



CONTI Modus Operandi and Bitcoin Tracking

February 2021
TLP:WHITE

(c) All rights reserved to ClearSky Cyber Security & Whitestream Ltd. 2021

Table of Contents

Exposing and Analyzing Negotiations with the CONTI Group and Wallets Associated with the Ransomware	3
Preface	3
Short Background on the Conti Ransomware Group	3
Locating and Accessing the Negotiations	5
Background	5
Analyzing the Correspondence	6
Blockchain Analysis	13
Analysis of the CONTI Ransomware's Affiliate Bitcoin Wallet	13
Blockchain analysis reveals the connection between CONTI and Ryuk.	13
Deposits from CONTI affiliate wallets to Binance (China)	14
CONTI affiliate sent \$93,000 to the Binance.com platform.	14
Deposits from CONTI affiliate wallets to Rocketr.net	16
CONTI affiliate sent \$27,500 to the Rocketr.net platform.	16
Conti – Negotiations Text Version	17

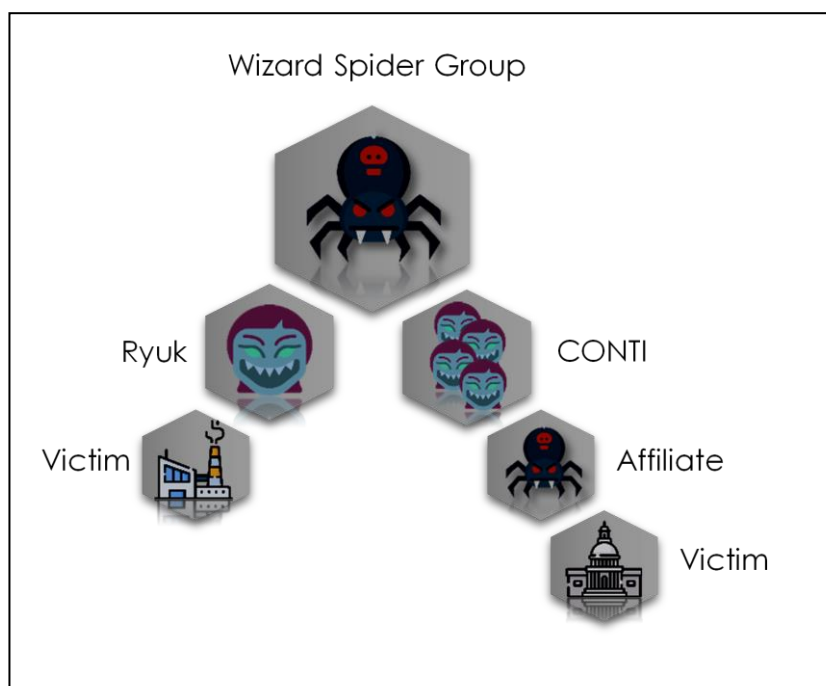
Exposing and Analyzing Negotiations with the CONTI Group and Wallets Associated with the Ransomware

Preface

During our routine monitoring of ransomware groups, we detected a sample of the CONTI ransomware uploaded to Virus Total from Canada. **ClearSky** and **Whitestream** were able to access the entire negotiation process between the company and the extortion group in real time by analyzing the sample. Furthermore, we succeeded in following the ransom payment, tracking all of the involved bitcoin blockchain transactions. The revealed bitcoin transactions allowed us to associate CONTI with Wizard Spider, as Ryuk was previously associated with the group. This association confirms the common theory that CONTI and Ryuk are connected. Following the negotiations closely assists in learning how to properly engage with the attackers, managing the most sensitive part of a ransomware attack.

Short Background on the Conti Ransomware Group

Originated by the 'Wizard Spider' Russian hacking group, CONTI ransomware is an evolution of one of the group's most successful ransomware – Ryuk. CONTI is a more accessible version of Ryuk, built for distribution by affiliates in a 'Ransomware as a service' model. CONTI ransomware was first spotted by cybersecurity teams in May 2020 and claim to have over 150 successful extortion attacks by the end of 2020, with at least \$20M in revenues paid by the victims.



During our routine monitoring of ransomware groups, we detected a sample of CONTI ransomware uploaded to Virus Total from Canada. From analyzing the sample, we were able to track all negotiations between the company and the extortion group. Furthermore, we succeeded in following the bitcoin transactions of the paid ransom.

We estimate that during the coming months many companies will be targeted by this group, suggesting that analyzing the negotiations, as an indication to CONTI's behavioral patterns, should prove beneficial when facing future attacks. Analyzing the sample allowed us to reach CONTI's website, in which the attackers were negotiating with a victim in real time (a Canadian energy company).

This article surveys and analyses the correspondence, providing insights regarding some of the negotiation methods employed. It is apparent that the Canadian company was initiated represented by an executive, who was replaced after approximately 6 days by a professional negotiator who led the communication towards an agreement.

We have several insights from the correspondence. We want to thank **Moty Cristal from NEST**, who reviewed and added insights:

- **The blackmailer uses service-oriented rhetoric, attempting to create a false pretense of a supplier and customer debating a legitimate deal:** the attacker addresses the victim as “customer”, and themselves as “support”. The attacker presents the attack as an issue that arose regardless of their illegitimate involvement, with them offering security and decryption services. The attacker leads the victim to a user interface that seems professionally established for customer management and support.
- **Clear negotiation rhetoric:** both the attacker and the victim are skilled and professional negotiation personnel, exhibiting experience in engaging with this sort of correspondence. Both sides speak “negotiations” fluently while respecting the conversation's limits and rules. The negotiations language is completely business-oriented, aiming to close a deal expeditiously. A pattern which is commonly seen by “Ivy league” attack groups: structured, reputational, technologically advanced and ransom-industry oriented.
- **The necessity of haggling:** like in other businesses, the attacker sets a high-impossible payment (“anchoring”) requirement as negotiations initiate. However, during the correspondence the attacker lowers the price, showing flexibility towards the victim. It is safe to assume that the attackers know what the organization can afford before negotiations begin, considering the extent of intelligence gathering that commonly precedes targeted ransomware attacks (including the organization's size and income). As the correspondence begins, it is apparent that the negotiator representing the victim is aware of the attackers' methods, as they request the documents used to calculate the ransom. It is inevitable that in this case the CONTI team has chosen, for certain reasons, the “haggling” method, rather than using a “take-it-or-leave-it” method, which characterizes less sophisticated threat actors.
- **At this point, it appears that patience pays off:** the negotiations were initiated in 30.12.2020, lasting up until 19.01.2021: the holiday season in the Western world as well as in the Christian Orthodox cultures. A factor that added to the morale of both sides. Both sides exhibit patience while conducting the correspondence. It appears that the nature of the stolen files and the level by which the organization was disabled are the main causes for the exhibited patience.

Locating and Accessing the Negotiations

Background

During January 21, a CONTI sample was detected by us in VirusTotal. The sample was detected and signed by numerous AV engines:

DETECTION	DETAILS	RELATIONS	BEHAVIOR	CONTENT	SUBMISSIONS	COMMUNITY
Antivirus results on 2021-01-13T09:58:35						
Ad-Aware	Gen:Variant.Zusy.356529	AegisLab	Trojan.Win32.Encoder.jlc			
AhnLab-V3	Malware/Win32.Generic.C4270607	Alibaba	Ransom:Win32/CONTI.e4ce8956			
ALYac	Trojan.Ransom.Conti	Antiy-AVL	Trojan[Ransom]/Win32.Conti			
SecureAge APEX	Malicious	Arcabit	Trojan.Zusy.D570B1			
Avast	Win32:Trojan-gen	AVG	Win32:Trojan-gen			
Avira (no cloud)	HEUR/AGEN.1138121	BitDefender	Gen:Variant.Zusy.356529			
BitDefenderTheta	Gen:NN.ZexaF.34760.luW@aazOSIdi	Bkav	W32.AIDetectVM.malware1			

One of the associated files was the ransom message, ordering the company to enter the [contirecovery\[.\]best](https://contirecovery[.]best) website and establish communications with the attacker. The message entails a unique victim identifier.

```
All of your files are currently encrypted by CONTI strain.
As you know (if you don't - just "google it"), all of the data that has been encrypted by our software cannot be recovered by any means without contacting
our team directly.
If you try to use any additional recovery software - the files might be damaged, so if you are willing to try - try it on the data of the lowest value.
To make sure that we REALLY CAN get your data back - we offer you to decrypt 2 random files completely free of charge.
You can contact our team directly for further instructions through our website :
TOR VERSION :
(you should download and install TOR browser first https://torproject.org)
http://m232fdxbfmbrchbrj5iayknxnggf6niqfj6x4iedrgtab4qupzjlaid.onion
HTTPS VERSION :
https://contirecovery.best
YOU SHOULD BE AWARE
Just in case, if you try to ignore us. We've downloaded a pack of your internal data and are ready to publish it on our news website if you do not respond.
So it will be better for both sides if you contact us as soon as possible.
---BEGIN ID---
[Redacted]
---END ID---
```

A message containing a unique identifier is routine in ransomware proceedings. We entered CONTI's website to identify the victim, which displayed an interface requesting the ransom message to begin communicating with the attackers.



CONTI recovery service

HOW I GOT HERE?

If you are looking at this page right now, that means that your network was successfully breached by CONTI team. All of your files, databases, application files etc were encrypted with military-grade algorithms. If you are looking for a free decryption tool right now - there's none. Antivirus labs, researches, security solution providers, law agencies won't help you to decrypt the data.

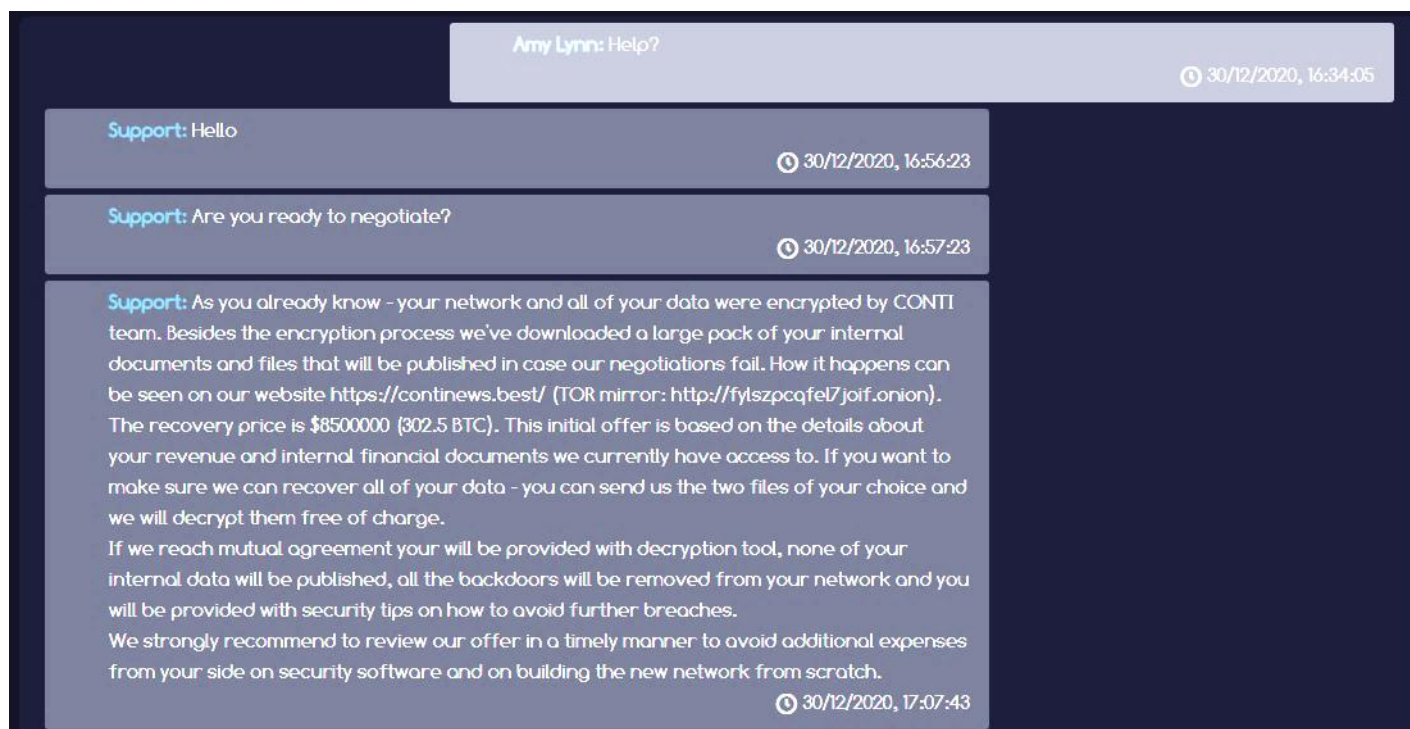
If you are interested in our assistance upon this matter - you should upload README.TXT file to be provided with further instructions upon decryption.

Choose file No file chosen

Analyzing the Correspondence

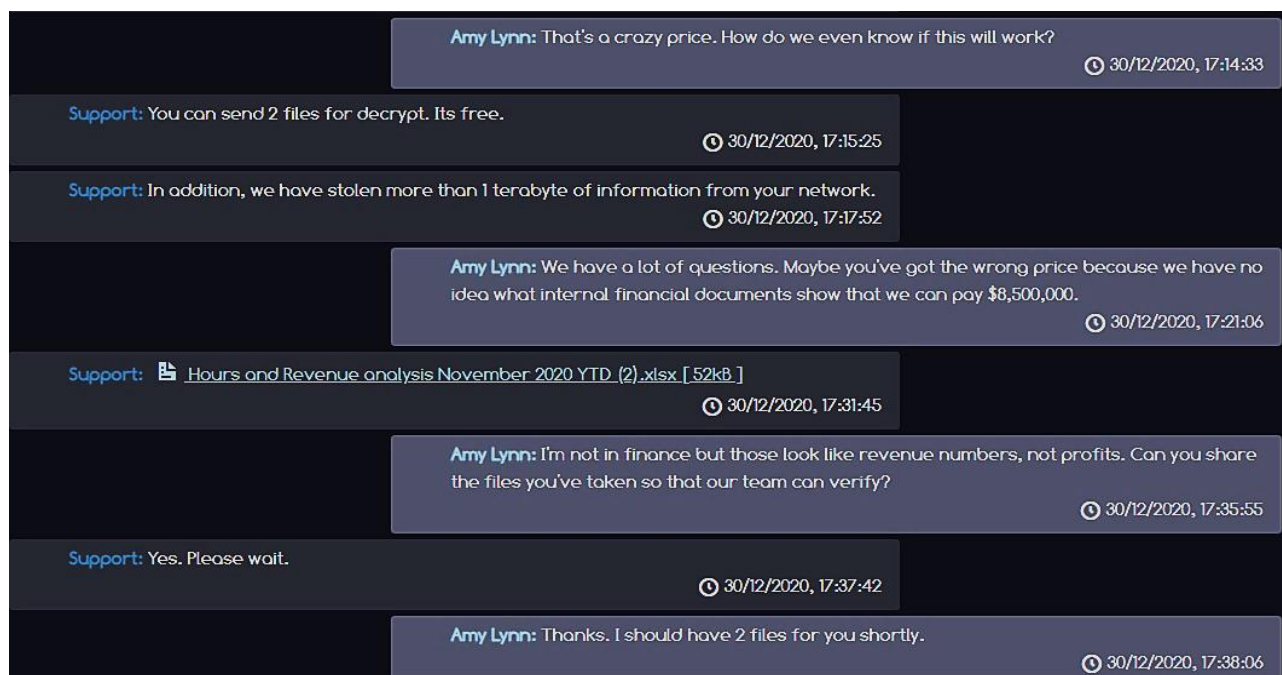
The correspondence is conducted between the ransomware operators (referring to themselves as “**Support**”) and the victim company’s appointed negotiation handler (referring to themselves as “**Amy Lynn**”). The full correspondence is added at the end of this document.

The conversation begins with a generic-seeming message from “Support” in which they define their demands and the rules of the negotiations directly. Their upfront statement: “Are you ready to negotiate?” serves as a undoubtable invitation to a “haggling game”. The attackers explains that the victim’s stolen and encrypted files will only be decrypted if the \$8.5 million ransom is paid in full. The attacker continues to state that they will release their hold of the organization once the ransom is paid, adding security advice to better protect the organization in the future. The attackers threaten to leak the stolen files publicly in the ransom is not paid.



The victim expresses surprise when confronted with the high ransom demand, doubting the attackers' credibility. Using an authentic language of "That's a *crazy* price", could hint that the first handler of these negotiations on behalf of the victim is not a professional negotiator.

The attackers offer to decrypt two files free of charge to prove their intentions. **Following this, the attacker provides the company's income report for 2020** to justify the ransom amount. The victim explains that the company's income does not represent its profits, invalidating the ransom calculation.



As the correspondence continues the victim requests proof for several random files to further prove the attackers' credibility. Once the attacker provides the files, they also send a list of all the stolen files, implying their credibility by offering the victim to choose any file for decryption.



The victim attempts to verify the attacker's credibility even further, requesting that the attackers share the method by which they stole over 1TB from the organization. The attacker succinctly explains the compression system that allowed them to compress the stolen information by more than 95%. Quickly changing the subject, the attacker returns to negotiate, and states that if the victim pays the ransom, an explanation as to preventing this sort of attack will be provided. The victim tests the attackers limits again by asking for proof that the information will not be sold after the ransom is paid.

	Amy Lynn: Thanks. We are looking now	04/01/2021, 18:21:12
Support: so ?		04/01/2021, 21:25:14
	Amy Lynn: This is a lot of data to review. How did you get these files off our network?	05/01/2021, 00:12:32
Support: Packing data into an archive provides compression up to 95%		05/01/2021, 00:16:59
Support: After the deal is concluded, we will give recommendations on how to prevent this.		05/01/2021, 00:18:35
Support: I propose to return to the discussion of the agreement		05/01/2021, 00:19:03
Support: After the conclusion of the agreement, we overwrite the data		05/01/2021, 00:27:23
	Amy Lynn: Yes, we want to discuss the agreement. \$8,500,000 is a lot of money. We're just trying to see all the details because that is still an unexpected amount.	05/01/2021, 00:46:43
	Amy Lynn: Even if we had that much money, how do we know you won't just take the money and resell the data?	05/01/2021, 00:47:05

One of the correspondence segments entails the attacker explaining that refraining from upholding the agreed upon conditions contrasts their interests, as their reputation will be harmed (also harming future negotiations), an argument commonly used by “leading members” in the ransomware industry.

Support: We will show the cleaning logs	05/01/2021, 00:49:20
Support: This price is indicated for restoring ALL data in your network and deleting data on our servers	05/01/2021, 00:53:38
Support: We will give a decryptor and you will restore all the work	05/01/2021, 00:54:46
Support: We value our reputation and never leak any data after the deal is closed	05/01/2021, 08:39:28

Once the victim is convinced, they explain that the company does not possess the funds to pay the demanded ransom. **The attacker suggests that the victim takes a loan.** The victim, probably at that point led by a professional negotiator, explains that the company does not require decryption, and as a negotiation tactic “frames” a possible deal and “anchors-back” for \$250,000 **solely to prevent information leakage.**

Amy Lynn: Yes, but how do we pay if we don't have the cash?
🕒 06/01/2021, 00:02:26

Support: There are plenty of ways to get the cash, like insurance or a corporate loan.
🕒 06/01/2021, 09:48:31

Amy Lynn: If those were option we would have pulled those levers already!
🕒 06/01/2021, 09:53:21

Support: We are ready to hear your proposal which is based on your abilities, but it should be relevant to the initial offer.
🕒 06/01/2021, 09:58:29

Amy Lynn: We are treating this as a data leak, no matter what. However, there is some upside to getting the files deleted (even though there are no assurances). Millions of dollars is excessive for this type of data and we don't have much need for a decryptor. Our proposal is \$250,000.
🕒 06/01/2021, 21:22:39

The next morning, at 11:00 AM, the attacker replies. They are prepared to lower the initial blackmail demand by 70%, to \$2,125,000. The conversation enters another hiatus.

Support: We've discussed internally, and taking in consideration the facts that you are trying to work this through and the fact that you don't need the decryption tool I've managed to convince my boss to provide you the huge discount by going down to \$2125000 (70% discount). If we close the deal this way we have to intention to sell or publish your data of course.
🕒 07/01/2021, 10:55:46

Amy Lynn: We are still far apart but we view this is a positive step. Thank you.
🕒 07/01/2021, 21:41:23

Amy Lynn: Can we discuss with our team?
🕒 07/01/2021, 21:41:34

Support: yes
🕒 07/01/2021, 21:41:54

Amy Lynn: This reduction is interesting. It's almost end of week here and some of our management wants to discuss. Can we reach out next week?
🕒 08/01/2021, 15:41:55

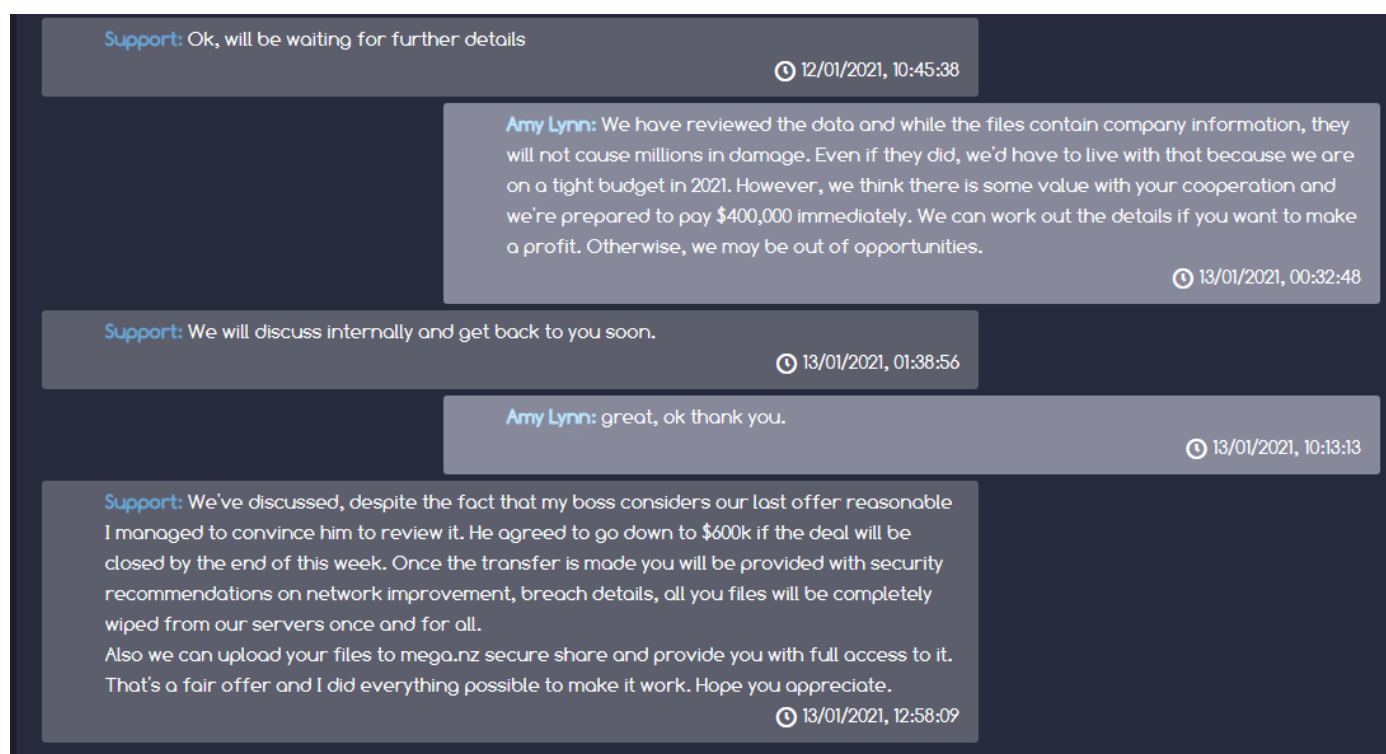
Support: Yes, sure, let's get back to this on Monday. Just keep us updated on the progress.
🕒 08/01/2021, 15:46:38

Amy Lynn: Ok
🕒 08/01/2021, 21:53:02

Amy Lynn: We're connecting on this topic later today and tomorrow morning. We may be able to increase the dollar amount.
🕒 11/01/2021, 20:15:35

The conversation is renewed as the weekend ends. The victim informs the attacker that the possible damage that may be caused by the stolen documents is not estimated by millions of dollars. The victim's negotiator states that the

company cannot pay the demanded ransom and maintain the haggling dance by stating that they are prepared to immediately transfer \$400,000 if the attackers will compromise further. The attackers “consult with their bosses” and informs the victim that the group decided to lower the ransom to \$600,000, providing insights regarding the breach, deleting the files from the attackers’ network, and potentially uploading the encrypted files to mega.nz.



The screenshot shows a chat interface with a dark background. It contains four messages in alternating light and dark grey bubbles, each with a timestamp in the bottom right corner.

- Support:** OK, will be waiting for further details. (12/01/2021, 10:45:38)
- Amy Lynn:** We have reviewed the data and while the files contain company information, they will not cause millions in damage. Even if they did, we'd have to live with that because we are on a tight budget in 2021. However, we think there is some value with your cooperation and we're prepared to pay \$400,000 immediately. We can work out the details if you want to make a profit. Otherwise, we may be out of opportunities. (13/01/2021, 00:32:48)
- Support:** We will discuss internally and get back to you soon. (13/01/2021, 01:38:56)
- Amy Lynn:** great, ok thank you. (13/01/2021, 10:13:13)
- Support:** We've discussed, despite the fact that my boss considers our last offer reasonable I managed to convince him to review it. He agreed to go down to \$600k if the deal will be closed by the end of this week. Once the transfer is made you will be provided with security recommendations on network improvement, breach details, all you files will be completely wiped from our servers once and for all. Also we can upload your files to mega.nz secure share and provide you with full access to it. That's a fair offer and I did everything possible to make it work. Hope you appreciate. (13/01/2021, 12:58:09)

The negotiations are somewhat derailed as the victim requests confirmation that a decryption key will be provided alongside the agreed upon terms. The attacker explains that maybe they have misunderstood, but the conversation thus far concluded that the victim does not need to decrypt their files.

The victim attempts to facilitate another decrease of the ransom, which the attacker apparently does not appreciate. The attackers’ tone changes, seemingly becoming more aggressive, stating that the victim’s “tricks” will not succeed. The attackers advise avoiding basing terms on previously reported deals with the CONTI group, as 75% of their transactions were not reported publicly. The attackers set an ultimatum – the victim has one day to decide whether they want to pay \$600,000 for the files, or a higher price for the entire package.

we have at the moment. Before we discuss, can you also confirm that we would receive a decryption tool in addition to the above deliverables?

🕒 13/01/2021, 20:24:56

Support: As I remember you do not need a decryption tool. Am I mistaken? Most of the discount was provided based on the fact that you do not need the decryption.

🕒 13/01/2021, 22:08:47

Amy Lynn: There are some files that would save us time. \$400,000 is not a small amount.

🕒 13/01/2021, 22:16:03

Support: That is way below our offer. Yes, surely the decryptor would save you some time, and time means money. The \$600k offer was for the data we hold. As you must understand we have some experience in negotiations, and you are trying to put us in the position that you think we accept, based on the basic information that is in the the press about usual sum we get. Relying on the press or public opinion is a mistake. About 75% of our deals are never leaked to the public or revealed. We will be waiting for your decision by tomorrow. \$600k for the files or something better for full pack.

🕒 13/01/2021, 22:27:04

It appears that the victim realizes that they crossed a line in attempting to decrease the price further. Despite this, they insist on \$450,000 as the final amount, explaining that they are unable to pay more. Using professional communication methods the negotiator manages to successfully convey the message that this \$450,000 is an authentic “reservation value”. A number beyond which the victim prefers the “no-deal” alternative.

The attackers agree to a final act of compromise, stating that they will consult with their “boss” once again to attempt and convince them to include file decryption in the \$600,000 offer. The victim emphasizes that an offer including decryption will be seriously considered.

Amy Lynn: Yes, we know you are very experienced. We can sense it. All we’re doing is seeing how much money we can spend, and \$400,000 is an large sum. If we go down this path, then we certainly want all of the items that are available.

🕒 14/01/2021, 00:28:14

Amy Lynn: We’ve read about you in the press but we have no idea about the usual sum that you get. No one here wants to play games, and that’s why we’re trying to finalize the deliverables in advance. We want a solution and we assume you want to get paid. But \$400,000 is only available if we can get everything. How else can we afford to pay that much?

🕒 14/01/2021, 00:30:33

Support: The \$400k is too low anyways. I will talk to my boss and try to get an offer for \$600k that will contain the decryptor. Give me few hours.

🕒 14/01/2021, 07:24:58

Amy Lynn: Alright - your best offer that includes the decryptor will be taken under very serious consideration. Thank you.

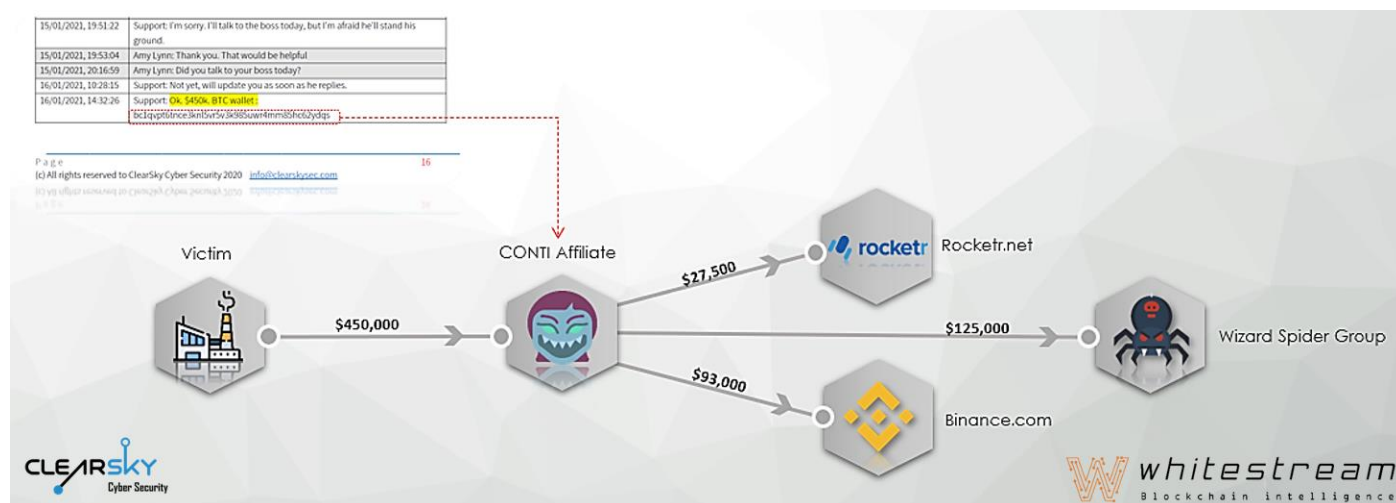
🕒 14/01/2021, 09:58:23

In 20/1/21 450,000 US\$ were paid to Conti.

Blockchain Analysis

Analysis of the CONTI Ransomware's Affiliate Bitcoin Wallet

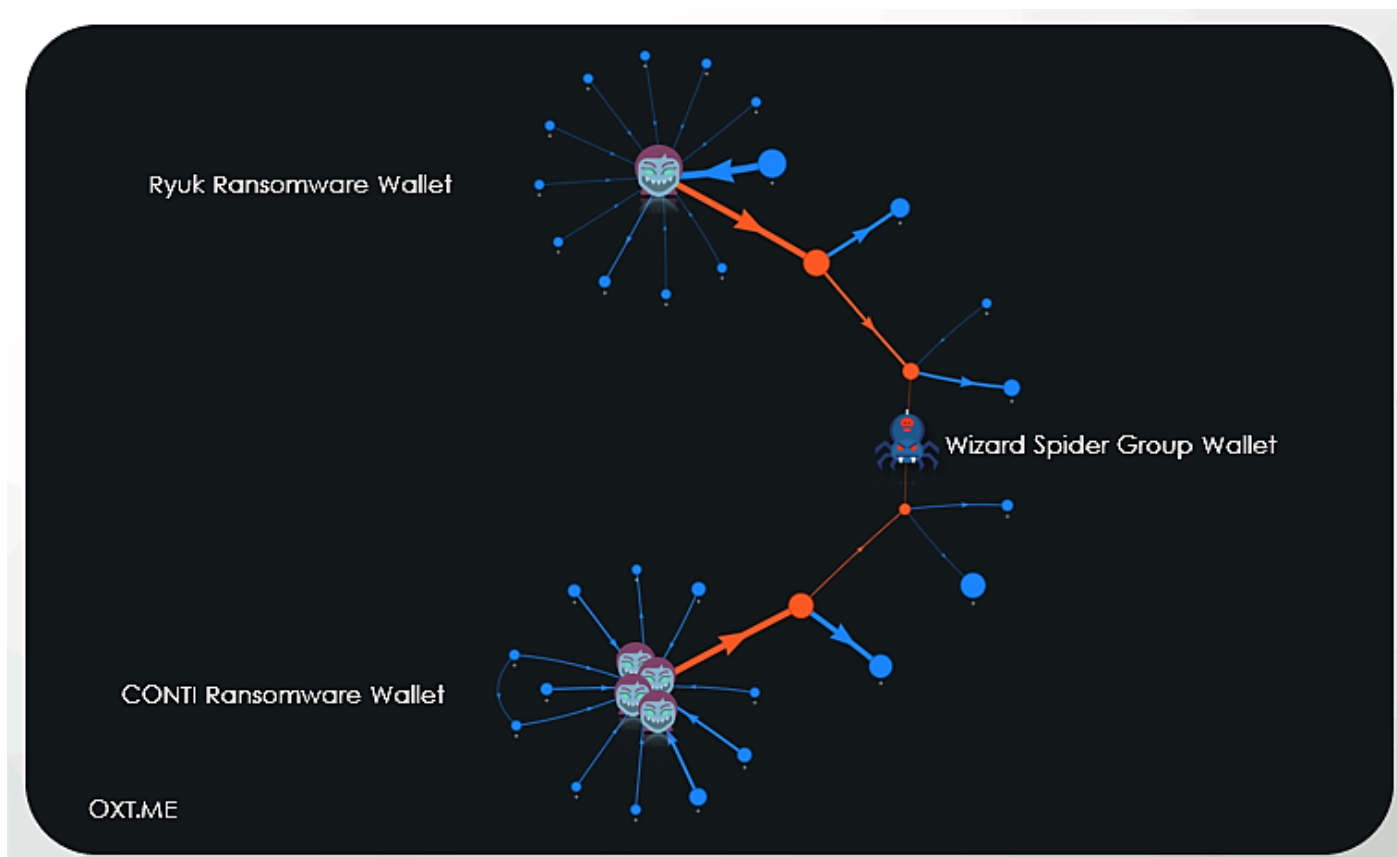
Tracking the \$450,000 ransom payment on the Blockchain indicates that the CONTI's affiliates deposited some of their funds to **Binance.com** digital currency exchange, and to **Rocketr.net**, a Bitcoin payments platform. Another significant amount was transferred to one of **Wizard Spider's** main Bitcoin wallets, probably as part of the revenue sharing frame.



Blockchain analysis reveals the connection between CONTI and Ryuk.

Analyzing the 'Wizard Spider' group Bitcoin wallets indicated that several Bitcoin addresses serve as a major hub in collecting the ransom payments from the victims. Ransom payments from Both Ryuk and CONTI victims were delivered to the same Bitcoin wallets that are managed by the 'Wizard Spider' group during the last three years.





Deposits from CONTI affiliate wallets to Binance (China)

CONTI affiliate sent \$93,000 to the Binance.com platform.

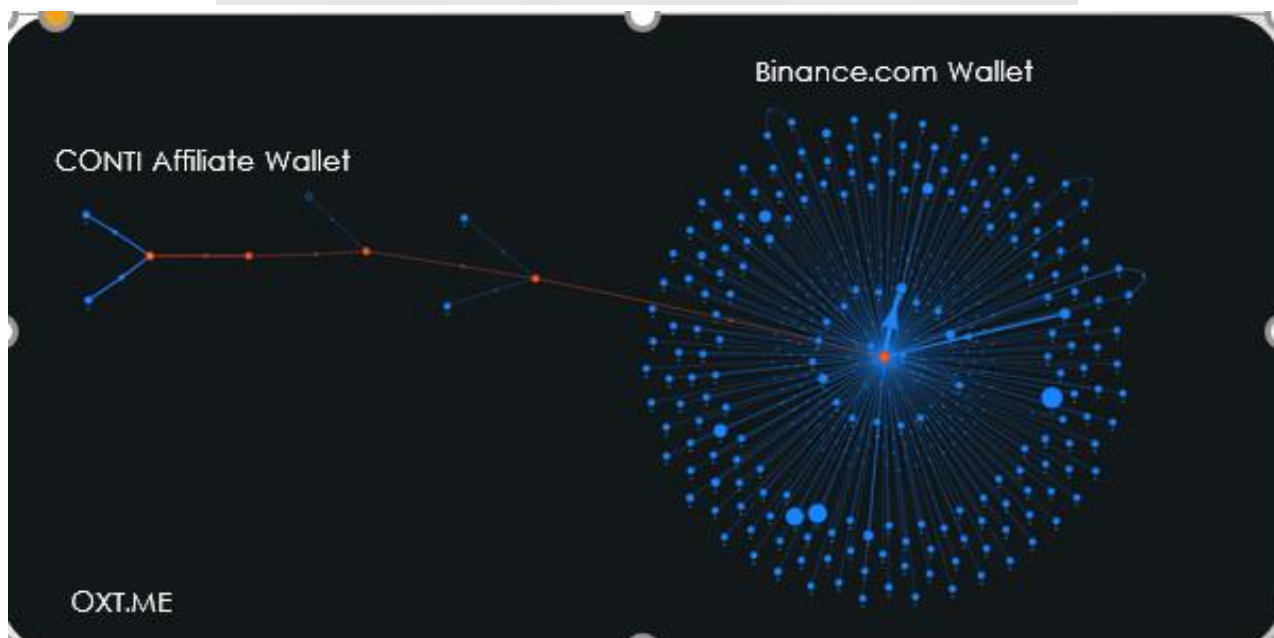
\$80,000 - 21/1/2021 Transaction ID: 93d9e89f8f1bc583cc9391d0c2f8e654bf2622eff9cc5095ed2e22d9848905ac
\$1,000 - 21/1/2021 Transaction ID: 3a81ba3b7dd75332fee0acc4d2d78d1710cbc95109921fdc62eaa3c68bccaa2f
\$12,000 - 23/1/2021 Transaction ID: 2dfb777387a8997c6a8743829454ebc57dabcac28a4d11a1f64708ce5620f99d

Addresses involved:

1NhNuPogvydJWfTGvp41Rgghqw8MNMjTh3
bc1qtaqrv6eeh83vk2hz9myns9lysrzmm4j4366mmw
bc1qff0xgtxm6ansnd7dpt9ptc5n0deh3zpw5f9s58



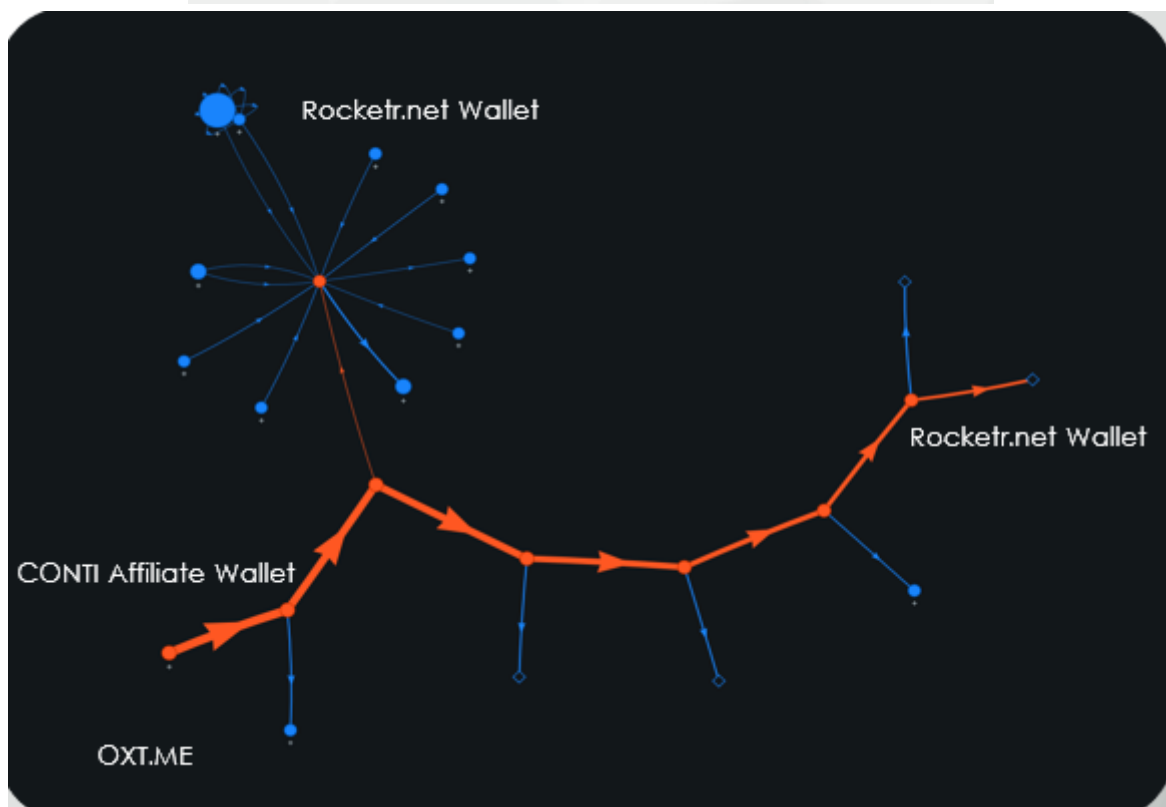
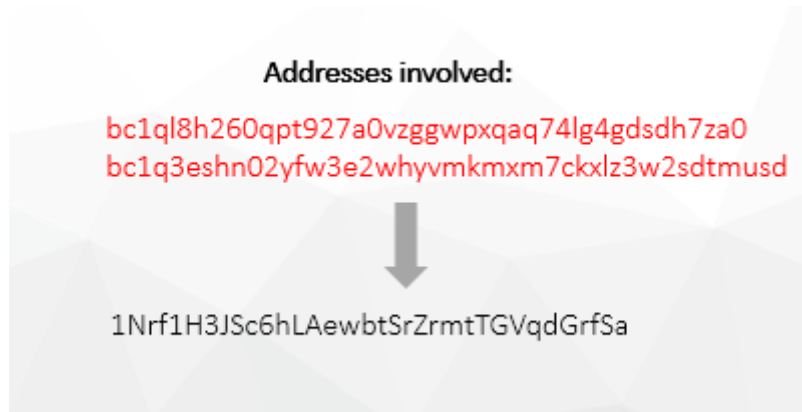
1KAUvPyKVNNNTpLQ5ECxZRiWRiBMxS2Nw
1KKyWeywsXGnizUXfvnwTHpYcSRWina1Ah
1CroVoEv556cwnu5eDe192JUCvmsbGjv9q



Deposits from CONTI affiliate wallets to Rocketr.net

CONTI affiliate sent \$27,500 to the Rocketr.net platform.

\$2,500 - 26/1/2021	Transaction ID: 9f4ec7ff26a014c2193e291645f7bb7a5d7ec0a5323f9d859321217496ea6ecd
\$25,000 - 1/2/2021	Transaction ID: 36fc4da7d78819c7eff61fc80ebd25017b91d4762496c8cda14aa50bf768881b



Conti – Negotiations Text Version

Date	Conversation
30/12/2020, 16:34:05	Amy Lynn: Help?
30/12/2020, 16:56:23	Support: Hello
30/12/2020, 16:57:23	<p>Support: Are you ready to negotiate?</p> <p>As you already know - your network and all of your data were encrypted by CONTI team. Besides the encryption process we've downloaded a large pack of your internal documents and files that will be published in case our negotiations fail. How it happens can be seen on our website https://continews.best/ (TOR mirror: http://fylszpcqfel7joif[.]onion).</p> <p>The recovery price is \$8500000 (302.5 BTC). This initial offer is based on the details about your revenue and internal financial documents we currently have access to. If you want to make sure we can recover all of your data - you can send us the two files of your choice and we will decrypt them free of charge.</p> <p>If we reach mutual agreement your will be provided with decryption tool, none of your internal data will be published, all the backdoors will be removed from your network and you will be provided with security tips on how to avoid further breaches. We strongly recommend to review our offer in a timely manner to avoid additional expenses from your side on security software and on building the new network from scratch.</p>
30/12/2020, 17:07:43	Amy Lynn: That's a crazy price. How do we even know if this will work?
30/12/2020, 17:14:33	Support: You can send 2 files for decrypt. Its free.
30/12/2020, 17:15:25	Support: In addition, we have stolen more than 1 terabyte of information from your network.
30/12/2020, 17:17:52	Amy Lynn: We have a lot of questions. Maybe you've got the wrong price because we have no idea what internal financial documents show that we can pay \$8,500,000.
30/12/2020, 17:21:06	Support: Hours and Revenue analysis November 2020 YTD (2).xlsx [52kB]
30/12/2020, 17:31:45	Amy Lynn: I'm not in finance but those look like revenue numbers, not profits. Can you share the files you've taken so that our team can verify?
30/12/2020, 17:35:55	Support: Yes. Please wait.
30/12/2020, 17:37:42	Amy Lynn: Thanks. I should have 2 files for you shortly.
30/12/2020, 17:38:06	Support: list_firstpart.zip [5MB]
30/12/2020, 17:44:47	Amy Lynn: What's this?
30/12/2020, 17:51:40	Support: Listing of the first part of the stolen information
30/12/2020, 17:52:15	Amy Lynn: Will we get more parts later?
30/12/2020, 17:58:55	Support: Yes, we are unpacking a terabyte. It will take a lot of time.

30/12/2020, 18:00:24	You can select any file from the listing and we will discard it as proof that we have these files.
30/12/2020, 18:06:27	Amy Lynn: Ok please let us know once it has been unpacked. It will be important to get the full listing
30/12/2020, 18:06:47	Amy Lynn: Mobile3-EMEA.xml.KKBKR [3kB]
30/12/2020, 18:07:10	Amy Lynn: Can you decrypt this?
30/12/2020, 18:08:50	Support: I have sent your file to the technical department. Wait.
30/12/2020, 20:00:58	Support: Mobile3-EMEA.xml [2kB]
31/12/2020, 01:20:05	Amy Lynn: We're going to review all these files.Any update on the 1 TB?
31/12/2020, 03:33:54	Support: Will upload the file listing as soon as it's ready.
31/12/2020, 16:01:24	Amy Lynn: Ok we'll be here. Thanks
31/12/2020, 16:29:43	Support: 25 % ready. This is a very slow process. Wait.
31/12/2020, 16:29:43	Support: It will take a few days
31/12/2020, 16:30:23	Support: You can choose ANY file from the listing above and we will discard it as proof
31/12/2020, 16:31:01	Amy Lynn: We'll work on that. Offices are closed the next few days but we'll be in touch. Ok?
31/12/2020, 23:23:03	Amy Lynn: This is our priority
31/12/2020, 23:23:11	Support: Ok, just keep us updated on your progress.
31/12/2020, 23:30:38	Support: 50% Ready
01/01/2021, 16:20:17	Support: 70% Ready
02/01/2021, 12:40:13	Amy Lynn: Thanks. We're still here
02/01/2021, 15:36:54	Amy Lynn: While you're pulling the file tree, can you send us this file? 05/07/2020 02:55 PM 106,393 Return to Office - Draft 2020 05 06 v2.docx
02/01/2021, 18:06:21	Support: Yes, will upload soon
02/01/2021, 19:08:27	Support: return-to-office---draft-2020-05-06-v2.docx [104kB]
02/01/2021, 20:43:36	Support: %90 ready
03/01/2021, 08:25:38	Amy Lynn: Thanks, still here and checking in.
03/01/2021, 18:38:25	Support: 100% ready.
03/01/2021, 19:18:45	Wait listing
03/01/2021, 19:24:33	Support: listing_1tb.zip [9.2MB]
03/01/2021, 19:25:13	Support: You can choose ANY file from the listing above and we will discard it as proof
04/01/2021, 15:36:29	Amy Lynn: Thanks. So this is a directory of every single file you've taken from our network?
04/01/2021, 16:21:52	Support: yes
04/01/2021, 16:22:42	Support: total of data more 1tb
04/01/2021, 16:29:38	Support: so, what other questions do you have?
04/01/2021, 18:21:12	Amy Lynn: Thanks. We are looking now
04/01/2021, 21:25:14	Support: so ?
05/01/2021, 00:12:32	Amy Lynn: This is a lot of data to review. How did you get these files off our network?

05/01/2021, 00:16:59	Support: Packing data into an archive provides compression up to 95%
05/01/2021, 00:18:35	Support: After the deal is concluded, we will give recommendations on how to prevent this.
05/01/2021, 00:19:03	Support: I propose to return to the discussion of the agreement
05/01/2021, 00:27:23	Support: After the conclusion of the agreement, we overwrite the data
05/01/2021, 00:46:43	Amy Lynn: Yes, we want to discuss the agreement. \$8,500,000 is a lot of money. We're just trying to see all the details because that is still an unexpected amount.
05/01/2021, 00:47:05	Amy Lynn: Even if we had that much money, how do we know you won't just take the money and resell the data?
05/01/2021, 00:49:20	Support: We will show the cleaning logs
05/01/2021, 00:53:38	Support: This price is indicated for restoring ALL data in your network and deleting data on our servers
05/01/2021, 00:54:46	Support: We will give a decryptor and you will restore all the work
05/01/2021, 08:39:28	Support: We value our reputation and never leak any data after the deal is closed
05/01/2021, 09:45:42	Amy Lynn: Alright, so we are thinking this through now. I will get back to you soon, alright?
05/01/2021, 09:46:25	Support: Ok, waiting.
05/01/2021, 21:06:47	Amy Lynn: We're trying to get answers on our end. Thanks for waiting
	Support: Ok waiting
05/01/2021, 21:10:31	Support: If you have any questions - we can help you
05/01/2021, 21:11:51	But the sooner you conclude an agreement, the sooner you will resume work and will no longer suffer losses due to this situation.
08/03/2020 05:14 PM	Amy Lynn: Can you send this file? 13,697 Maple Refridgerated Copy_v4 CL.docx
05/01/2021, 21:40:18	Support: Yes
05/01/2021, 21:41:36	Wait
05/01/2021, 21:42:23	Support: maple-refridgerated-copy_v4-cl.docx [13kB]
05/01/2021, 21:47:36	Amy Lynn: Thanks for the quick response
05/01/2021, 21:48:00	Support: Are you convinced? There is really a lot of your data here
05/01/2021, 21:53:54	Amy Lynn: We certainly see that you have our data. Nothing to hide there
05/01/2021, 21:54:11	Amy Lynn: It's the price that's causing us heartburn...
05/01/2021, 21:57:28	Support: Publishing data will cause customer churn and you will lose much more. It is more profitable to work with us
06/01/2021, 00:02:26	Amy Lynn: Yes, but how do we pay if we don't have the cash?
06/01/2021, 09:48:31	Support: There are plenty of ways to get the cash, like insurance or a corporate loan.
06/01/2021, 09:53:21	Amy Lynn: If those were option we would have pulled those levers already!
06/01/2021, 09:58:29	Support: We are ready to hear your proposal which is based on your abilities, but it should be relevant to the initial offer.
06/01/2021, 21:22:39	Amy Lynn: We are treating this as a data leak, no matter what. However, there is some upside to getting the files deleted (even though there are no assurances). Millions of dollars is

	excessive for this type of data and we don't have much need for a decryptor. Our proposal is \$250,000.
06/01/2021, 21:48:08	Support: That is way lower than your abilities and not as relevant to our expectations as we thought. Although I will pas your offer to my boss and get back to you.
07/01/2021, 09:46:05	Amy Lynn: Sounds good. Thanks.
07/01/2021, 10:55:46	Support: We've discussed internally, and taking in consideration the facts that you are trying to work this through and the fact that you don't need the decryption tool I've managed to convince my boss to provide you the huge discount by going down to \$2125000 (70% discount). If we close the deal this way we have to intention to sell or publish your data of course.
07/01/2021, 21:41:23	Amy Lynn: We are still far apart but we view this is a positive step. Thank you.
07/01/2021, 21:41:34	Amy Lynn: Can we discuss with our team?
07/01/2021, 21:41:54	Support: yes
08/01/2021, 15:41:55	Amy Lynn: This reduction is interesting. It's almost end of week here and some of our management wants to discuss. Can we reach out next week?
08/01/2021, 15:46:38	Support: Yes, sure, let's get back to this on Monday. Just keep us updated on the progress.
08/01/2021, 21:53:02	Amy Lynn: Ok
11/01/2021, 20:15:35	Amy Lynn: We're connecting on this topic later today and tomorrow morning. We may be able to increase the dollar amount.
12/01/2021, 10:45:38	Support: Ok, will be waiting for further details
13/01/2021, 00:32:48	Amy Lynn: We have reviewed the data and while the files contain company information, they will not cause millions in damage. Even if they did, we'd have to live with that because we are on a tight budget in 2021. However, we think there is some value with your cooperation and we're prepared to pay \$400,000 immediately. We can work out the details if you want to make a profit. Otherwise, we may be out of opportunities.
13/01/2021, 01:38:56	Support: We will discuss internally and get back to you soon.
13/01/2021, 10:13:13	Amy Lynn: great, ok thank you.
	Support: We've discussed, despite the fact that my boss considers our last offer reasonable I managed to convince him to review it. He agreed to go down to \$600k if the deal will be closed by the end of this week. Once the transfer is made you will be provided with security recommendations on network improvement, breach details, all you files will be completely wiped from our servers once and for all. Also we can upload your files to mega.nz secure share and provide you with full access to it. That's a fair offer and I did everything possible to make it work. Hope you appreciate.
13/01/2021, 12:58:09	Amy Lynn: We do appreciate that but we'll need to discuss since it's more money than what we have at the moment. Before we discuss, can you also confirm that we would receive a decryption tool in addition to the above deliverables?

13/01/2021, 20:24:56	Support: As I remember you do not need a decryption tool. Am I mistaken? Most of the discount was provided based on the fact that you do not need the decryption.
13/01/2021, 22:08:47	Amy Lynn: There are some files that would save us time. \$400,000 is not a small amount.
13/01/2021, 22:16:03	Support: That is way below our offer. Yes, surely the decryptor would save you some time, and time means money. The \$600k offer was for the data we hold. As you must understand we have some experience in negotiations, and you are trying to put us in the position that you think we accept, based on the basic information that is in the the press about usual sum we get. Relying on the press or public opinion is a mistake. About 75% of our deals are never leaked to the public or revealed. We will be waiting for your decision by tomorrow. \$600k for the files or something better for full pack.
13/01/2021, 22:27:04	Amy Lynn: Yes, we know you are very experienced. We can sense it. All we're doing is seeing how much money we can spend, and \$400,000 is an large sum. If we go down this path, then we certainly want all of the items that are available.
14/01/2021, 00:28:14	Amy Lynn: We've read about you in the press but we have no idea about the usual sum that you get. No one here wants to play games, and that's why we're trying to finalize the deliverables in advance. We want a solution and we assume you want to get paid. But \$400,000 is only available if we can get everything. How else can we afford to pay that much?
14/01/2021, 00:30:33	Support: The \$400k is too low anyways. I will talk to my boss and try to get an offer for \$600k that will contain the decryptor. Give me few hours.
14/01/2021, 07:24:58	Amy Lynn: Alright - your best offer that includes the decryptor will be taken under very serious consideration. Thank you.
14/01/2021, 09:58:23	Support: Talked to my boss. When he heard about the decryption tool being needed, at first he was ready to move back to the previous offer or at least move to 1.2mil (x2 from the data offer), but we've decided not too be hard on you and are ready to stay at \$750k. Take this to the management and let me know what they decide.
14/01/2021, 15:57:30	Amy Lynn: I appreciate you trying. We have a lot of money set aside for this but \$750,000 just won't be possible. If the price was \$600,000 then we may have been able to push closer to that. But at \$750,000, it is just so far...
14/01/2021, 17:02:47	Support: We can leave it \$600k if the transfer will be done today or tomorrow.
14/01/2021, 17:05:00	The BTC wallet is : bc1qvpt6tnce3kn15vr5v3k985uwr4mm85hc62ydds
14/01/2021, 17:10:31	Amy Lynn: Let me discuss with the team. This is still above our budget but we can try to work towards it quickly. Thanks.
15/01/2021, 00:51:32	Amy Lynn: We took this management and discussed. They were certainly appreciative of you being able to include the decryptor in the \$600,000 price. While the price itself is still high for us, we feel more confident in being able to move past this with you. We may be paying more than the value, but want to keep the positivity in our discussions. As a result, we can increase our offer to \$450,000 and can begin the transfer soon if you are with us. Thank you.
	Support: \$600k. take it back.

15/01/2021, 02:23:42	Support: And the sum will be increased if we will not receive the funds within mentioned time frames.
15/01/2021, 02:24:47	Amy Lynn: Well, increasing the sum is not going to get us any closer. I will get back to you in a bit.
15/01/2021, 09:44:07	Amy Lynn: We had an early morning call. \$450,000 is our limit and this is more than what we anticipated paying. We can start the payment process soon if you can agree. Otherwise, this may not be the ending we had hoped for.
15/01/2021, 15:06:43	Amy Lynn: We know you worked hard to make this work and we appreciate it. It's just that we're at our limit.
15/01/2021, 15:11:35	Support: You still have a little time to conclude an agreement on the terms above. Then the price will increase.
15/01/2021, 19:48:18	Amy Lynn: We have worked day and night to make this work and we understand you're doing the same. If the price goes up then there is no way we can pay. All we ask is for a little help so that we can get the cash in your hands. \$450,000 is not a small amount for us.
15/01/2021, 19:51:22	Support: I'm sorry. I'll talk to the boss today, but I'm afraid he'll stand his ground.
15/01/2021, 19:53:04	Amy Lynn: Thank you. That would be helpful
15/01/2021, 20:16:59	Amy Lynn: Did you talk to your boss today?
16/01/2021, 10:28:15	Support: Not yet, will update you as soon as he replies.
16/01/2021, 14:32:26	Support: Ok. \$450k. BTC wallet : bc1qvpt6tnce3knl5vr5v3k985uwr4mm85hc62ydqs
16/01/2021, 17:28:31	Amy Lynn: Thank you. Can you confirm what we will receive in return of a \$450,000 payment?
16/01/2021, 17:59:08	Support: - Decryption tool. - Your data will be wiped from our servers - Security improvement tips
16/01/2021, 18:11:58	Amy Lynn: And the files will be uploaded to mega.nz for us to review?
16/01/2021, 18:25:54	Support: we can upload on mega. yes.
16/01/2021, 18:41:15	Amy Lynn: Ok, we'll be in touch. It may be hard since this is a holiday weekend but we'll send an update
16/01/2021, 18:45:20	Amy Lynn: We're hoping to pay by tomorrow, since today is a holiday. Ok?
18/01/2021, 15:59:59	Support: Yes. Let me know as soon as the transfer is made.
18/01/2021, 17:06:36	Amy Lynn: Still here? Can you confirm the wallet for \$450,000?
19/01/2021, 16:04:16	Support: Yes, just a minute.
19/01/2021, 16:14:23	Support: The BTC wallet is the same : bc1qvpt6tnce3knl5vr5v3k985uwr4mm85hc62ydqs
19/01/2021, 16:14:45	Amy Lynn: We have paid. Please confirm
19/01/2021, 21:17:31	Support: The payment is pending. As soon as it's confirmed you will be provided with decryption software with the instructions on how to use it.
19/01/2021, 21:19:28	Amy Lynn: Ok. And when will get access to the files that you took?
19/01/2021, 21:32:36	Support: We will upload them to the mega.nz share the soonest possible.
19/01/2021, 21:33:30	Amy Lynn: Do you have our tool yet?
20/01/2021, 12:24:25	Support: Will be ready within next 4-5 hours.

20/01/2021, 15:12:06	[DECRYPTION TOOL ATTACHED]
20/01/2021, 17:22:04	Amy Lynn: We're taking a look now. Any updates on mega.nz?
20/01/2021, 17:22:59	Support: It's pretty much data so it keeps being uploaded. Will update you as soon as it's ready.
20/01/2021, 18:24:43	Amy Lyn: Thank you. Please keep us updated!

Email:
Website:

info@clearskysec.com
clearskysec.com



Ahead of the Threat Curve

CONTI Modus Operandi and Bitcoin Tracking

(C) all rights reserved to ClearSky Cyber Security 2021

TLP:White