.2%	United States	19.5%	United States	23.4%	United States	21.1%	United States	22.2%
2	China	10.7%	France	7.2%	Hong Kong	9.9%	France	7.5%	France	6.3%	France	7.3%
3	India	6.1%	India	6.5%	Germany	7.9%	Italy	5.0%	Belgium	4.4%	Hong Kong	7.0%
4	Germany	4.8%	Hong Kong	5.8%	France	4.6%	Belgium	4.5%	Italy	4.4%	Italy	5.7%
5	Brazil	4.8%	Germany	4.6%	Turkey	4.2%	Brazil	3.8%	Hong Kong	4.3%	India	5.3%

Detection by business size

Dec-21	Top 1 - United States		Top 2 - France		Top 3 - Hong Kong		Top 4 - Italy		Top 5 - India	
1	MAZE	220	WCRY	168	WCRY	41	WCRY	20	WCRY	1,274
2	LOCKY	145	LOCKBIT	30	LOCKY	2	GANDCRAB	15	GANDCRAB	96
3	CRYPTOR	125	HIDDENTEAR	15	RYUK	1	MOUNTLOCKER	12	MOUNTLOCKER	66
4	MOUNTLOCKER	106	Gorf	12	Crypmodadv	1	SODINOKIBI	8	EGREGOR	42
5	MORRISCRYPT	71	THANOS	7	Crypmod	1	EGREGOR	7	SODINOKIBI	33
					Enterprise					
1	MAZE	176	WCRY	168	WCRY	41	WCRY	19	WCRY	1,131
2	LOCKY	63	LOCKBIT	7	LOCKY	2	HIVE	2	GANDCRAB	94
3	GANDCRAB	61	HIDDENTEAR	4	Crypmodadv	1	LOCKY	2	MOUNTLOCKER	66
4	WCRY	46	WANA	3	ERIS	1	CRYPCTB	2	EGREGOR	42
5	Filecoder	43	Gorf	3	WANA	1	CONTI	1	SODINOKIBI	33
					SMB					
1	CRYPTOR	125	LOCKBIT	21	Genasom	1	GANDCRAB	15	WCRY	120
2	MORRISCRYPT	71	Gorf	6			MOUNTLOCKER	12	StopCrypt	3
3	MOUNTLOCKER	70	CRYPTESLA	1			SODINOKIBI	8	BABUK	3
4	LOCKY	55	CRYTOX	1			EGREGOR	7	PolyRansom	2
5	MAZE	44	CRYSIS	1			CONTI	5	LOCKBIT	2
					Consumers					
1	CERBER	32	THANOS	6	RYUK	1	CERBER	6	WCRY	23
2	LOCKY	27	HIDDENTEAR	5	Crypmod	1	StopCrypt	4	StopCrypt	12
3	Crypmodadv	5	Gorf	3	COBRA	1	Gorf	2	VIRLOCK	6
4	GANDCRAB	5	StopCrypt	3			LOCKY	2	CERBER	5
5	WCRY	4	CERBER	2			SHADE	1	PETYA	4

Frequency versus severity?





Leaks sites

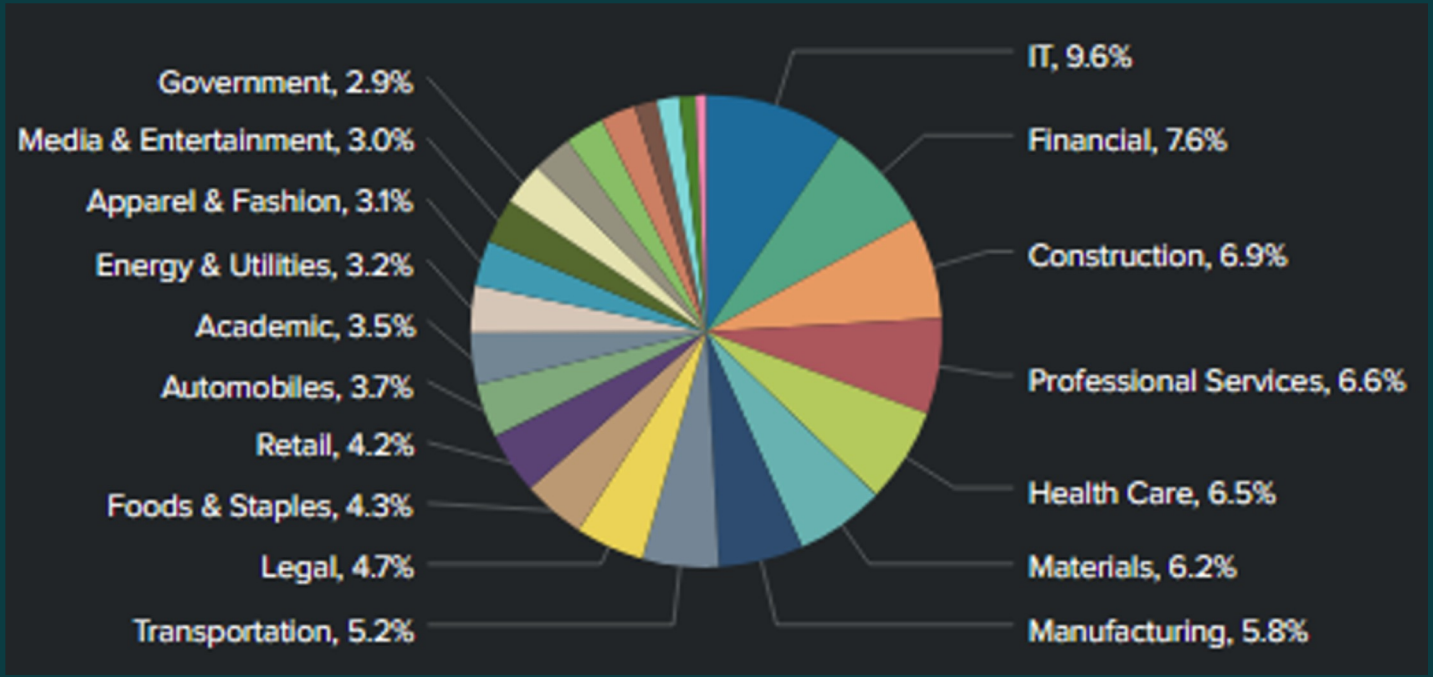
Top 10 Ransom & Extorsion Groups

	Ransom	count
1	Conti	805
2	LockBit	666
3	MAZE	330
4	Sodinokibi	309
5	Pysa	307
6	DoppelPaymer	206
7	Egregor	197
8	Avaddon	184
9	NetWalker	178
10	CLOP	119

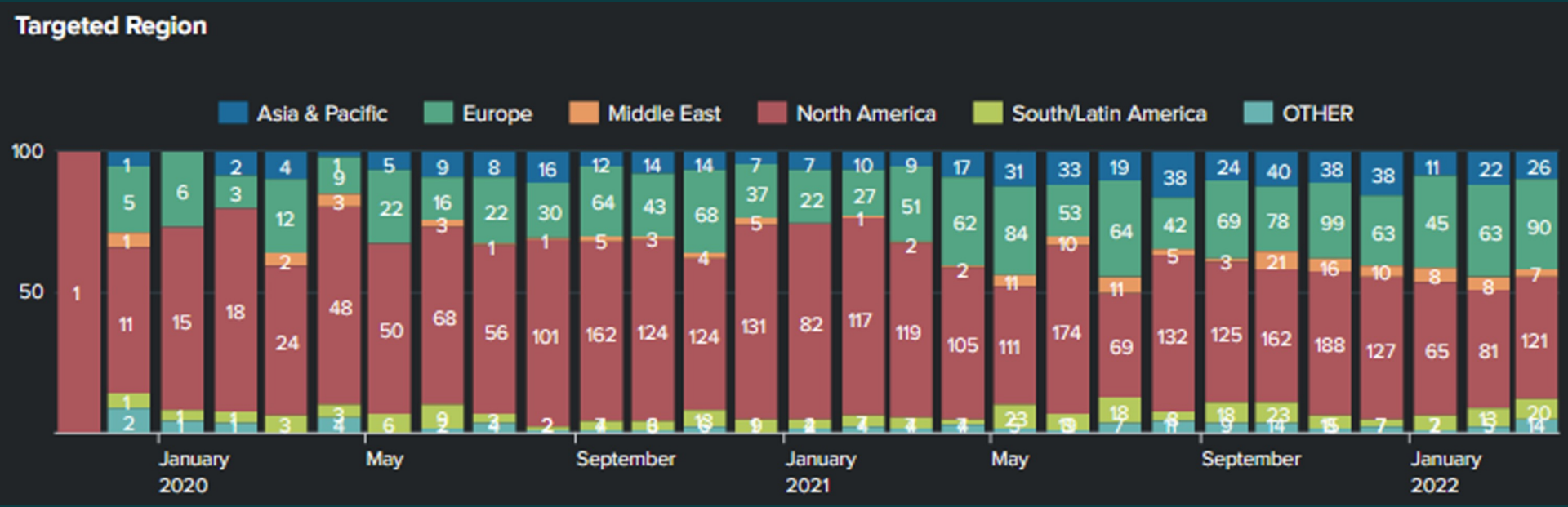
Top 10 Countries

	Country	count
1	United States	2477
2	United Kingdom	263
3	France	251
4	Canada	234
5	Germany	201
6	Italy	189
7	Australia	96
8	Spain	93
9	India	88
10	Brazil	86

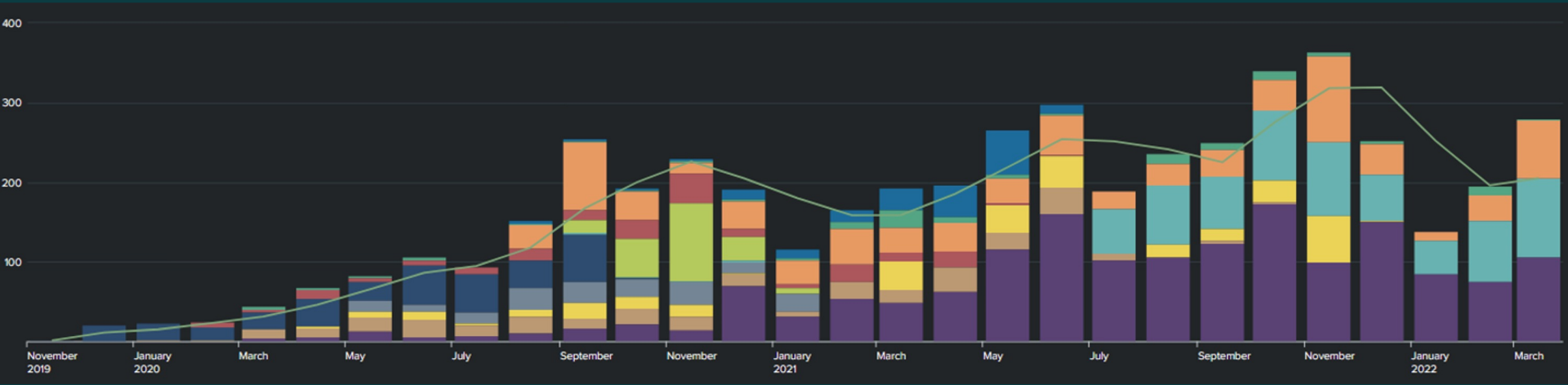
Leaks: Targeted sector



Leaks: Targeted region over time

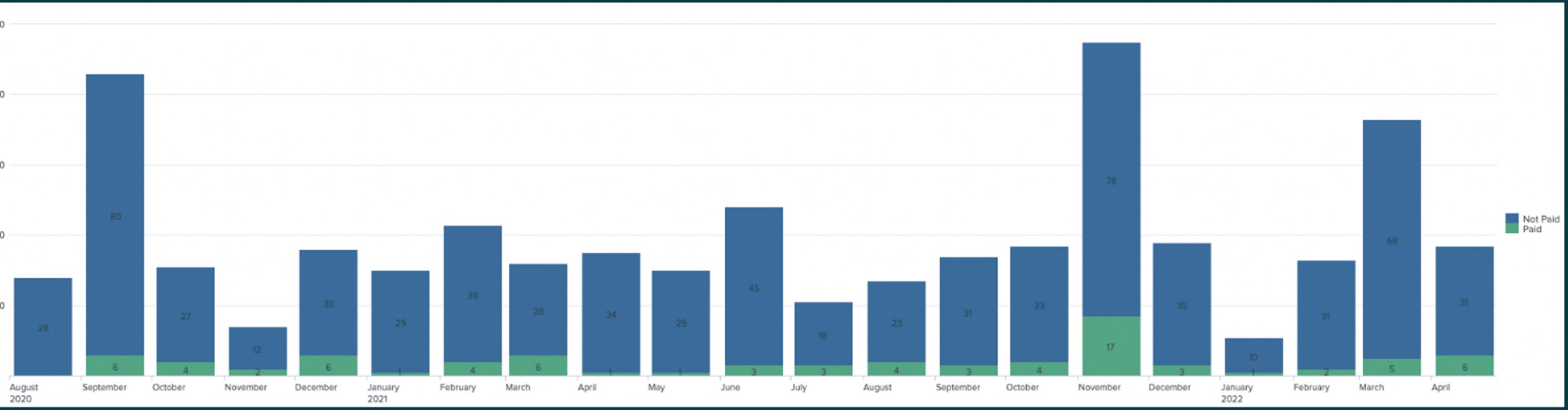


Leaks: Groups activity over time

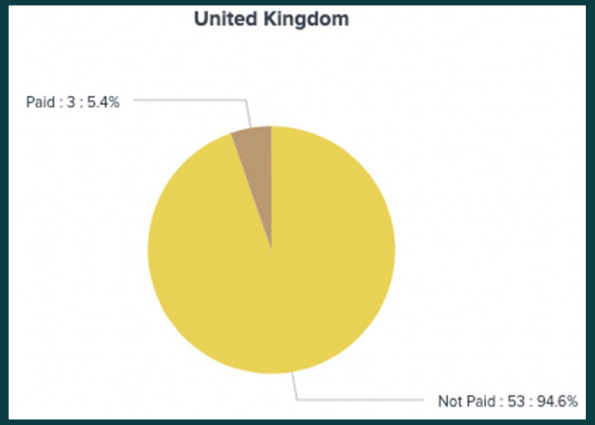


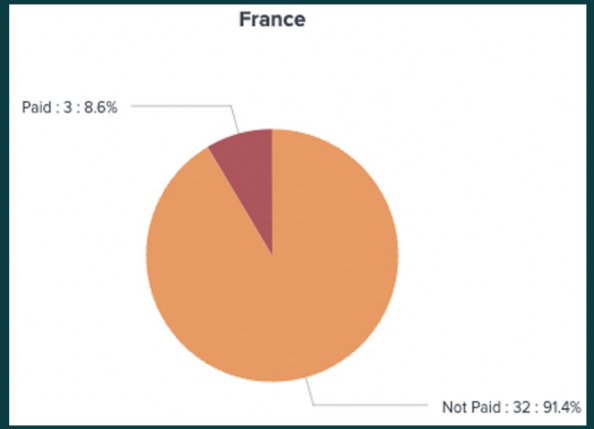
Number of leaks over time Conti

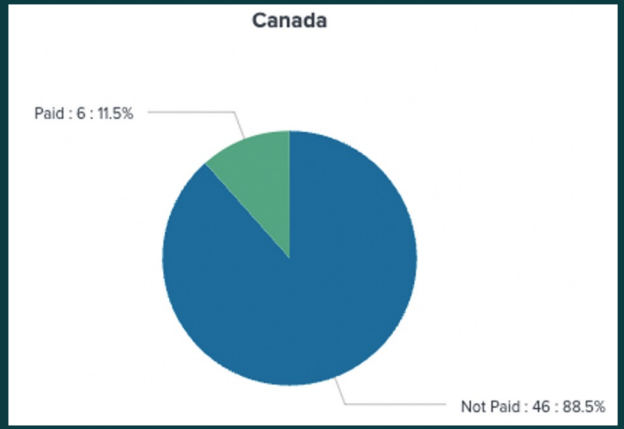
Time (monthly since august 2020 till April 2022) Paid/Not Paid

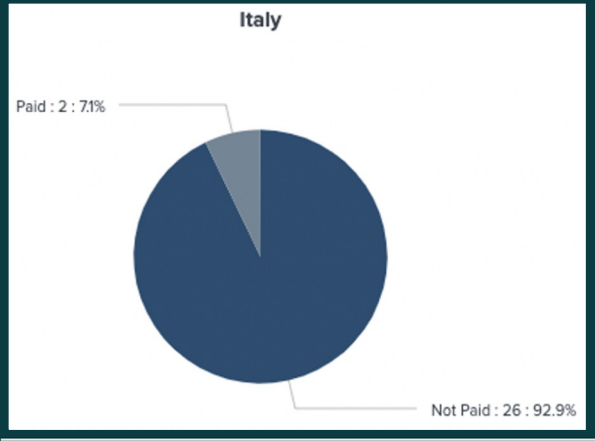


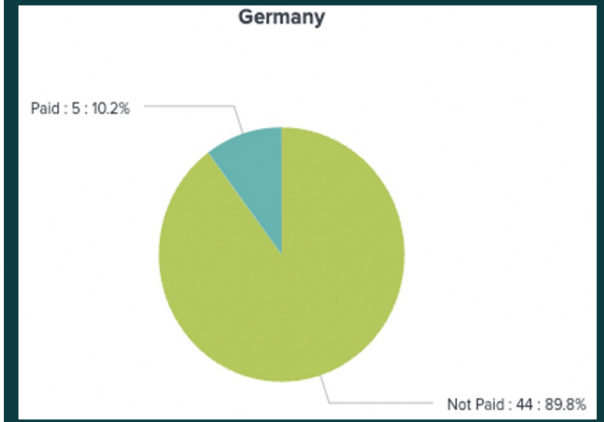
Where paid?

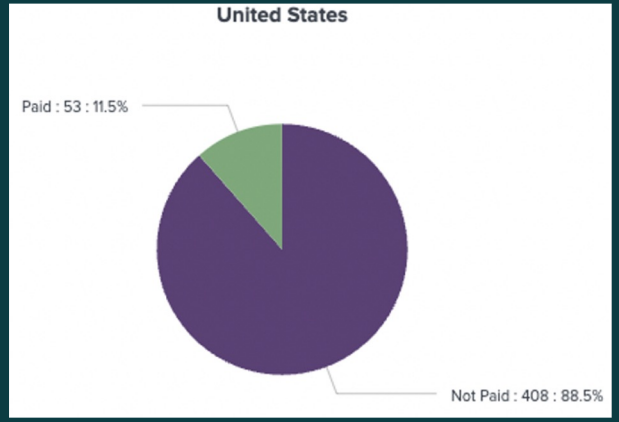

United Kingdom
Paid : 3 : 5.4%
Not Paid : 53 : 94.6%


France
Paid : 3 : 8.6%
Not Paid : 32 : 91.4%


Canada
Paid : 6 : 11.5%
Not Paid : 46 : 88.5%


Italy
Paid : 2 : 7.1%
Not Paid : 26 : 92.9%

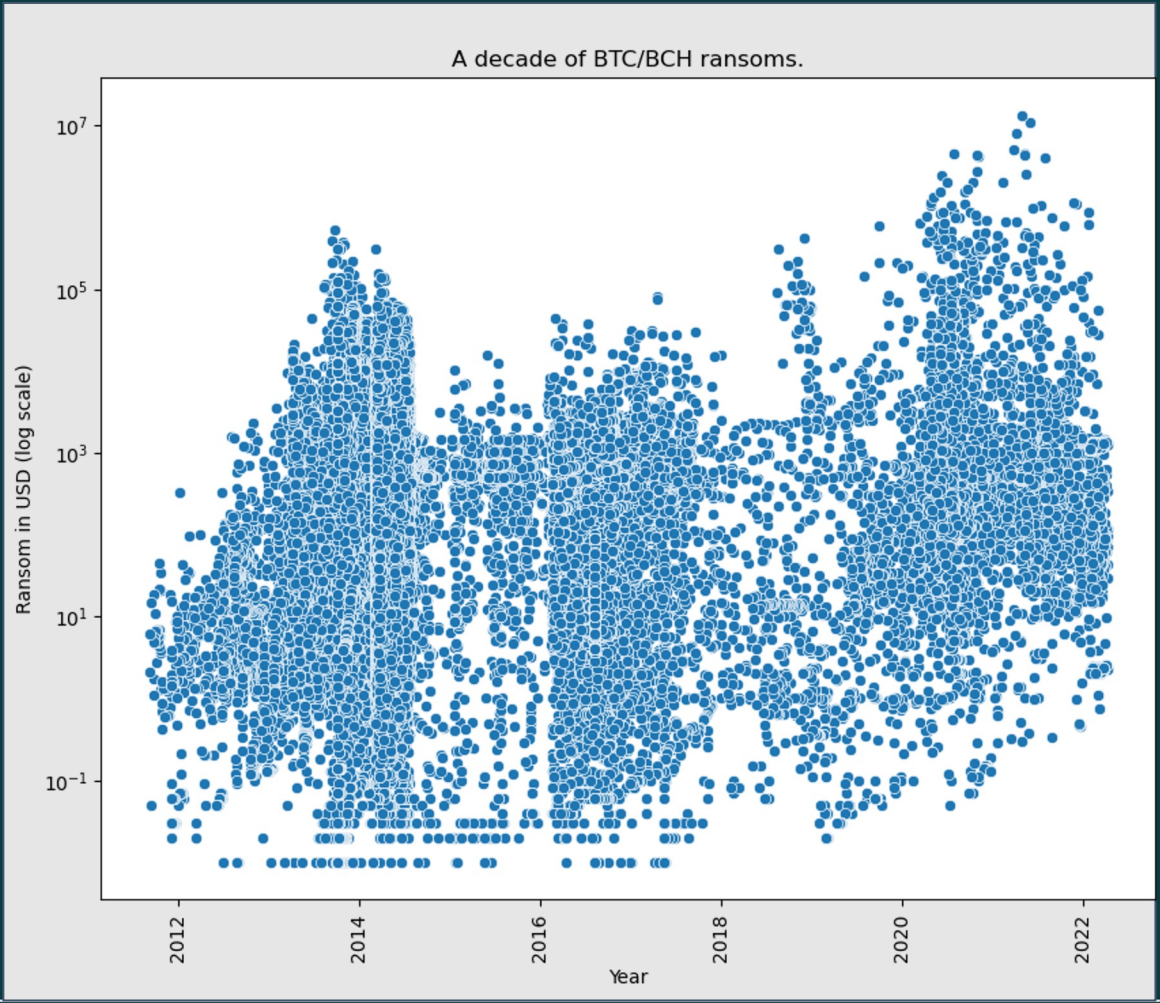

Germany
Paid : 5 : 10.2%
Not Paid : 44 : 89.8%

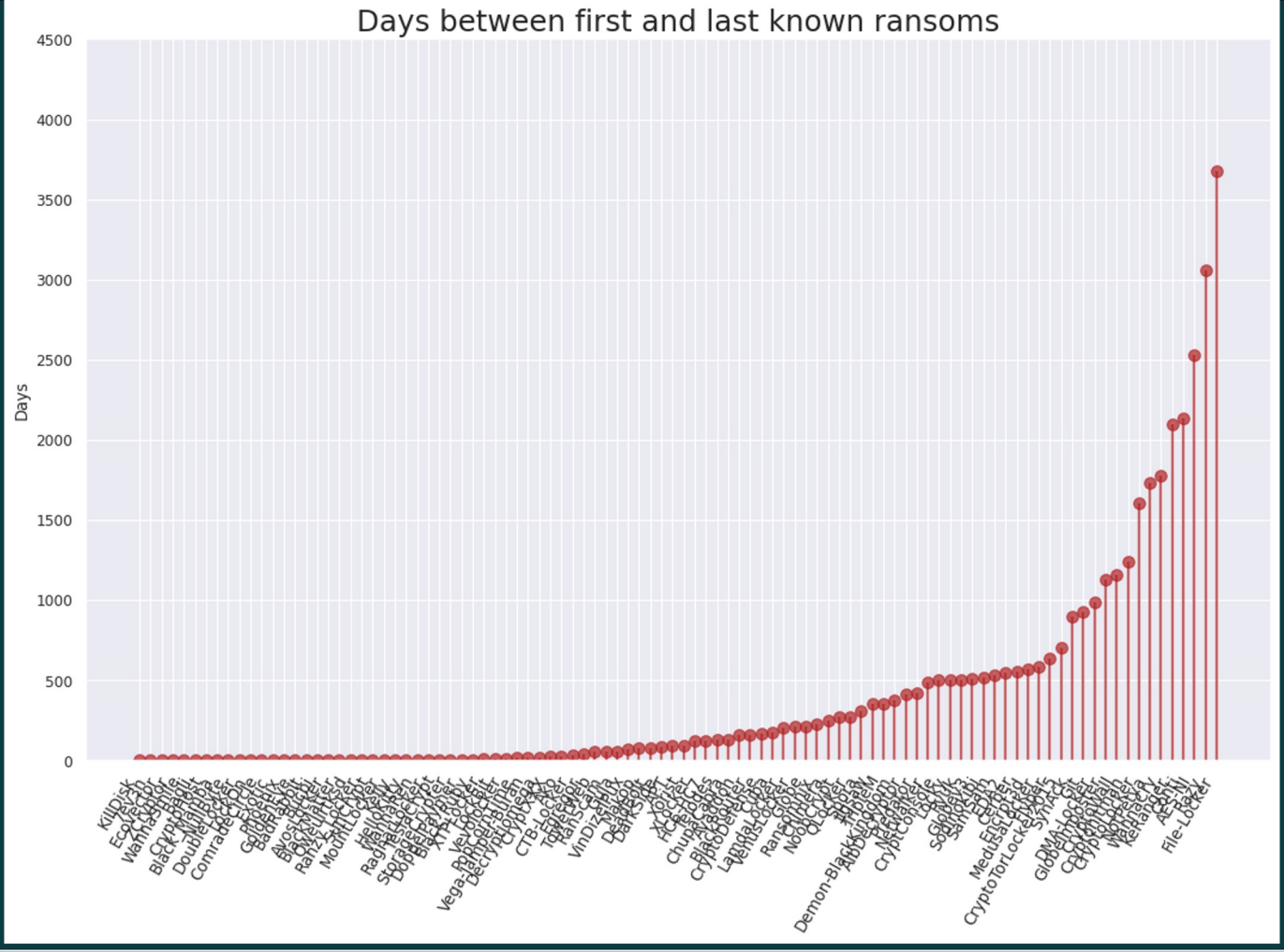

United States
Paid : 53 : 11.5%
Not Paid : 408 : 88.5%

Ransoms/time

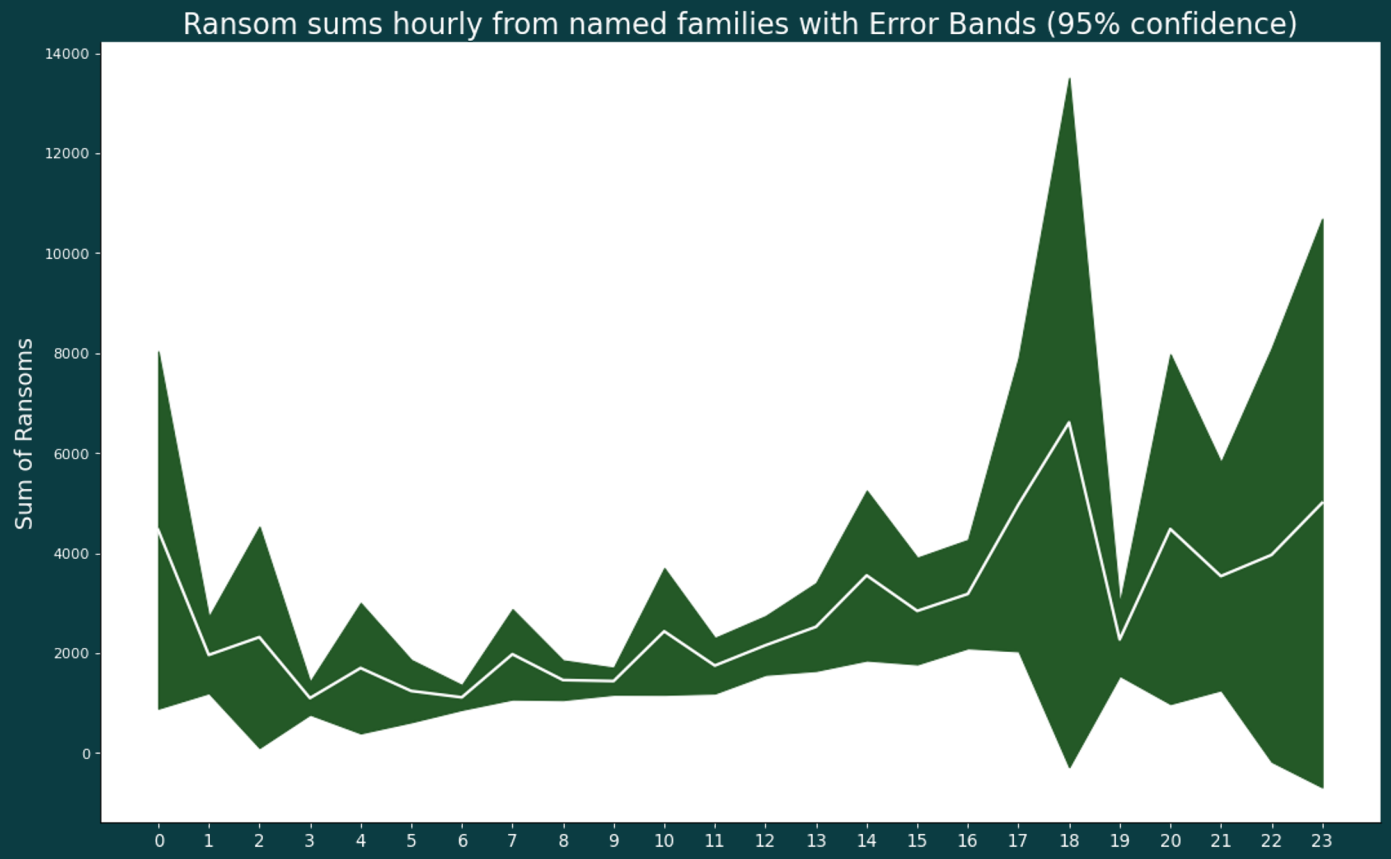
A decade of ransoms isn't an emergency.

This is a long game now, and we need better strategy.

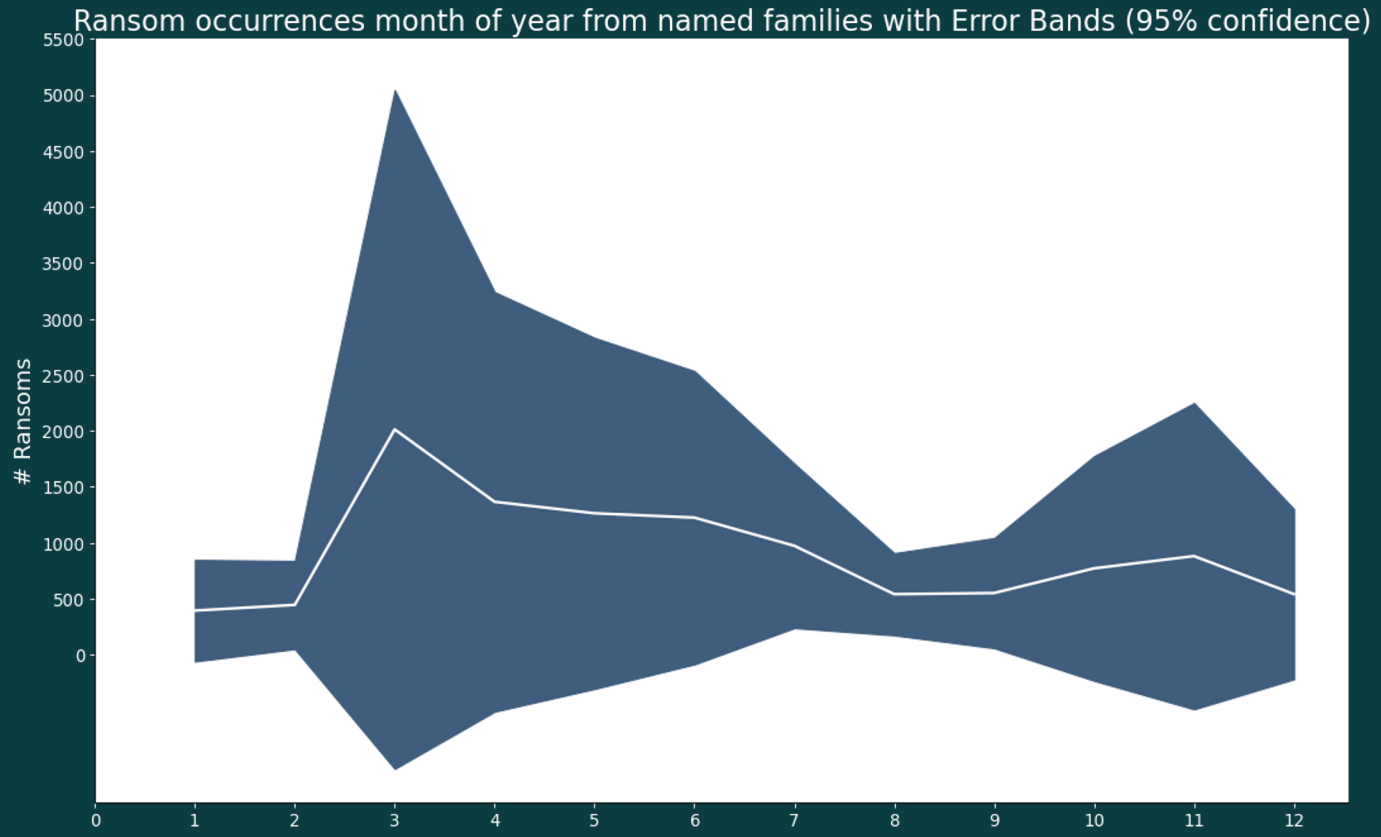



Days between first and last known ransoms
Days
4500
4000
3500
3000
2500
2000
1500
1000
500
0
KillDisk
EvilEye
EcoRansom
WannaCrypt
CryptBrout
BlackMatter
DoubleLocker
ComradeCircle
Gandcrab
Babuk
Avoslocker
BlackCat
Ransomexx
MountLocker
Hellokitty
Hellcat
RadiumLocker
StormRansomware
DoppelPaymer
BlackRuby
XTRLocker
Vevocker
RansomBlitzen
Vega-Locker
DecryptorBitman
CryptoPlus
CTB-Locker
TeleWeb
TransCrypt
VinDizel
DarkSide
Lilith
DarkRaven
XCorpLtd
Ice-Cherry
ChupaCabra
BlackLabel
CryptoBeetle
LamaLocker
LockBit
Ransomware
NoobCrypter
QLocker
Thanos
Thebem
Demon-Black
AbbeyLocker
Netwalker
CryptoConsole
LockNL
GlobeImposter
SamSam
Cerber
MedusaLocker
EncryptedRansomware
CryptoTorLocker2015
SynAck
DMALocker
GlobeImposter
CryptoHitman
CryptoWall
WannaCry
Kerkanef
AES-NI
File-Locker

Ransoms summed by time of day in UTC



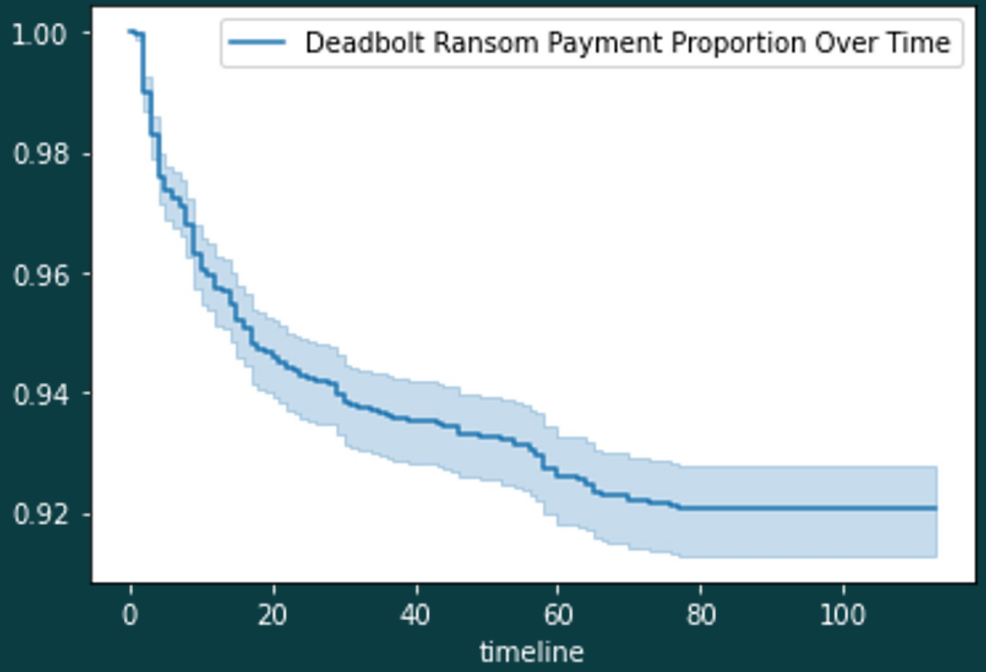
Ransom frequency by month



Most people pay very quickly

Delaying payment might be a good nudge towards not paying.

As you can see here, 50% of those who pay do so in about a week.



Understanding the data

What are the risks to the RAAS users?

Access to the “victim” infrastructure

Risks of “victims” not paying the ransom

Ransomware infrastructure

Ransomware group: services and people

Cost of Access 40k, lower bound of ransom >40K

Forum › Marketplace › ACCESSES: shells, FTP, root, DB, sql-inj, dediks ›

Access electronics manufacturing conglomerate (Admin rights in 2 domains) branch

Bassterlord · 10/14/2020 · citrix rce vpn accesses

Track

Bassterlord
(L3) cache
User

check in:	05/13/2019
Posts:	156
Reactions:	170
Deposit:	0.16 $

10/14/2020 #1

Access conglomerate electronics manufacturing (Admin rights in 2 domains)
Access country IN branch
Access to 2 of the three domains in the private network.
VPN Access
Approximate income of the main company for 2019
75 843 774 059 USD
Monthly branch income of at least $ 500 million
Company is a shareholder and manufacturer of home electronics and electrical equipment.
Every 5 people on earth had a technique for their production, or at least every 5 people know this company.
Price tag $ 40,000 BTC
I agree to a guarantor at your expense or at the expense of the transaction amount.
Also, after the transaction, I will provide all the evidence + gigabytes of employee data inside the company of the entry point and all the information that is.

Company name not disclosed

Any questions about company name will be ignored!
Contact:
Jabber: basterlord@thesecure.biz

Last edited: 10/14/2020

* Sounds of a maximum security colony *
Hohlocartel and lard tracks

A complaint Like + Quote Answer

frapster2k, DarkGod3 and What So Not

2 weeks later attempt to extort for 500k (upper bound)

India corporate data

... a normal price for a corporation of this level. A buyback notice has been sent to the corporate addresses of the company's employees. Additional contacts: Jabber: **basterlord** @ thesecure.biz Mail: Basster@protonmail.com The link to the archive The password will be in 7 days in the same post if the payment is not received

Bassterlord · Theme · 10/29/2020 · data | leaked database | panasonic | ransom · Replies: 1 · Section: SPAM: mailings, responses, databases, mail-dumps

The archive also contains backups of corporate emails of employees!

The company must redeem the data within 7 days, otherwise the password from the data archive will become public.

Price list $ 500,000

This is a normal price for a corporation of this level. A

notice of redemption was sent to the corporate addresses of the company's employees.

Additional contacts:
Jabber: basterlord@thesecure.biz
Mail: Basster@protonmail.com

Link to archive

Password will be in 7 days in the same post if payment is not received

Data Fusion

Threat Actor Metrics

Persistence of attack attempts (single, low hanging fruits, advanced)

Dependence Ransom on the victim size, revenue, industry

Does Ransom is negotiable?

Targeted/opportunistic

Victim selection criteria (geo region, company scale, industries, geo/industry exclusion list i.e. not target medical and education

Operational cadence (frequency of access) -victims per week/size?

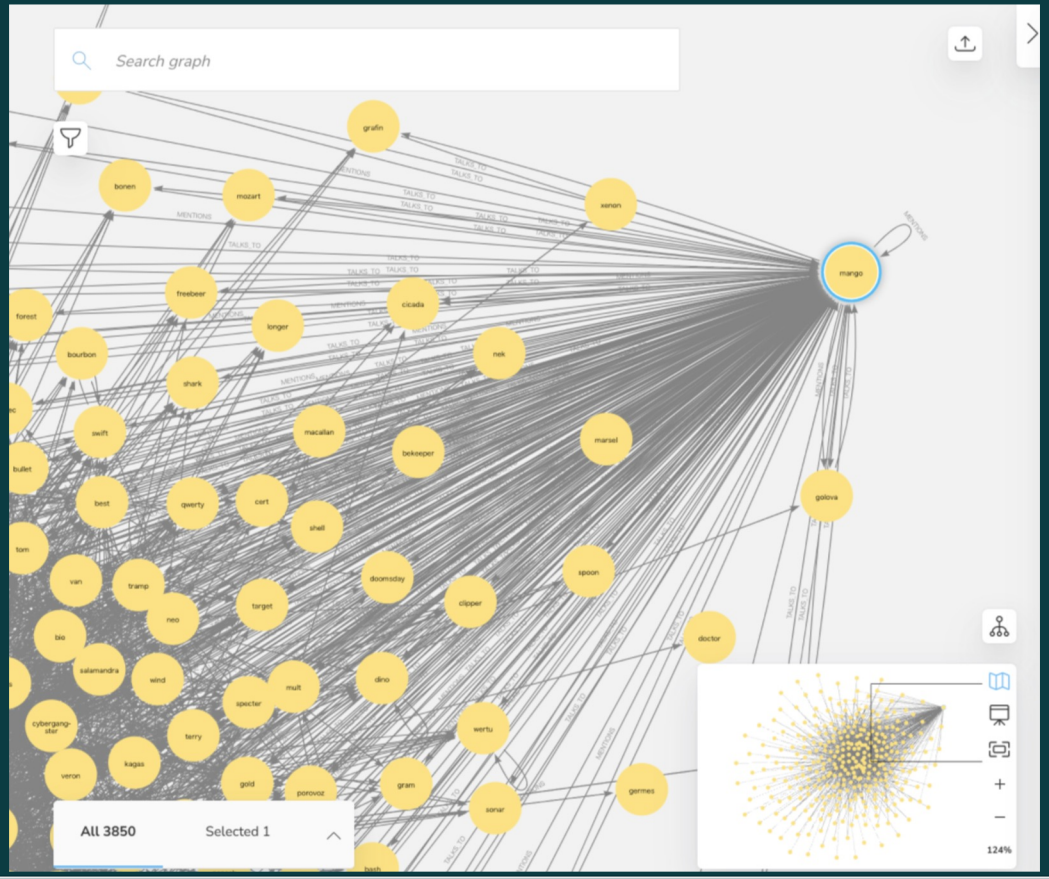
Method of initial access

Money….

33. An online public blockchain explorer identified at least 23 other addresses collected together with address XXXXXXXXXXXXXuRTnHQA8tNuG7S2pKedNxB in one wallet. [redacted] on May 27, 2021, funds from the collection of addresses, totaling 69.60422177 BTC, including 63.70000000 BTC accessible from address XXXXXXXXXXXXXuRTnHQA8tNuG7S2pKedNxB was transferred to address XXXXXXXXXXXXX950klpjcawuy4uj39ym43hs6cfsegq (the "Subject Address"), and it has not moved since.

34. The private key for the Subject Address is in the possession of the FBI in the Northern District of California.

People…


Search graph
grafin
bonen
mozart
xenon
mango
freebeer
cicada
longer
forest
bourbon
nek
shark
swift
macallan
bekeeper
marsel
bullet
best
qwerty
cart
shell
golova
tom
van
tramp
doomsday
spoon
target
clipper
neo
doctor
bio
salamandra
wind
mult
dino
specter
cybergang-ster
terry
wertu
veron
kagas
gold
porovoz
gram
germes
sonar
All 3850
Selected 1
124%

Ransoms correlate strongly to malware family

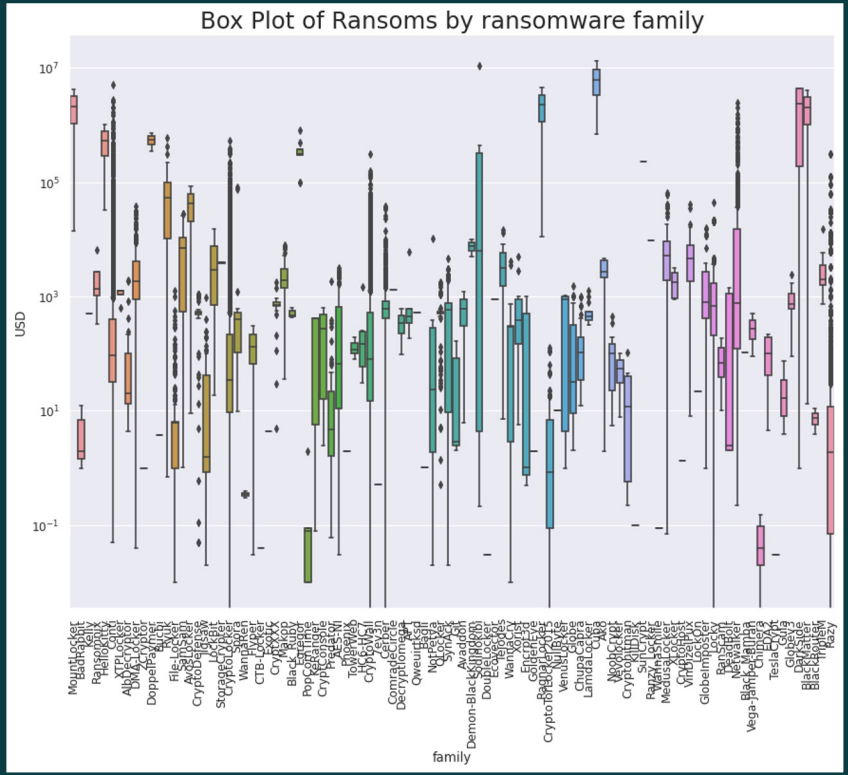
Spearmans correlation coefficient for family:

0.951

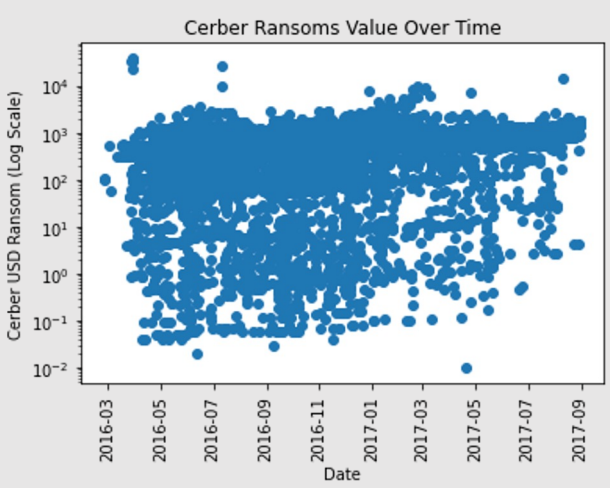
Samples are correlated (reject null hypothesis if $p < 0.05$):

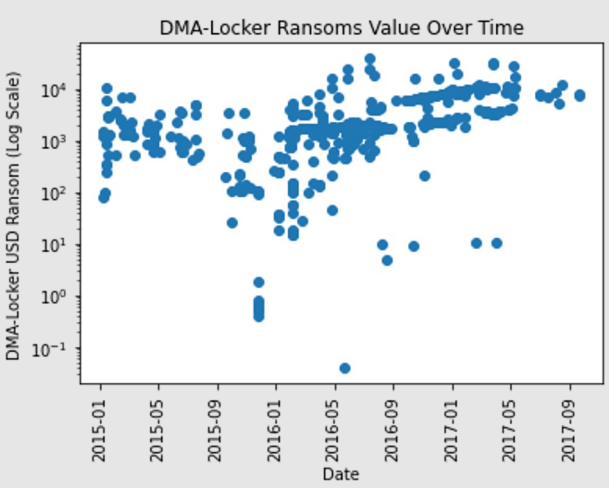
p=0.000

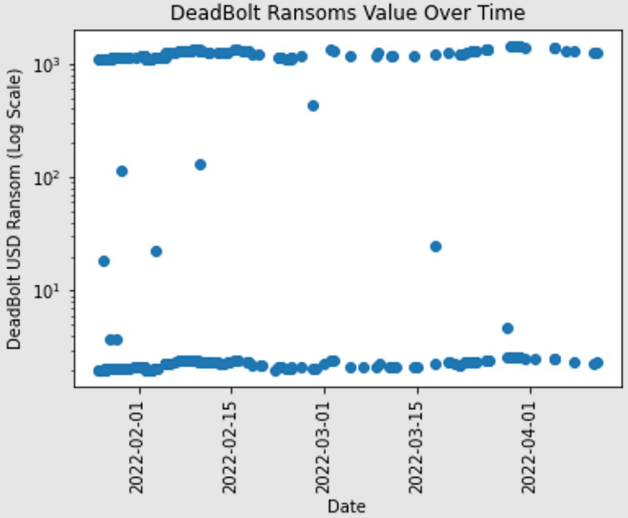
N=116761

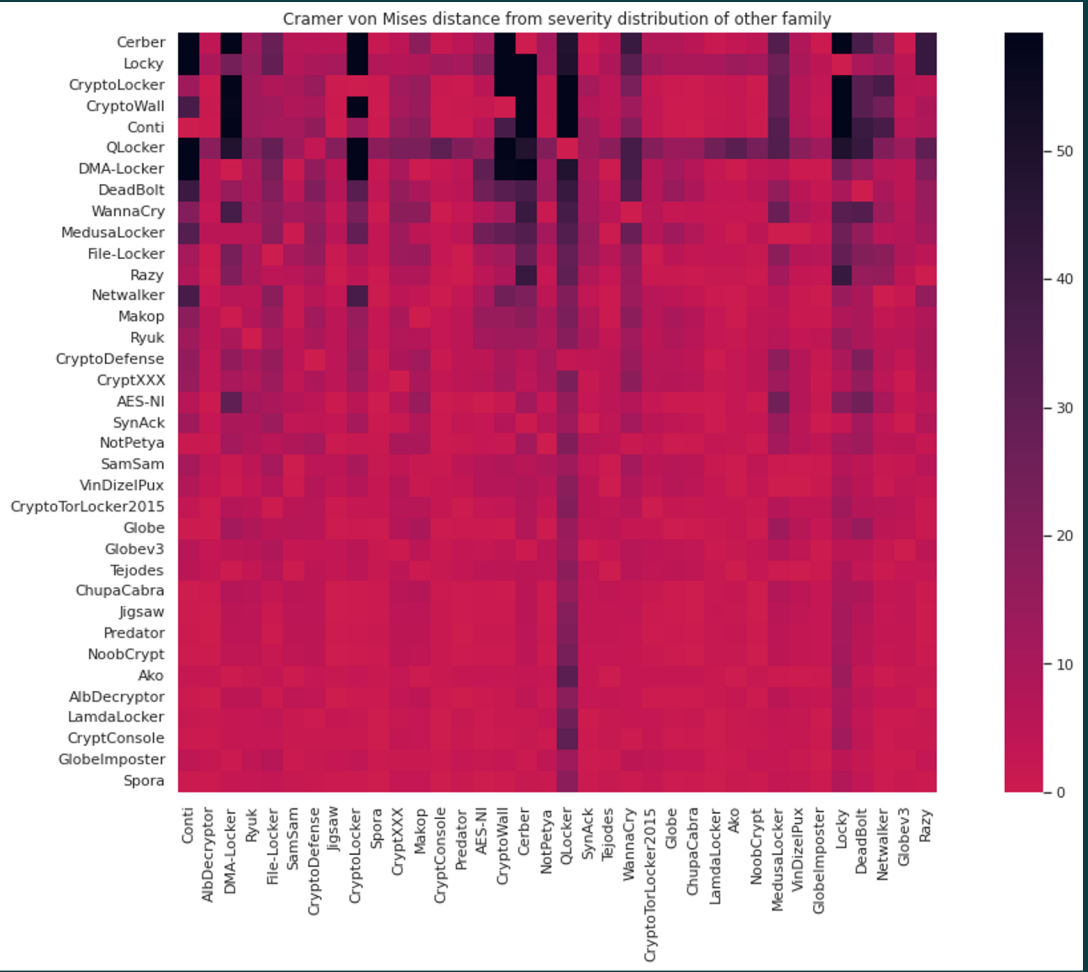


Severity characterizations

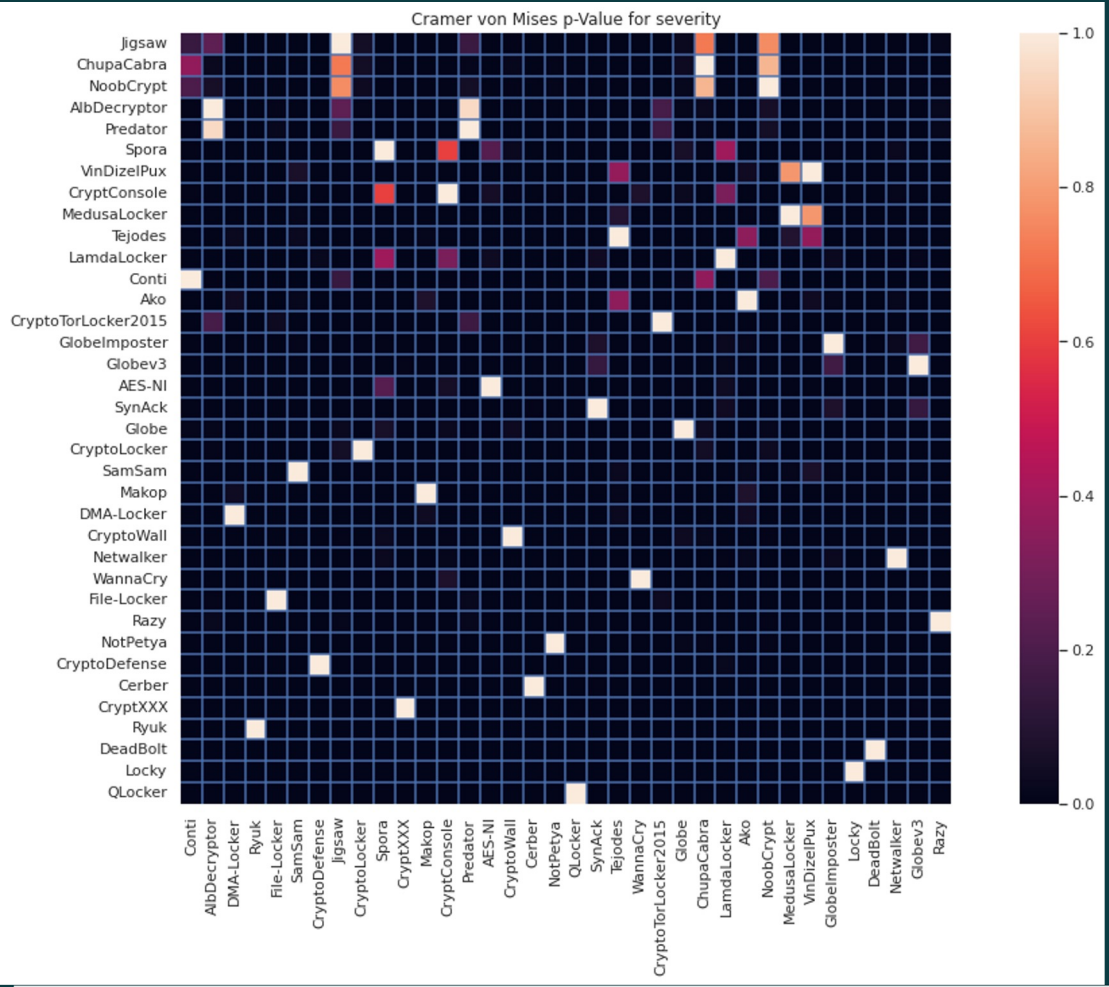








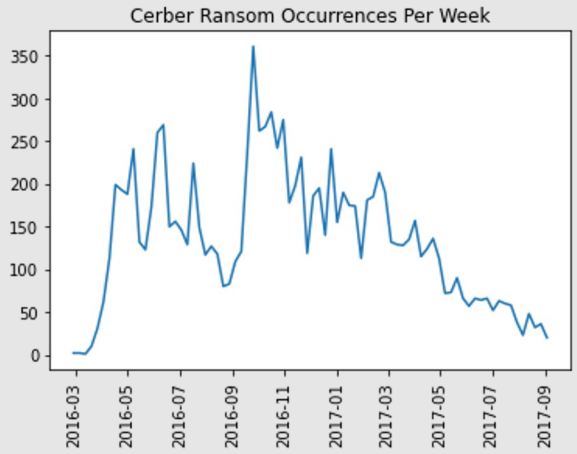
We can measure that statistical distance using the Cramer von Mises metric. Red shows they are similar and black shows they are very different. A better way to view that though is with the associated p-value of the distance metric.

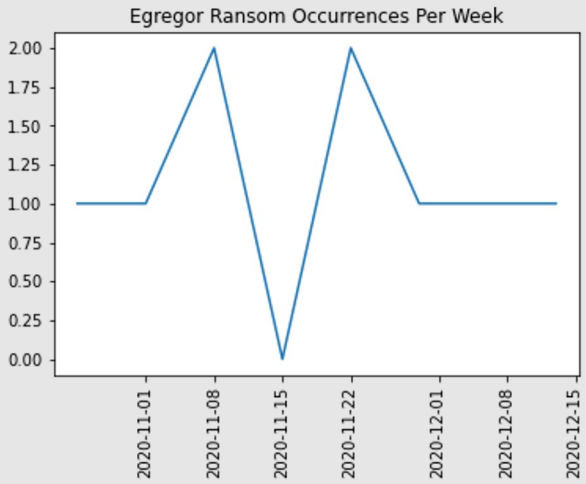


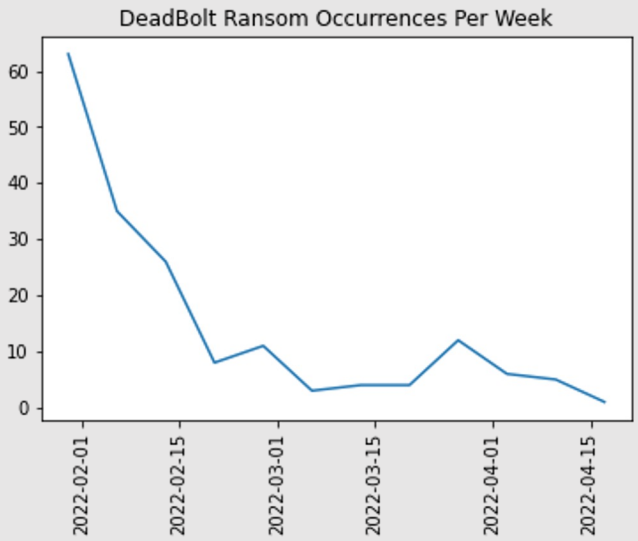
Black here means we are almost certain the ransoms are drawn from different distributions, and white means it is highly likely they are drawn from the same distribution.

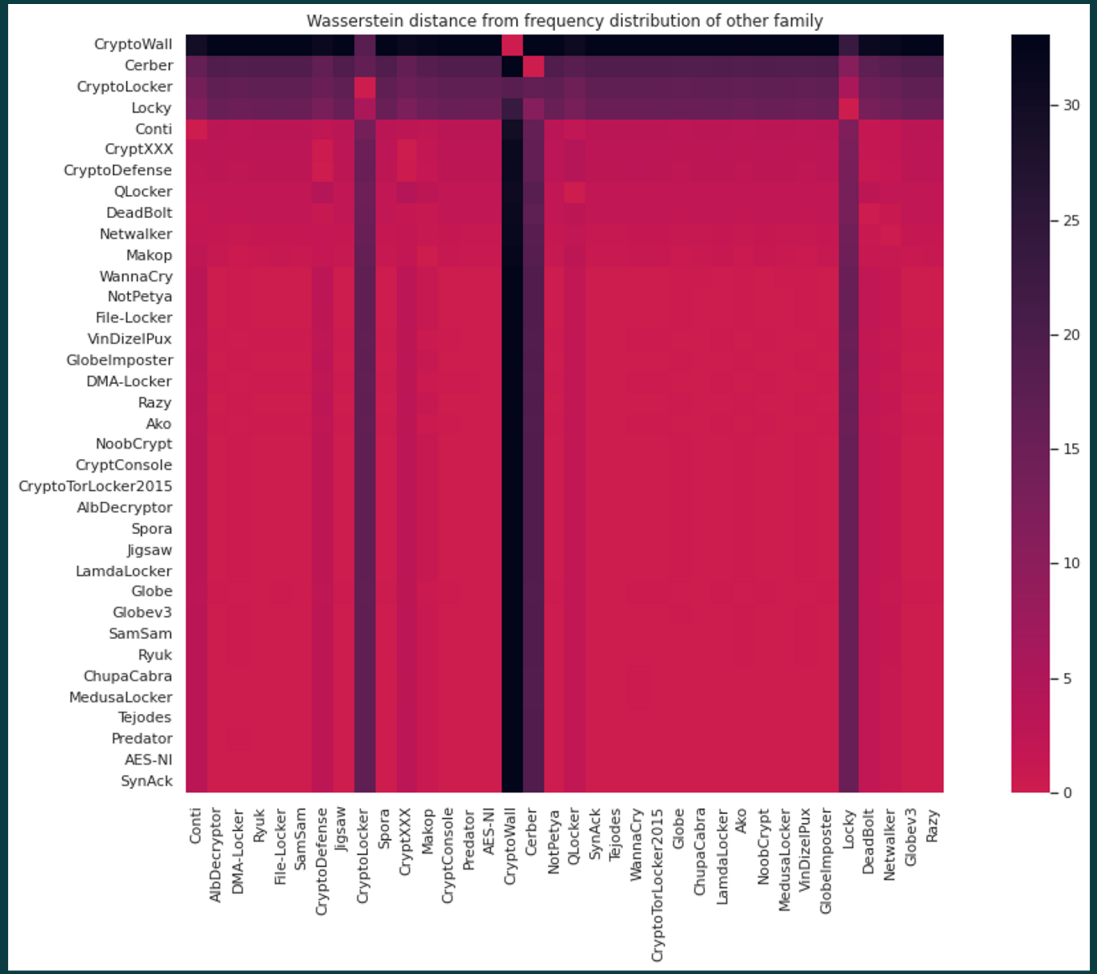
This could be a predator effect, or it could be a prey effect. In other words, because the victims are all similar (all use a certain technology or are a similar size), or it could be because the gangs negotiation tactics are similar.

Frequency Characterizations



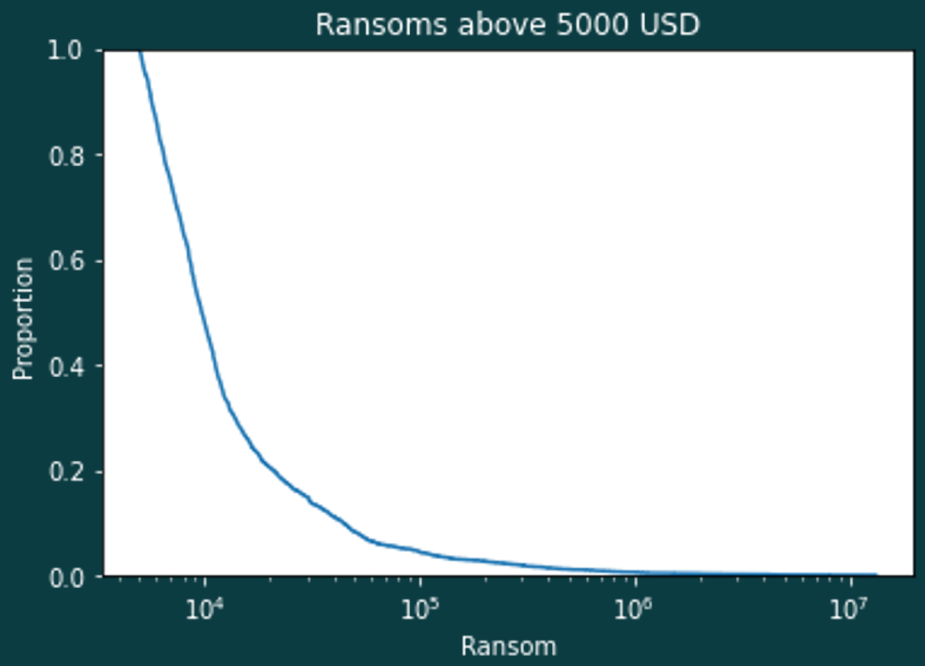





Wasserstein distance from frequency distribution of other family
CryptoWall
Cerber
CryptoLocker
Locky
Conti
CryptXXX
CryptoDefense
QLocker
DeadBolt
Netwalker
Makop
WannaCry
NotPetya
File-Locker
VinDizelPux
GlobeImposter
DMA-Locker
Razy
Ako
NoobCrypt
CryptConsole
CryptoTorLocker2015
AlbDecryptor
Spora
Jigsaw
LamdaLocker
Globe
Globev3
SamSam
Ryuk
ChupaCabra
MedusaLocker
Tejodes
Predator
AES-NI
SynAck
Conti
AlbDecryptor
DMA-Locker
Ryuk
File-Locker
SamSam
CryptoDefense
Jigsaw
CryptoLocker
Spora
CryptXXX
Makop
CryptConsole
Predator
AES-NI
CryptoWall
Cerber
NotPetya
QLocker
SynAck
Tejodes
WannaCry
CryptoTorLocker2015
Globe
ChupaCabra
LamdaLocker
Ako
NoobCrypt
MedusaLocker
VinDizelPux
GlobeImposter
Locky
DeadBolt
Netwalker
Globev3
Razy
30
25
20
15
10
5
0

Rapid cost estimation:

The impact of an event will typically cost between 10-50% of the Annual Returning Revenue of the company involved. Assuming no network segregation, no endpoint protection, and lateral movement on behalf of the attacker.



A theory of change beyond “make backups”

Most people aren’t paying. Given we know this, should we optimise DFIR for those who DON’T?

How do we increase the friction of people to pay?

- Sanctions
- KYC/AML
- Delays (less likely to pay as time goes on)?

How do we reduce the losses of those who choose not to pay?

- Transition from “backup” to RESTORATION

A theory of change beyond “make backups” II

Traceability of transactions

Infrastructure policing

Micro-perimeterization

Business process policy

Negotiation onion denylisting

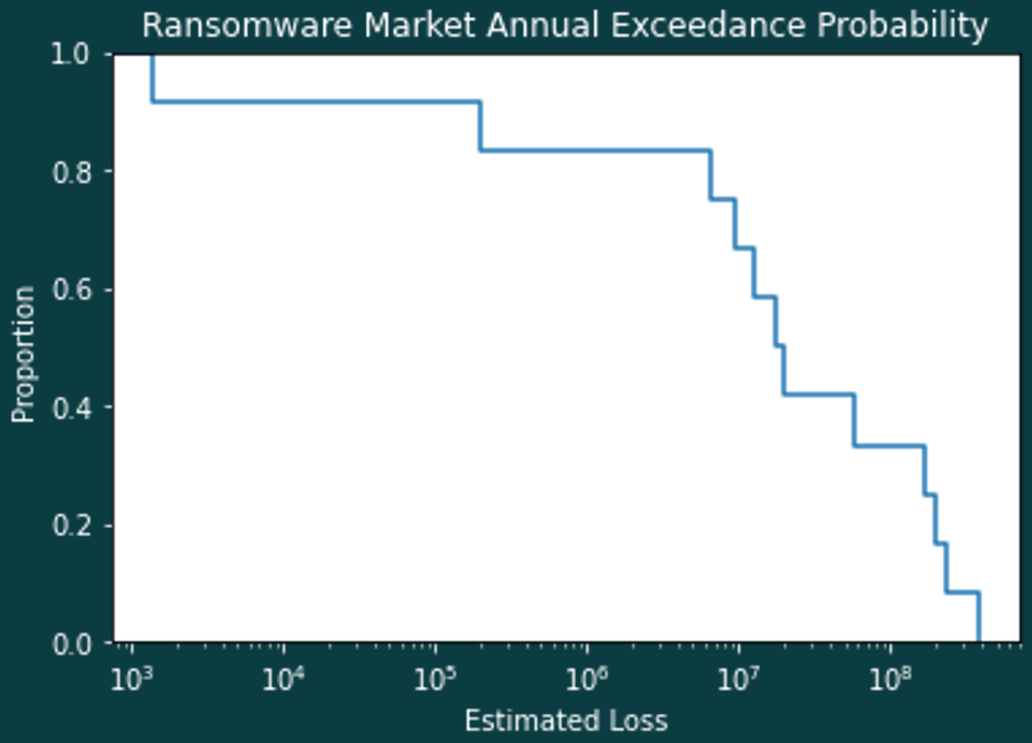
When you pay, you’re paying to victimise 10-20 others

Turn the tide:

- Calling out that most people are not paying regularly and with evidence

How much does this cost society?

- Estimated cost to society: $1,062,322,217.08
- Estimate fast where you are
- Prediction of risks and evolution of the threat landscape



Conclusion and Q&A

Scope of ransomware impacts

Broad overview of operating patterns of gangs

Time series analysis for DFIR

Evidence based policy recommendations

Join the MSR-SIG Data WG

Research team