STORMGuidance

Ransomware Negotiation

Royal Mail International-LockBit Transcript Analysis

This report is an analysis of the ransom negotiation transcript relating to the ransomware attack on Royal Mail International in January 2023.

Report date: March 2023

stormguidance.com
contact@stormguidance.com

Contents

STORM overview

STORM Guidance Ltd (STORM) is an information risk advisory firm specialising in Cyber Risk Management and Incident Response.

STORM has been responding to, and managing cyber incidents for decades, and with this experience is ideally placed to help clients better assess and manage cyber risk, improve the management of potential cyber incidents, increase the effectiveness cyber investigations, and optimise other related prevention measures. Our advisors are based in the UK, Mauritius, India, and the USA.

Threat Actor Engagement

Threat Actor Engagement (TAE) describes the interaction between cybercriminals and their victims in negotiation of an extortion demand.

This most commonly involves ransomware incidents but can also be a key requirement in other data breach incidents.

We have been working on ransomware negotiation for several years, after decades negotiating and managing negotiators in kidnap and ransom, product contamination and other crimes.

With several years' experience themselves, cybercriminal Threat Actors (TAs) are now wellversed (but not necessarily good) at negotiating ransoms. The ransomware extortion 'offer' is to provide the victims with decryptors necessary to recover their data along with a promise to delete the stolen business and personal data.

Demands, usually made in US dollars and requiring the cryptocurrency (usually Bitcoin) equivalent to be paid to incident-specific wallet addresses, are often enhanced by deadlines to which the victim is pressured to meet. The threats are the destruction of decryption keys and release of stolen data on publicly accessible online forums.

There are now several companies offering ransomware negotiation services and we have noticed that many ransom negotiators have, by their own admission, reached these positions by chance and are not formally trained negotiators. This poses a financial, legal, and reputational risk, to both the victims and those supporting them i.e., cyber insurers, as an untrained ransom negotiator is likely to make mistakes that results in unnecessary loss.

STORM established our TAE team, headed by Nick Shah OBE, in 2019. Our team differs from many in that we have formal training in ransom negotiation. We view the negotiation discipline objectively, as a science. Our TAE service includes both negotiation and ransom settlement, incorporating the required sanctions checks to ensure legality of settlement.

All TAE engagements are provided with a full report upon completion.

A point on ethics

STORM's position on the ethics of interacting with cybercriminals is one of necessity on behalf of our clients as victims of cyber incidents.

We always assist our clients in thorough investigation and recovery activities and attempt to find every conceivable way to avoid paying a ransom demand by exploring every practical option for recovery and minimisation of reputational harm.

TAE is not merely undertaken to facilitate the payment of a demand. STORM negotiators use their skills to gain intelligence and information from TAs that enable clients, and their professional advisors, to better understand and assess the risks resulting from the incident.

If clients are in a position where negotiation is needed, we advocate a professional interaction with the threat agents from a negotiator that is both experienced and professionally trained in ransom negotiation. The aim being solely to minimise the impact on the client's business.

Our work in this field in no way conveys support for ransom payments but for whatever is in the best interests of the victim organisation whose situation will vary widely dependent on any specific incident.

Full sanctions checks are inclusive in our TAE service and are both thorough and complete with a separate report to support the client in their compliance with regulatory and legal obligations.

Good practice objectives in ransom negotiations

Best-practice tactics in ransom negotiation is extensive, and it is not practical to describe this in detail in this paper.

There are five key objectives that any professional negotiation should make core to a strategy which the victim's executive management wish to pursue. In our support for our clients, we clearly explain these objectives which are as follows:

1. Obtain 'Proof of Life' of the stolen data.

It is vital to ensure that the criminals with which the negotiation is proceeding are indeed those in possession of the stolen data and not, as can occur, other criminals who, after monitoring leaks sites and other sources, attempt to divert ransom payments. Such interlopers will not provide a path to recovery.

2. Obtain proof of the ability of the TAs to decrypt the stolen data.

There may be reasons why attackers cannot decrypt data. These include technical issues during the attack, internal disagreements between cybercriminal groups and others. It is vital that TAs can evidence a decryption capability for negotiations to proceed.

3. Introduce time delays.

Whilst one may consider that victims would ordinarily wish to proceed rapidly with a ransom negotiation, in many cases they need time to consider their options, notify stakeholders, regulators, clients, other partners and even data subjects put at risk because of the data breach. Winning extended time is therefore an important aim of many negotiations, regardless of the intention to settle the demand.

4. Obtain assurance of data deletion.

Regardless of the question of credence which a promise of secure data destruction may raise, it remains an important objective, if only for the purposes of record-keeping.

5. Reach an acceptable negotiated settlement.

For those incidents where the victim is forced to cede to the ransom demand, a key objective for a professional negotiator is to reduce the quantum of such a demand to a level which is acceptable to both parties.

There are many other secondary objectives and techniques in both good and mandatory practices that must be used in ransom negotiations. As you will read, some practices can

support detection in cybercriminal investigations whilst others may lead to unnecessary risk for the victim.

One critical practice in negotiation is never to become emotive in your posts. They should always be cordial, and never committal.

Also, of importance is the adoption of 'maker-checker' processes to ensure that good practice is observed, and the negotiation is developed carefully and positively. The STORM TAE unit have an overall Communications Controller who operates this vital control.

The Royal Mail International ransomware incident

The cyber-attack on Royal Mail International (RMI) was first alerted on 11th January 2023 when reports began to emerge that RMI were experiencing severe service disruption to international export services.

Within a few days, it became apparent that RMI were the victim of a ransomware attack by the LockBit ransomware gang; likely to be a LockBit affiliate.

Reports stated that the UK National Cyber Security Centre (NCSC) and National Crime Agency (NCA) were assisting RMI in both investigation and recovery.

The ransom demand was for $80 million US dollars in crypto currency (LockBit demands are usually for Bitcoin/BTC).

Sources reported that RMI were still working to restore operations over two weeks later although the transcript shows that engagement with the LockBit TAs began on 12th January and ended around twenty-eight days later, on 9th February. RMI negotiators appear to have terminated their interactions several days earlier, on 4th February, by which time they managed to recover to an acceptable operational state without the need to settle the ransom demand. According to press releases on 26th January, RMI were indeed resuming services.

On 7th February, the LockBit TAs posted an intention to release the stolen RMI data just hours before the penultimate entry in the negotiation transcript, and at a point where it was highly likely the RMI negotiators would not respond.

Sources reported on 14th February that the LockBit TAs had released the transcript of the ransom negotiations[1], an unusual action by cybercriminals.

[1] https://www.itpro.co.uk/security/ransomware/370067/lockbit-releases-negotiation-history-royalmail-ransom-65-million

By 23rd February, the TAs deadline time had run down and been reset; just as it has on several previous occasions, with no apparent release of stolen data. However, soon afterwards, the RMI dataset was released but not immediately downloadable due to sustained DDoS attacks on the LockBit site, presumably by RMI supporting entities. Since that time, however, the data has been acquired and is available via several sources and comprises a significant dataset which is 44GB in compressed format.

Analysis of the negotiation transcript

Introduction

Before we begin, we should make it clear that STORM has had no interaction with RMI or any other party relating to this incident. The negotiation transcript is purported to be a record of the negotiations between RMI and the LockBit TAs but we have no way of confirming this.

The transcript was downloaded from the LockBit TAs dark web leak site.

All our insights are informed by our training and experience as ransom negotiators and have been drawn solely from the analysis of the negotiation transcript and supporting information from standard open-source threat intelligence and press releases.

We make no definitive claims as to accuracy of our analysis and offer this report to assist the reader to understand how such a transcript may divulge significant useful information about both attacker and victim. None of our analysis should be considered as critique of any specific parties but as a generic review that can be applied to any similar ransom negotiation record.

For reference, we include the negotiation transcript as an addendum to this report with our key analysis points as observations in red boxes. The date/time stamps follow each post. We have used highlighted colour to indicate both obvious and possible changes in negotiator on both sides.

> **Note:** *Although the initial transcript contained the Royal Mail logo, we have removed this. No other changes to posts have been made and additions are purely the results of the analysis.*

Negotiation Transcript Analysis

We have several observations from our analysis of the transcript which was released by the LockBit TAs on or soon after 14th Feb 2023, over a week ahead of the release of the stolen data.

The negotiations begin by indicating a former, but brief, discussion had taken place via an alternative chat session. However, the negotiations only begin in earnest, as the transcript begins, in the early afternoon 12th January 2023.

Negotiations begin cordially with the RMI negotiators using good practice in polite wording; a ***"thank you"*** in response to being sent a link to download a file containing a folder tree listing as proof that stolen RMI data was in the hands of the LockBit TAs.

'Proof of Life' of Data obtained

More good practice by the RMI negotiators is recorded when they request confirmation that the tree listing comprises the entirety of the stolen data which the TAs confirm.

Of course, such confirmation may not be reliable, but can help to inform the scope of the data breach.

Within 25 seconds of the confirmation, the RMI negotiators state that they have downloaded and opened a specific file. We assume that they performed this action following strict operational security (OpSec) practices as to do so without protection risks infection with further malware. Furthermore, because TAs would expect the use of OpSec; even by IT staff, (the fake identity or 'legend' that the RMI negotiators were using), the speed of the reply post indicates a missed opportunity to introduce a plausible time delay.

Shortly after, in response to a TA question, the RMI negotiators introduce themselves as working in IT and state that their Management have asked them to contact the TAs as directed in the ransom note. Again, it is good practice for the victim's negotiators to adopt a legend through which to negotiate.

Basic legend established

There are several good practices when establishing legends.

The most important is to ensure legitimacy whilst also allowing for several layers of escalation before reaching decisionmakers. In this case, the RMI negotiators simply stated that they worked in IT. Sometimes it is useful to use a first name and to give the legend an air of relative naivety and ignorance, which can assist in the negotiation

process. However, if a more descriptive legend is used it is important to ensure that information about the legend is provided in relevant online sources e.g., websites, social media, in case the TAs decide to research for authenticity.

Dialogue language analysis

The use of language is key in ransom negotiations.

Whilst the primary objectives of all parties to a negotiation is to maintain anonymity, it is useful to identify key language traits of the TAs as they may support any subsequent cybercriminal investigation or indicate potential ambiguities in semantics if the negotiation language is not their first language. Similarly, it is vital that the victim's negotiators use nothing other than dialogue which would be expected from the legend they are adopting. We refer to such potential identifiers as a 'Tell'.

In this case, at 13:54 UTC on 12th January, the TAs are the first to offer a Tell in the language of their dialogue when they post ***"to whom am i speaking"***. This wording indicates that the TA negotiator has been formally educated in English language. Other posts also indicate a similar conclusion. However, other posts which are close together in the timeline also exhibit poorer use of English. An example occurs on the 12th of January at 13:53 UTC, ***"Yes, don't delay. time is not playing in your favor. so far, we have not reported the attack on our blog."*** is an interesting potential Tell because the grammar is inexact and because American English is used in the word ***"favor"*** (English spelling 'favour'). This dialogue may indicate that the TA negotiator is trained and fluent in American English.

Much later, on the 25th of January at 18:05 UTC, the RMI negotiators also provide a tell when they post, ***"Just name the amount already so we can let the leadership know."***. The use of the word 'already' in this context indicating the negotiators use of English American words.

Another post on the 27th of January at 23:21 UTC provides an additional tell. The post reads ***"Anyways, time for bed. The board has meetings this weekend and we will not have anything new to speak about until Monday while they make their decision."***. The use of the word 'Anyways' again indicating the negotiators use of an English American phrase.

These are unnecessary giveaways to the TAs as it would be logical for them to assume that IT staff working for RMI, would be English and not American, therefore this would reinforce any suspicions that RMI are using professional negotiators. Such a revelation may change the nature of the dialogue and place the RMI negotiators at a disadvantage.

Multiple negotiators

Analysis of the transcript indicates that both the TAs and RMI may have used multiple negotiators.

The RMI negotiation proceeds, in the first third of the transcript dialogue, with short, punchy single or two-sentence posts. Then on or around the 20th January, the use of much longer posts begins, indicating a distinctive style of negotiation with the latter appearing less experienced (see 'Lengthy posts' below).

The TA negotiators also appear to change from a lead negotiator style established at the outset, to one that appears more in technical support (posts recorded from 21st to 27th January) before either reverting to the original or a different negotiator as it becomes clear that progress; from the TAs point-of-view, is not positive.

Another potential indicator of multiple negotiators on both sides (highlighted in the transcript by Red, Yellow and Orange representing possible different TA negotiators and Green and Blue representing RMI negotiators), is that there are changes in writing style which include subtle variations:

- In the use of first person 'I am' versus 'we are'
- In the use of British English versus American English
- In preference for short posts to much longer posts
- Between technical and business style

There may be fewer negotiators (3 TAs vs 2 RM) however there is unlikely to be just one for each side unless they are relaying post content from others advising them.

Lengthy posts

At a couple of points, we note that the dialogue becomes both extended i.e., when discussing file sizes to decrypt around 21st January at 13:24 UTC, to a point where it is in danger of becoming diatribe i.e., when attempting to reduce the ransom demand around 26th January at 21:58 UTC.

Lengthy posts are sometimes needed; however, they do raise the following risks and should therefore be avoided wherever possible:

- Revealing the authoring by a party other than that adopting the legend.
- Raising the temperature of the negotiation, becoming emotive and antagonising the TAs.
- Inadvertently revealing tells.

Posting cadence

Whilst one may consider that the victim's negotiators are at a disadvantage in a ransom negotiation, this need not be the case.

With careful thought it is possible to effect certain control over the dialogue. The timing between posts is one such control; what we refer to as 'posting cadence'.

The reason why posting cadence is important is that it enables control over timed delays (see below). Optimum cadence consists of concise posts where timing is well-controlled.

Of course, it is not possible to control what and when the TAs post. However, as criminals driven by greed, they will often respond soon after the victim's negotiators post, in this way it is possible to effect control over the posting cadence.

Good negotiation requires that all promises are kept. This is why, when it comes to many aspects of negotiation, the victim's negotiators should not make promises, especially when it comes to agreeing the ransom, except right at the very point when they are ready to settle.

However, the use of promises can be made to control the posting cadence and therefore control timed delays.

Our analysis of the negotiation transcript shows that the RMI negotiators do not appear to have considered the posting cadence, how it can be used to control timed delays and keep the TA negotiators calm and as close to rational as possible. As a result, on 28th January, the discussion descends into a multi-lined spat. Even if, at this point, RMI had no intention of settling the ransom demand, this resulted in needlessly antagonising the TAs.

Timed delays

Related to posting cadence, timed delays are a key strategic objective (see point 3. above) in an extortion demand scenario.

They interrupt the TAs demand process to provide vital time for the victim's senior management to consider reputational harm in the need for regulatory reporting, the observation of contractual obligations and to consider, plan and execute notifications to third parties and data subjects at high risk (of fraud, identity theft and cyberattack). Timed delays also give technical first responders the window they need to determine whether systems can be recovered without the need for decryptors.

Our analysis of the timed delays appears to show that little or no consideration was given by the RMI negotiators to their importance. In some cases, opportunities for introducing a timed delay were missed; examples include places where it would have been natural to take time to download and review 'Proof of Life' of the stolen data, yet no such delays were introduced.

In other cases, clearly excessive delays in posting by the RMI negotiators have served little use except to increase the risk of antagonising the TAs. Examples are 13th January at 20:00 UTC, (a Friday), where RMI negotiators make a promise by posting ***"We shall return to speak on Monday following the weekend and lengthy discussions with our internal stakeholders."***.

This promise is not kept. Having waited for the time promised, the TA negotiators post at 20:59 on Monday 16th January asking for a response. However, this is not provided until 22 hours later, at 19:12 on 17th January. A subsequent delay lasts over 40 hours.

Whilst we do appreciate that the RMI IT and Executive teams would have been working hard to determine both whether recovery was possible and the business impact flowing from pending release of the stolen data, we consider it is the role of the RMI negotiators to use timed delays in an effective way (usually several holding posts spread out over time), giving consideration to the posting cadence and without risking the overall negotiation.

Time zone tells

Revealing the potential time zones from which either party is operating can assist the other side to better understand their adversary.

On 21st January the RMI Negotiator posts at 04:00 UTC and again at 04:03 UTC. As RMI are a UK-based company, posting at this time may give the TAs a hint that the RMI negotiator is based outside the UK, probably in the USA, where it would be late evening. An alternative reason would hint at desperation in late working.

On its own, this tell may be of limited value, however when combined with other tells i.e., the use of American English and the use of an 'IT staff' legend, this strongly indicates to the TAs that the RMI negotiator is not who they claim to be. It is never good to unnecessarily compromise an established legend.

Potential identification tells

The legend used by the RMI negotiators was likely compromised when it was revealed that they may be native American English speakers.

In addition, an exceptionally long post on 26th January at 21:58 UTC added credence to the tell.

This post is long and appears to be dictated content i.e., that which a negotiator with an IT legend would be unlikely to know. This is poor practice.

If a negotiator is asked to relay such information, it is important that they do so whilst ensuring the maintenance of their legend. Actions to degrade the authenticity of a legend negate the benefits in having one. Care should always be taken to restrict information flowing to the TAs which could undermine the victims negotiating position.

Our analysis shows that TA negotiators revealed even more. First, that they may have been formally educated in American English, although this is unlikely to be their native language.

Secondly, that they have been operating as Ransomware TAs for four years i.e., the post on 26th January at 20:11 UTC ***"You don't have to worry, thousands of people have successfully decrypted their files for almost four years."***. Also, that they are operating from a location with poor internet speeds indicated with the post on 26th January at 19:35 UTC ***"My internet does not allow me to download such huge files, my internet speed is 50 kilobytes per second, send me files up to 50-100 megabytes at most."***. It is important to note that these tells may not always be reliable.

Emotive and Flippant wording

Regardless of how one may naturally feel towards criminals, it is never recommended to become emotional or flippant when negotiating with them.

To do so achieves nothing and passes control to the criminals. There is one exception to this; when covertly encouraging TAs to provide identification tells which may assist law enforcement in subsequent investigations. However careful consideration must be given when employing this tactic.

It is to be expected that the TA negotiators may well use emotive or flippant wording and it is important that the victim's negotiators do not rise to such bait and maintain composure. To maintain realism however, there may occasionally be a need to respond with emotion but only with consideration of the likely impact and not in a way that would escalate matters.

Analysis of the transcript reveals a few points where unnecessary wording is used by the RMI negotiators. One such post occurs on 27th January at 23:21 UTC, the post reads ***"Anyways, time for bed. The board has meetings this weekend and we will not have anything new to speak about until Monday while they make their decision."***.

The timing and content of this post is detrimental to the negotiation overall as it is both flippant and reveals to the TA negotiators the disdain for any continued negotiation. The TA negotiators respond by stating that they realise they are being manipulated.

From this point, the TA posts become increasingly emotive and appear increasingly resigned to publishing the stolen data. At this point, RMI may have confirmed (as an internal action), that there is no need to settle any demand, but it is not a good idea to negatively end a negotiation in this way as it closes the door on any need to resume serious dialogue later should this be needed.

Posting integrity checks

Due to the results of our analysis overall, it is unlikely that RMI negotiators were using a 'maker-checker' process to ensure the specific and overall quality and integrity of the posts and to avoid many of the pitfalls identified.

It is always recommended to have a second pair of eyes to ensure the cadence is optimal, that content of posts is consistent and does not compromise the legend or present any unplanned tells the TAs. Such checks can be performed by another negotiator or an overall controller.

Conclusion

It is clear, given our analysis of what is known, that mistakes in the negotiation were made by both sides. We found that the dialogue became unnecessarily emotive and antagonising.

Whilst the RMI negotiators may have experience in negotiating ransomware demands it appears clear that many of the mistakes made are due to a lack of formal training in ransom negotiation.

It is noteworthy that TAs release of the ransom transcript is a retaliatory attempt to cause RMI as much damage as possible.

The release of the stolen data (45Gb) may well cause further reputational harm and lead to legal and/or regulatory action against RMI.

Reducing risk of antagonising TAs can be achieved with short, polite, and specific posts with careful wording and attention to posting cadence resulting in a quiet and considered control over the negotiations.

It is good practice to establish a legend with options open for escalation which naturally justify the need for delays. However, once established, great care must be taken not to needlessly compromise a legend, indicating to TAs that the negotiations cannot be trusted.

The tells revealed by the TAs may provide law enforcement investigations with supporting evidence should they be able to identify specific cybercriminals and bring them to justice.

Ensuring that the integrity of posts made by the victim's negotiators using a careful review process ('maker-checker') provides a reliable way to avoid negotiation risks.

In closing, we hope this analysis has made clear, with the limited information available, that effective ransom negotiation must be an activity where each interaction needs to be considered carefully.

Both individual and aggregate posts, considered in the round, contribute to the overall outcome, with potential risks identified and managed as an ongoing activity.

In this case, the ransom amount was not negotiated and settled, and our analysis may lead one to consider that if it had been necessary then further mistakes may have risked damage to the overall outcome including the quantum of the agreed and settled amount, successful recovery of data, adherence to assurances of data destruction or to optimise the provision of supporting evidence to law enforcement investigations.

For the victims of cybercriminal extortion or those who support them, such as insurers or law enforcement, it is most important that only professionally trained negotiators are used as failure to do so risks unnecessary loss, heightened risk of retribution as well as inviting scrutiny and questions by regulators and third parties to whom the victim organisation may be liable.

Report ends.

files
are encrypted
by Lock Bit
Files
are
published

Deadline: 14 Feb, 2023 14:45:02 UTC

Clearly TAs unimpressed

royalmailgroup.com
Royal Mail need new negotiator.
All available data published !
Uploaded:
06 Feb, 2023 12:55 UTC
Updated:
14 Feb, 2023 13:46 UTC
×

Data apparently released

Indicates previous chat

Chat: **********E3E68C

[Chat started]
12.01.2023 13:44:06 UTC
Hi. Did this work?
12.01.2023 13:44:19 UTC
hi
12.01.2023 13:46:44 UTC
i'm here
12.01.2023 13:46:48 UTC
http://lockbitflle2fcudkcqqt2ve6btssyvqwlizbpv5vz337lslmhlf2uad.onion/r/Qf1vQvhUFe#4SeWqsOuiIIDvxVX34FQW+Ew2pN4lDmJ7K+lVuDJYY=
12.01.2023 13:47:01 UTC
(see stolen data)
12.01.2023 13:47:02 UTC
password:@IA@KM@YY(X2%Z%tbvHn%re2h
12.01.2023 13:47:34 UTC
Now I am worried about the other link with data in the other chat. Is that link gone now? so no one sees it
12.01.2023 13:47:40 UTC
If you have already downloaded it, it is no longer available
12.01.2023 13:48:54 UTC
Thank you.
12.01.2023 13:49:09 UTC
Is this showing all the data you have taken from us?
12.01.2023 13:49:28 UTC
the link is not available, did you download the tree or download it again?
12.01.2023 13:49:41 UTC
Yes, all stolen data
12.01.2023 13:50:05 UTC
I did open it and download a file from it. Is that the data?
12.01.2023 13:50:15 UTC
there was a tree of data stolen from us at the link. you can select some files, we will send them to you
12.01.2023 13:51:04 UTC
I will open the file and show it to my management
12.01.2023 13:52:12 UTC
Yes, don't delay, time is not playing in your favor. so far we have not reported the attack on our blog
12.01.2023 13:53:54 UTC
to whom am I speaking?
12.01.2023 13:54:10 UTC
I work in our I.T. Our senior management have asked me to contact you as it said in your note
12.01.2023 13:55:54 UTC
ok
12.01.2023 14:14:34 UTC
what does management say?
12.01.2023 19:44:46 UTC
Hi. I gave them the file. I am still waiting for them to come back to me.
13.01.2023 15:31:42 UTC
ok. hurry up
13.01.2023 17:32:45 UTC
We shall return to speak on Monday following the weekend and lengthy discussions with our internal stakeholders.
13.01.2023 20:00:02 UTC
I try to spend them productively, and please us. our patience is not infinite
13.01.2023 20:56:51 UTC
what can we expect by monday?
13.01.2023 20:58:19 UTC
We will let you know
13.01.2023 20:58:47 UTC
ok
13.01.2023 20:59:18 UTC
Hello. We waited the time you asked for. Now it's time to pay.
16.01.2023 21:47:26 UTC
Apologies for the delay as this is a lot for us to deal with. We shall get back to you tomorrow with some file names from your large list to request to see.
17.01.2023 19:12:33 UTC
File: **[requested_files.txt]**
18.01.2023 17:16:04 UTC
These are the files we would like to see that you have
18.01.2023 17:16:27 UTC
http://lockbitflle2fcudkcqqt2ve6btssyvqwlizbpv5vz337lslmhlf2uad.onion/r/pLvXayqIYa#qnGb1vVJO5/b3H3+J3GzDDd1/bEQw/aXxx3Qqb745nE=
18.01.2023 19:16:19 UTC
pass pMjd07L82^VYVexJyF6etQZ31
18.01.2023 19:16:34 UTC
Hello, it's time to pay.
20.01.2023 11:29:08 UTC
What do we need to test your decryption ability with our files?
20.01.2023 14:54:24 UTC
each machine has its own ID. In order to decrypt the file you need to take the file from one PC, and go to the chat with the ID of this PC, then the test decrypt will be successful
20.01.2023 19:30:05 UTC
Okay, we'll see what we can do to identify the ID from each. Will come back to you.
20.01.2023 20:07:52 UTC
Also you can send me 5-10 files, I will decrypt it for you
20.01.2023 21:28:19 UTC
Use this sites File Share: lockbitflle2fcudkcqqt2ve6btssyvqwlizbpv5vz337lslmhlf2uad.onion lockbitflzhrvt6eya2lvnp7fe4iifzmwybendqelgujqbzu3k4gaid.onion lockbitflfzu5e62fybhieutf6653epvr6wco7twgjtkqwdgubn4q5rad.onion
20.01.2023 21:28:36 UTC
Think I did this right. Here's some files: http://lockbitflfzu5e62fybhieutf6653epv6wco7twgjtkqwdgubn4q5rad.onion/r/wU1f8mauk0V/fLYMcNlu8khgdhuoQGG8OybtV9LZknTxkYR7JGKOk5c=
21.01.2023 04:00:32 UTC
I also have a 6 GB file that is very important. It's associated with medical devices that can't yet be shipped out because this file is locked. Please please if you can unlock this too it will help save lives. I don't know how to send it over
21.01.2023 04:03:07 UTC
File: **[1.png]**
21.01.2023 13:12:02 UTC
File: **[2.png]**
21.01.2023 13:12:08 UTC
File: **[3.png]**
21.01.2023 13:12:15 UTC
File: **[smh_installer.log.7z]**
21.01.2023 13:12:49 UTC
File: **[WindowsUpdate.log.7z]**
21.01.2023 13:12:58 UTC
You gave me valuable files that can help restore your systems without paying for a decryptor, so I only gave back some of your files, and screenshots of the valuable files.
21.01.2023 13:22:32 UTC
About 6 gigabytes of data that will supposedly save someone's life, is it one file weighing 6 gigabytes, or is it many files weighing 6 gigabytes in total? Something tells me that you are bluffing and you are doing system recovery and want to get free decryption of critical files needed for recovery. Tell me in detail what the medical equipment is and what the 6 gigabyte files are.
21.01.2023 13:24:40 UTC
There are 2 files that are a combined 6 gigabytes when compressed. You know how much of our data is encrypted and when you see the files, you will understand that they will not allow us to recover. We are only pressing this because of the medical concern and we do not believe that your intent is to hurt anyone.
21.01.2023 16:28:17 UTC

TA appears to be offering PoL

Confirms previous chat

Good Practice

Well asked

TAs confirm PoL

Hopefully securely - short time

OK Escalation

Formal English

Good Practice

OK Good continuity over time

Why reveal this ?

Risky 22h delay

Another risky 40h delay

Appreciating setting the scene for attempted recovery but posts are becoming too long and risk antagonising the TAs

What are these files? What is their function? What medical equipment are these files for? And what does the postal service have to do with medical software? Where is the logic?
21.01.2023 20:35:45 UTC
We are not just a postal service. We handle both letters and parcels, where roughly 60% of our business is parcels - international export of global medical supplies, contribute to a significant element of that! These supplies include vital replacement equipment parts, COVID-19 test kits, prescription drugs etc. The files that we have provided should allow us to resume shipping some of this equipment, not only here in the UK, but globally as well. Our transportation of this medical equipment does play a vital role in ensuring that people in need are being helped by these products. Given that the files are renamed, we are making our best assumption that this is the right dataset, and we would greatly appreciate the assistance.
22.01.2023 18:15:53 UTC
If you pretend that you do not believe that the decryptor really works, you can send me 10-20 other less important files, e.g. not related to virtualization systems and not containing RAM dumps, you can send me personal documents, photos, and many other things that do not help you without paying for my postpaid pentest services. If you were really worried about medical equipment, just pay for my work and get a decryptor within 5 minutes. You are making multi-billion dollar profits from your business and don't want to part with the money, don't you think that's odd? It's your greed that makes the people who are waiting for their packages suffer.
22.01.2023 18:39:32 UTC
We are not pretending anything and apologise if it appears that way. It is just that my management have heard that your decryptor might not work on large files, that is why they asked and wanted to see if it did. I am trying to convince them to work with you here, they are just asking for more proof of what we will get from you. As you probably know, we are already a loss making company, so we are not gaining anything from dragging this out. There are several articles on Google about our financial situation and how bad it is currently.
24.01.2023 12:51:35 UTC
You can send me other large files, I will decrypt for you those files that I think are not valuable, that way you can be sure that the decryptor works on large files. Your financial situation is fine, you have a multi-billion dollar turnover, and a huge profit, the sooner you pay, the sooner this whole nightmare will be over for you. If you continue to stretch time I will be forced to publish your information on the blog with an offer to change negotiators, thank you for your understanding.
24.01.2023 13:47:58 UTC
We are collecting some larger files that are not valuable to provide you. It's important for us to understand these can be decrypted of course so we appreciate you providing that opportunity to us. Ahead of this, we haven't even heard from you what it is that you want.
25.01.2023 17:27:01 UTC
I'm waiting for the next batch of files to be decrypted. We want as 0.5% of your revenue.
25.01.2023 17:52:34 UTC
And how much is that
25.01.2023 17:55:27 UTC
How much your revenue?
25.01.2023 17:55:48 UTC
All we have had is losses. Here, you can read about it yourself: https://www.thetimes.co.uk/article/royal-mail-losses-rise-to-450m-ls8bjvv5b https://www.theguardian.com/business/2022/oct/14/royal-mail-to-cut-up-to-10000-roles-blaming-strikes-and-lower-parcel-volumes
25.01.2023 17:57:54 UTC
We understand you very well, we are all suffering from the global crisis and our income has fallen as much as yours, anyway you are hundreds of times richer than us. 0.5% of annual global turnover is much less than a 4% fine from your government.
25.01.2023 18:05:40 UTC
Just name the amount already so we can let the leadership know.
25.01.2023 18:12:52 UTC
$80 million is 0.5% of your revenue, $640 million is 4% of your revenue. We are asking 8 times less than your state. In addition to this price you get a decrypt of your data.
25.01.2023 18:17:10 UTC
Do you really think the government doesn't already know about this? Even if they were to fine us, paying you or not does not change this.
25.01.2023 18:28:24 UTC
We'll get you the files and we can continue these talks later.
25.01.2023 18:32:06 UTC
As long as we haven't published any of your files, you can't be fined. If you can negotiate with us, the government will be left without your $640 million. It is much better for you to negotiate with us and continue your very successful business with a long history and impeccable reputation. I personally used the services of your company and was very satisfied. I wouldn't want you to suffer so much from the government.
25.01.2023 18:32:49 UTC
Talk to you later
25.01.2023 18:34:07 UTC
Ok
25.01.2023 18:34:15 UTC
How do I give you these large files? They are larger than your 2GB limit
26.01.2023 19:35:54 UTC
My internet does not allow me to download such huge files, my internet speed is 50 kilobytes per second, send me files up to 50-100 megabytes at most. At the same time I can offer you to do the following, I will create a build of the encryptor and give you together with the decryptor, you will encrypt any files on your virtual machine and this way you can check the successful decryption of files larger than 2 gigabytes.
26.01.2023 19:46:40 UTC
Okay, I guess we can try that. We just want to have confidence your decryption tool will work on these large files
26.01.2023 20:04:08 UTC
You don't have to worry, thousands of people have successfully decrypted their files for almost four years.
26.01.2023 20:11:35 UTC
I believe you, but we need to see it ourselves before we can consider this
26.01.2023 20:12:23 UTC
http://lockbitflle2lcudkcqqt2ve6btssyvqwlizhpv5vz337lslmhflf2uad.onion/r/8oqC8jKaBN#1EE8yMFqPpjD5q9wrPPejtEpdhWwEUH1OhHx+lm6CAM=
26.01.2023 20:17:33 UTC
Encrypt any of your computers or virtual machines, any amount or amount of information. Write to me via a note and I will give you a decryptor in a new chat in which you will write to me.
26.01.2023 20:18:51 UTC
To start the encryption, simply run the file as administrator.
26.01.2023 20:23:33 UTC
There is still some confusion over who we are, you are basing your revenue on what is a holding company and not Royal Mail Group. IDS (International Distribution Services) have several companies that exist under that umbrella who are independent to each other. We are Royal Mail International who is a separate entity, with an entirely independent Managing Director and Senior Official. Our Company's revenue is in decline, as we have tried to explain to you previously and Royal Mail International is the Company that is affected by your penetration testing. Our current financial turnover is expected to be 800 million. Based on your calculation for payment (1.5% of total revenue) this equals 4 million dollars. If there is any negotiation at this percentage level the starting figure needs to represent what I have just described. I am trying to help our Senior Teams understand this and I am grateful that you have offered to help them see that your decryptor can work to restore our services, by offering to decrypt some larger files. We will have to accept what we have for now and will see if this is good enough for them or not.
26.01.2023 21:58:06 UTC
You're bluffing. 800 million is your net profit per year, so 80 million is not that much money for you.
26.01.2023 23:41:08 UTC
What company are you looking at to get those numbers?
27.01.2023 13:45:18 UTC
https://en.wikipedia.org/wiki/Royal_Mail
27.01.2023 19:40:56 UTC
https://en.wikipedia.org/wiki/Simon_Thompson_(Royal_Mail)
27.01.2023 19:41:15 UTC
https://techcrunch.com/2023/01/17/royal-mail-cyberattack-disruption-lawmakers/?guccounter=1&guce_referrer=aHR0cHM6Ly95d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAHuwvya8Vr_ETqomIFym90OHoOGvCLILONYPwCbLmCiF19qs4A2x68Rge0lCtwVtRfnOeQIctYx5A0epJT5t2u73JkDFGhBtrJFtpwWWlf3Y_Qbxtj8aL5TcfVxyrg_tvh7vJNNb3y9Ex0WXLu5iuj7visZOGG5yE8wufn912Bq
27.01.2023 19:41:37 UTC
Trying to explain we are Royal Mail International, who is a separate entity, with an entirely independent Managing Director and Senior Official, and not "Royal Mail" as the overall entity. What you attacked is just a small portion and our revenue is not that of Royal Mail.
27.01.2023 21:29:22 UTC
Anyways, time for bed. The board has meetings this weekend and we will not have anything new to speak about until Monday while they make their decision.
27.01.2023 23:21:48 UTC
You are a very clever negotiator. I appreciate your experience in stalling and bamboozling, when you are trying to deceive you need to provide evidence for greater credibility, only a fool would believe in the honest word of a lawyer defending his client.
28.01.2023 01:33:39 UTC
Not here to deceive or bamboozle. Just being transparent about what we're doing. The board having meetings this weekend shows our seriousness. Please confirm you will wait for their decision on Monday.
28.01.2023 13:06:43 UTC
Your seriousness can consist only in a desire to pay 80 million dollars, all other promises of meetings of your management, which allegedly will be held, this is just a tactical move, increasing the time of negotiations calculated that I will be nervous and agree to a smaller amount of money that you will offer. I am ready to wait until Monday, I am sure that your directors have more than 100 million dollars on their personal cryptocurrency wallet, so it will not take much time to finish this nightmare.
28.01.2023 16:25:17 UTC
As we informed you, we have a response from our board to provide you. Under no circumstances will we pay you the absurd amount of money you have demanded. We have repeatedly tried to explain to you we are not the large entity you have assumed we are, but rather a smaller subsidiary without the resources you think we have. But you continue to refuse to listen to us. This is an amount that could never be taken seriously by our board.
31.01.2023 21:12:55 UTC
If I did not want to make a deal with you, your data would have already been published and the decryptor deleted. I am not forcing you to prove anything, I just kindly asked, refusing to give me such simple information says that you do not intend to cooperate with me honestly and tell me the truth. We are not attacking critical infrastructure, your commercial mail company with dozens of similar competitors is not. If you believe the news that your management is releasing, your mail services are fully restored and you are functioning as you are, humanitarian and medical supplies will be successfully delivered by your competitors, you will just get a little less profit, because you are very greedy and don't want to pay for my services. I'm sure you could easily pay $80 million, your income allows you to do so. If you want a discount, then make a counter offer, we are here to have constructive negotiations, not for me to give you a discount after every bluff you make until you say I'm fine with getting a free decryptor and free removal of stolen information. Any specific offer you make will be considered. You have a chance to make me an adequate payment offer by consulting with your board of directors, whose salaries are in the hundreds of thousands of pounds, but that does not stop them from being very greedy and not making concrete proposals to save the reputation of your commercial company which has more reasonable competitors who have already paid us money and successfully continue to earn new excess profits billions of pounds. Good day gentlemen.
31.01.2023 23:55:53 UTC
I am still trying to work with you here. I am trying to get the board to find a solution with you, but they have two major concerns. You haven't showed us that you could handle the large files, and your starting point here is way too high. We have told you who we are, and our numbers wouldn't at all justify the demand you have put forward. I am doing what I can to drive things forward on my end, but your demand is simply too high for the board to consider. If you can give me a lower starting point, I think I may be able to get the board to work with you. I really want to find a solution here, please help me do that.
01.02.2023 21:41:07 UTC
I'm ready to help you, I want to make money just like you, you and I have the same motivation in the form of money, your task is to reduce the price as much as possible, my task is to get the maximum amount. I have shown you that I can handle large files, you can encrypt and decrypt any files you want, why haven't you done that until now? The price is based on a multi-billion dollar company's profits, it's not the case that a company making billions of dollars pays the same price as an ordinary company making tens of millions of dollars. The more profits a company makes, the higher the buyout price, that's the math, you and your board of directors should understand that. Out of respect for you, I'm willing to step up and give you a 12.5% discount.
01.02.2023 23:24:58 UTC
Thank you for this. I appreciate you coming forward like this. I will bring this to my management and get back to you.
02.02.2023 21:16:44 UTC
Ok
03.02.2023 10:14:28 UTC
I just want to let you know, that I am still waiting for a reply. My manager told me, that he is waiting to hear back from the board. He has promised me I'll get an answer on Monday. I will let you know as soon as I hear anything.
03.02.2023 20:54:50 UTC
Very long, the company from the UK paid on the second day after the attack because they care more about their business and reputation, strange that for you it is not so important, because you make a lot more money.
03.02.2023 21:01:26 UTC
Maybe you didn't ask them for such a large amount. That would probably make it easier to pay quickly. My manager hasn't gotten an update from the board yet, can I check back in with you Monday?
04.02.2023 13:26:31 UTC
Naturally, I asked them for a smaller amount, their revenue is 58 times less than yours, they earn money 58 times less than you, I always ask for a fair and adequate amount from each company, I do not ask for what the company can not pay. Why do you have such a long chain of middlemen? why can't you communicate directly with the director? I will wait until Monday, but I think it is time to end this case. The journalists are asking me why I haven't published your information while I ignore their questions, they really want to see your files.
04.02.2023 16:40:24 UTC
You need pay!
06.02.2023 11:17:00 UTC
http://lockbitapt2d73krllbewgv27iquljgxr33xbwwsp6rkyieto7u4ncead.onion/post/TqvYTKKoycawsXyg63e0f8ce66113
06.02.2023 12:52:43 UTC
You have 50 hours for payment.
06.02.2023 12:52:56 UTC
I just want to let you know, that I am still waiting to hear back from my management. It is not a quick decision for them, and I can't just tell the board to hurry up. To be honest with you I have heard that they might not want to pay you for this. In our perspective the files got leaked when you took them from our system, and paying you won't undo that in any way. I will get back to you as soon as I have further news.
06.02.2023 22:20:26 UTC
I just want to let you know that the data is ready to be published and the decryptor is ready to be deleted. You have had plenty of time to make your decision, your time is up.
07.02.2023 03:42:02 UTC
Do you have any offer for me?
09.02.2023 12:41:40 UTC
*See chat history
OPEN CHAT

Modem Speeds?

American Style

Tell

Good

Business dialogue unlikely from a negotiator with an IT staff legend

American Style

Flippant and indicates no intention to pay

Legend burned for no apparent reason

Interesting that no intention to settle is so obvious

American Style

American Style

Posted by TAs. Unsure what this is