TLP: WHITE

Analyzing ransomware negotiations with CONTI: An in-depth analysis

DFIR Research Group (https://difr.unipi.gr/)

Team Cymru (https://team-cymru.com/)

CONTI is a ransomware group that uses a double extortion attack to force its victims into paying. The group has more than $14m confirmed payments in bitcoin and has several high-profile victims in its portfolio. The latter is verified by the publication of the exfiltrated data of the victims who did not pay the requested ransom. Given the modus operandi of the group, we managed to intercept many of their negotiations, which provided us with intelligence into how they operate. The studied interactions correspond to more than a third of their earnings and are therefore quite indicative of how they work as a group.

Index terms— Ransomware, CONTI, cybercrime, blockchain forensics

Introduction

CONTI is a ransomware that uses the double extortion model to force their victims to pay the ransom. In essence, the attackers will not only lock up a victim's files by encrypting them and demand ransom for their decryption, but they will also steal files and threaten to publish them on a website or otherwise leak them if their initial ransom request is not met. This model is not novel, as it has been introduced by MAZE and then used in other ransomware campaigns such as REvil, Ragnar, and Egregor, to name a few.

The group is being operated in the Ransomware as a Service (RaaS) model. Therefore, there is a group of developers who have developed the ransomware and distribute it to some affiliates that they recruit. These affiliates will use it once they penetrate a host. Each party keeps a share of the paid ransom, which are paid in some cryptocurrency.

The confirmed earnings of the CONTI group, based on a specialised Open Source Intelligence (OSINT) source that tracks ransomware - ransomwhere[1], are currently $14,740,000. These earnings position CONTI among the most highly paid ransomware operation and due to the high impact on USA-based organisations "caused" the Federal Bureau of Investigations (FBI) to issue a dedicated flash alert[2], with the Cybersecurity and Infrastructure Security Agency (CISA) also issuing a dedicated alert more recently[3]. In what follows, we provide an insight into the transactions of more than a third (34.96%) of CONTI earnings. According to the dedicated CONTI news site, which is currently available through the "open" web[4] and through TOR,[5] there are more than 450 organisations that have been hacked, and some of their data are now publicly available.

The basic phases of the means of infiltration, which are utilized by CONTI, are illustrated in Figure 1.

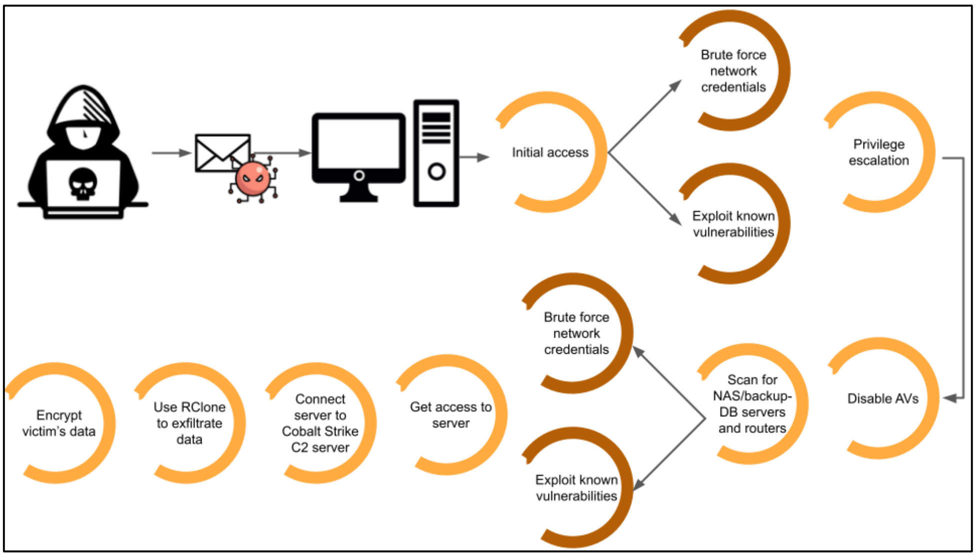

Initial access
Brute force network credentials
Exploit known vulnerabilities
Privilege escalation
Disable AVs
Scan for NAS/backup-DB servers and routers
Brute force network credentials
Exploit known vulnerabilities
Get access to server
Connect server to Cobalt Strike C2 server
Use RClone to exfiltrate data
Encrypt victim's data

Figure 1 – Overview of the CONTI Infiltration Process

[1] https://ransomwhe.re/

[2] https://www.aha.org/system/files/media/file/2021/05/fbi-tlp-white-report-conti-ransomware-attacks-impact-healthcare-and-first-responder-networks-5-20-21.pdf

[3] https://us-cert.cisa.gov/ncas/alerts/aa21-265a

[4] https://continews.click

[5] https://continewsnv5otx5kaoje7krkto2qbu3gtqef22mnr7eaxw3y6ncz3ad.onion

In principle, infiltration starts with the attackers sending a phishing email to the potential victim. Once the victim opens the email and unbeknown to him/her runs the malicious dropper, the attackers get initial access to the victim's network and can execute code. Having gained initial access, the attackers try to establish a better foothold and perform lateral movement to perform the aimed objectives, with the end goal being to hold the victim hostage and force the victim to pay a ransom (a) to regain access to his/her data, which at the final stage of the attack are encrypted by CONTI, (b) to prevent publication/selling of his/her data.

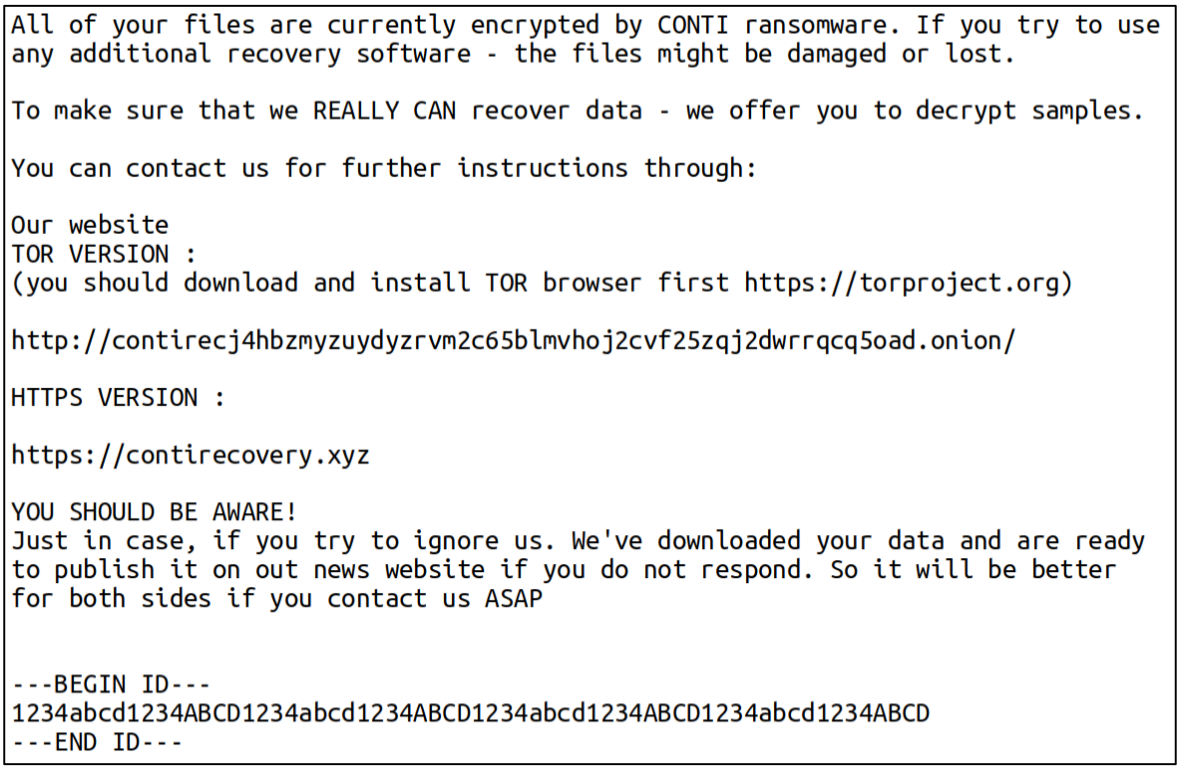
In this context, the attackers try to brute force credentials, perform an LSASS memory dump, or even exploit some existing vulnerabilities to elevate privileges. Once this is done, the attackers try to turn off infected/infiltrated systems' antivirus solutions (AVs) as well as other existing security mechanisms. Subsequently, the attackers will scan the network for other servers/workstations to gain additional access.

Then, the infected/infiltrated host(s) is (are) attached to a Cobalt Strike C2 server controlled by the attackers. Afterwards, the attackers use RClone[6] to upload the exfiltrated data to a cloud service (usually Mega[7]).

Finally, the attackers launch the ransomware "encryptor" to lock the victim's files. After the encryption, CONTI leaves a "README" file in each folder that it encrypts, which notifies the victim of the attack that his/her data have been encrypted and provides means to contact the CONTI team to pay the ransom and get the decryption software. In prior versions, the team used email addresses as means of communication. However, they developed a portal later, where users could contact CONTI using an ID that they were assigned. In these cases, the template of the ransomware notice is in the form of Figure 2.

[6] https://rclone.org/

[7] https://www.hhs.gov/sites/default/files/analyst-note-conti-ransomware-tlp-white.pdf



```
All of your files are currently encrypted by CONTI ransomware. If you try to use
any additional recovery software - the files might be damaged or lost.

To make sure that we REALLY CAN recover data - we offer you to decrypt samples.

You can contact us for further instructions through:

Our website
TOR VERSION :
(you should download and install TOR browser first https://torproject.org)

http://contirecj4hbzmyzuydyzrvm2c65blmvhoj2cvf25zqj2dwrrqcq5oad.onion/

HTTPS VERSION :

https://contirecovery.xyz

YOU SHOULD BE AWARE!
Just in case, if you try to ignore us. We've downloaded your data and are ready
to publish it on out news website if you do not respond. So it will be better
for both sides if you contact us ASAP


---BEGIN ID---
1234abcd1234ABCD1234abcd1234ABCD1234abcd1234ABCD1234abcd1234ABCD
---END ID---
```

Figure 2 – A Sample of the Ransomware Notice Left by CONTI

CONTI has been used in several attacks of high-profile organizations, has been deployed along with BazarLoader,[8] and is considered a stakeholder of the ransomware cartel, as a member of the Wizard Spider threat group (ClearSky Cyber Security 2021; DiMaggio 2021).

Up to now, there are many detailed technical reports about several ransomware and how they operate. Among them, many of these reports deal with CONTI.[9] Moreover, there are reports which showcase how CONTI works operates when infiltrating an organization.[10]

More generally, there are studies about ransomware payments, economics (Laszka, Farhang, and Grossklags 2017; Hernandez-Castro, Cartwright, and Cartwright 2020) or

[8] https://thedfirreport.com/2021/09/13/bazarloader-to-conti-ransomware-in-32-hours/

[9] https://www.sentinelone.com/labs/conti-unpacked-understanding-ransomware-development-as-a-response-to-detection/ and https://unit42.paloaltonetworks.com/conti-ransomware-gang/

[10] https://news.sophos.com/en-us/2021/02/16/what-to-expect-when-youve-been-hit-with-conti-ransomware/

theoretical strategies (Caporusso, Chea, and Abukhaled 2018; Cartwright, Hernandez Castro, and Cartwright 2019; Li and Liao 2020; Hofmann 2020).

To the best of our knowledge, this is the first public report about the actual negotiation process used in a ransomware campaign and not just about a small fragment of the process, e.g. (ClearSky Cyber Security 2021). The basic reason is that up to now, this intelligence was internal. Besides the perpetrator, only the victim and the delegated victim's personnel would have access to this information, while there would not be any further communication of this exchange beyond perhaps the payment wallet address.

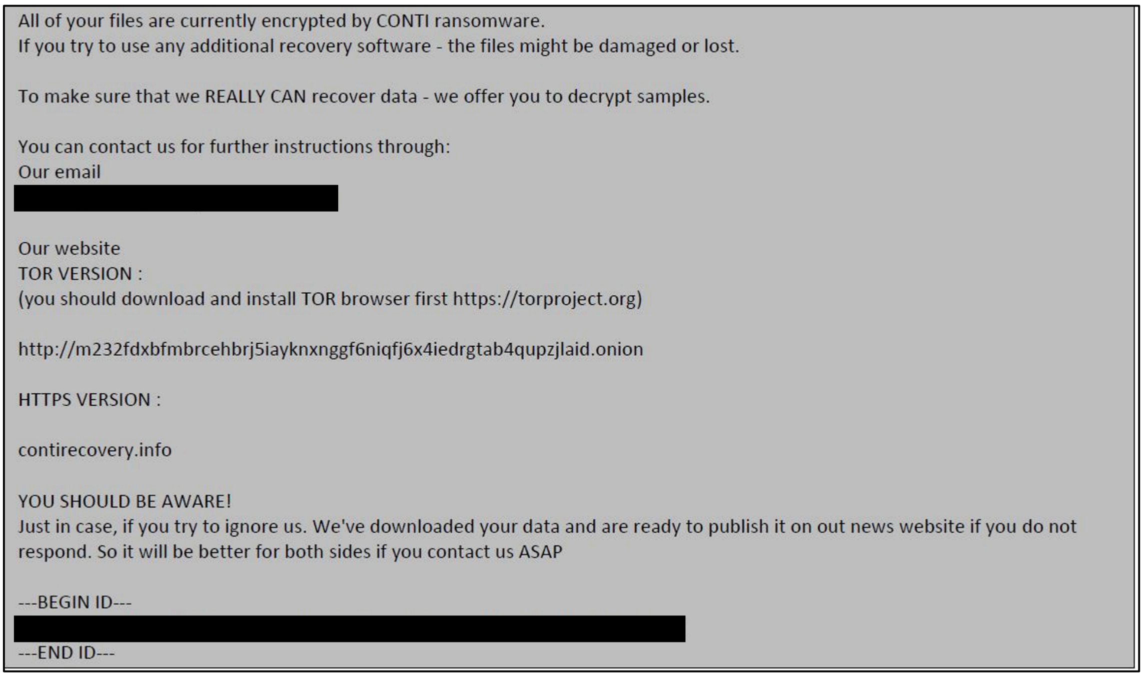
Therefore, operational information, statistics about the steps of the performed negotiations, possible ransom discounts, errors, or even other requests of both sides are not publicly documented nor discussed. Filling this gap, this report provides a good insight into the internal operations of such processes and can be considered rather representative based on the profiles of the compromised organisations. Several patterns emerge from both negotiating sides (victims and ransomware operators) in terms of followed processes, existing pitfalls, and provided services.

We argue that this report sheds light on a very shady topic which, despite all technical and legal measures to counter it, remains a very thorny issue for cybersecurity professionals and continues to grow as ransomware groups evolve their tactics.

Data collection methodology

To collect the samples for conducting our research, we used various open malware repositories and analysis services including, but not limited to Malware Bazaar, Triage, Hybrid Analysis, CAPE, JOE Sandbox, and VirusShare. Note that in all cases, we used publicly available samples.

Finally, it is worth highlighting that many web pages that discuss CONTI infections contain images that depict the ransomware notice without obfuscating the ID (see Figure 3).



```
All of your files are currently encrypted by CONTI ransomware.
If you try to use any additional recovery software - the files might be damaged or lost.

To make sure that we REALLY CAN recover data - we offer you to decrypt samples.

You can contact us for further instructions through:
Our email
[redacted]

Our website
TOR VERSION :
(you should download and install TOR browser first https://torproject.org)

http://m232fdxbfmbrcehbrj5iayknxnggf6niqfj6x4iedrgtab4qupzjlaid.onion

HTTPS VERSION :

contirecovery.info

YOU SHOULD BE AWARE!
Just in case, if you try to ignore us. We've downloaded your data and are ready to publish it on out news website if you do not
respond. So it will be better for both sides if you contact us ASAP

---BEGIN ID---
[redacted]
---END ID---
```

Figure 3 – An Example of a CONTI Ransomware Note Including the Victim ID (Redacted)

The latter implies that the security consultants who shared these screenshots did not understand how they were publicly exposing their clients for the sake of publicity. The same applies to security consultants or internal IT/security teams, who uploaded the collected samples to malware analysis services, to have them analysed, without realising that in this way they put the targeted organisations at risk by revealing potentially targeted / maybe even internal not publicly available information[11], as well as useful intelligence to any attackers, which might attempt a newer attack to the organisations, on how the latter handle malware-related incidents.

While there are several hundreds of CONTI samples online, the number of unique IDs is quite limited, which implies that during several campaigns, the spear-phishing emails may have contained different droppers; however, the encryptor (delivered in the final

[11] see for example https://krebsonsecurity.com/2014/01/new-clues-in-the-target-breach/, https://krebsonsecurity.com/wp-content/uploads/2014/01/POSWDS-ThreatExpert-Report.pdf and https://www.qualityplusconsulting.com/res/pos/2014-1-24_InsideTargetBreach_Dell.pdf, where in Target data breach incident the used POS malware, based on relevant reports, was uploaded to Symantec, and contained an internal IP address and as believed by information security researchers, a domain name in Target's network

stage of the attack - the encryption phase -) that was used contained a specific ID per victim at a time, which we later noticed that was reused. Notably, in many of the collected samples, one may notice that the ransomware notice asks the victim to contact the attacker by using ProtonMail, an email service provider which is well-known for the provided privacy and security features and provides also an "open" web[12] and a TOR website URL.[13] [14] This is especially relevant for the first versions of CONTI.

Table 1 illustrates some of these email addresses used by the earlier versions of CONTI. In many of the most recent collected samples, the ID is hardcoded within the binary and, in most cases, can be extracted by simply collecting the strings of the binary. The same applies to the used Protonmail email addresses[15].

Email address
elsleepamlen1988@protonmail.com
southbvilolor1973@protonmail.com
maxgary777@protonmail.com
ranosfinger@protonmail.com
polzarutu1982@protonmail.com
flapalinta1950@protonmail.com
xersami@protonmail.com
heibeaufranin1971@protonmail.com

Table 1 – Some of the ProtonMail email addresses used by CONTI

In total, we extracted 115 unique IDs that we used to connect to the CONTI negotiation platform and extract the relevant negotiations in HTML format. From these IDs, 68 were

[12] https://contirecovery.info

[13] http://m232fdxbfmbrcehbrj5iayknxnggf6niqfj6x4iedrgtab4qupzjlaid.onion

[14] https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5759-ccn-cert-id-02-21-conti-v3-ransomware-1/file.html

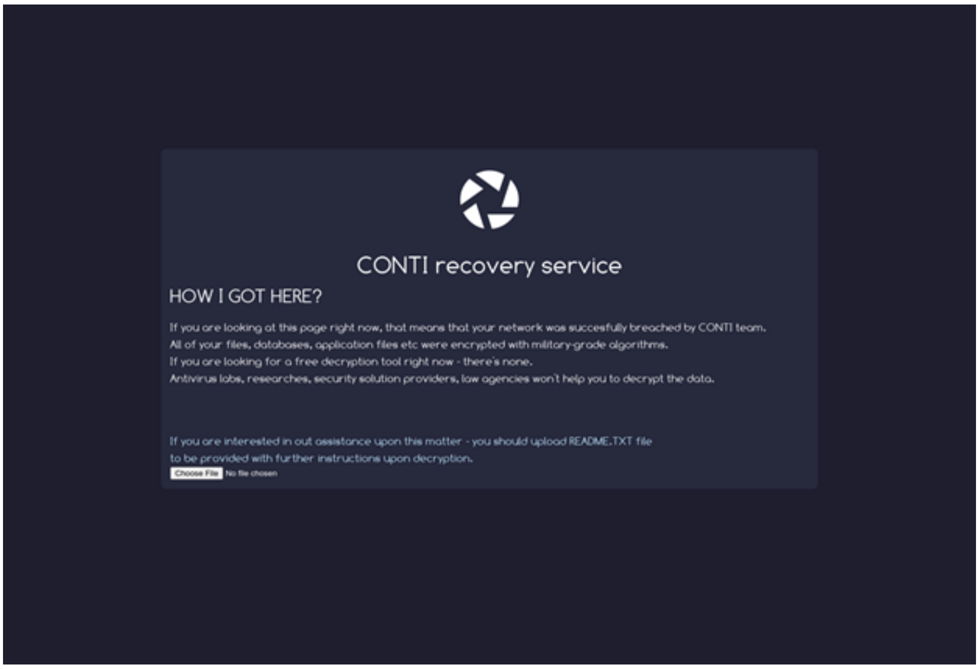
[15] More ProtonMail email addresses used by Conti exist in various OSINT sources, ex. https://www.pcrisk.com/removal-guides/17011-conti-ransomware

valid, and 47 contained negotiations or confirmed victims, i.e., the CONTI operators expected input from the victims.

Negotiations

The CONTI negotiations in general are relatively short, but they may last several weeks. The victims are communicating with the CONTI team through the provided CONTI Recovery Service links that are left in the ransomware notice and discuss the means of infiltration and encryption of their data. Please note that in the first versions of CONTI, the negotiations were initiated through email exchanges. Gradually, in the later versions, the CONTI team developed a specialised platform for the negotiations. The webpage was available on the "open" web with various TLDs (.top, .xyz, .best, etc.) and also through TOR. At the time of writing, it is available through web[16] and through TOR.[17]

The site's design changes over time from the form of Figure 4 to the form of Figure 5.



CONTI recovery service

HOW I GOT HERE?

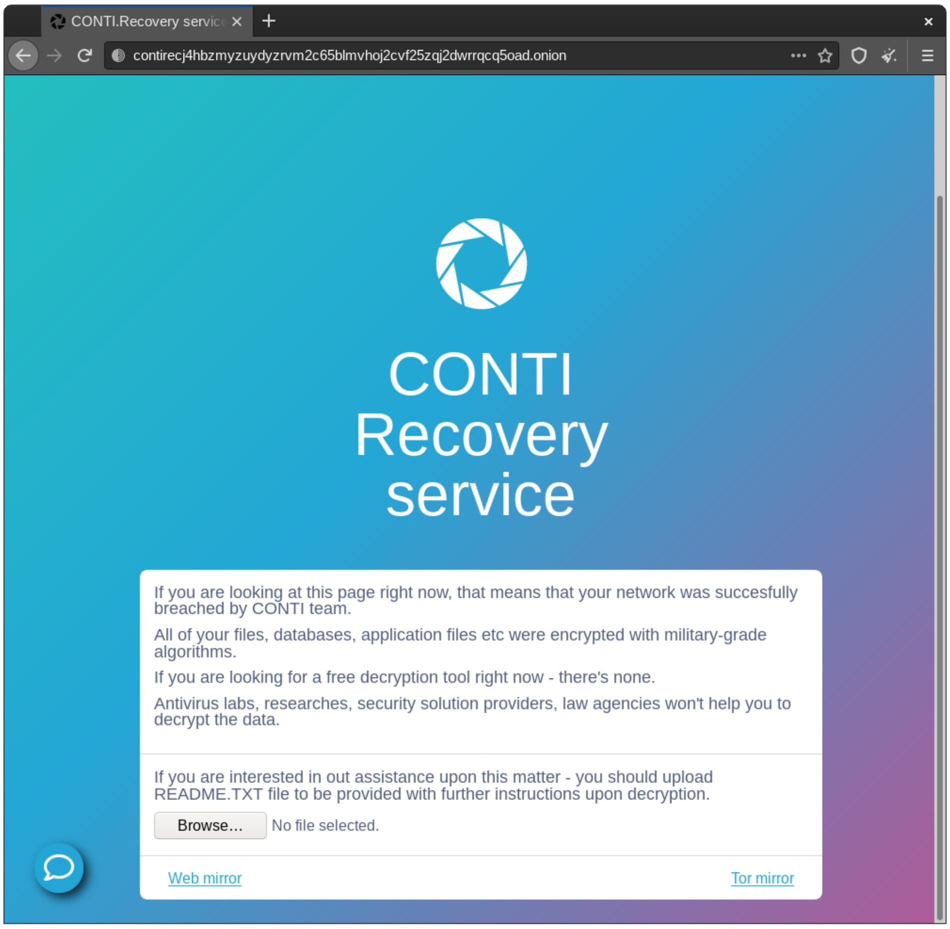
If you are looking at this page right now, that means that your network was succesfully breached by CONTI team.
All of your files, databases, application files etc were encrypted with military-grade algorithms.
If you are looking for a free decryption tool right now - there's none.
Antivirus labs, researches,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

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

Figure 4 – Recovery Site of CONTI (contirecovery.best - contirecovery.info)

[16] https://contirecovery.ws

[17] https://http://contirecj4hbzmyzuydyzrvm2c65blmvhoj2cvf25zqj2dwrrqcq5oad.onion/



CONTI.Recovery servic
contirecj4hbzmyzuydyzrvm2c65blmvhoj2cvf25zqj2dwrrqcq5oad.onion
CONTI Recovery service

If you are looking at this page right now, that means that your network was succesfully 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.

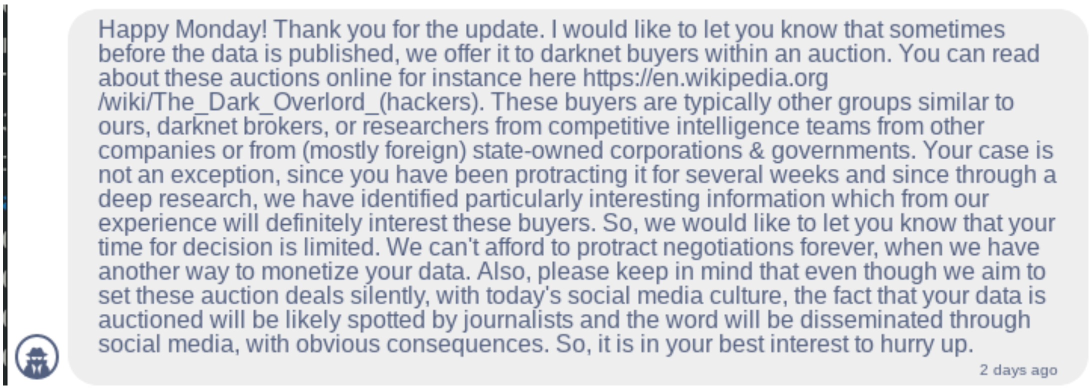
If you are interested in out assistance upon this matter - you should upload README.TXT file to be provided with further instructions upon decryption.

Figure 5 – Recovery Site of CONTI Accessed via TOR

In principle, each victim is assigned with an ID that consists of 64 alphanumeric characters, and the victim must upload the README file to the web form as displayed in Figure 5.

In most cases, the CONTI team requires the representative of the victim to identify himself/herself as well as the victim organization. The latter implies that the people performing the negotiations are not always the same ones who penetrated the victim as the attacker should already know who the victim is.

Nevertheless, on several occasions, the chat is prepared, welcoming the victim organization with their title. If there is no interaction from the victims, the CONTI team starts issuing threats, which initially concern the publication of the collected data on the CONTI News site, with additional threats to sell access to the data. See Figure 6.

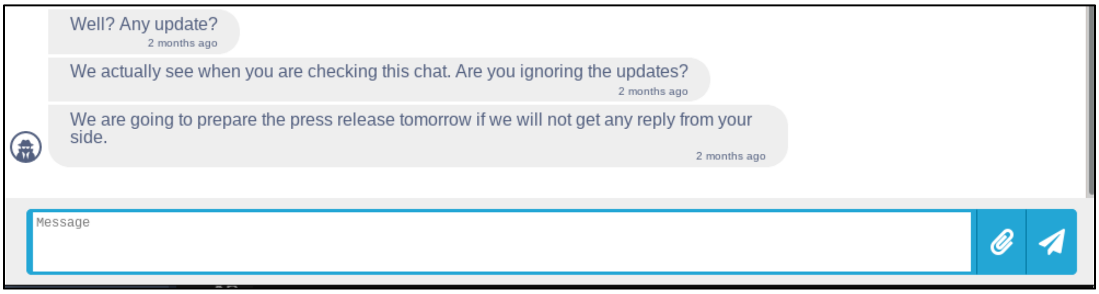


Happy Monday! Thank you for the update. I would like to let you know that sometimes before the data is published, we offer it to darknet buyers within an auction. You can read about these auctions online for instance here https://en.wikipedia.org/wiki/The_Dark_Overlord_(hackers). These buyers are typically other groups similar to ours, darknet brokers, or researchers from competitive intelligence teams from other companies or from (mostly foreign) state-owned corporations & governments. Your case is not an exception, since you have been protracting it for several weeks and since through a deep research, we have identified particularly interesting information which from our experience will definitely interest these buyers. So, we would like to let you know that your time for decision is limited. We can't afford to protract negotiations forever, when we have another way to monetize your data. Also, please keep in mind that even though we aim to set these auction deals silently, with today's social media culture, the fact that your data is auctioned will be likely spotted by journalists and the word will be disseminated through social media, with obvious consequences. So, it is in your best interest to hurry up.

2 days ago

Figure 6 – CONTI Team Threatening to Sell the Victim's Data

On several occasions, the CONTI team notifies the victims, which did not give in to their threats before the deadline provided by the CONTI team, that the publication of their data has started/finished and/or that a buyer for the data has been found. The chat activity is occasionally monitored by the operators, e.g., that a person logged in, see Figure 7.



Well? Any update?
2 months ago

We actually see when you are checking this chat. Are you ignoring the updates?
2 months ago

We are going to prepare the press release tomorrow if we will not get any reply from your side.
2 months ago

Figure 7 – Excerpt from the CONTI Negotiation Platform

The threats for publication/selling of the data, in the beginning, do not have a strict nor specific deadline. Depending on the interaction of the victim with the CONTI team (or lack of it), they evolve from generic to 'soon', 'next week', etc. Refer to Figure 7 for an example of a generic deadline.

When victims decide to negotiate the price, typically, they require a guarantee that their files will be recovered. Therefore, CONTI operators provide a 'data pack' as they call it, which shows through the contained files the name of the victim and usually 30% of the directory listing tree for the encrypted files. Moreover, they might ask the victim to "provide two files for a test decryption", which they subsequently decrypt. The decrypted files as well as the 'data pack' are provided to the victims through various usually "obscure" file services. More precisely, for exchanging files with the victims, the CONTI team uses the following services:

- https://qaz.im/
- https://transfer.sh/
- https://dropmefiles.com/
- https://www.sendspace.com/

The main reason for using these services is probably some of their features, e.g., the services provide a deletion mechanism for the recipient of the uploaded files, they are free, they do not require strong authentication.

The exchanged files are encrypted by using default mechanisms (e.g., the embedded encryption mechanism of compression programs) and simple passwords (e.g., 123123) to prevent compatibility issues for the recipients of the files.

After the introductions, the negotiation starts with an initial ransom price from the CONTI team. Since all the negotiations did not lead to a deal, we report in Table 2 the initially requested ransom and the agreed one that was paid for the payments that we could verify through the bitcoin transactions.

Initially requested ransom	Paid ransom	Steps	BTC
1,250,000	1,000,000	1	20.05326047
3,000,000	800,000	6	17.084
5,000,000	746,500	6	15.43
999,000	512,000	8	10.22997602
900,000	450,000	6	8.00275566
1,500,000	350,000	10	9.69536871

Initially requested ransom	Paid ransom	Steps	BTC
900,000	325,000	15	8.90692000
980,000	300,000	7	7.87000000
400,000	200,000	9	5.42840261
1,700,000	120,000	8	2.61000000
300,000	150,000	5	2.46426081
200,000	100,000	7	2.46426081
150,000	100,000	3	2.65200000
	3607000	7 (average)	112.8912051

Table 2 – Statistics from the confirmed payments of the collected negotiations.

Moreover, we report in sum the negotiation steps (how many different ransom amounts were asked by CONTI team and how many counteroffers the victims performed) as well as the ransom amounts in Bitcoin, which were paid to the corresponding wallets.

It should be highlighted that the attackers use the financial status and public reports of each separate victim to assess the requested ransom and stress this information through the discussions to press for increased prices. The latter is verified by the operational/training documents of the group, which were leaked in August by a "disgruntled employee", who "left" the group.

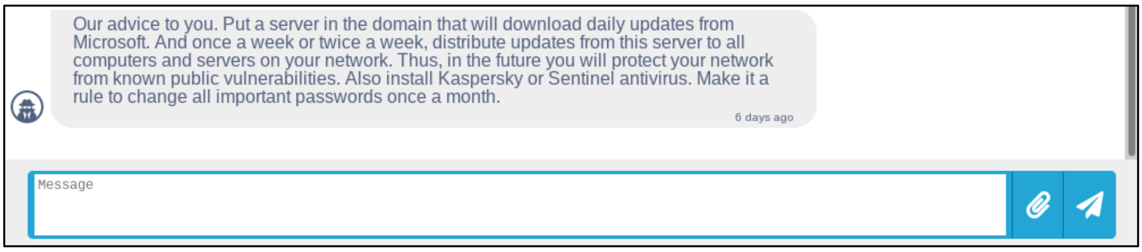
After the payment is made by the victims, CONTI operators provide the victim with a decryptor. A typical issue of the decryptor, which is reported by the victims, is that many files, subsequent to have been decrypted, keep the added ransomware extension (e.g., .LSNWX as in the intercepted chats and according to other sources[18]), which the victim has to manually remove, to access the decrypted files.

On some occasions, the victims requested feedback on how the attack was made. The response from the operators was rather generic as, e.g., the corresponding person was "inaccessible". The operators notified that an employee opened a malicious

[18] https://www.splunk.com/en_us/blog/security/conti-threat-research-update-and-detections.html

link/attachment on an email that gave them access to the host to execute malicious code. From there, they only report the use of Mimikatz and other tools, as well as that they performed lateral movement to extract the domain/admin passwords. The latter is also aligned with the leaked operational/training documents of the group.

In some instances, the operators recommend their victims to use SentinelOne, Kaspersky, or Symantec security solutions, see Figure 8. Note again that the leaked operational/training documents of the group contained instructions on how to turn off Microsoft Defender and Sophos AV solutions. Apart from the decryptor, they often provide the log file of gshred, which they used to shred the files that they exfiltrated from their victim.

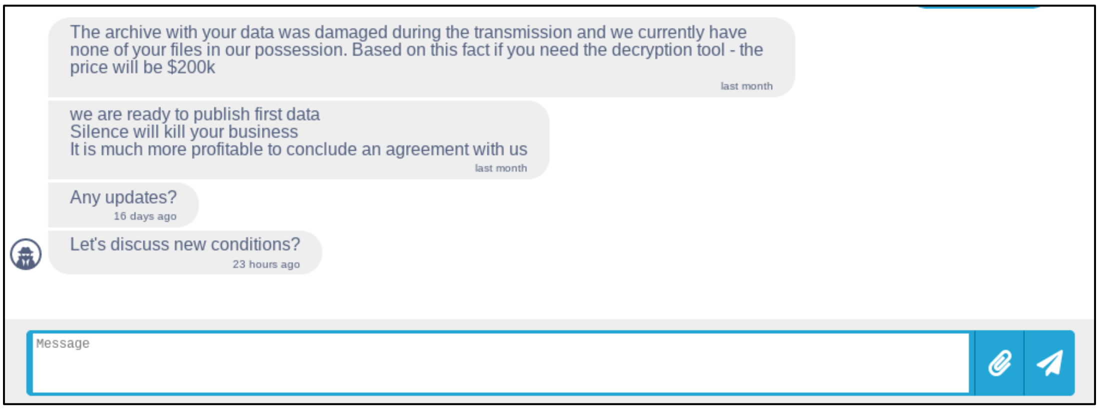


Our advice to you. Put a server in the domain that will download daily updates from Microsoft. And once a week or twice a week, distribute updates from this server to all computers and servers on your network. Thus, in the future you will protect your network from known public vulnerabilities. Also install Kaspersky or Sentinel antivirus. Make it a rule to change all important passwords once a month.

6 days ago

Figure 8 – Security 'Advice' From the Negotiators After the Payment

It should be noted that in one negotiation the team admitted having lost the files during exfiltration. Therefore, since the extortion for publishing the files could not work for them, they proposed a discount of 50% to the victim for the decryption tool, see Figure 9.



The archive with your data was damaged during the transmission and we currently have none of your files in our possession. Based on this fact if you need the decryption tool - the price will be $200k

last month

we are ready to publish first data
Silence will kill your business
It is much more profitable to conclude an agreement with us

last month

Any updates?

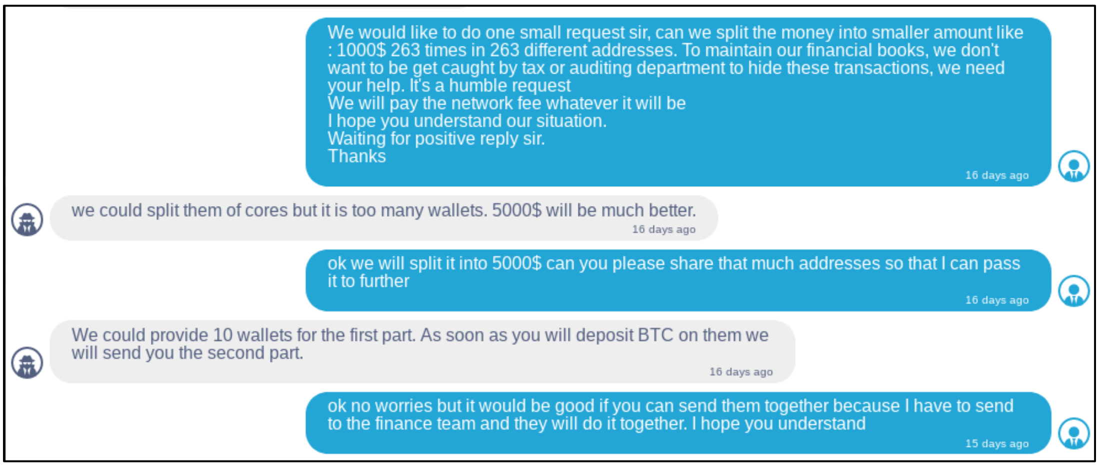
16 days ago

Let's discuss new conditions?

23 hours ago

Figure 9 – Notification of Losing the Victim's Files.

Examples have also been observed where the victims have successfully negotiated the payment of the ransom in smaller chunks, see Figure 10.



We would like to do one small request sir, can we split the money into smaller amount like : 1000$ 263 times in 263 different addresses. To maintain our financial books, we don't want to be get caught by tax or auditing department to hide these transactions, we need your help. It's a humble request
We will pay the network fee whatever it will be
I hope you understand our situation.
Waiting for positive reply sir.
Thanks
16 days ago

we could split them of cores but it is too many wallets. 5000$ will be much better.
16 days ago

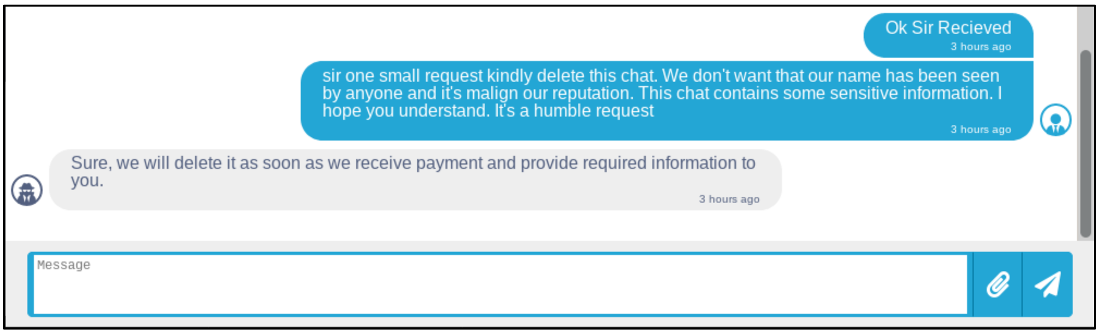
ok we will split it into 5000$ can you please share that much addresses so that I can pass it to further
16 days ago

We could provide 10 wallets for the first part. As soon as you will deposit BTC on them we will send you the second part.
16 days ago

ok no worries but it would be good if you can send them together because I have to send to the finance team and they will do it together. I hope you understand
15 days ago

Figure 10 – Request for payments in smaller chunks.

We should also highlight that some negotiators seem to be aware that people may monitor these negotiations. Therefore, they may specifically request the deletion of these chats, see Figure 11.



Ok Sir Recieved
3 hours ago

sir one small request kindly delete this chat. We don't want that our name has been seen by anyone and it's malign our reputation. This chat contains some sensitive information. I hope you understand. It's a humble request
3 hours ago

Sure, we will delete it as soon as we receive payment and provide required information to you.
3 hours ago

Figure 11 – Request for Chat Deletion

Finally, of specific interest is the very well-known case of the Irish Health Service Executive (HSE)[19]. The initially requested price was $19,999,000. The HSE representative asked the team only for proof that they indeed had access to the data. After the proof was provided, it is probable that the public outcry forced the CONTI team to provide the

[19] https://www.reuters.com/technology/irish-health-service-hit-by-ransomware-attack-vaccine-rollout-unaffected-2021-05-14/

decryptor for free without any further discussion. Then, the HSE side proceeded with notifying the perpetrators of the legal actions that had been initiated against them.

Since there was no payment, CONTI team notified that they would try to sell the collected data. Notably, this negotiation was trolled by another person who accessed the relevant ID negotiation page.

Discussion

While it is rather common to share malware samples, it is rather odd to have such samples in the open. Clearly, the infected organizations or the tasked analysts opted to upload the samples as public samples without thinking of the consequences. In essence, without prior analysis, this is a rather lousy practice since, in targeted attacks, this may leak sensitive information.

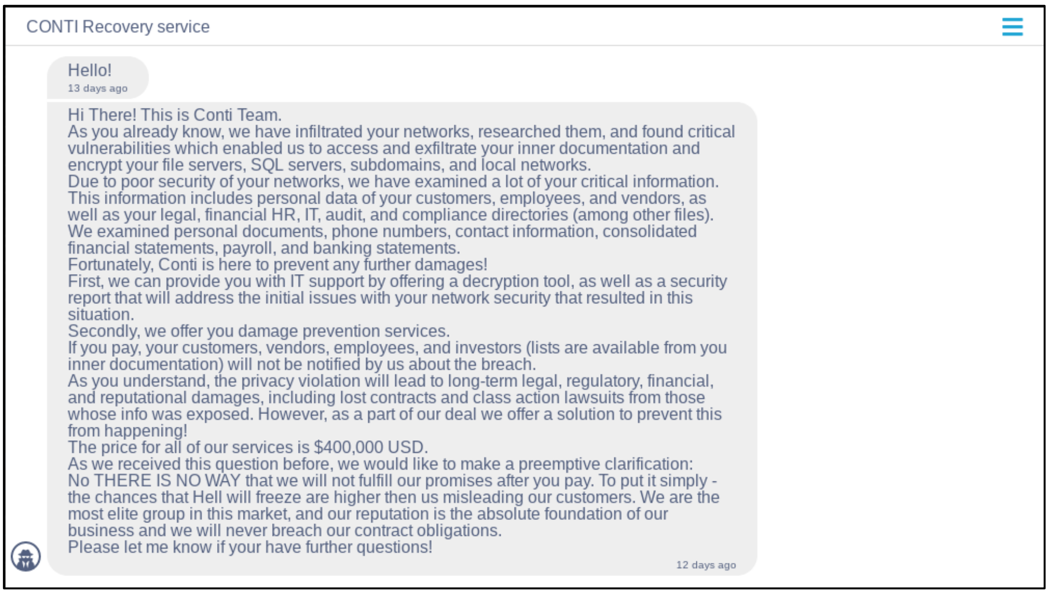
Indeed, despite the fact this allows for snooping of the negotiations, it also impedes the process. As observed, third parties had intervened and 'trolled' the negotiations twice (not only in the HSE case) or made the perpetrators see that there is traffic and expect interactions from their victims when this was not the case. In an isolated case, the negotiations were continued in another platform since they were conducted with someone that according to the victim, should not have access to them. Even more, in several cases, the victims did not request proof of the decryption of their files or the shredding log, which shows a lack of capacity in handling such cases.

We should report that we have three cases where we do not have the full negotiations. Therefore, we do not know how they ended nor any bitcoin address to determine whether the victims paid the requested ransom. However, the victims are not listed in the exposure web page.

A very interesting finding has to do with the handling of the negotiations. As discussed, one would expect that each ID is targeted to a single organization, as this would be a result of a spear-phishing campaign. However, the latter is not actually the case as we have noticed that the same IDs are used with new victims. Therefore, previous victims may look at the negotiations of new victims.

Moreover, we have observed that the negotiation chat is occasionally cleared. More precisely, not all chats are available continuously and not to their full extent. In fact, we have observed the removal of fragments of the discussion, with the most noticeable being the removal of bitcoin addresses. This implies that the operator of each negotiation has the option to clear part of the chat and that different operators could be assigned per ID. The reuse of IDs may imply the use of the same encryption key, so decryptors may work for other victims; however, with the ones at hand, this claim cannot be verified.

It should also be noted that the operators reuse a lot of wordings for, e.g., salutation, requesting interaction, ransom bidding. For instance, the exact same wording as in Figure 12 has been intercepted more than once. Indicatively, we point out that the exact same text with Figure 8 is used in another chat with the sole change that instead of Kaspersky, it was referring to Symantec. The above implies that apart from the leaked training/operational manuals, there is another 'playbook' for the negotiations, which includes what should be said and how.



Hello!
13 days ago

Hi There! This is Conti Team.
As you already know, we have infiltrated your networks, researched them, and found critical vulnerabilities which enabled us to access and exfiltrate your inner documentation and encrypt your file servers, SQL servers, subdomains, and local networks.
Due to poor security of your networks, we have examined a lot of your critical information. This information includes personal data of your customers, employees, and vendors, as well as your legal, financial HR, IT, audit, and compliance directories (among other files).
We examined personal documents, phone numbers, contact information, consolidated financial statements, payroll, and banking statements.
Fortunately, Conti is here to prevent any further damages!
First, we can provide you with IT support by offering a decryption tool, as well as a security report that will address the initial issues with your network security that resulted in this situation.
Secondly, we offer you damage prevention services.
If you pay, your customers, vendors, employees, and investors (lists are available from you inner documentation) will not be notified by us about the breach.
As you understand, the privacy violation will lead to long-term legal, regulatory, financial, and reputational damages, including lost contracts and class action lawsuits from those whose info was exposed. However, as a part of our deal we offer a solution to prevent this from happening!
The price for all of our services is $400,000 USD.
As we received this question before, we would like to make a preemptive clarification:
No THERE IS NO WAY that we will not fulfill our promises after you pay. To put it simply - the chances that Hell will freeze are higher then us misleading our customers. We are the most elite group in this market, and our reputation is the absolute foundation of our business and we will never breach our contract obligations.
Please let me know if your have further questions!
12 days ago

Figure 12 – Reused salutation by the CONTI team.

During the negotiations, the operators try to appear as professionals, to belong to a greater group as in a formal organization and to be friendly to the victim without initiating further discussions. In fact, the group has been reported to be recruiting people through advertisements[20]. The negotiation depending on the organization, may take several iterations and immediate payments are favored and discounted. The negotiators of the CONTI group, appearing as professionals, sometimes mention their victims as customers/clients and not as victims.

Finally, after the recent leaks of chats on the media, CONTI has introduced a CAPTCHA mechanism in the negotiation site.

Conclusion

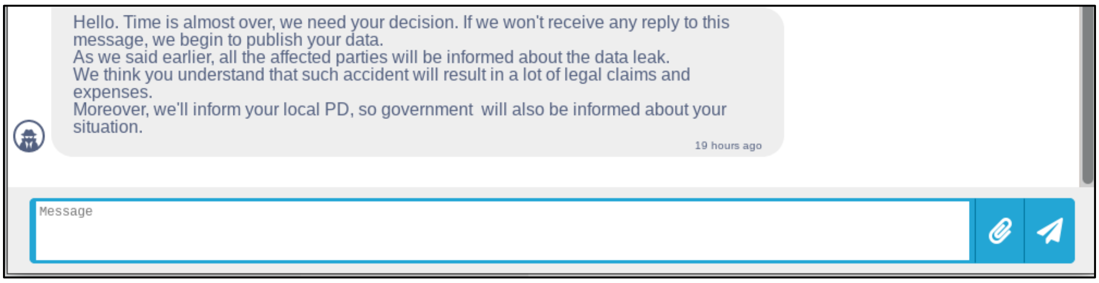
The authors of this work do not by any means promote the payment of ransom. On the contrary, we illustrate how this trend has evolved into a multi-million industry worldwide and made organizations suffer. We illustrate in this research that several practices, such as sharing malware samples without proper sanitization of the binary, may have a boomerang effect on the victim by further exposing him/her.

Indeed, one can understand how such negotiations could be derailed by third parties entering the negotiations. Moreover, even if the victim paid for the ransom, third parties had access to the sensitive data and that the exposure could be even more augmented. In a wilder scenario, another adversary could jump in the conversation and convince the victim of being the original adversary and luring him/her into paying the ransom in another wallet or double encrypting the victim's files.

Given the public leaks and their size, an obvious question that should be investigated is whether the victim organizations have reported these attacks appropriately, as legal obligations of, e.g., GDPR, set specific deadlines for these actions. The question is even

[20] https://www.sekoia.io/en/an-insider-insights-into-conti-operations-part-one/

more relevant for the cases of organizations that paid the ransom and whose data leakages cannot be verified through the public leaks. In fact, the legal implications are an aspect that the CONTI team is often trying to use to convince their victims in paying the ransom, see Figure 13.



Hello. Time is almost over, we need your decision. If we won't receive any reply to this message, we begin to publish your data.
As we said earlier, all the affected parties will be informed about the data leak.
We think you understand that such accident will result in a lot of legal claims and expenses.
Moreover, we'll inform your local PD, so government will also be informed about your situation.

19 hours ago

Figure 13 – Stressing of Legal Obligations by the CONTI Negotiator

References

[1] Caporusso, Nicholas, Singhtararaksme Chea, and Raied Abukhaled. 2018. “A Game-Theoretical Model of Ransomware.” In International Conference on Applied Human Factors and Ergonomics, 69–78. Springer.

[2] Cartwright, Edward, Julio Hernandez Castro, and Anna Cartwright. 2019. “To Pay or Not: Game Theoretic Models of Ransomware.” Journal of Cybersecurity 5 (1): tyz009.

[3] ClearSky Cyber Security. 2021. “CONTI Modus Operandi and Bitcoin Tracking.” https://www.clearskysec.com/wp-content/uploads/2021/02/Conti-Ransomware.pdf.

[4] DiMaggio, Jon. 2021. “RANSOM Mafia. ANALYSIS of the World’s First Ransomware Cartel.” https://analyst1.com/file-assets/RANSOM-MAFIA-ANALYSIS-OF-THE-WORLD%E2%80%99S-FIRST-RANSOMWARE-CARTEL.pdf.

[5] Hernandez-Castro, J, A Cartwright, and E Cartwright. 2020. “An Economic Analysis of Ransomware and Its Welfare Consequences.” Royal Society Open Science 7 (3): 190023.

[6] Hofmann, Tom. 2020. “How Organizations Can Ethically Negotiate Ransomware Payments.” Network Security 2020 (10): 13–17.

[7] Laszka, Aron, Sadegh Farhang, and Jens Grossklags. 2017. “On the Economics of Ransomware.” In International Conference on Decision and Game Theory for Security, 397–417. Springer.

[8] Li, Zhen, and Qi Liao. 2020. “Ransomware 2.0: To Sell, or Not to Sell a Game-Theoretical Model of Data-Selling Ransomware.” In Proceedings of the 15th International Conference on Availability, Reliability and Security, 1–9.