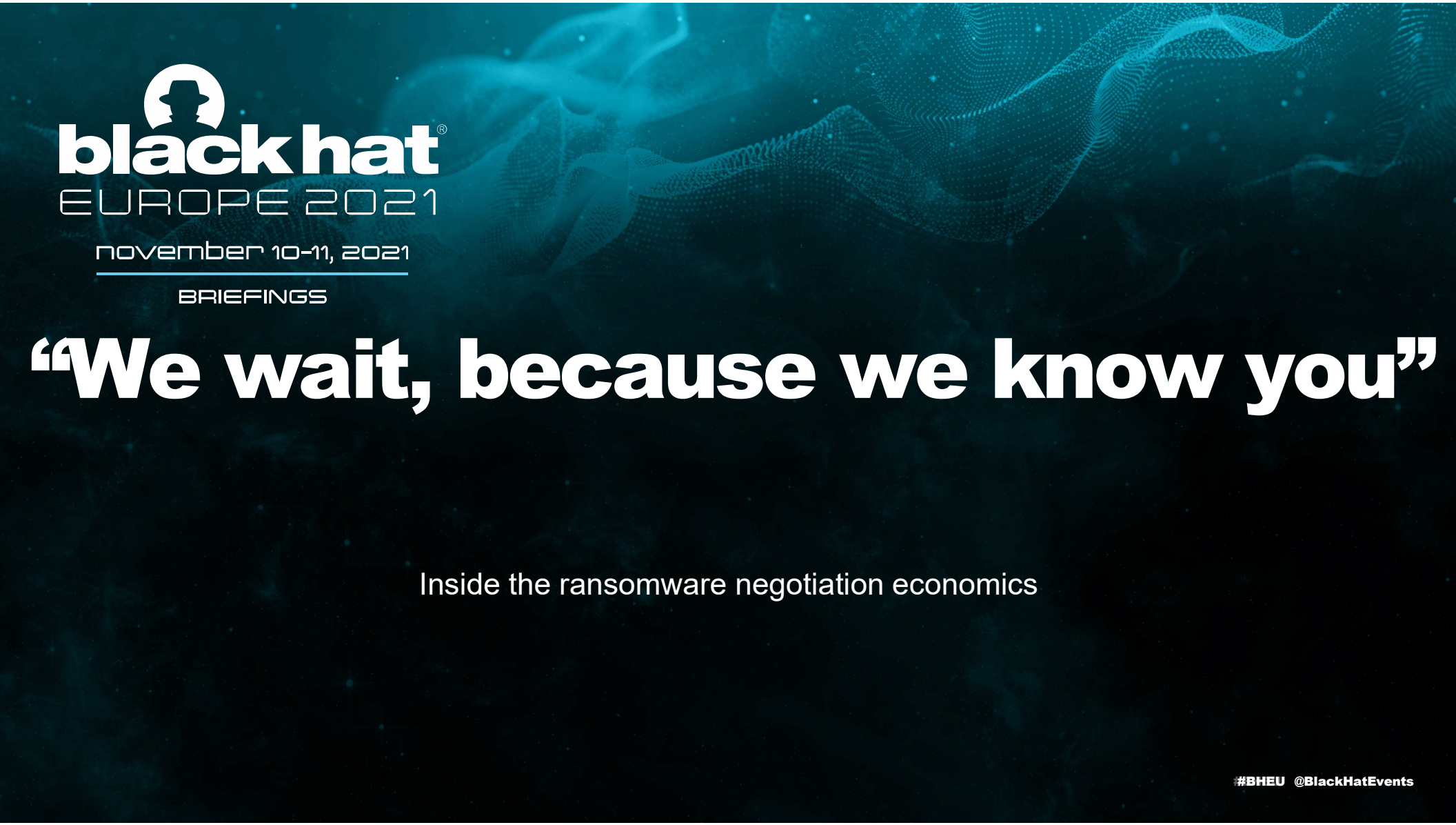

black hat
EUROPE 2021
november 10-11, 2021
BRIEFINGS
“We wait, because we know you”
Inside the ransomware negotiation economics
#BHEU @BlackHatEvents

$whoami

Pepijn Hack

- Cybersecurity Analyst at TI, DetACT and CTO office
- Background in Criminology and Crisis and Security Management

Zong-Yu Wu

- Threat Analyst at dep. Threat Intel (TI)
- Doing all kinds of technical things – malware reversing, auto-analysis development, threat hunting, campaign tracking, etc

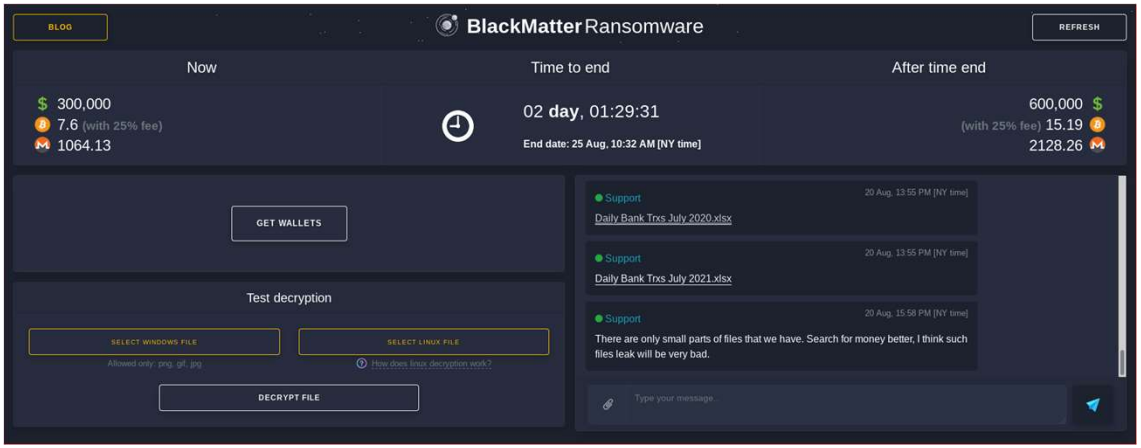
"We wait"

- How do adversaries set their price?
- How does information asymmetry influence the negotiation?
- What negotiation strategies can be used?

Two price tags

Initial price – how it is set is beyond this research.

Final price – it (maybe) indicates the profit baseline.



Economics – think like an attacker

Important factors:

- The final ransom price
- The victims' final decsion (to pay or not to pay)
- Cost and risk
- How many attacks are successfully carried out?

A simple decision question?

A ***small*** number (percentage) of victims pay but each ransom is ***larger***?

A ***large*** number (percentage) of victims pay but the ransom is ***smaller***?

Data collection

	Dataset-first	Dataset-second
Total #	681	105
Proceeded to pay	17% (N=116)	14% (N=15)
Average ransom	$400,767	$2,392,661
Date of collection	Mid-2019	Late-2020
# of estimated revenue is known	31 out of 116	4 out of 15
Remarks	One of the initiator of ransomware epidemic	Affiliates intend to target conglomerates

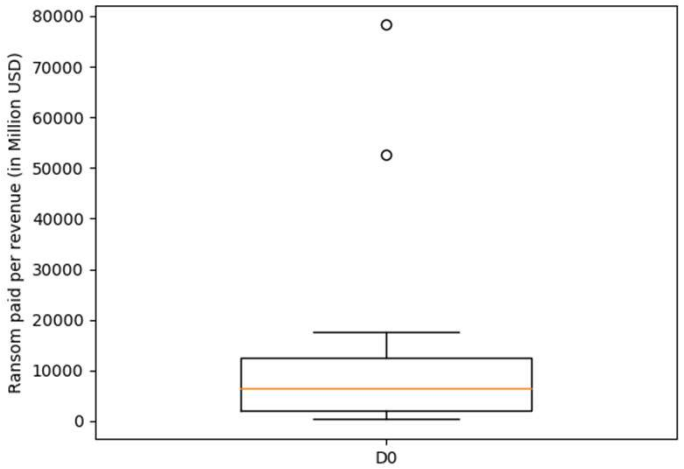
Introducing the metric. (RoR)

Ransom over Revenue (in Million) (RoR) –

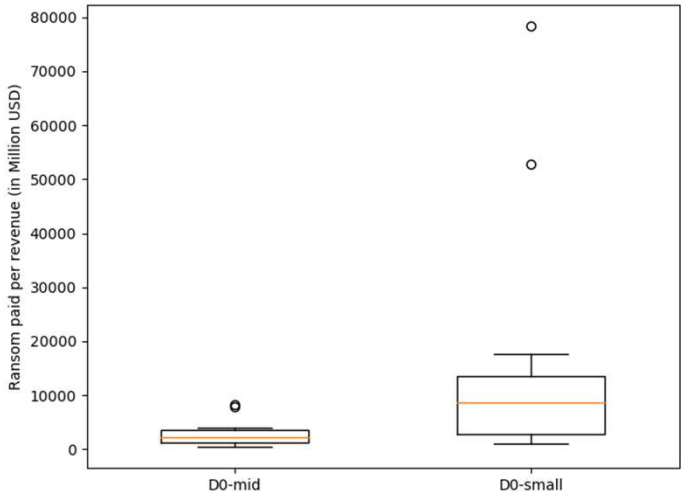
for every million a victim earned in the year; how much is paid for the decryptor.

For example, in our data:

Revenue (M) USD	Ransom Paid	RoR
$100	$36,270	363
$151	$59,177	392
$401	$405,068	1010



I know your cards.



	Dataset-first	
Total #	681	
Proceeded to pay	17% (N=116)	
# victim paid	116	
Identifiable victims	31	
Dataset name	D0-small	D0-mid
#	10	21
Annual Revenue	< $100 M	>= $100M

Data Set	Revenue	#	Quartile	Medium	Third Quartile
D-first-mid	>= 100 million $	10	1,000	2,200	3,900
D-first-small	< 100 million $	21	3,200	10,550	13,700

What we have learned...

Our result shows that adversaries have adapted an optimization strategy.

- A third-degree price discrimination strategy

Third degree price discrimination means "**charging a different price to different consumer groups**"

- One of the key factors – **revenue**

What we have learned... (cont.)

The adverdary knows how much a victim is going to pay.

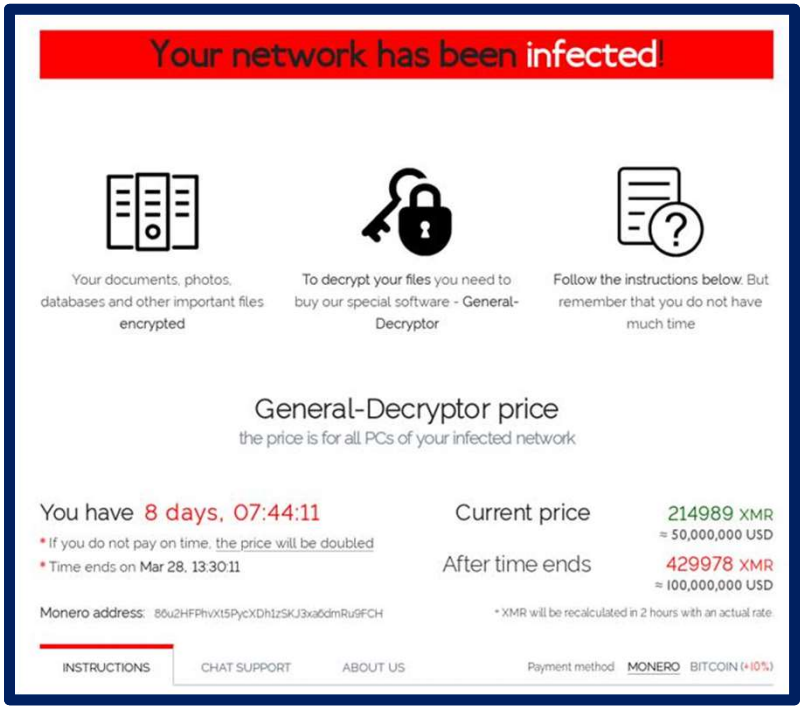
- A victim – plays the game for the first time under pressure
- The adversary – has played many times, plus he has access to the victims' private information (like financial statements.)

Negotiation strategies

Strategy 1: Be respectful

"Thanks Sir. We can pay 750,000 USD in XMR, provided that you will share with me the exact scope, volume, and significance of data that is in your possession. (...) I do stress the data, rather than the decryption key, ***since I learned about your very positive reputation in providing decryption keys. Looking forward hearing your thoughts. Respectfully****, {victim's name}."*

Strategy 2: Ask for more time



Strategy 2: Ask for more time

"*Hello, I'm going to be as up front and honest as I can be right now and let you know that we have not been able to secure the 12 million dollars (...)* ***we need some more time*** *(...). Coming up with the 12 million is almost impossible but if it doubles, there's no way we will be able to come up with the money. Just a few more days and we should be in a position to give you a realistic and reasonable offer. Any help would be greatly appreciated!"*

Strategy 2: Ask for more time

"*Hello, I'm going to be as up front and honest as I can be right now and let you know that we have not been able to secure the 12 million dollars (...)* ***we need some more time*** *(...). Coming up with the 12 million is almost impossible but if it doubles, there's no way we will be able to come up with the money. Just a few more days and we should be in a position to give you a realistic and reasonable offer. Any help would be greatly appreciated!"*

"I understand that and trust me, we are really trying here. (...) We have been working all night to gather just the funds to buy more time and we aren't there. ***1 million isn't going to be possible right now*** *(...). All we've asked for is more time and you are going to pass up on a potentially big payday over just giving us a few more days? (...) Give us the time and we'll get whatever we can get together (...) or don't give us the time and get nothing. We'll recover from this or we won't (...).*

Strategy 3: Promise to pay a small amount now or a larger amount later.

"I spoke to my boss and explained your situation to him. He approved a payment of 350k dollars. There will be no more discounts. (...) raise your price by 50k and ***we will close this deal now.****"*

Strategy 4: Convince the adversary you cannot the the high ransom amount

"Hello. We thank you again for your patience. We are asking for you to take into account the difficult position we are in. We do not have the cash funds available or insurance to pay the amount you are seeking. We are not even able to borrow the money right now. We are only able to offer you a little more money right now and this is the most we can do. ***We can only pay up to $500k. This is our final offer and are prepared for what will happen if you do not accept.*** *If you accept we will arrange for the payment. Thank you for your consideration."*

Strategy 5: If possible do not tell anyone you have cyber insurance

"Yes, we can prove you can pay 3M. Contact your insurance company, you paid them money at the beginning of the year and this is their problem. You have protection against cyber extortion. (...) I know that you are now in trouble with profit. ***We would never ask for such an amount if you did not have insurance."***

Look, we know about your cyber insurance. Let's save a lot of time together? You will now offer 3M, and we will agree. ***I want you to understand, we will not give you a discount below the amount of your insurance.*** *Never. If you want to resolve this situation now, this is a real chance."*

Conclusion

- Ransomware negotiations are an unfair game
- However, criminals are also just humans
- Multiple strategies to lower the ransom