On the leaked files from Conti ransomware group

Jambul Tologonov
jambul.tologonov@trellix.com

Jair Santanna
jair.santanna@northwave.nl

19/10/2022

Who we are?

Trellix

/newsroom/stories/research/conti-leaks-examining-the-panama-papers-of-...

northwave | Personal | UTwente | Threat Intel | UFRGS | UNISC

Conti Leaks: Examining the Panama Papers of Ransomware

By John Fokker, Jambul Tologonov · March 31, 2022

Introduction

It isn't often the whole world gets an inside look of the business operations of a top tier cybercriminal group. Very early on in the Russian-Ukrainian Crisis the predominantly Russian based ransomware group Conti made a public statement where they expressed their loyalty to the Russian Administration.

"WARNING"

The Conti Team is officially announcing a full support of Russian government. If any body will decide to organize a cyberattack or any war activities against Russia, we a re going to use our all possible resources to strike back at the critical infrastructures of an enemy.

2/25/2022 | 55 | 0 [0.00 B]

Figure 1. Conti expressing their support to the Russian Administration. Source: BleepingComputer

As a reaction to this statement and the current conflict, a Ukr researcher, operating by the twitter handle @contileaks decic years of Conti's internal Jabber conversations online. The cha dumped span across several years consisted of thousands of making this the "**Panama Papers of Ransomware**".

This wasn't the first time the Conti gang got hit, last summer affiliate posted their attack playbook online, which was full of

Jambul

+

NORTHWAVE

NU HULP NODIG BIJ EEN CYBER INCIDENT: 0

HOME | SERVICES | ABOUT | NEWS | MARATHONS

WHEN THE HACKERS GET HACKED – PART II

A BLOG SERIES UNVEILING THE CONTI RANSOMWARE FAMILY

In the previous blog, we presented the contents and origins of the leaked data related to Conti ransomware gang [1]. In addition to that, we translated the entire dataset and made it publicly available to the security community [2]. In this blog, we dive into details of the internal conversation among Conti gang actors. Our goal in this blog is to show what meaningful information we can subtract from the data. For this reason, we do not display all possible findings. Instead, we focus on the significant (most frequent) information. We acquired this information from an analysis of leaked files [3]: "Conti Chat Logs 2020.7z" and "Conti Jabber Chat Logs 2021 – 2022.7z". These two files compress hundreds of thousands of internal conversations from 2020 till 2022. The analysis in this blog is intended to provide answers to the following questions:

- **What is in the data (an overview of the communication)?**
- **What roles are played by actors in the Conti gang?**
- **Can we identify the real identity of the Conti actors?**
- **What IP addresses and URLs (HTTP and HTTPS) are part of Conti's infrastructure?**
- **How many Conti victims are there and who are they?**

Besides answering these questions, we explain how we arrived at those answers. Opp blogs and webpages that performed analysis on the same data, we are one of the few context to the data, employing data enrichments and using our vast experience from r ransomware incidents.

Jair

Timeline of events till the leak

conti leaks @ContiLeaks · Feb 28

Glory for Ukraine!

4 17 154

conti leaks @ContiLeaks · Feb 28

fuck russian inviders!

1 7 79

“WARNING”

The Conti Team is officially announcing a full support of Russian government. If any body will decide to organize a cyberattack or any war activities against Russia, we a re going to use our all possible resources to strike back at the critical infrastructures of an enemy

2/25/2022 62 0 [0.00 B]

conti leaks @ContiLeaks · Feb 27

conti jabber leaks anonfiles.com/eP6K6K5xc/1_t...

16 140 295

vx-underground @vxunderground · Mar 1

February 27th, a Conti member began leaking data from Conti ransomware group, after Conti released a message siding with the Russian government.

Today, February 28th, the Ukrainian affiliate has leaked more data. It is a lot.

Download it here: share.vx-underground.org/Conti/

10 219 621

Focus on Jabber Chat data

544 .json files

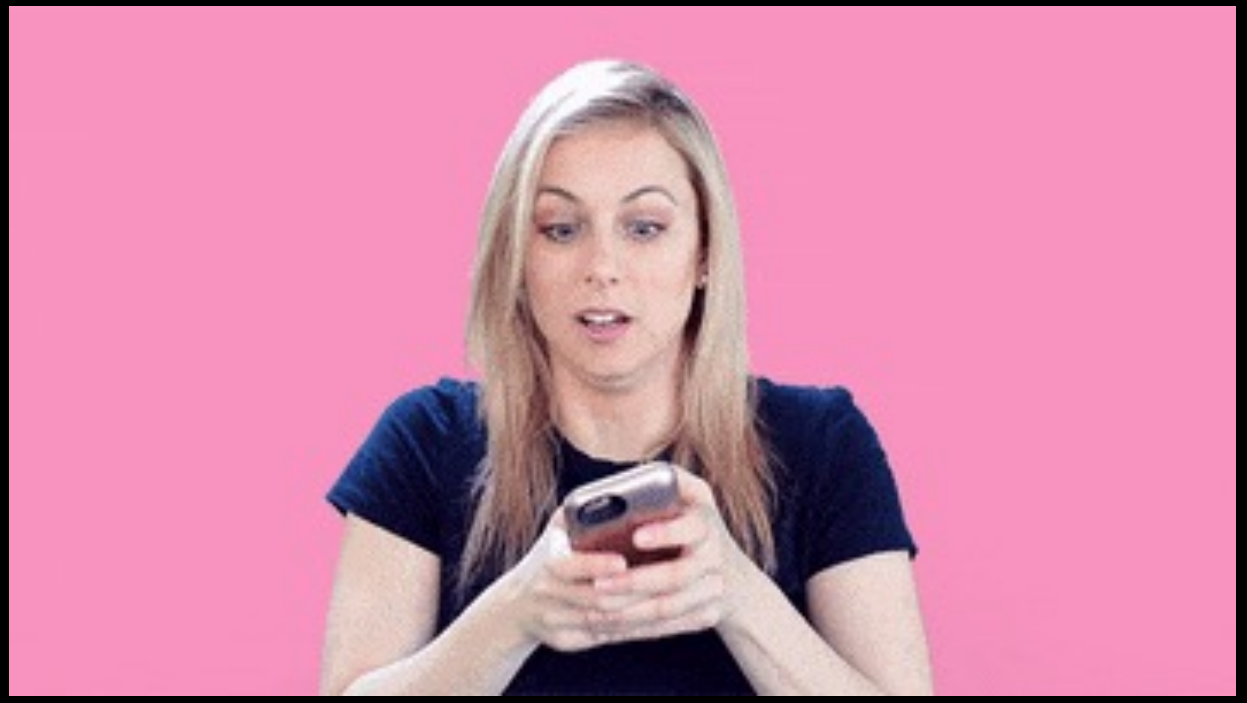
169k records

2020-2022

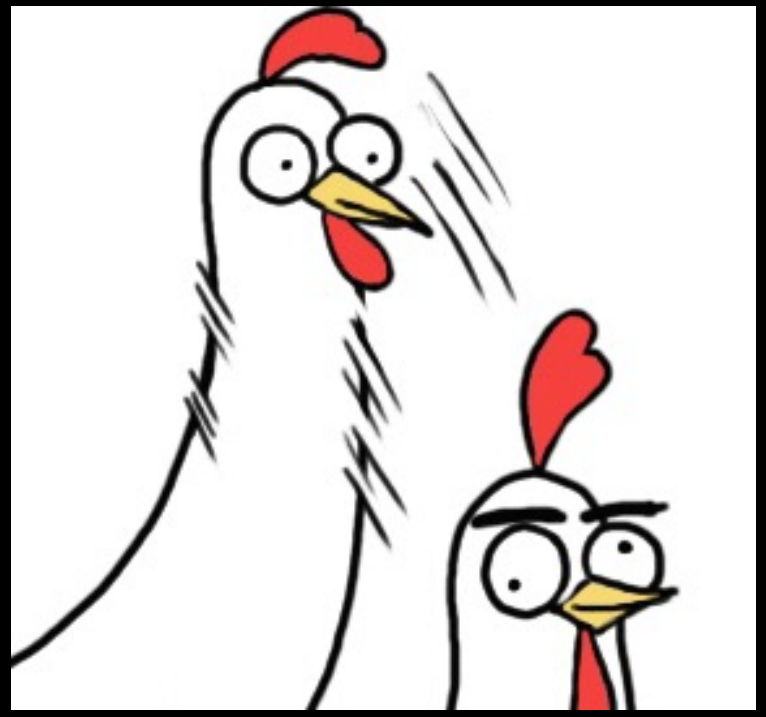
https://share.vx-underground.org/Conti/

What communication platform do you use at work?

What sort of things you tell your colleagues?



NOT our goal!



IoC TTP IoC TTP IoC IoC IoC IoC TTP TTP IoC TTP IoC IoC IoC IoC

Our goal

Help you to understand (with evidences)

How mature is the ransomware ecosystem!

We think not everyone understands it.

This data is a unique piece of evidence.

“If you know the enemy and know yourself,
you need not fear the result of a hundred battles.”
[Sun Tzu]

Another good motivation

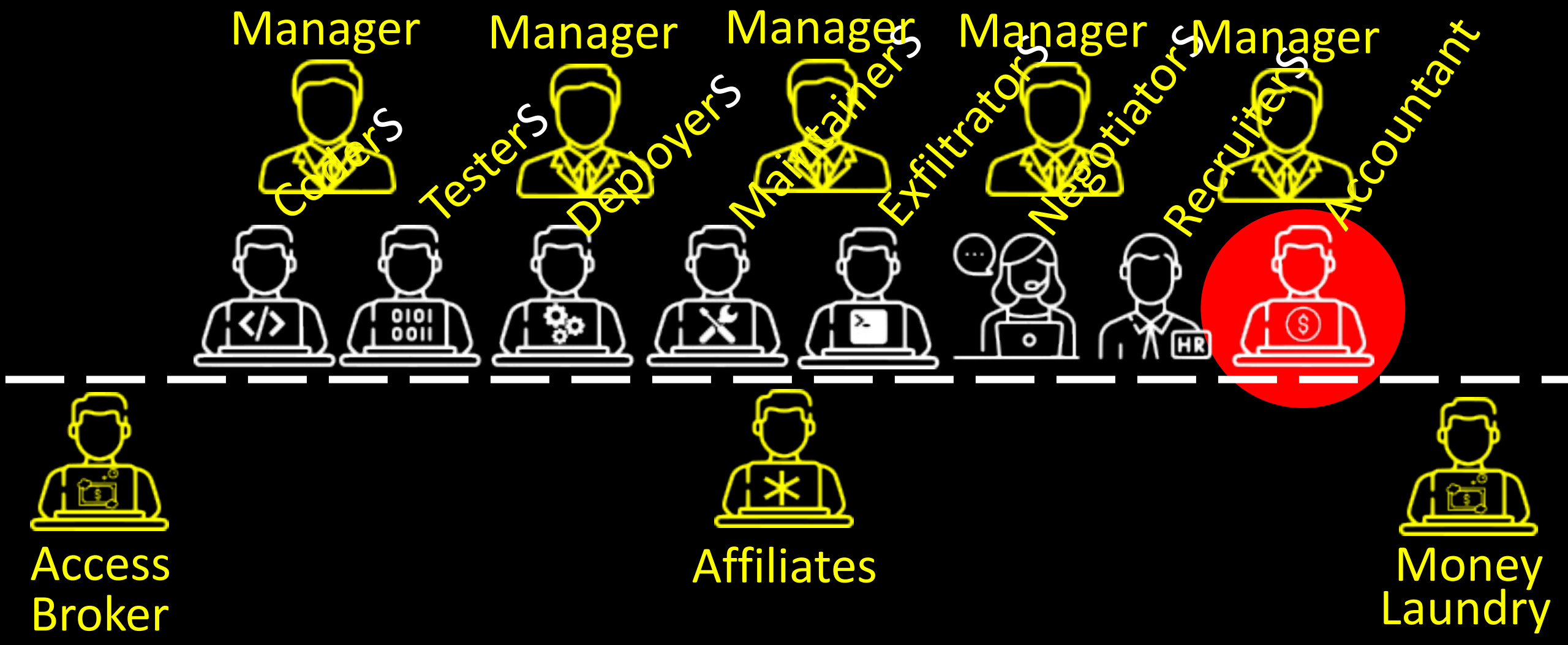
How many are they?

465

**distinct users*

But...

What they do?


Manager
Manager
Manager
Manager
Manager
Coders
Testers
Deployers
Maintainers
Exfiltrators
Negotiators
Recruiters
Accountant
HR
Access Broker
Affiliates
Money Laundry

Who is the accountant?

bentley

For salary write to
stern@q3mcco35auwcstmt.onion

azot

2020-10-01 15:33:52.025624

How many they are? How much they earn? How often they earn?

Mango

Tomorrow is salary day:

main team - 97 447; 52 people (1873,98 p.p)

new team - 4000; 3 people, (1333,33 p.p)

one has not yet started the reverse team - 23,347; 16 people (1459,18p.p)

research team - 12,500; 6 people (2083,33 p.p)

team of OSINT intelligence - 9,000; 4 people (2250,00 p.p)

total 146 294 \ 2 = 73 147 for salary

+ 700 bucks will go to commissions for transfers from wallets / withdrawals from exchanges and

3-4k are needed for expenses on routers / servers / gaskets
bc1q5aqs5hrlt3wj5xrnj0craykgsq6h8mse3cftf8

Stern

2021-06-29 10:11:59.543976

52+3+16+6+4 = 81 employees

How many they are? How much they earn? How often they earn?

Mango

Tomorrow is salary day:

main team - 97 447; 52 people

new team - 4000; 3 people,

one has not yet started the reverse team - 23,347; 16 people

research team - 12,500; 6 people

team of OSINT intelligence - 9,000; 4 people

total 146 294 \ 2 = 73 147 for salary

+ 700 bucks will go to commissions for transfers from wallets / withdrawals from exchanges and

3-4k are needed for expenses on routers / servers / gaskets

bc1q5aqs5hrlt3wj5xrnj0craykgsq6h8mse3cftf8

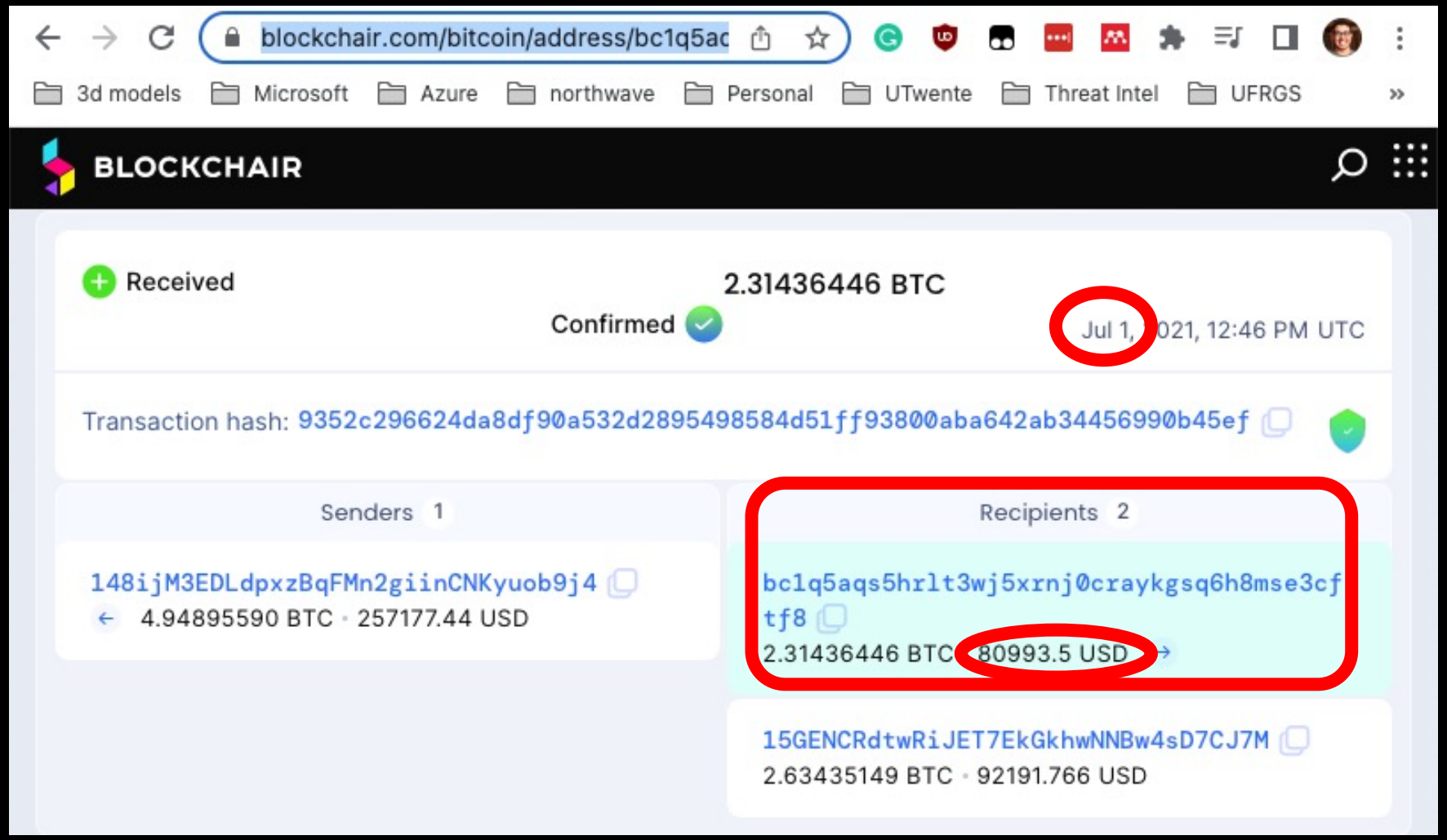
73k+0,7k+4k =~78k

Stern

2021-06-29 10:11:59.543976

Can we proof the transaction?

73k+0,7k+4k =~78k



What happened 15 days later?

Mango

ZP bande here bc1qkmyv5860pe24h9ytadkzgqltkjuuk9z9s027df
sum total 85k
99947 the main team is 62 people, (1112,04 p.p)
33847 - reverse team, 23 people (1471,60 p.p)
8500 - new team of coders, 6 people, only 4 salaries received so far (1416,66 p.p)
12500 reverses, 6 people (2083,33 p.p)
10000 OSINT department 4 people (2500,00 p.p)
3000 for expenses (servers pads tests for new people)
164.8k total per month

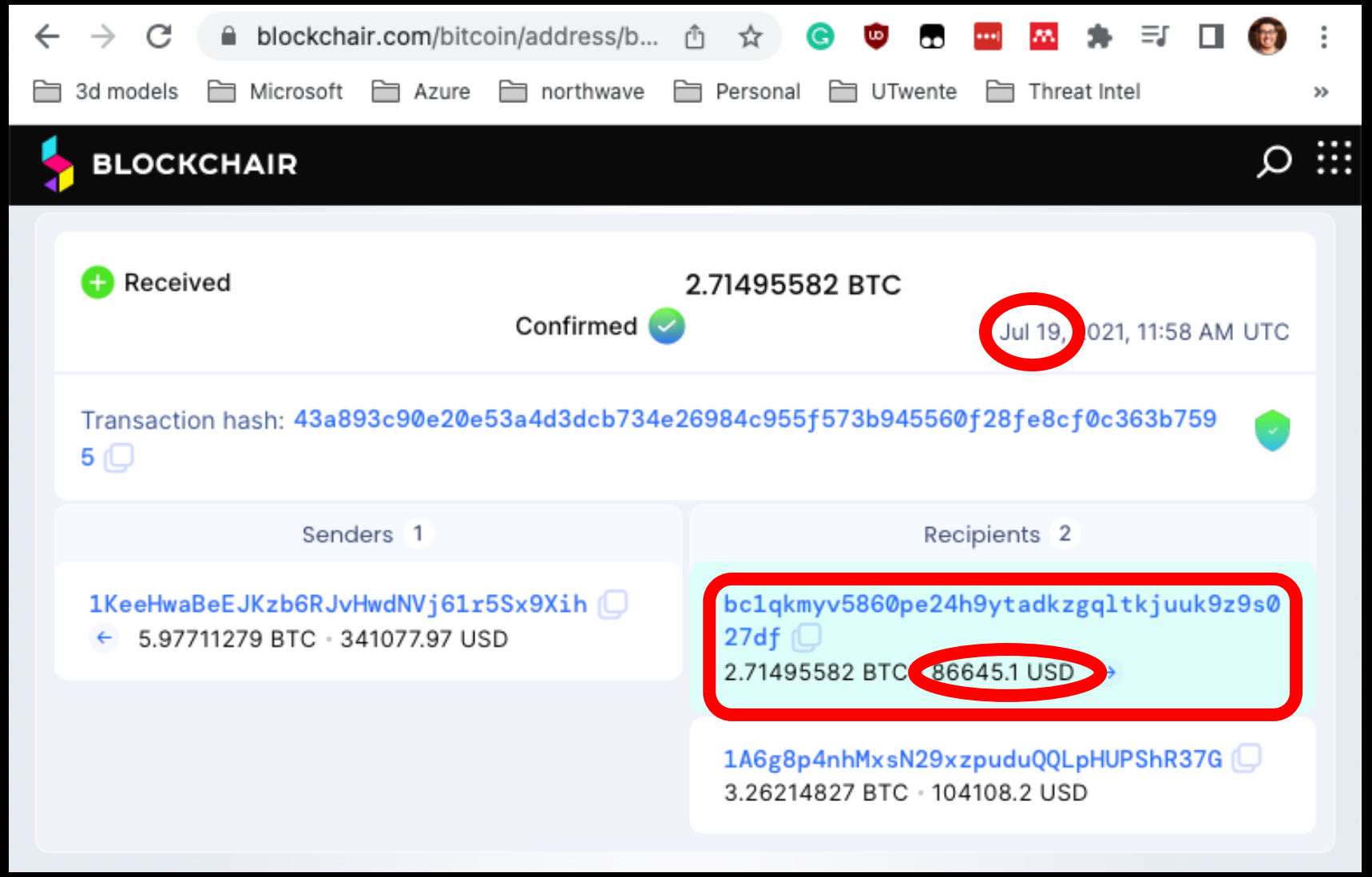
Stern

202[illegible]-07-16 [illegible]0:28:56.793831

62+23+6+6+4 = 101 employees

Can we proof the transaction? again

100k +34k+8,5k+12,5k+10k =165k /2=82,5 +3k =~85 ,5k



Were those ~100 people the only ones in the payment?

Stern

Hello. Create a payment

Van
Cosmos
Elon
Flip
Ghost
Globus
Kaktus
Bullet
Price
...

22 people

2020-07-01 11:08:*

65

How the answer back to Stern looks like?

Kaktus

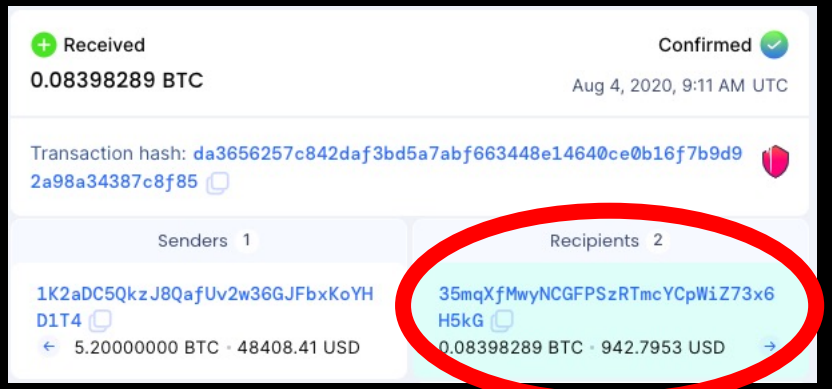
Hey!

0.106089

3MwHyMvY6Hs5mETfyv4bLbHZnaphZDngPa

Stern

2020-07-01 11:10:54.710649



How the HR talks? What are the conditions to negotiators?

Viper

Hello, I want to offer you a job in our team that deals with ..... in self-isolation mode, our team offers you a current vacancy for a completely remote job for the position of .....

Responsibilities : Receiving calls and communicating with clients

Required skills: - Good knowledge of spoken English,

- Age from 18 to 25

Conditions: - We offer you a timely salary in the amount of 450–500 (increase in salary by 100 - 200– 300, depending on positions of the Supervisor)

- Work is completely REMOTE, Work schedule 18:00 - 2:00 Moscow time. 5/2. Sat and Sun weekend.

- Paid vacation

- WITHOUT registration according to the TC

If you are interested in the offer, send your resume by replying to this email.

8:00 – 16:00 Los Angeles
12:00 – 20:00 São Paulo
17:00 – 01:00 Amsterdam

Derek

2020-08-31 12:20:30.838021

How recruiter works?

Derek

Hello, I want to offer you a job in our team that is engaged in the maintenance of an online store abroad. In self-isolation mode, our team offers you a current vacancy for a fully remote job for the position of a call center operator.

Responsibilities: Taking calls and communicating with clients

Required skills: - Good knowledge of spoken English (level B2-C1)

- Age from 18 to 25

Conditions: -We offer you timely wages in the amount of 450-500 (Increase in salary by 100 - 200 – 300, depending on the success in the work of the call center)

- Work is completely REMOTE, Work schedule 18:00 - 2:00 Moscow time. 5/2. Sat and Sun weekend. - Paid vacation

- WITHOUT registration according to the Labor Code

If you are interested in the offer, send your resume by replying to this letter.

Salamandra

2020-10-05 09:47:08.925161

How does it sound a call center / negotiator?

"Data recovery?!"

How many offices they have?

Target

[…] 1) these are operators current expenses + expansion = total 2 offices with large teams - one main and one new for training

2) hacker offices (3 pcs) - interviews, equipment, rent, interviews, deposits, servers inside, equipment, hiring and assistance in hiring and a whole lot more, and in a week another salary will be added for those who will work there (20+ hackers)

3) an office with programmers and equipment for everything for them + a good team leader has already been hired and he is the team to collect there will be a pro, this is an important devops for a pro, a pro is happy with everything and he really needs it + we hire third-party specialists with a pro to speed up various processes […]

Stern

2020-08-27 01:21:03.188115

2+3+1 = 6 Offices

- What is the connection to RU gov?
- Do Conti act in RU gov's interests?
- What is the involvement with other ransomware groups?
- How do they cash out the money? How the money laundering is done?

What is the connection to RU gov?

target: Liteyny av. 4 is in charge the guys are asking how late we are going to be, should they order food or not, omar is not responding

…

professor: did you see stern today? any clue whether he will be or not?

What is the connection to RU gov?

angelo: may be S at the ministers' reception
hammer: or may be he is himself a minister
…
angelo: my personal opinion is that he is close to FSB or other structures

What is the connection to RU gov?

elroy: Yes, smells bad indeed

angelo: I thought S is almighty as God

...

elroy: If he was not almighty, we all would have ended up as Revil

elroy: It is written there in the article, the only big organization in Russia

angelo: yes, I already figured that S is in service of Pu

angelo: I understand that everything is on a large scale))

angelo: what orders we do and who sometimes our clients are

What is the connection to RU gov?

target: https://twitter.com/search?q=[redacted]&
src=typeahead_click&f=live

...

troy: and all their backups were destroyed there

target: ok awesome

...

target: you will also get a reward/prize

...

target: in the Kremlin

What is the connection to RU gov?

…

elroy: Or are you from FSB?

basil: I am not going to tell you where I am from (you understand that) But I have very serious intelligence that on the border is not a training

Do Conti act in RU gov's interests?

professor: what do we need from [redacted]?
professor: is it an office request, from one of the two?
...
professor: what are we looking?
stern: chat
professor: are they paying or are we playing pioneers?
stern: contracts
professor: =)
stern: accounting
stern: yes fuck the money
stern: we will play)
professor: yes no probs
professor: will wear a red tie then
...
professor: Cozy Bears already started down the list there

Do Conti act in RU gov's interests?

troy: RU ru.[redacted].com
troy: not this one
troy: removing it
target: such idiots
...
target: is it an outsourcer from RU
...
target: that is a fucking enormous corporation
troy: what if I did not notice that?
troy: then would have been fucked
target: bitch and what a chance this freak is from RU internet space
target: yes good job!
target: listen, who would have known

Do Conti act in RU gov's interests?

target: when I saw an OOO in the report my heart stop beating
Thanks god some pranker of yours translated LLC as OOO
...
troy: there is purely China
troy: 3 networks
target: big ones
target: I think
target: around 4.5 bln
...
target: do we have a stop on China?
troy: yes
...
target: China +

Do Conti act in RU gov's interests?

professor: did you see how they fucked it up?

professor: regarding the affiliation?

professor: I fucking almost exploded

professor: they put a part of Trickbot's code which is responsible for the check on CIS

professor: into the build of Diavol

professor: Although I specifically asked do not touch the task with determining the geolocation at all

professor: and immediately the entire project is on the news as fully affiliated

What is the involvement with other ransomware groups?

target: As for Ryuk - as of next week we will kick off and for 1-2 weeks my people from the office will work together with his people...
target: to sum up the next week:
- Ryuk and our people will learn how to interact with each other: will start slowly and little by little
...
from 10 to 20 September
- will be increasing Ryuk
- will give to prof's online team and less to do for the office
from 20 to 30 September
- Ryuk's people and my senior managers are interacting on their own
- slowly will start loading the office with prof's work
target: in October if everything works out as per prof's plan
- will load Ryuk
- will load our office hackers

Conti-Ryuk

What is the involvement with other ransomware groups?

target: troy also locked 2 very big firms
target: from 1 bln
target: and 3 bln
target: prof said they paid us 1.5 mln
target: fx1-16 | usa | server: 1200/1200 |computer: 3000/1000+ | memory: 380+tb | revenue: 3bill | Employees: 12000 | site: https://www.steelcase.com
...
target: fx3-16 | IP: 192.168.54.6 | USA, IT, ESP | server: 702/866 | computer: 1000+/2300 | memory: 243TB revenue: 1B | Employees: 7,000 | site: [redacted]
target: FX1-10 | usaserver:5000/3000+ | comps 50000/1000+ | revenue: 9 bill employees:50000 | website: www.soprasteria.com | www.soprabanking.com
...
target: fx2-12 | IP: 10.1.10.250 | USA | server: 5/5 | computer: 9/9 memory: 1 TB | revenue: 6b | Employees: 19,800 website: www.[redacted].com

Conti-Ryuk

What is the involvement with other ransomware groups?

stern: we will give them money, and let Carbon lay there, maybe it will be as of use later

mango: why did not we need Carbon at the end?

mango: nobody can work with it?";

mango: let's sell it then, there is a demand for it

stern: it was Ryuk who needed it

stern: they wanted to research it

stern: they wanted it for a long time

stern: and later they rejected it

Conti-Ryuk

What is the involvement with other ransomware groups?

stern: [18:11:13] <professor> did the first one with maze, just a small random network - replied back within a day
…
stern: make that the locker works better than maze
reshaev: Will check now, check the reviews
reshaev: It is possible to send me the build?
reshaev: With the decryptor
stern: no decryptor at the moment
stern: for the build ask Prof
…
stern: We need to make it not worse than maze
stern: and even better

"...Maze will take 25-30%..."

Conti-Maze

What is the involvement with other ransomware groups?

stern: and gain a foothold there
revers: all the others are there
revers: and indeed I already set a foothold there
stern: and contracts
stern: for the start
revers: Target already has AD users from every domain
revers: name position
revers: and mail address
revers: which are in the trusts
revers: and we have already from the hq
revers: in the weekend I am gonna have a look into the data
revers: [redacted] domain is already taken
revers: [redacted] we took it too
revers: [redacted] AD is taken by us
revers: also there in the network 1
revers: Maze has negotiations there

Conti-Maze

What is the involvement with other ransomware groups?

netwalker: Arma asked 300k
netwalker: You said that you will give us some bonus after the first lock! We really need it bro.
...
stern: a guy gave some citrix'es, hors passed them to you, and you gave it to another person from whom they actually originated from) a kind of a circle)
netwalker: What ? I will find out who gets a slap on the forehead. Although everyone anyway knows each other.
...
netwalker: We figured things out. Apologized to each other.
My bad, all I want is to show you more results because we are sitting here without any targets.
And while everyone is busy with loading/analysing and exfiltrating, we asked the guy just to check, and he apparently passed it further. Funny. But the truth is nobody wanted to fool anyone that is the fact. It is not going to happen again ever.

Conti-Netwalker

What is the involvement with other ransomware groups?

netwalker: [redacted] DEV1 (\\PGMDC) [redacted] 900кк gave it to hors for further work I have all [redacted] 700к busy with. Don't forget please to pay to spamilka. He was so joyful.

netwalker: Bro ping.

netwalker: [21:44:35] <netwalker>)> 16evvEiZ6HKkV9WAbysJfJG1Qa7DzJGUFp wallet. Please don't forget to send the motivation to the guy, he did his best. and we need to give him some incentive. We did not even pay him the whole base bro.

stern: sent 1BTC

Conti-Netwalker

What is the involvement with other ransomware groups?

mango: We did not understand each other with lockbit... You wrote to give him networks for work, he is writing that he actually needs troy) And on what terms also not clear, I gave him your contact here, he said he will reach out to you himself
...
mango: On what terms in case we need to give him troy?
mango: I wrote him that usually we take a part of the botnet, but what part I do not know))
stern: say 20 percent
stern: let's try that
mango: 20% bots with the networks are ours
mango: ок
stern: 20 percent of revenue not the bots

Conti-LockBit

How do they cash out the money? How the money laundering is done?

fire: I transfer BTC into Monero

fire: via the exchanger

fire: with one time email address

fire: then to another Monero wallet, then either to USDT on ledger or to the card

fire: but often I exchange USDT to cash

fire: less questions from the authorities to ask

snow: ok got it, but what is the USDT

fire: USDT - it is a cryptocurrency of Ethereum I store in it as the rate is always equals to 1 dollar

fire: stability compared to BTC

BTC > Monero > Monero > USDT/Ledger/Cash/Card

How do they cash out the money? How the money laundering is done?

tramp: Take the money through a mixer

tramp: And then withdraw

tramp: It will be accurate in general

...

tramp: they will be searching only on money laundering

tramp: the most important is that the mixer won't fuck it up, mixer also adds weird shit

tramp: http://crypmix4m5iunofa25mpmiihdb56oaqg57tvrebqatc6otn3w65qhlid.onion/

How do they cash out the money? How the money laundering is done?

bio: regarding BTC - Monero - Monero - cash how do you convert from BTC to Monero? or where?

fire: from a dark/dirty PC via bestchange(.ru)

bio: and where do you then do withdrawing from Monero and into what, you own card?

fire: Monero-Monero

fire: and then into cash

fire: I have a connection in the exchanger in the neighbouring city

fire: guys there take Monero and then bring back a bag of cash

fire: and part of that cash into the card

bio: got it, now I am thinking what shall I do...

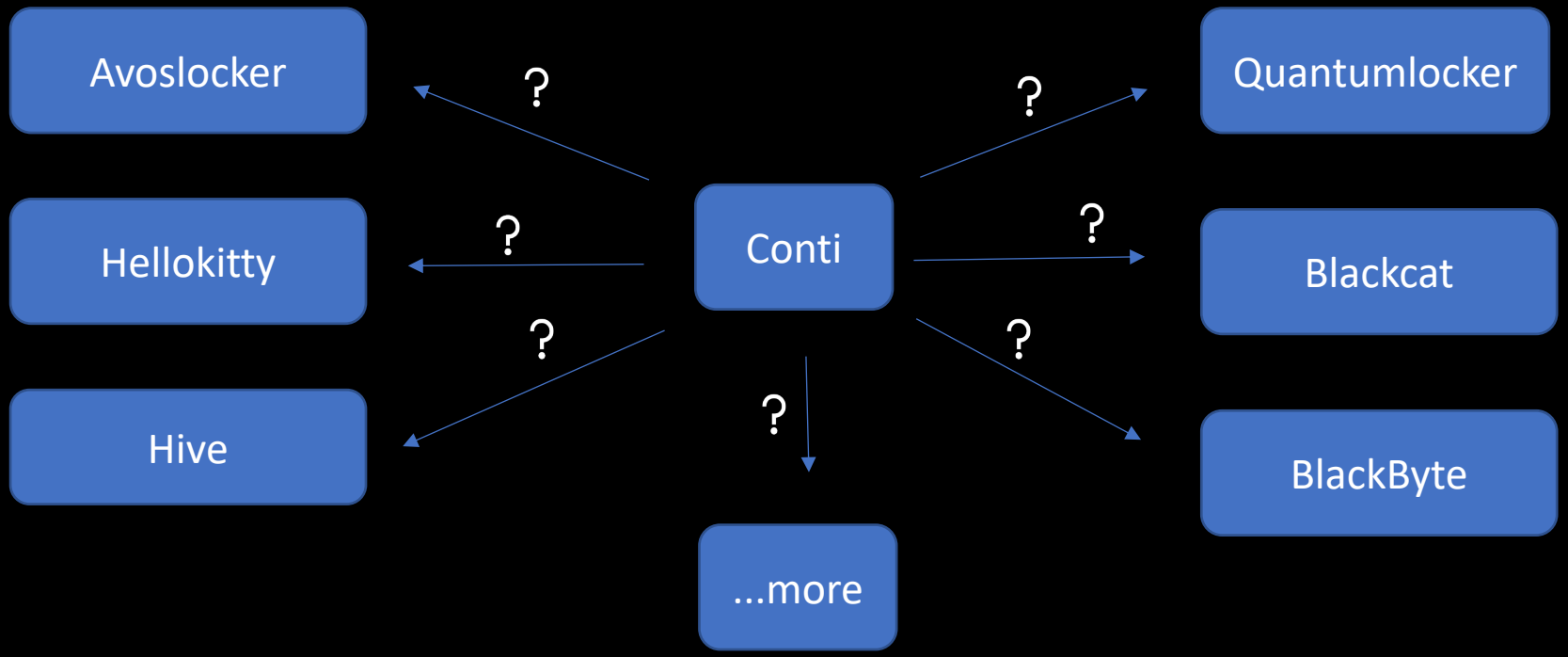
fire: if it is a large city, check out the exchangers in the city

fire: most of them exchange monero into cash

bio: OK will look for those. thx.

What happen when a ransomware group shuts down?

Rebrand and/or disperse into other ransomware/partnership/affiliate programs



TTPs/tradecraft/knowledge gained remain

On the leaked files from Conti ransomware group

Jambul Tologonov
jambul.tologonov@trellix.com

Jair Santanna
jair.santanna@northwave.nl

19/10/2022