



◆ Crystal

The Conti Leaks Part Two: Who Did They Target & Why?

Who did the Conti group target for ransom and why?
More insights revealed ...

Report by Crystal Blockchain's Analytics Team

Copyright © 2022 Crystal Blockchain B.V. All rights reserved.

Table of Content

Executive Summary	3
Cruel intentions of a ransomware network	4
Ambitious profit goals for a ruthless team	5
Companies attacked by Conti	11
Pfizer	11
Ridgeview Medical	12
Angelica	12
Clarus	12
Loomisco	13
Radial	17
SAI Global	20
Connecting wallets to the ransomware attacks	21
Confirmed crypto payments made by companies to the Conti group	28
The lack of ransomware reporting due to the stigma attached	30
Contact Crystal	30
Appendix	31
US-based Companies:	31
Other Regions:	35
Disclaimer	36

Executive Summary

- ◆ The Conti Leaks Part Two is the second report in a series where the Crystal intelligence and investigations team analyzed the recently leaked Conti chat logs.
- ◆ This report includes previously unseen chat logs from 2020 and 2021.
- ◆ From their logs, we know that Conti planned to attack 20-30 companies a day, and if a business didn't comply, they would threaten to destroy it.
- ◆ Evidence shows huge anti-US sentiment amongst Conti members, while businesses in CIS regions were not attacked.
- ◆ We researched and verified that out of 89 companies found in the Conti chat logs, 76 were US-based, and only 13 came from other regions.
- ◆ Crystal's findings show that the most significant payment request in the logs was 3,000 BTC, and Conti's most considerable single ransom payment was 725 BTC.
- ◆ One of the biggest names mentioned in the logs was Pfizer. We've included original chat logs between Pfizer employees, chat logs related to other companies, and English translations of each chat.
- ◆ The Crystal team noted that most Conti ransom attacks were not made public or reported to law enforcement by the businesses involved.

Cruel intentions of a ransomware network

In the first part of the series by the Crystal analytics and investigations team, [The Conti Leaks Part One: A Modern Criminal Network Unveiled](#) we introduced the Conti group. We described who they were when they got discovered first and what cybercrimes they worked with. The key source for this report series is the leaked internal chat logs by one of the members following Conti's support of the Russian invasion of Ukraine.

Crystal's team has been analyzing the leaked data to understand this group's inner workings and potentially help solve crimes committed by Conti. In Part One, we examined the logs released from 2021. Still, since the first report, we have come into possession of Conti chat logs from 2020, logs that offer further insights into this group's malicious and truly inhumane intentions as they targeted "clients" for ransom.

Ambitious profit goals for a ruthless team

Conti is a large Ransomware-as-a-Service (RaaS) network with connections in the criminal underworld. We know the group had big plans to extricate revenue from targeted companies — **their chat logs note plans to ransom 20–30 companies per day.**

If successful, that would add up to 7,300 companies a year. With ransom requests anywhere from 50 Bitcoin (BTC) up to 3000 BTC in 2020 and 2021 — if even half of the companies Conti planned to attack agreed to pay even 5 BTC to Conti — it could have come to around 18,250 BTC. That equals USD 714,374,350 at today's prices.

Original chat log

2020-10-06 T01:53:18. 412365	target@q3mcco35 auwcstmt.onion	stern@q3mcco35a uwcstmt.onion)) я думаю только о том ")) I'm just thinking"
2020-10-06 T01:53:28. 051674	target@q3mcco35 auwcstmt.onion	stern@q3mcco35a uwcstmt.onion	чтобы игла лочил по 2-3 десятка в день "That the [lgla] should lock in 20-30 per day"
2020-10-06 T01:53:56. 468092	target@q3mcco35 auwcstmt.onion	stern@q3mcco35a uwcstmt.onion	и думаю они выйдут на этот объем за месяц "And I guess they will reach this volume in a month"
2020-10-06 T01:54:04. 854320	target@q3mcco35 auwcstmt.onion	stern@q3mcco35a uwcstmt.onion	сегодня вообще что то там творят нереальное "They're doing something crazy there today"

It's clear that if **companies aren't prepared to pay a ransom, the Conti team is ready to destroy their business** without remorse.

Original chat log

2020-10-09 T11:33:39. 585901	target@q3mcco35 aawcstmt.onion	dandis@q3mcco35 aawcstmt.onion	1 час на линии с их руководством "1 hour on the line with their management"
2020-10-09 T11:33:42. 445668	target@q3mcco35 aawcstmt.onion	dandis@q3mcco35 aawcstmt.onion	и они ебут мозги нам "And they are f**king with us"
2020-10-09 T11:33:43. 729986	target@q3mcco35 aawcstmt.onion	dandis@q3mcco35 aawcstmt.onion	Ахахахах "hahaha"
2020-10-09 T11:33:45. 407195	target@q3mcco35 aawcstmt.onion	dandis@q3mcco35 aawcstmt.onion	Угрозы "threats"
2020-10-09 T11:33:51. 597493	target@q3mcco35 aawcstmt.onion	dandis@q3mcco35 aawcstmt.onion	ебали мы их "We f**ked them"
2020-10-09 T11:33:54. 893069	target@q3mcco35 aawcstmt.onion	dandis@q3mcco35 aawcstmt.onion	ну вот "well"
2020-10-09 T11:33:57. 756883	target@q3mcco35 aawcstmt.onion	dandis@q3mcco35 aawcstmt.onion	о чем думаю капиталисты "What are capitalists thinking about?"
2020-10-09 T11:34:01. 271803	target@q3mcco35 aawcstmt.onion	dandis@q3mcco35 aawcstmt.onion	о демократии? "About democracy?"
2020-10-09 T11:34:03. 434070	target@q3mcco35 aawcstmt.onion	dandis@q3mcco35 aawcstmt.onion	ебать их "f**k them"
2020-10-09 T11:34:12. 405235	target@q3mcco35 aawcstmt.onion	dandis@q3mcco35 aawcstmt.onion	пусть умрут суки "let the b**ches die" 1 час времени портаили моего офиса "They've wasted an hour of my office"

With considerable anti-US sentiment among the group, Conti preferred to target companies in the US and the EU. Their chat logs reveal a lot of comments like **"Fck USA... they should suffer... I want to destroy their businesses."**

Original chat log

2020-10-19 T19:20:58. 682789	target@q3mcco35 aawcstmt.onion	troy@q3mcco35au wcstmt.onion	думаю еще мес другой "I think another month or two"
------------------------------------	-----------------------------------	---------------------------------	---

2020-10-19 T19:21:03. 022508	target@q3mcco35 auwcstmt.onion	troy@q3mcco35au wcstmt.onion	и будет по 30-50 сертов в месяц "And there'll be 30-50 certificates/month"
2020-10-19 T19:21:05. 971598	target@q3mcco35 auwcstmt.onion	troy@q3mcco35au wcstmt.onion	вот там сша ебать и ебать "That's where we can f**k and f**k the US"
2020-10-19 T22:22:50. 635430	target@q3mcco35 auwcstmt.onion	troy@q3mcco35au wcstmt.onion	вы готовы разьебывать сша будете "Will you be ready to f**k the US"

At one point, the Conti & Ryuk Groups planned to attack 428 hospitals in the US.

Original chat log

2020-10-30 T03:19:05. 881629	target@q3mcco35 auwcstmt.onion	stern@q3mcco35a uwcstmt.onion	будет паника "There'll be panic" 428 госпиталей "428 hospitals" по 2-4 согласованных контакта "About 2-4 coordinated contacts"
2020-10-30 T03:19:11. 676780	target@q3mcco35 auwcstmt.onion	stern@q3mcco35a uwcstmt.onion	это я пишу трую "It's me writing [Troy]"
2020-10-30 T03:19:20. 754193	target@q3mcco35 auwcstmt.onion	stern@q3mcco35a uwcstmt.onion	под ОТР, 100% "Under OTR, 100%"
2020-10-30 T03:19:28. 435129	target@q3mcco35 auwcstmt.onion	stern@q3mcco35a uwcstmt.onion	и смотри что "And look what"
2020-10-30 T03:19:53. 453433	target@q3mcco35 auwcstmt.onion	stern@q3mcco35a uwcstmt.onion	кребс публикует у себя новость вчера, вот перевод русский https://www.securitylab.ru/news/513510.php "Krebs published news yesterday, here's the Russian translation https://www.securitylab.ru/news/513510.php "

Conti also attacked nursing homes. One of the members wanted to skip such places but the manager said something like: **"Fck them all, they all should pay."**

Original chat log

2020-09-25 T10:17:56. 991435	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	watermarkcommunities.com - вот такой еще подняли права, начали качать инфо, но выяснили что это чет типа домов престарелых... наверное не будем их? "watermarkcommunities.com - here's one more, we started downloading info, but have found out that it's a kind of nursing home...perhaps not attack them?"
------------------------------------	-----------------------------------	--	--

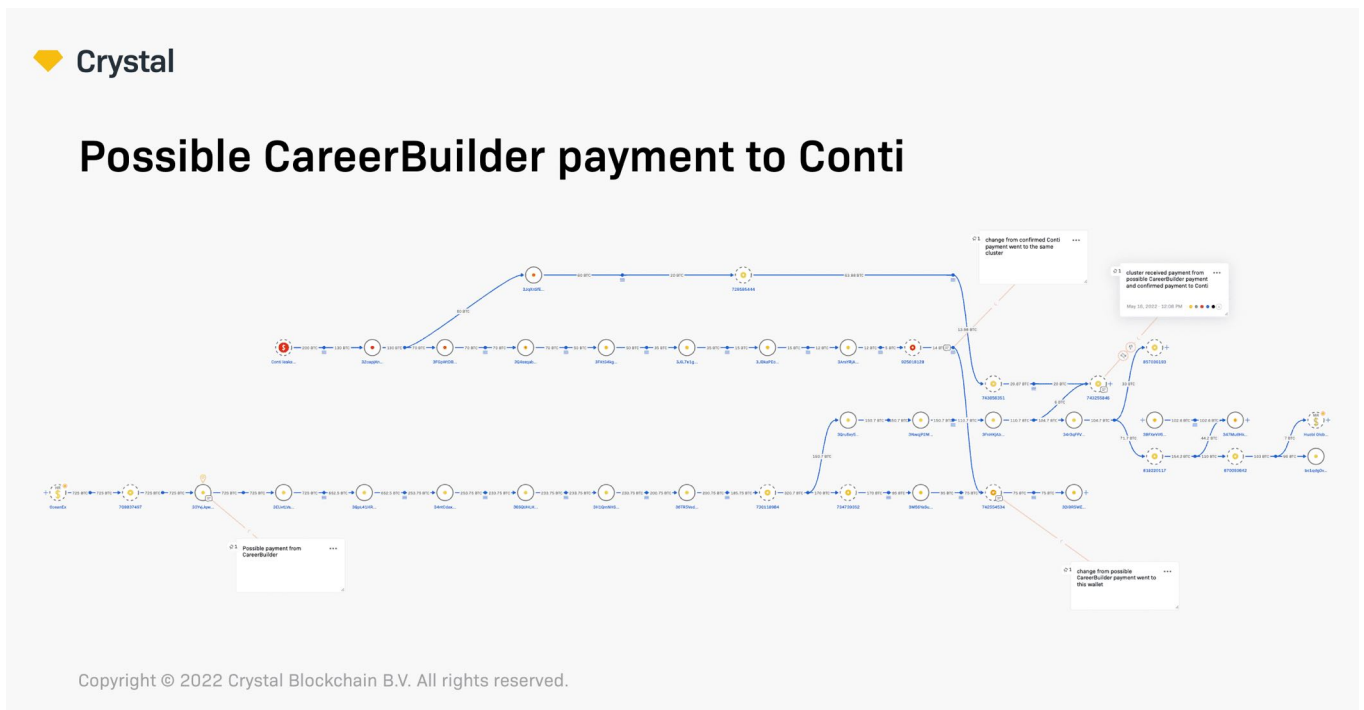
2020-09-25 T10:17:57. 693600	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	Будем "We will"
2020-09-25 T10:18:00. 115763	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	Нахуй "f**k them"
2020-09-25 T10:18:03. 133681	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	они деньги сдирают "They're charging money"
2020-09-25 T10:18:08. 054233	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	окей) "okay"
2020-09-25 T10:18:08. 510824	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	со стариков "They charge the elderly"
2020-09-25 T10:18:13. 614177	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	платите бабки "Pay the money"
2020-09-25 T10:18:14. 844225	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	или на улицу "Or get out of here"
2020-09-25 T10:18:16. 912012	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	там так говорят "That's what they say"
2020-09-25 T10:18:19. 314373	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	а ым их что "And we"
2020-09-25 T10:18:20. 901051	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	жалеть будем? "Will we feel sorry for them?"
2020-09-25 T10:18:22. 929862	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	пошли они нахуй "F**k them"
2020-09-25 T10:18:29. 136979	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	ок) "ok)"
2020-09-25 T10:18:31. 721365	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	они там ток разводят стариков "They're just cheating on the elderly"
2020-09-25 T10:18:38. 491214	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	а не к аппаратам подключают "Instead of putting then on life support machines"
2020-09-25 T10:18:44. 419915	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	пошли они нахуй "f**k them"
2020-09-25 T10:18:47. 755219	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	прямо так и напишите в записке "Write this on a note"
2020-09-25 T10:18:53. 226644	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	пусть платят за все грехи "Let them pay for all the sins"

The biggest request to pay was from a "biotech" company, the name was written only in Russian, Conti requested 3,000 BTC.

Original chat log

2020-10-10 T20:02:21. 161085	target@q3mcco35 auwcstmt.onion	stern@q3mcco35a uwcstmt.onion	725 + 270 + еще кто то перевели деньги за ключ "725 + 270 + those who transferred money for the key"
2020-10-10 T20:02:22. 815943	target@q3mcco35 auwcstmt.onion	stern@q3mcco35a uwcstmt.onion	Поздравляю "congrats"
2020-10-10 T20:02:40. 896036	target@q3mcco35 auwcstmt.onion	stern@q3mcco35a uwcstmt.onion	пусть еще биотех переведут 3к бтс))))) "Let Biotex transfer 3k BTC)))))"

The most substantial amount paid was 725 BTC from an "employment" firm (possibly Career Builder, but our team has not confirmed the name yet).



There were also mentions of payments for 235 BTC, 75 BTC, 115 BTC, and 200 BTC from other companies. However, the Crystal intelligence and investigations team is still looking into those transactions to comprehend the context entirely. **Keep an eye out for Conti Part 3.**

We noted in **Part 1** that funds from payment wallets moved to exchanges without any obstacles - see the visual "withdrawals from Conti wallets to various exchanges."

Original chat log

2020-10-10 T13:54:12. 318159	target@q3mcco35 auwcstmt.onion	stern@q3mcco35a uwcstmt.onion	ок 725 Карьер "Ok 725 'Carrier'"
2020-10-10 T13:54:13. 475135	target@q3mcco35 auwcstmt.onion	stern@q3mcco35a uwcstmt.onion))))))))))
2020-10-10 T13:55:08. 840808	target@q3mcco35 auwcstmt.onion	stern@q3mcco35a uwcstmt.onion	и 270 перевели "And transferred 270"
2020-10-10 T13:55:11. 046966	target@q3mcco35 auwcstmt.onion	stern@q3mcco35a uwcstmt.onion))))))
2020-10-10 T13:56:26. 896647	target@q3mcco35 auwcstmt.onion	stern@q3mcco35a uwcstmt.onion	Поздравляю "congrats"

Conti decided on the amount of ransom payment to be requested based on open-source data of companies' revenue such as [zoom.info](https://www.zoominfo.com/c/careerbuilder-llc/50843163). See the Appendix below.

Original chat log

2020-10-09 T10:54:31. 791168	target@q3mcco35 auwcstmt.onion	stern@q3mcco35a uwcstmt.onion	"Revenue: \$837 Million Employees: 2000" https://www.zoominfo.com/c/careerbuilder-llc/50843163 "
------------------------------------	-----------------------------------	----------------------------------	--

As we mentioned, **CIS countries were spared from ransom attacks in favor of US or EU-based. Russia, Ukraine, & Belarus were always exempt** from any Conti attacks.

Original chat log

2020-10-08 T03:03:27. 697988	target@q3mcco35 auwcstmt.onion	voron@q3mcco35a uwcstmt.onion	если кто то посягнется на СНГ "If anybody trespasses CIS"
------------------------------------	-----------------------------------	----------------------------------	--

2020-10-08 T03:03:34. 569708	target@q3mcco35 auwcstmt.onion	voron@q3mcco35a uwcstmt.onion	сразу стреляй такому в голову "Shoot in their head at once"
------------------------------------	-----------------------------------	----------------------------------	--

2020-10-08 T03:03:42. 847349	target@q3mcco35 auwcstmt.onion	voron@q3mcco35a uwcstmt.onion	или битой по голове "smash them with bats"
------------------------------------	-----------------------------------	----------------------------------	---

*Commonwealth of Independent States

Crystal noted within the logs that **Conti at one point received an official request to hack astronautics.com**, but for information rather than money. The company seems to be connected to the military, a defense contractor. Crystal will explore these logs further.

Original chat log

2020-10-09 T14:21:42. 127355	professor@q3mcc o35auwcstmt.oni on	target@q3mcco35 auwcstmt.onion	astronautics.com откройте пожалуйста пионерское деяние сделаю там, просили близкие очень оттуда подергать данных "astronautics.com Open it please and I'll hack into it, close ones asked very much to pull data from there"
------------------------------------	--	-----------------------------------	--

2020-10-09 T14:22:03. 948820	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	а это случайно не та сетка "Isn't that the network"
------------------------------------	-----------------------------------	--	--

2020-10-09 T14:22:06. 850358	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	по которой мне стучал реверс "that the [Reverse] was using"
2020-10-09 T14:22:10. 625055	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	и предлагали какие то данные от туда "And offering some data from over there"
2020-10-09 T14:22:12. 010957	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	по космосу "Over space"
2020-10-09 T14:22:30. 463885	professor@q3mcc o35auwcstmt.oni on	target@q3mcco35 auwcstmt.onion	возможно я там всем мозги вынес когда она отвалилась "I probably blew everyone's minds when it fell off"
2020-10-09 T14:22:35. 598972	professor@q3mcc o35auwcstmt.oni on	target@q3mcco35 auwcstmt.onion	там не фин вопрос "There's no financial issue"
2020-10-09 T14:23:00. 379233	professor@q3mcc o35auwcstmt.oni on	target@q3mcco35 auwcstmt.onion	это дефенс контрактор "It's a defense contractor"

Companies attacked by Conti

Here we list some of the named companies attacked by Conti, along with the chat logs. Included is Pfizer, Ridgeview Medical, Angelica, Clarus, Loomisco, Radial and SAI Global.

Pfizer

Original chat log

185.25.51.173-2 0210622.json	2021-06-22 T20:56:40. 274724	stern@q3mcco35a uwcstmt.onion	leo@q3mcco35auw cstmt.onion	просто надо грузить крупные конторы и все "We just need to load big companies and that's it"
185.25.51.173-2 0210622.json	2021-06-22 T20:57:04. 258656	stern@q3mcco35a uwcstmt.onion	leo@q3mcco35auw cstmt.onion	ну давай pfizer "Let's go with Pfizer"
185.25.51.173-2 0210622.json	2021-06-22 T20:57:11. 694029	stern@q3mcco35a uwcstmt.onion	leo@q3mcco35auw cstmt.onion	pfizer зарази мне "pass on the virus to Pfizer"
185.25.51.173-2 0210622.json	2021-06-22 T20:57:18. 438603	stern@q3mcco35a uwcstmt.onion	leo@q3mcco35auw cstmt.onion	я хочу посмотреть что там есть у них "I wanna see what they have there"
185.25.51.173-2 0210622.json	2021-06-22 T20:57:42. 150473	stern@q3mcco35a uwcstmt.onion	leo@q3mcco35auw cstmt.onion	выкачаем все что есть "Will download everything"

Ridgeview Medical

Original chat log

Good morning. We are ready to pay when we can agree to an amount. Our Max offer is \$2MM or 151 BTC. If we can agree, we are ready to send funds to your wallet for the key.

игла не хочет, хочет 300 бтс
 "[lgla] doesn't want, he wants 300 BTC"

я молчу) решайте сами
 "I clam up, decide yourselves"

это те где 75 писем)
 "That's where we had 75 letters"

Angelica

Original chat log

2020-10-12 T14:00:47. 164657	stern@q3mcco35a uwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	вот анжелика написала "Angelica.com has written"
------------------------------------	----------------------------------	--	--

2020-10-12 T14:00:50. 687479	stern@q3mcco35a uwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	что ждет файлы "that she's waiting for files"
------------------------------------	----------------------------------	--	---

2020-10-12 T14:00:52. 349343	stern@q3mcco35a uwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	я им отправил "I've sent them"
------------------------------------	----------------------------------	--	--

2020-10-12 T14:00:55. 571969	stern@q3mcco35a uwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	и она будет думать "And she'll be thinking"
------------------------------------	----------------------------------	--	---

2020-10-12 T14:00:57. 941394	stern@q3mcco35a uwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	155 бтц "155 BTC"
------------------------------------	----------------------------------	--	-----------------------------

Clarus

Original chat log

2020-10-07 T17:20:24. 569243	professor@q3mcc o35auwcstmt.oni	stern@q3mcco35a uwcstmt.onion	а сколько ты у кларускорп запросил? "How much did you ask from Claruscorp.com for?"
------------------------------------	------------------------------------	----------------------------------	---

2020-10-07 T17:20:35. 450751	stern@q3mcco35a uwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	90 "90"
2020-10-09 T17:09:16. 059976	stern@q3mcco35a uwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	32 битка выплатили "32 btc were paid"
2020-10-09 T17:14:14. 476704	professor@q3mcc o35auwcstmt.oni on	stern@q3mcco35a uwcstmt.onion	Кларускорп? "Claruscorp.com?"
2020-10-09 T17:25:35. 361821	stern@q3mcco35a uwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	https://www.zoominfo.com/c/clarus-corporation/8373107
2020-10-09 T17:25:36. 580635	stern@q3mcco35a uwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	Да "yes"

Loomisco

Original chat log

2020-10-09 T02:23:55. 109922	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	Лумиус "Lumius"
2020-10-09 T02:23:57. 449112	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	Отписали "answered"
2020-10-09 T02:24:06. 225851	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	созвонились с ними по видео связи "We contacted via the video connection"
2020-10-09 T02:24:10. 718726	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	они поебали нам мозги "they f**ked our brains out"
2020-10-09 T02:24:12. 597009	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	18 бтс предложили "They offered 18 btc"
2020-10-09 T02:24:15. 276986	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	оборот у них 30 м "They have a turnover of 30 m"
2020-10-09 T02:24:19. 732654	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	лол блядь "Lol f**k"
2020-10-09 T02:24:25. 689126	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	4 раза созвнивались по видео "We had video calls 4 times"
2020-10-09 T02:24:31. 647346	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	и еще раз 30 блядь голосом просто "And 30 more using just f**king voicemail"

2020-10-09 T02:24:33. 313091	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	они заебали нас "They f**ked us"
2020-10-09 T02:24:40. 318706	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	пусть сдохнут суки "Let the b**ches dies"
2020-10-09 T02:24:47. 368322	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	мы весь менеджмент их ебем сейчас "We're f**king their whole management"
2020-10-09 T02:24:56. 175485	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	чтобы они поименно знали своих героев "So that they knew their heroes by name"
2020-10-09 T02:24:56. 989174	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	Суки "b**ches"
2020-10-09 T02:25:13. 697834	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	18 бтс лол блядь "18 btc lol f**k"
2020-10-09 T02:25:21. 238227	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	пусть платят миллионы суки "Let the b**ches pay millions"
2020-10-09 T02:25:33. 599429	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	у конторы "The firm"
2020-10-09 T02:25:35. 048909	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	с 30м "with 30 m"
2020-10-09 T02:25:39. 270050	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	миллионы есть блядь "They have millions f**k"
2020-10-09 T02:25:43. 638953	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	Миллионы" "Millions"
2020-10-09 T02:25:47. 219128	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	мы им это объясняем "We're explaining this to them"
2020-10-09 T02:25:49. 417814	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	а они нам угрожают "But they are threatening us"
2020-10-09 T02:25:54. 537782	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	что нас найдут потом "That they'll find us later"
2020-10-09 T02:25:56. 131228	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	Хахаха "haahaha"
2020-10-09 T02:26:00. 771306	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	ждем в гости блядь "Welcome f**ck"
2020-10-09 T02:26:07. 259655	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	18 бтс сраные "18 f**king btc"

2020-10-09 T02:26:10. 448963	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	в жопу пусть затолкают "shove it up their a*se"
2020-10-09 T14:36:43. 169505	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	нам звонят тишина в зале "They're calling us, silence in the hall"
2020-10-09 T14:36:44. 299071	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on))))))))) ")))))))))"
2020-10-09 T14:36:46. 018286	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	меня просят "They're asking me"
2020-10-09 T14:36:47. 409358	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	Послушать "To listen"
2020-10-09 T14:36:59. 729856	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	Ща "A sec"
2020-10-09 T14:37:01. 092631	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	подожди) "wait)"
2020-10-09 T14:37:33. 822583	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	Умоляют "They're begging"
2020-10-09 T14:37:35. 692259	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	ХАХАХАХАХАХ "НАНАНАНАНАН"
2020-10-09 T14:37:37. 528061	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	были угрозы "They were threatening"
2020-10-09 T14:37:39. 115212	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	а теперь умоляют "And now they're begging"
2020-10-09 T14:37:40. 825567	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	ХАХАХАХАХА "НАНАНАНАНАН"
2020-10-09 T14:37:43. 980384	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	короче хуй с ними "f**k them"
2020-10-09 T14:37:50. 705027	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	пусть платят скок есть "Let them pay what they have"
2020-10-09 T14:37:52. 083240	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	щас закинут "They'll transfer now"
2020-10-09 T14:37:58. 869611	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	75 бтс договорились "agreed on 75 btc"
2020-10-09 T14:38:11. 830697	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	с 30м сетки оч мало, но норм "From the 30 m network it's very little, but okay"

2020-10-09 T14:38:49. 143871	professor@q3mcc o35auwcstmt.oni on	target@q3mcco35 auwcstmt.onion	Отлично "excellent"
2020-10-09 T14:38:55. 399367	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	да хуйня "Fuck it"
2020-10-09 T14:38:56. 987152	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	сюр какой то "it's surreal"
2020-10-09 T14:39:03. 292689	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	Так "well"
2020-10-09 T14:39:05. 271048	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	хуй с ними "f**k them"
2020-10-09 T14:39:05. 813225	professor@q3mcc o35auwcstmt.oni on	target@q3mcco35 auwcstmt.onion	по чатам больше 30 бы не заплатили с таким ревенью "In chats they wouldn't pay more than 30 with such revenue"
2020-10-09 T14:39:08. 461581	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	ток настроенеи испортили "Just spoiled the mood"
2020-10-09 T14:39:17. 374546	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	да ебал я эти все чаты "f**k all this chats"
2020-10-09 T14:39:20. 701681	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	и спамеров ваших "And your spammers"
2020-10-09 T14:39:37. 348827	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	это все такой абсурд "All this is so absurd"
2020-10-09 T14:39:53. 619244	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	они угрожали операторам "They were threatening operators"
2020-10-09 T14:39:55. 334339	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	Запугивали "intimidating"
2020-10-09 T14:39:59. 059270	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	4 человека сдали нервы "4 people lost their nerves"
2020-10-09 T14:40:05. 160833	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	сказали давайте другие поговорят "And said others would talk instead"
2020-10-09 T14:40:08. 323544	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	а щас блядь умоляют "And now they're begging"
2020-10-09 T14:40:14. 713050	target@q3mcco35 auwcstmt.onion	professor@q3mcc o35auwcstmt.oni on	капитализм надо ебать "We should f**k capitalism"

2020-10-08 T20:35:53. 064599	target@q3mcco35a uwcstmt.onion	stern@q3mcco35au wcstmt.onion	loomisco бухгалтера, бенефит провайдеры, пейролл 55 серваков, около 200 ПК "Loomisco accountants, benefit providers, payroll 55 servers, about 200 PCs"
2020-10-08 T20:36:04. 940575	target@q3mcco35a uwcstmt.onion	stern@q3mcco35au wcstmt.onion	70 бтс выплатят сегодня "They'll pay 70 btc today"
2020-10-08 T20:36:34. 567889	target@q3mcco35a uwcstmt.onion	stern@q3mcco35au wcstmt.onion	это лок офиса в 10 утра) "This is office, lock (attack) at 10 am)"
2020-10-08 T20:38:30. 219307	target@q3mcco35a uwcstmt.onion	stern@q3mcco35au wcstmt.onion	правда операторы теперь спрашивают, зачем мы их так жестоко "But to tell the truth operators are now asking why we were that cruel"

Radial

Original chat log

2020-10-28 T19:06:12. 587809	target@q3mcco35a uwcstmt.onion	stern@q3mcco35au wcstmt.onion	локи есть "There're locks (successful attacks)"
2020-10-28 T19:06:13. 970841	target@q3mcco35a uwcstmt.onion	stern@q3mcco35au wcstmt.onion	крупные есть "There are large ones"
2020-10-28 T19:06:18. 914509	target@q3mcco35a uwcstmt.onion	stern@q3mcco35au wcstmt.onion	больницы локов штук 5-7 "There are about 5-7 locks of hospitals"
2020-10-28 T19:07:12. 264755	target@q3mcco35a uwcstmt.onion	stern@q3mcco35au wcstmt.onion	кто то предлагает 2м, игла просит 17 кто то предалгает 600к, игла просит 2м редиад в полной заднице, просим 1300 бтс, у них там все леглой, крупнейший екоммерс процессинг, по общению у них в жопе все "Somebody offers 2m, [Igl] asks for 17, someone offers 600k, [Igl] asks for 2m Radial is totally screwed, we're asking 1300 btc, everything has gone down there, the largest ecommerce processing, according to the conversation they're totally screwed"
2020-10-28 T19:07:15. 576827	target@q3mcco35a uwcstmt.onion	stern@q3mcco35au wcstmt.onion	пока так "That's it for now"
2020-10-28 T19:07:30. 192299	target@q3mcco35a uwcstmt.onion	stern@q3mcco35au wcstmt.onion	200 бтс выплатили на днях "They've paid 200 btc lately"
2020-10-25 T17:48:48. 985642	target@q3mcco35a uwcstmt.onion	troy@q3mcco35auw cstmt.onion	редиад должны суки выплтайть будут нормально "f**king Radial have to pay a lot"

2020-10-25 T17:48:52. 687555	target@q3mcco35a uwcstmt.onion	troy@q3mcco35auw cstmt.onion	это очень курпный процессинг "It's a large processing service"
2020-10-25 T17:48:52. 953754	troy@q3mcco35auw cstmt.onion	target@q3mcco35a uwcstmt.onion	Zaebis "f**king brilliant"
2020-10-25 T17:48:59. 856356	target@q3mcco35a uwcstmt.onion	troy@q3mcco35auw cstmt.onion	ну это не точно)))))) "I'm not completely sure"
2020-10-25 T17:49:01. 372103	target@q3mcco35a uwcstmt.onion	troy@q3mcco35auw cstmt.onion	Но "but"
2020-10-25 T17:49:05. 856879	target@q3mcco35a uwcstmt.onion	troy@q3mcco35auw cstmt.onion	у них выбора нет "They have no choice"
2020-10-25 T17:49:07. 492489	troy@q3mcco35auw cstmt.onion	target@q3mcco35a uwcstmt.onion)) "))"
2020-10-25 T17:49:09. 214076	target@q3mcco35a uwcstmt.onion	troy@q3mcco35auw cstmt.onion	они судя по диалогу "Judging from the dialogue"
2020-10-25 T17:49:11. 703493	target@q3mcco35a uwcstmt.onion	troy@q3mcco35auw cstmt.onion	встряли сильно "They're pretty much screwed"
2020-10-25 T17:49:16. 374487	target@q3mcco35a uwcstmt.onion	troy@q3mcco35auw cstmt.onion	и они идиоты "And they're idiots"
2020-10-25 T17:49:17. 379900	target@q3mcco35a uwcstmt.onion	troy@q3mcco35auw cstmt.onion	Спалились "Got busted"
2020-10-25 T17:49:27. 778821	target@q3mcco35a uwcstmt.onion	troy@q3mcco35auw cstmt.onion	сказав что они редиал "By saying they're Radial"
2020-10-25 T17:49:34. 666112	target@q3mcco35a uwcstmt.onion	troy@q3mcco35auw cstmt.onion	это одна из трастов "It is one of the trusts"
2020-10-25 T17:49:36. 703734	target@q3mcco35a uwcstmt.onion	troy@q3mcco35auw cstmt.onion	Там "there"
2020-10-25 T17:49:36. 872381	target@q3mcco35a uwcstmt.onion	troy@q3mcco35auw cstmt.onion	один из "It is"
2020-10-25 T17:49:42. 211004	target@q3mcco35a uwcstmt.onion	troy@q3mcco35auw cstmt.onion	там был на 300 "It was for 300"
2020-10-25 T17:49:45. 178192	target@q3mcco35a uwcstmt.onion	troy@q3mcco35auw cstmt.onion	а редиал сами на 900 "While Radial itself for 900"
2020-10-25 T17:49:51. 304703	target@q3mcco35a uwcstmt.onion	troy@q3mcco35auw cstmt.onion	это крупны йпроцессинг "It's a large processing service"

2020-10-25 T17:50:02. 391485	target@q3mcco35a uwcstmt.onion	troy@q3mcco35auw cstmt.onion	а щас стонут "and now they are moaning"
2020-10-25 T17:50:04. 207785	troy@q3mcco35auw cstmt.onion	target@q3mcco35a uwcstmt.onion	da znau bili drugie trasti "I know, there were other trusts (trust companies)"
2020-10-25 T17:50:12. 760969	troy@q3mcco35auw cstmt.onion	target@q3mcco35a uwcstmt.onion	18 shtuk ya videl "I've seen 18 items"
2020-10-25 T17:50:19. 873591	troy@q3mcco35auw cstmt.onion	target@q3mcco35a uwcstmt.onion	no popast ne smog "But I couldn't get in there"
2020-10-25 T17:50:31. 382709	troy@q3mcco35auw cstmt.onion	target@q3mcco35a uwcstmt.onion	prinyal reshenie ne tyanut "I've decided not to linger"
2020-10-25 T17:50:34. 738298	troy@q3mcco35auw cstmt.onion	target@q3mcco35a uwcstmt.onion	Postavili "So I did that"
2020-10-25 T17:50:47. 368332	target@q3mcco35a uwcstmt.onion	troy@q3mcco35auw cstmt.onion	ну метко поставили "You did it well"
2020-10-25 T17:50:54. 862362	target@q3mcco35a uwcstmt.onion	troy@q3mcco35auw cstmt.onion	редаил у меня проситли сделать "Radial asked me to do"
2020-10-25 T17:50:55. 770959	target@q3mcco35a uwcstmt.onion	troy@q3mcco35auw cstmt.onion	Хакеры "hacks"
2020-10-25 T17:50:56. 769102	target@q3mcco35a uwcstmt.onion	troy@q3mcco35auw cstmt.onion	под карты "For cards"
2020-10-25 T17:50:57. 958645	target@q3mcco35a uwcstmt.onion	troy@q3mcco35auw cstmt.onion	когда то "once"
2020-10-25 T17:51:03. 605149	target@q3mcco35a uwcstmt.onion	troy@q3mcco35auw cstmt.onion	и говорили "And they were saying"
2020-10-25 T17:51:10. 684020	target@q3mcco35a uwcstmt.onion	troy@q3mcco35auw cstmt.onion	что там ебать типо сетка веков может быть "what the f**king kind of network of ages could be there"
2020-10-25 T17:51:11. 296935	target@q3mcco35a uwcstmt.onion	troy@q3mcco35auw cstmt.onion	Лол "lol"
2020-10-25 T17:51:17. 352295	target@q3mcco35a uwcstmt.onion	troy@q3mcco35auw cstmt.onion	ну вот эта сетка "Here's this network"
2020-10-25 T17:51:25. 711276	target@q3mcco35a uwcstmt.onion	troy@q3mcco35auw cstmt.onion	в локе "In the lock (successful attack)"
2020-10-25 T17:51:29. 070443	target@q3mcco35a uwcstmt.onion	troy@q3mcco35auw cstmt.onion	судьба ее настигла "fate caught up with it"

2020-10-25 T17:51:29. 944021	target@q3mcco35a uwcstmt.onion	troy@q3mcco35auw cstmt.onion	с тобой "With you"
2020-10-25 T17:51:35. 656590	target@q3mcco35a uwcstmt.onion	troy@q3mcco35auw cstmt.onion	чему я и рад "And I'm happy about it"
2020-10-25 T17:51:38. 103146	troy@q3mcco35auw cstmt.onion	target@q3mcco35a uwcstmt.onion)) "))"
2020-10-25 T17:52:18. 288690	target@q3mcco35a uwcstmt.onion	troy@q3mcco35auw cstmt.onion	если все ок "If everything is okay"
2020-10-25 T17:52:21. 289110	target@q3mcco35a uwcstmt.onion	troy@q3mcco35auw cstmt.onion	поставите больничек "Provide hospitals"
2020-10-25 T17:52:21. 865156	target@q3mcco35a uwcstmt.onion	troy@q3mcco35auw cstmt.onion	штук 30 "30 items"
2020-10-25 T17:52:23. 584268	target@q3mcco35a uwcstmt.onion	troy@q3mcco35auw cstmt.onion	за неделю "Per week"
2020-10-25 T17:52:25. 576009	target@q3mcco35a uwcstmt.onion	troy@q3mcco35auw cstmt.onion	Лол "lol"
2020-10-25 T17:52:29. 195449	target@q3mcco35a uwcstmt.onion	troy@q3mcco35auw cstmt.onion	думаю будет эбс "I think it's going to be f**king great"
2020-10-25 T17:52:32. 772300	target@q3mcco35a uwcstmt.onion	troy@q3mcco35auw cstmt.onion	посмотрим) "We'll see"

SAI Global

Original chat log

2020-10-08 T02:09:58. 333429	target@q3mcco35a uwcstmt.onion	professor@q3mcco 35auwcstmt.onion	поэтому если сияглобал ответят "So if SAI Global answer"
2020-10-08 T02:10:01. 638123	target@q3mcco35a uwcstmt.onion	professor@q3mcco 35auwcstmt.onion	поставим им 10к битков "We'll provide 10k bitcoins"

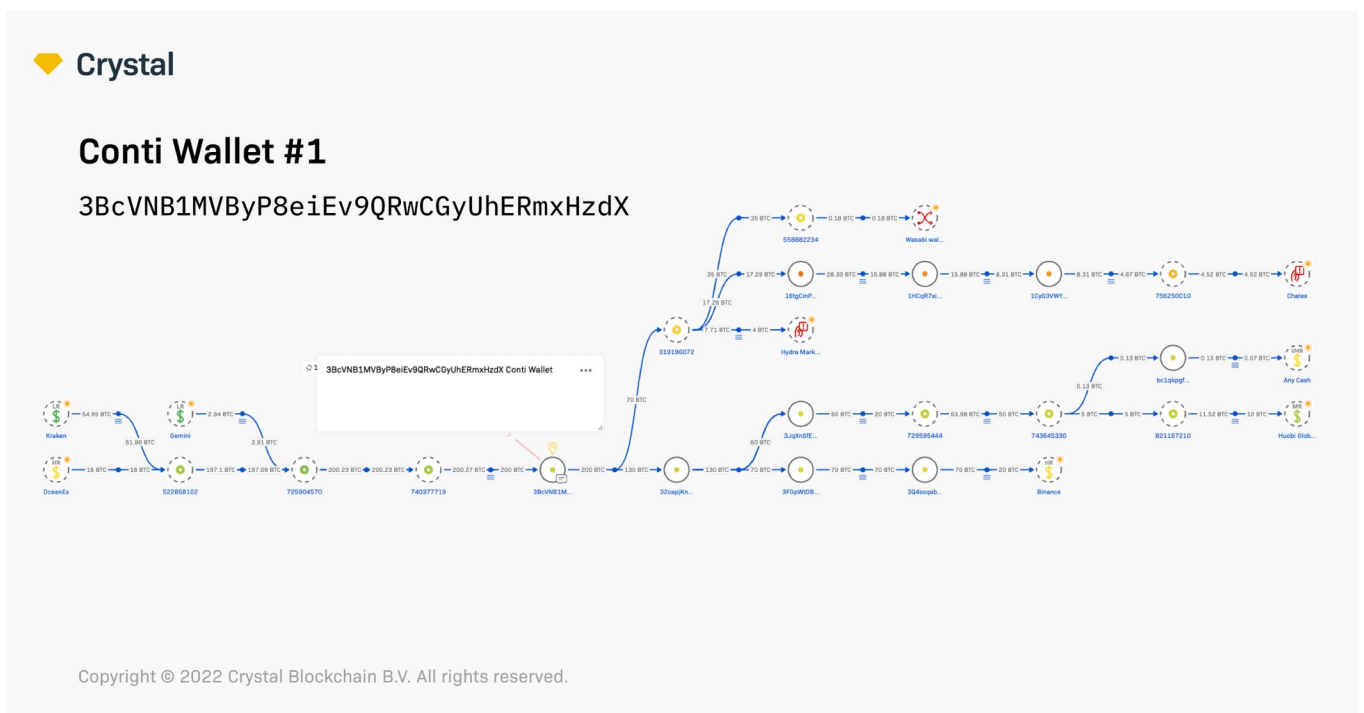
Connecting wallets to the ransomware attacks

Below are some of the largest crypto wallets we found involved in Conti attacks:

Conti Wallet #1

3BcVNB1MVByP8eiEv9QRwCGyUHERmxHzdX

In our research we noted that this wallet received 200 BTC from a "portfolio company".



Original chat log

2020-10-29 T21:25:42. 633100	target@q3mcco35a uwcstmt.onion	stern@q3mcco35au wcstmt.onion	стерн а что это за 3.8 бтс? "Stern what are the 3.8 btc?"
2020-10-29 T21:26:01. 987525	target@q3mcco35a uwcstmt.onion	stern@q3mcco35au wcstmt.onion	там нам выплатили 200 бтс, ты с них что то переводил? и что это за 3.8 бтс пришли или сколько там "We were paid 200 btc, have you transferred any of those? And what are the 3.8 btc I got or wahtever"
2020-10-29 T21:26:39. 794281	target@q3mcco35a uwcstmt.onion	stern@q3mcco35au wcstmt.onion	игла тебе 70 бтс перевел, это с них 3.8 бтс ? "[lgla] transferred you 70 btc, are the 3.8 btc from those?"
2020-10-29 T21:26:48. 486924	target@q3mcco35a uwcstmt.onion	stern@q3mcco35au wcstmt.onion	или с чего эти 3.8 не пойму просто "Or where are these 3.8 from I just can't understand"

2020-10-29 target@q3mcco35a stern@q3mcco35au
 T21:28:16. uwcstmt.onion wcstmt.onion
 233217

<https://www.blockchain.com/btc/address/3BcVNB1MVBYP8eiEv9QRwCGyUHERmxHzdX>
 это то что закинули портфели 200 бтс

"<https://www.blockchain.com/btc/address/3BcVNB1MVBYP8eiEv9QRwCGyUHERmxHzdX>
 This is what the portfolio company sent 200 btc"

Conti Wallet #2

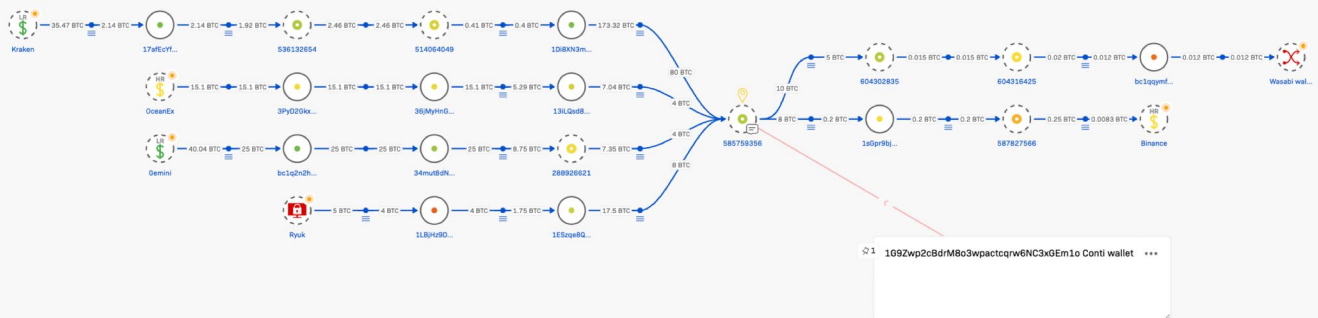
1G9Zwp2cBdrM8o3wpactcqrw6NC3xGEm1o

This wallet was confirmed to have been used for covering office expenses

Crystal

Conti Wallet #2

1G9Zwp2cBdrM8o3wpactcqrw6NC3xGEm1o



Copyright © 2022 Crystal Blockchain B.V. All rights reserved.

Original chat log

2020-07-16 target@q3mcco35a stern@q3mcco35au
 T17:42:58. uwcstmt.onion wcstmt.onion
 674757

сколько у тебя просить на июль, август и новый? не нравится мне это, мы давно обсуждали что офис должен себя окупать сам и по объектам способны это делать, а не лезть в карманы к нам
 "How many times should I ask you for the funds for July, August and the new one? I don't like it, we discussed a long time ago that the office should pay off itself and people on places should be able to do so, instead of getting into our pockets"

2020-07-16 target@q3mcco35a stern@q3mcco35au
 T17:45:27. uwcstmt.onion wcstmt.onion
 913159

решай сам, поинтересуйся у ребят, может там что то выстрелило или выстрелит уже "сейчас"
 "Decide yourself, ask the guys if there's been any success or if it will be "now""

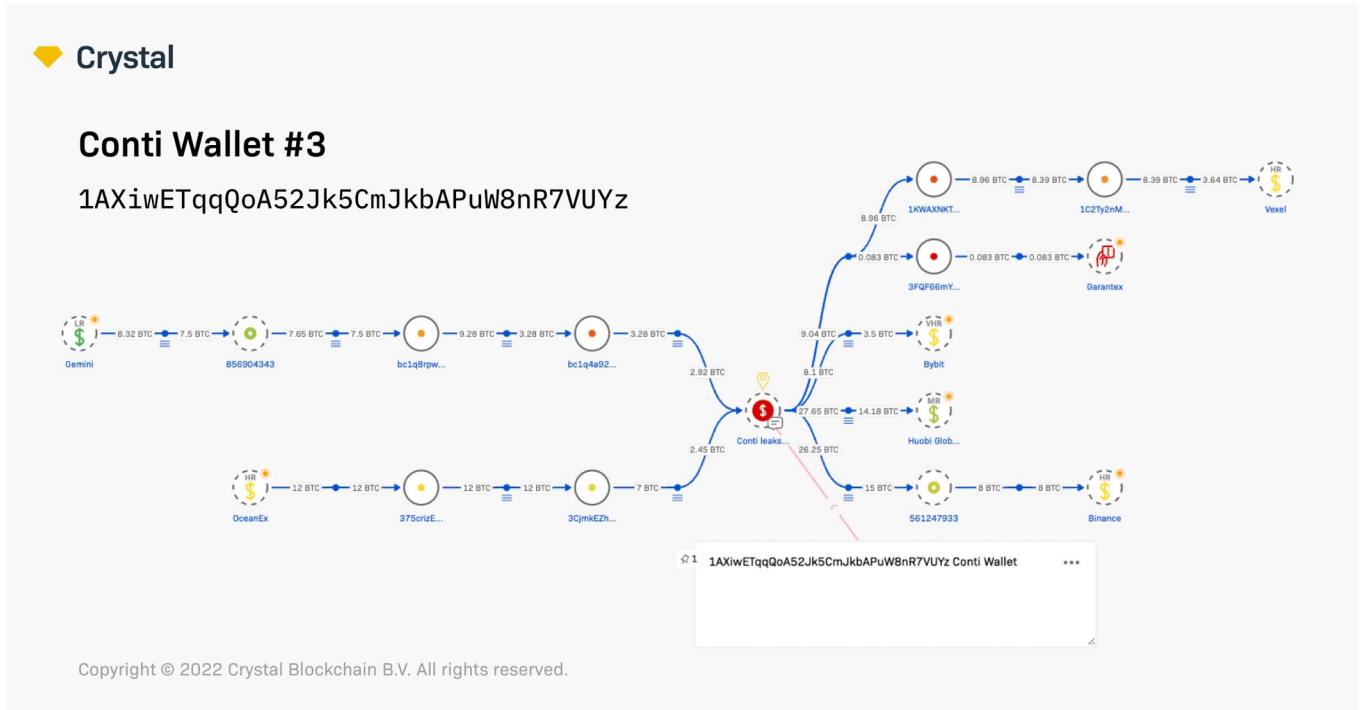
2020-07-16 target@q3mcco35a stern@q3mcco35au
 T17:45:37. uwcstmt.onion wcstmt.onion
 180969

кошелек тот же
1G9Zwp2cBdrM8o3wpactcqrw6NC3xGEm1o
 "The same wallet 1G9Zwp2cBdrM8o3wpactcqrw6NC3xGEm1o"

Conti Wallet #3

1AXiwETqqQoA52Jk5CmJkbAPuW8nR7VUYz

This wallet is confirmed to have received a percentage of funds from various attacks.



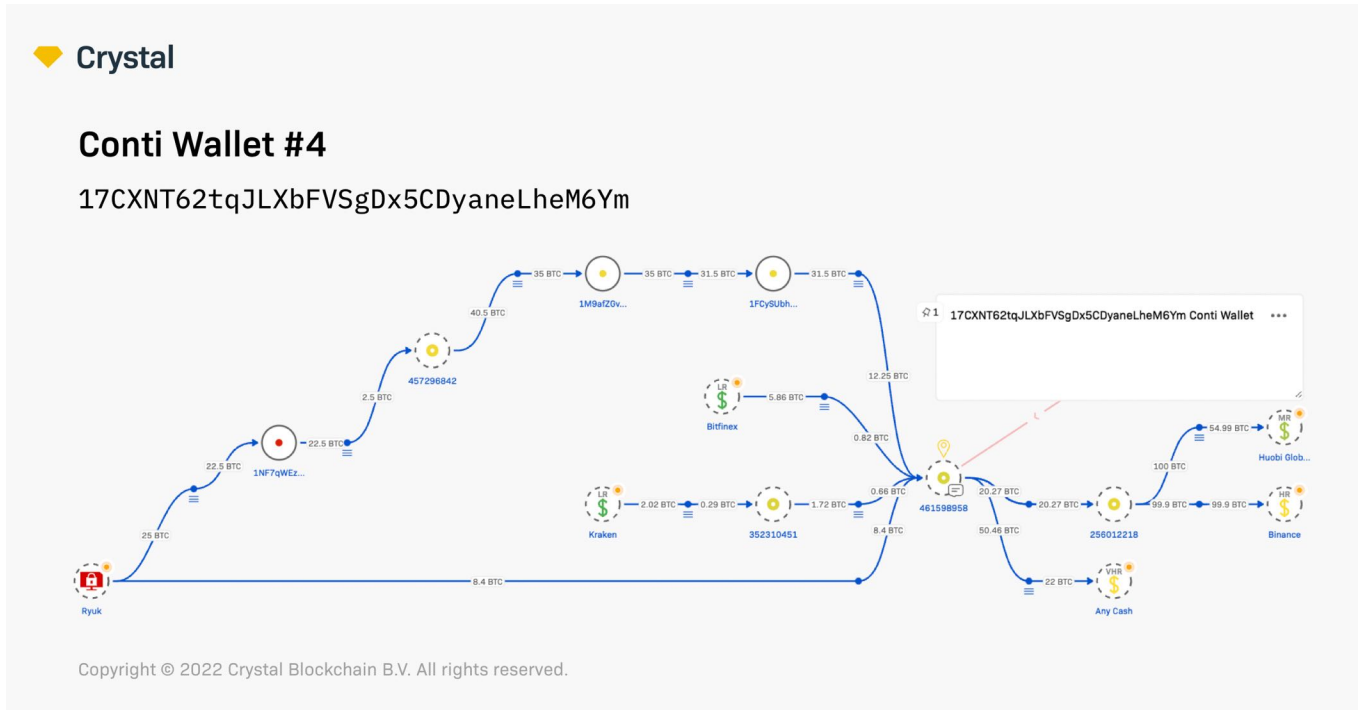
Original chat log

185.25.51.173-2 0210507.json	2021-05-07 T12:57:09. 894275	bentley@q3mcco3 5aucstmt.onion	stern@q3mcco35a uwcstmt.onion	Понял. Куда закинуть что мне пуля вчера скинул? "I see. Where should I transfer the money [Pulya]transferred to me yesterday?"
185.25.51.173-2 0210507.json	2021-05-07 T12:57:28. 860578	stern@q3mcco35a uwcstmt.onion	bentley@q3mcco3 5aucstmt.onion	1AXiwETqqQoA52Jk5CmJkbAPuW8nR7VUYz "1AXiwETqqQoA52Jk5CmJkbAPuW8nR7VUYz"

Conti Wallet #4

17CXNT62tqJLXbFVSGDx5CDyaneLheM6Ym

This wallet is confirmed to have received a percentage of funds from various attacks.



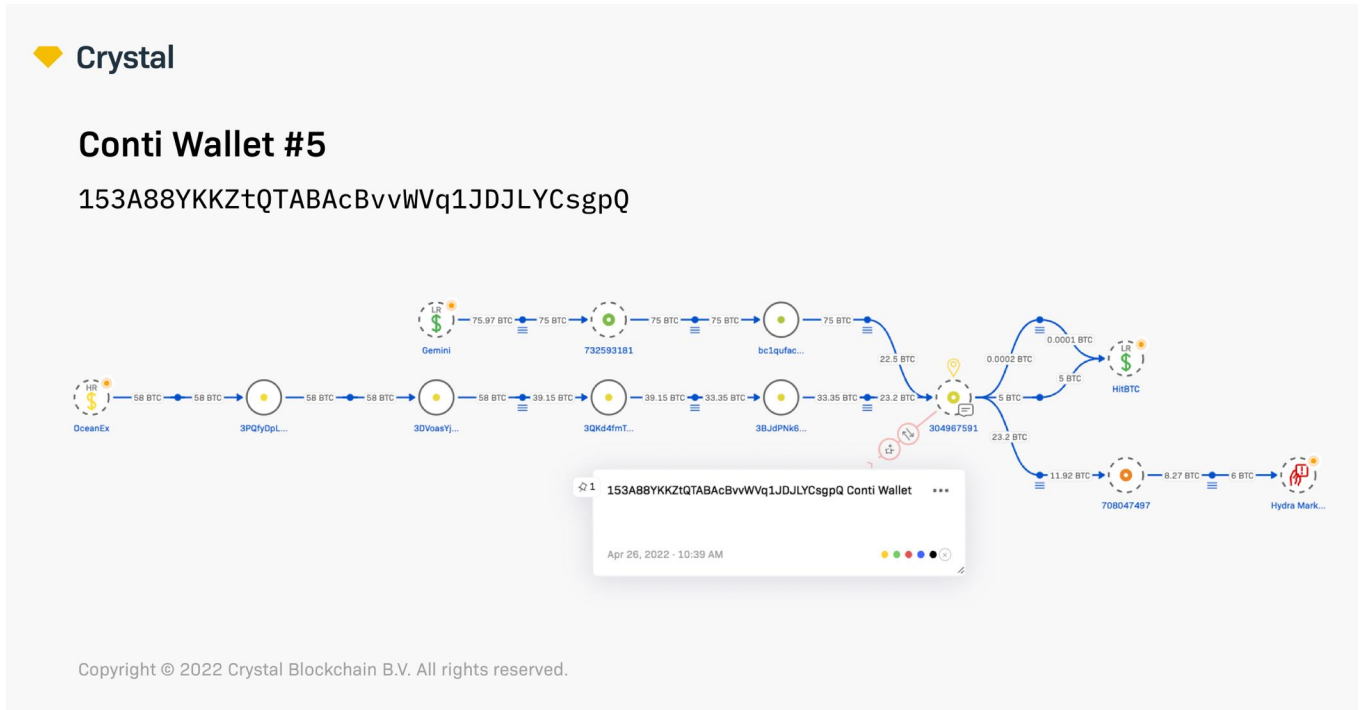
Original chat log

2020-07-04 T10:56:20. 705349	logan@q3mcco35au wcstmt.onion	stern@q3mcco35au wcstmt.onion	17CXNT62tqJLXbFVSGDx5CDyaneLheM6Ym актуальный? "17CXNT62tqJLXbFVSGDx5CDyaneLheM6Ym relevant?"
2020-07-04 T10:56:32. 737934	logan@q3mcco35au wcstmt.onion	stern@q3mcco35au wcstmt.onion	денег хотел выдать "Wanted to send money"

Conti Wallet #5

153A88YKKZtQTABAcBvvWVq1JDJLYCsgpQ

This wallet is confirmed to have received a percentage of funds from various attacks.



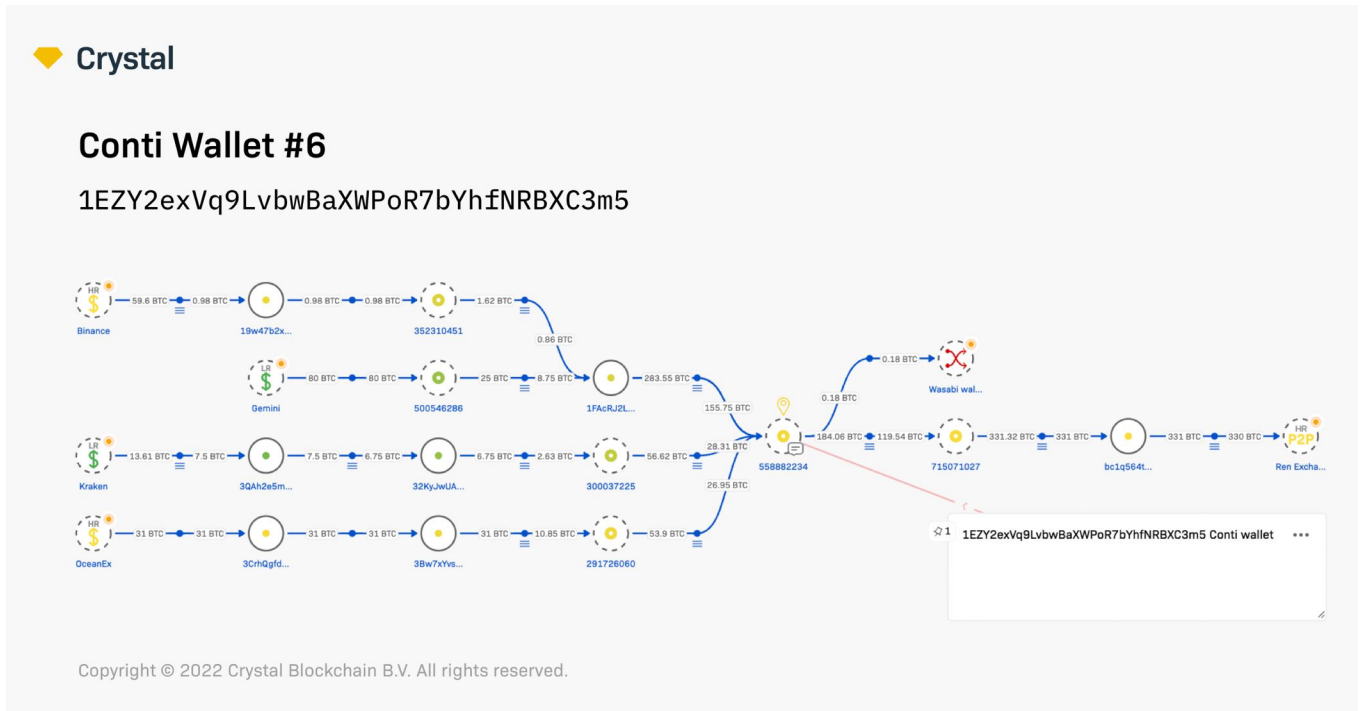
Original chat log

2020-10-09 T17:17:19. 985410	stern@q3mcco35au wcstmt.onion	target@q3mcco35a uwcstmt.onion	в итоге весь цикл замкнулся "As a result the whole cycle closed"
2020-10-09 T17:18:42. 462447	stern@q3mcco35au wcstmt.onion	target@q3mcco35a uwcstmt.onion	153A88YKKZtQTABAcBvvWVq1JDJLYCsgpQ 30%, это мне и решаеву "30% is for me and [Reshaev]"

Conti Wallet #6

1EZY2exVq9LvbwBaXWPoR7bYhfNRBXC3m5

We know that this wallet received a percentage of funds from various ransom attacks, and the majority of its funds were moved to RenBTC and were then swapped for ETH.



Original chat log

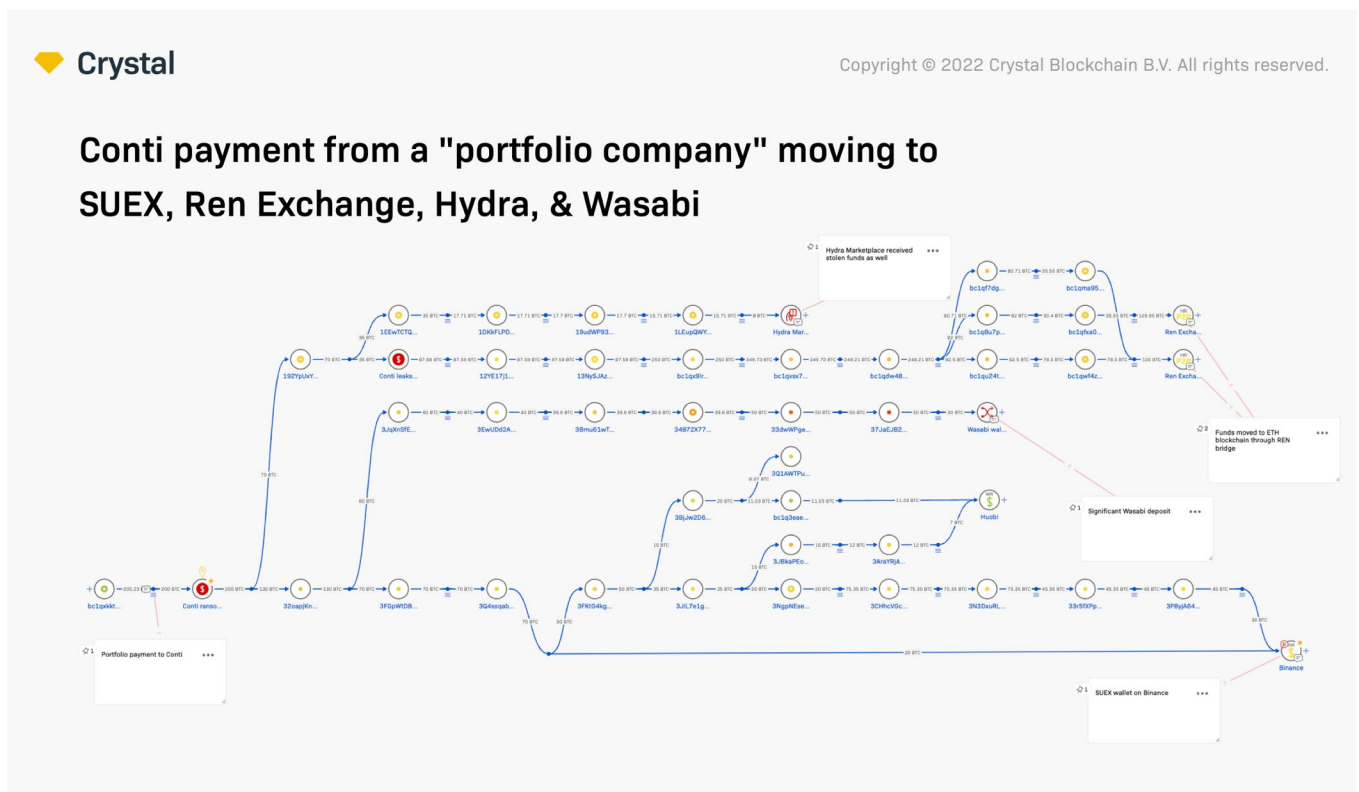
2020-10-23 T15:23:33. 869896	target@q3mcco35a uwcstmt.onion	stern@q3mcco35au wcstmt.onion	[16:33:30] <bob> tam viplatili odni, 22btc "Someone has paid, 22 btc"
2020-10-23 T15:23:40. 703019	target@q3mcco35a uwcstmt.onion	stern@q3mcco35au wcstmt.onion	вот этот еще "This one as well"
2020-10-23 T15:23:46. 044397	target@q3mcco35a uwcstmt.onion	stern@q3mcco35au wcstmt.onion	выплатил) "Has paid)"
2020-10-23 T15:34:47. 217704	stern@q3mcco35au wcstmt.onion	target@q3mcco35a uwcstmt.onion	Да "yes"
2020-10-23 T15:34:48. 793032	stern@q3mcco35au wcstmt.onion	target@q3mcco35a uwcstmt.onion	дай кош "Give me a wallet"
2020-10-23 T15:46:13. 157697	target@q3mcco35a uwcstmt.onion	stern@q3mcco35au wcstmt.onion	1EZY2exVq9LvbwBaXWPoR7bYhfNRBXC3m5 "1EZY2exVq9LvbwBaXWPoR7bYhfNRBXC3m5"

2020-10-23 T15:46:20. 605660	target@q3mcco35a uwcstmt.onion	stern@q3mcco35au wcstmt.onion	Крупных "Large ones"
2020-10-23 T15:46:22. 449318	target@q3mcco35a uwcstmt.onion	stern@q3mcco35au wcstmt.onion	штук 25 новых "About 25 new ones"
2020-10-23 T15:46:23. 539315	target@q3mcco35a uwcstmt.onion	stern@q3mcco35au wcstmt.onion	Суммарно "In total"
2020-10-23 T15:46:24. 549859	target@q3mcco35a uwcstmt.onion	stern@q3mcco35au wcstmt.onion	за неделю "Per week"
2020-10-23 T15:46:26. 615601	target@q3mcco35a uwcstmt.onion	stern@q3mcco35au wcstmt.onion	от 1 млрд "From 1 mlrd"
2020-10-23 T15:46:28. 456901	target@q3mcco35a uwcstmt.onion	stern@q3mcco35au wcstmt.onion	300-500 мл "300-500 ml"

Confirmed crypto payments made by companies to the Conti group

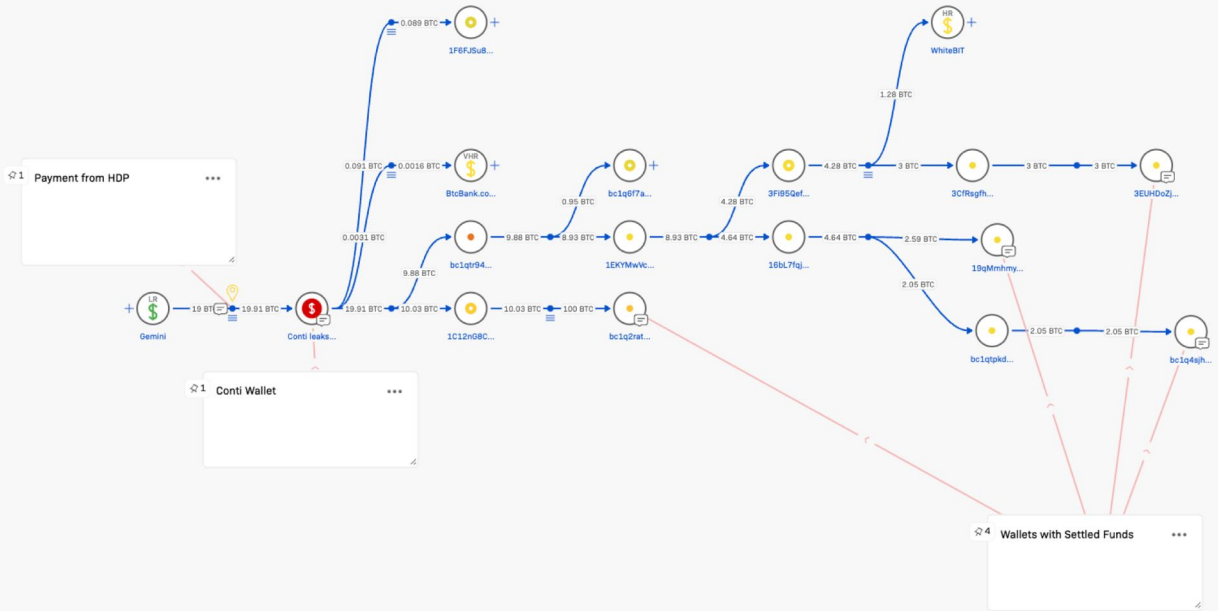
In the below visualization from Crystal's platform, we can see a payment being made by a "portfolio company", with the funds then moving to Suex (the blocklisted Russian exchange that nested services on Binance), to **Hydra Darkmarket**, to **Ren exchange**, and to **Wasabi** mixer.

Regarding Suex, as reported by CNBC: "The Treasury alleged that the crypto exchange Suex 'has facilitated transactions involving illicit proceeds from at least eight ransomware variants.'"



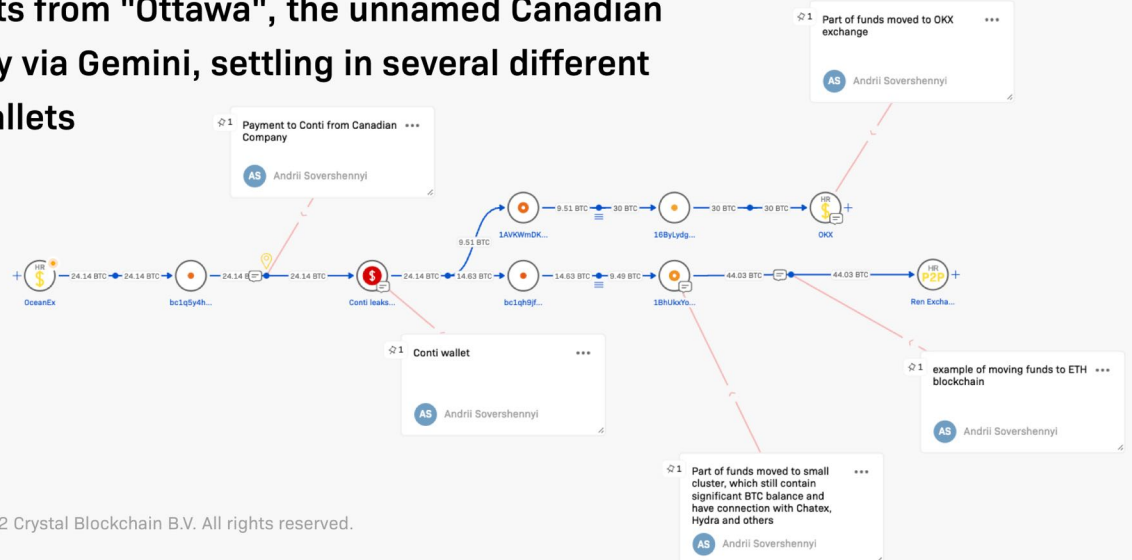
Below we can see a transfer of funds from "HDP" to the Conti group on May 4, 2022, which then moved to **OKX exchange** (formerly OKEx), and then the Conti group crossed chains from Bitcoin (BTC) to Ethereum (ETH) where the funds moved to **Ren exchange**.

HDP transfer of funds to the Conti group on May 4, 2022, then moving to OKX, and cross-chain BTC/ ETH to Ren



In the below visualization, we can see payments from "Ottawa" (a Conti nickname for the unnamed Canadian company) that transferred funds to the criminal group via Gemini, with several transactions then "settling" in various different Conti wallets

Payments from "Ottawa", the unnamed Canadian company via Gemini, settling in several different Conti wallets



The lack of ransomware reporting due to the stigma attached

The sheer scale of Conti's activity is remarkable; the lack of humanity in its selection and the pursuit of victims is deplorable. But what's key to note is the overwhelming majority of Conti attacks were not public, with business owners potentially preferring to hide the ransom attack from their shareholders or other interested people. These businesses may not intentionally be supporting Conti, but they aren't stopping the cycle.

We need more focus on the services that may inadvertently support groups like Conti. Does your compliance policy require outbound transaction screening, and do you seek to understand the business nature of the transaction? Here are a few red flags to consider if a business may be paying a ransom. Practically speaking, this means finding additional information about the purpose or nature of a transaction:

- ◆ Is there a large purchase of cryptocurrency by an organization or individual with no obvious purpose or against the typical business model of the organization?
- ◆ Are there media reports of a cyber attack against a business, either named directly or from the same region or industry? (This could also take the form of claims of an attack by a group against the business, prolonged service outages, or breach notification.)
- ◆ Has there been any leak of the company's sensitive information online? These are usually held in specific forums or message boards, however often security researchers will post about these on social media platforms.

We'll discuss the stigma attached to ransomware reporting in our next webinar, "The Conti Leaks & Crypto-Ransomware Reporting, on June 9, 2022, at 2:00 pm CET and why we think it's important that we work to remove reputational issues so that more companies can come forward and report the attack, so more criminals can be caught. [**Register for the webinar here.**](#)

In the Conti Leaks: Part 3, we'll give insights into the level of work put into making this group seem like a legitimate business, from company numbers and salaries and where they sourced their hires, to office setup and how they may have conned unaware employees eg. developers into doing ransomware work unbeknownst to themselves.














To find out more about our research or to get in touch about your own case you can contact Crystal's investigations team at [**investigations@crystalblockchain.com**](mailto:investigations@crystalblockchain.com)





















In case you missed it... [**The Conti Leaks Part One: A Modern Criminal Network Unveiled**](#)





















Appendix






















NOTE: The below tables show **89 companies mentioned by name by the Conti Group** in their chat logs (there were likely more attempts on more companies on further research, below are the company names we could verify for now). Crystal observed that of the 89 named companies revealed in the chat logs, **76 are US-based, six are Canada-based, one is UK-based, one in Scotland, one in Australia, one in Saudia Arabia, one in France, and one is based out of China.**




US-based Companies

	Company	Industry	Location	Revenue
	<u>Defender Marine</u>	Marine Outfitter	Waterford, Connecticut	<u>\$68 Million</u>
	<u>Help at Home</u>	Homecare	Chicago, Illinois	<u>\$2 Billion</u>
	<u>Angelica</u>	Textile	Chicago, Illinois	<u>\$300 Million</u>
	<u>Aspen Pointe</u>	Healthcare	Colorado Springs, Colorado	<u>\$73 Million</u>
	<u>Astronautics</u>	Aviation Manufacturing	Milwaukee, Wisconsin	<u>\$307 Million</u>
	<u>Atlanta Housing</u>	Real-estate	Atlanta, Georgia	<u>\$147 Million</u>
	<u>Bretzrv</u>	Car Dealership	Boise, Idaho	<u>\$70 Million</u>
	<u>Broe</u>	Real-estate	Denver, Colorado	<u>\$600 Million</u>
	<u>Career Builder</u>	Human Resources	Chicago, Illinois	<u>\$837 Million</u>
	<u>Clarus Corp</u>	Manufacturing	Salt Lake City, Utah	<u>\$333 Million</u>
	<u>eCampus</u>	Education/ Retail	Lexington, Kentucky	<u>\$54 Million</u>
	<u>Flemington</u>	Dealership	Flemington, New Jersey	<u>\$147 Million</u>
	<u>Hallag</u>	Facility Management	Kerman, California	<u>\$4.2 Million</u>














Company	Industry	Location	Revenue	
 PIPER LOGISTICS	<u>Piper Logistics</u>	Logistics	Indianapolis, Indiana	<u>\$5 Million</u>
 WESTERN OVERSEAS CORPORATION	<u>Western Overseas</u>	Logistics	Cypress, California	<u>\$37 Million</u>
 Capitol Cable Communications, Inc.	<u>Capitol Cable</u>	Design & Consulting Services	Marlboro, Maryland	<u>\$5 Million</u>
 KRUSECOM	<u>Krusecom</u>	IT	Palm Beach, Florida	<u>\$5 Million</u>
 pillar	<u>Pillar Support</u>	Healthcare	Crestwood, Kentucky	<u><\$5 Million</u>
 Sam's Furniture - Appliances - Mattresses	<u>Sams Furniture</u>	Retail	Arlington, Texas	<u>\$10 Million</u>
 Credit One Bank	<u>Credit One Bank</u>	Banking	Las Vegas, Nevada	<u>\$223 Million</u>
 GREAT FALLS PDS GREAT FALLS, MONTANA	<u>Great Falls Public Schools</u>	Education	Great Falls, Montana	<u>\$115,957,403</u>
 Agricultural Hall An Urban Agriculture Supply & Resource Center	<u>Aghall</u>	Agriculture	Jamaica Plain, Massachusetts	<u><\$5 Million</u>
 HistoTrac AUTOMATING YOUR LABORATORY	<u>Histotrac</u>	Software	Reston, Virginia	<u><\$5 Million</u>
 MID OCEAN Partners	<u>MidOcean Partners</u>	Financial Services & Investments	New York City, New York	<u>\$58 Million</u>
 network capital	<u>Network Capital</u>	Financial services	Miami, Florida	<u>\$71 Million</u>
 Rowmark	<u>Rowmark</u>	Manufacturing	Findlay, Ohio	<u>\$35 Million</u>
 SHOOK CONSTRUCTION	<u>Shook Construction</u>	Construction	Moraine, Ohio	<u>\$222 Million</u>
 SKY LAKES MEDICAL CENTER	<u>Skylakes</u>	NGOs	Klamath Falls, Oregon	<u>not-for-profit, community-owned</u>
 Steelcase	<u>Steelcase</u>	Manufacturing	Grand Rapids, Michigan	<u>\$2 Billion</u>
 Stockton	<u>Stockton</u>	Education	Stockton, Missouri	<u>not-for-profit, community-owned</u>
 SYKES	<u>Sykes (previously Alpine Access)</u>	Human Resources & Marketing	Tampa, Florida	<u>\$9 Billion</u>
 UHS	<u>Uhsinc</u>	Healthcare	King of Prussia, Pennsylvania	<u>\$12 Billion</u>
 LifeQuotes.com Over 400,000 Customers Insured	<u>Lifequotes</u>	Insurance services	Darien, Illinois	<u>\$14 Million</u>

Company	Industry	Location	Revenue
 THE LOOMIS COMPANY	<u>Loomisco</u>	Insurance services	Wyomissing, Pennsylvania <u>\$38 Million</u>
	<u>Northtown Auto</u>	Retail	Amherst, New York <u>\$153 Million</u>
	<u>Panavision</u>	Manufacturing	Los Angeles, California <u>\$328 Million</u>
	<u>Qmix</u>	Entertainment	Columbus, Indiana <u>\$19 Million</u>
	<u>Seacoast Security</u>	Electrical work and services	West Rockport, Maine <u>\$20 Million</u>
	<u>Tampa Bay Times</u>	News Services	Petersburg, Florida <u>\$156 Million</u>
	<u>System Technology inc.</u>	Technology manufacturing	Joliet, Illinois <u><\$5 Million</u>
	<u>Watermark Communities</u>	Healthcare & Retirement facilities	Tucson, Arizona <u>\$111 Million</u>
	<u>Western News</u>	News Services	Prescott Valley, Arizona <u>\$50 Million</u>
	<u>Broe</u>	Real-estate	Denver, Colorado <u>\$76 Million</u>
	<u>Calahan Law</u>	Law	Baton Rouge, Louisiana <u><\$5 Million</u>
	<u>CAO Group</u>	Software & Services	West Jordan, Utah <u>\$9 Million</u>
	<u>Chefs Produce</u>	Food Wholesaler	Dallas, Texas <u>\$81 Million</u>
	<u>Conn-Selmer</u>	Manufacturing and Retail	Elkhart, Indiana <u>\$301 Million</u>
	<u>DHastings</u>	Logistics	Laredo, Texas <u>\$22 Million</u>
	<u>Exide</u>	Technology	Alpharetta, Georgia <u>\$3 Billion</u>
	<u>Fresno Equipment</u>	Heavy-duty vehicle retail	Fresno, California <u>\$30 Million</u>
	<u>Geogroup</u>	Human resources	Boca Raton, Florida <u>\$2 Billion</u>
	<u>Homtex</u>	Textile	Cullman, Alabama <u>\$32 Million</u>
	<u>Merieux Nutrisciences</u>	Consultancy Services	Chicago, Illinois <u>\$1 Billion</u>

Company	Industry	Location	Revenue	
 NORTHERN TRUST	<u>Northern Trust</u>	Financial Services	Chicago, Illinois	<u>\$6 Billion</u>
 quench	<u>Quench Water</u>	Retail Services	King of Prussia, Pennsylvania	<u>\$68 Million</u>
 RIDGEVIEW You Matter Here	<u>Ridgeview Medical</u>	Healthcare	Arlington, Minnesota	<u>\$323 Million</u>
 SCHMIDT ELECTRIC	<u>Schmidt-Electric</u>	Technology Services	Katy, Texas	<u><\$5 Million</u>
 Radial a bpost company	<u>Radial.com</u>	Entertainment	King of Prussia, Pennsylvania	<u>\$1 million</u>
 MUELLER, INC. METAL BUILDINGS, ROOFING & COMPONENTS	<u>Mueller Inc</u>	Building & Roofing	Ballinger, Texas	<u>\$203 Million</u>
 Foursquare HEALTHCARE	<u>Foursquare Healthcare</u>	Healthcare	Dallas, Texas	<u>\$27.95 million</u>
 B:OMARIN	<u>Biomarin</u>	Pharmaceuticals	San Rafael, California	<u>\$1 Billion</u>
 Cheney Brothers <small>C-B-I</small>	<u>Cheney Brothers</u>	Foodservice Distributor	Florida	<u>\$2 Billion</u>
 APPLIED CONSULTANTS, INC.	<u>Applied Consultants</u>	Energy	Longview, Texas	<u>\$179 Million</u>
 CONCENTRIX CONVERGYS	<u>Concentrix</u>	Consultancy	Cincinnati, Ohio	<u>\$2.951 billion</u>
 Nexstar MEDIA GROUP, INC.	<u>Nexstar</u>	Entertainment	Irving, Texas	<u>\$4 Billion</u>
 SCOTT J. CORWIN A PROFESSIONAL LAW CORPORATION	<u>SJC Law</u>	Law	Los Angeles, California	<u><\$5 Million</u>
 THE MONEY STORE	<u>The Money Store</u>	Financial Services	Florham Park, New Jersey	<u>\$49 Million</u>
 network capital.	<u>Network Capital</u>	Financial Services	Irvine, California	<u>\$191 Million</u>
 Pac-Van 	<u>Pac-Van</u>	Logistics	Indianapolis, Indiana	<u>\$66 Million</u>
 Siegfried	<u>Siegfried Group</u>	Human Resources	Wilmington, Delaware	<u>\$218 Million</u>
 ADVANCE TABCO SMART FABRICATION	<u>Advance Tabco</u>	Retail / Manufacturing	Jackson, Georgia	<u>\$48 Million</u>
 NVIDIA A Mellanox	<u>Mellanox</u>	Semiconductors	Austin, Texas	<u>\$1.33 Billion</u>
 NEW CASTLE BUILDING PRODUCTS	<u>Ncbp</u>	Construction	White Plains, New York	<u>\$69 Million</u>

Company	Industry	Location	Revenue
 PayneWest	Insurance	Billings, Montana	\$84 Million
 Verdin	Technology manufacturing	Cincinnati, Ohio	\$21 Million
 Tomholzerford	Car dealerships	Farmington, Michigan	\$22 Million

Other Regions

Company	Industry	Location	Revenue
 Nasscaff	Construction	Saudi Arabia	\$6 Million
 Saiglobal	Consultancy	Sydney, New South Wales, Australia	\$416 Million
 Smiths	Technology manufacturing	London, United Kingdom	\$3 Billion
 Arneg	Manufacturing	Quebec, Canada	\$24 Million
 Soprasteria	Technology Services	Paris, France	\$4 Billion
 TMS Direct	Retail	Glasgow, Scotland	<\$5 Million
 Esfox	Construction	Niagara Falls, Ontario, Canada	\$636 Million
 Hull and Hull	Law	Toronto, Ontario, Canada	\$53 Million
 Hikvision	Technology manufacturing	Hangzhou, Zhejiang, China (Global)	\$12 Billion
 Rdi marketing	Marketing / Services	Richmond, Victoria, Australia	\$5 Million
 Evertz	Technology Manufacturing	Burlington, Ontario, Canada	\$307 Million
 Softub Canada	Manufacturing & Distribution	Greater Sudbury, Ontario, Canada	<\$5 Million
 Transbec	Autoparts	Québec, Canada	\$21 Million

Disclaimer

Information presented does not constitute legal advice. Crystal Blockchain B.V. accepts no responsibility for any information contained herein and disclaims and excludes any liability in respect of the contents or for action taken based on this information

Yours in analytics,
The Crystal Blockchain Team

Email: enterprise@crystalblockchain.com, contact@crystalblockchain.com, investigations@crystalblockchain.com

Facebook: <https://www.facebook.com/CrystalBlockchainAnalytics>

Twitter: <https://twitter.com/CrystalPlatform>

Crystal is the world-leading all-in-one blockchain analytics tool for crypto AML compliance, providing blockchain analytics and crypto transaction monitoring for thousands of cryptocurrencies in real-time.

Crystal Blockchain works globally with customers in the digital asset industry, the banking, and FI sectors. We help streamline their Know Your Transaction (KYT) and Anti-Money Laundering (AML) procedures for meeting international compliance standards.

Available as a free demo version, SaaS, API, and for on-premise installation. Engineered by Bitfury.