Influence of victims during ransomware negotiations and its outcomes

Alisa Bayerlen (s2704188)

Bachelor Thesis in Psychology of Conflict Risk and Safety

Faculty BMS

University of Twente

First supervisor: Michalis Georgiou, Msc

Second supervisor: prof. dr. Ellen Giebels

24th of June, 2024

Word Count: 6,211

Abstract

This exploratory study aimed to investigate the tonal influence of victims and their counteroffer strategy during ransomware negotiations and its impact on outcomes. As victim behavior during negotiations remains under-researched, identifying correlations can offer valuable guidance for future victims. Using a mixed-method, exploratory approach, 134 transcripts were coded, analyzed and categorized into three distinct tonal groups – aggressive, calm and pleading. The calm tone was linked with the lowest likelihood of payment, while the emotional tone showed the highest likelihood of payment. Additionally, the number of counteroffers made by victims emerged as a statistically significant predictor of payment success – more counteroffers increased the likelihood of payment. These findings suggest that a victim's persistence, as reflected by the number of counteroffers made, may play a more critical role in negotiation outcomes than the tonal approach they use.

Introduction

Ransomware attacks have become one of the most pressing cybersecurity threats facing organizations today (Singh & Kumar, 2020). In such incidents, ransomware groups gain unauthorized access to company systems and encrypt sensitive data. Afterwards, such groups demand huge payments in exchange for unlocking the systems or decrypting data, or threatening with public exposure of that data. These attacks put immense pressure on victims, forcing them to consider whether to engage in such negotiations. Such actions and their consequences can be best seen through a real life example.

In May 2021, the Colonial Pipeline Company suffered a massive cyberattack. The DarkSide ransomware group gained access to the company's network through an employee's VPN account, which allowed them to encrypt data (Gawazah et. al., 2024). As the billing system was compromised, Colonial had to shut down the entire network as a safety procedure. As the largest transporter of refined petroleum products in the U.S., this led to fuel shortages and a regional emergency (Gawazah et. al., 2024). This incident became one of the most prominent examples of ransomware in recent years, drawing widespread attention to the growing impact of such attacks.

This case illustrates the threat that ransomware presents, as well as the difficult decisions victims have to face when confronted with such risk. Upon the gain of the network data, the hackers are able to harm companies in a variety of ways: operational disruptions, as seen in the Colonial Pipeline attack (Gawazah et. al., 2024); identity theft and leaks of personal information in the Hacking of Sony Pictures in 2014 (Steinberg et. al., 2021); loss of customer trust and damage to company's reputation in the Equifax data breach in 2017 (Schneider & Arnold, 2019); and ransom demands are a big risk that is present in all cyberattack cases, as for all the networks that hackers access they request huge amounts of money.

Companies are faced with difficult decisions during ransomware negotiations. In such situations, a CEO often faces a complex decision between paying the ransom and attempting to restore the compromised data manually, each option carrying significant risks. Paying the ransomware group is not encouraged as that will encourage more attacks, as well as that does not guarantee that the network or data will be restored (National Cyber Security Center, 2020). On the other hand, manual restoration can be a slow and costly process, potentially leading to severe operational and economic consequences. These decisions demonstrate the importance of understanding how victim's behavior may influence negotiation outcomes.

The willingness of the victim to pay the ransom may play an important role in the negotiation process (Boticiu & Teichmann, 2023). Since ransom demands are calculated as a percentage of the company's income, which is sometimes based on an overestimated or outdated number, victims are able to negotiate by providing accurate financial information. Other factors can also shape the negotiation outcome including the amount and value of the data that was stolen (Amann et. al., 2022). The victim may have the opportunity to restore their data manually, which would not require them to pay or would substantially lower the price.

Although the first ransom request is typically set by the ransomware group, it is important to recognize that victims do have the opportunity to negotiate and potentially lower the ransom amount. In negotiation theory, the concept of "anchoring" plays an important role, with research from Galinsky and Mussweiler (2001) showing that the first offer often sets the tone of the entire negotiation process. The ransomware group's first offer functions as an anchor – a reference point that the victim must respond to. Besides a financial reference, this anchor point can also have an emotional and psychological impact on the ransomware negotiation process.

Victims can respond to this anchor through counteroffers, which serve as their active attempt to adjust the terms and regain some control. These counteroffers can reflect the victim's willingness to cooperate and potentially influence the ransomware group to accept a lower price. Galinsky and Mussweiler (2001) discuss that initial offers can set an emotional tone for negotiations, which affects how victims engage in the conversation. Victims who approach negotiations strategically and with controlled emotions may be more likely to use counteroffers effectively, whereas those overwhelmed by fear or urgency might forget to use such strategies. Ultimately, these emotional and behavioral responses affect the victim's final decision to pay or not to pay.

While there is research on ransomware group's influence tactics and general victim strategies, there has been limited research focusing specifically on how victims navigate ransomware negotiations and how they influence these negotiations. Specifically, little is known about how victims' behaviors shape the dynamics of the conversation and affect the final outcome. Victims are not passive – they can actively shape the direction and tone of the negotiations. By adopting a controlled, resistant or cooperative position, victims may influence the trajectory and the final outcome of the negotiation. An important behavioral indicator of engagement is engagement in price negotiation – making counteroffers. This act signals as a willingness to cooperate and readiness to compromise, which may increase the likelihood that the ransomware group will lower their demands. Based on this, the first hypothesis proposes:

H1: Victims who engage in counteroffer exchanges during ransomware negotiations are more likely to pay the ransom than those who do not make any counteroffers.

Emotional tone has been shown to play a crucial role in high-stake interactions (Druckman & Olekalns, 2008). In particular, calm and composed tones can help reduce tension, promote cooperation, and encourage faster resolutions. Conversely, aggressive or confrontational language may escalate conflict and obstruct constructive dialogue. In the context of ransomware negotiations, a victim's use of a calm tome may showcase rationality, credibility and willingness to resolve the situation (Mattern, 2024). Based on this reasoning, the second hypothesis is proposed:

H2: Victims who use a calm tone during negotiations have a greater likelihood of ransomware agreement (i.e. pay and recover data) than those who use other tones.

Additionally, there may be a connection between the victim's persistence in price negotiation and willingness to pay. Victims who make repeated counteroffers intending to lower the ransom amount may not only be more committed to reaching a resolution, but may also be signaling flexibility and seriousness to the ransomware group. This effort can promote mutually acceptable price adjustment, increasing the likelihood of payment. Based on this, the third hypothesis is proposed:

H3: Victims who make more than one counteroffer are more likely to pay the ransom than those who fail to shift the original demand.

Together, these hypotheses aim to explore the extent to which victims can influence ransomware negotiations both in the communication process and the final outcomes.

Methods

Participants

The participants of this study were ransomware negotiation chat logs involving various victim organizations and ransomware groups (e.g., REvil, Black Basta, Babuk, Akira). A total of 27 negotiation chats were selected based on accessibility, completeness, and relevance to the research question. These chats included messages exchanged between ransomware actors and victims from initial contact through final resolution or breakdown of negotiations. As this study used publicly available anonymized secondary data (i.e., chat transcripts), no personal identifiable information (PII) of individuals was processed. Therefore, ethical approval and informed consent from human subjects were not required.

Design

This study employed a mixed-method design, which included qualitative inductive coding and further quantitative analysis. The analysis aimed to explore the communication strategies used by both ransomware attackers and victims throughout the negotiation process. Rather than applying a predefined coding scheme, codes were developed inductively based on recurring patterns and strategies observed in the chats. Each message was treated as a separate unit of analysis. Codes were iteratively created, refined, and organized into a structured codebook as the analysis progressed. This approach allowed for a flexible categorization of emerging negotiation tactics and behaviors specific to ransomware negotiations.

Materials

The primary materials for this study consisted of ransomware negotiation chat logs collected from publicly accessible sources and breach data archives. These logs contained detailed text-based conversations between attackers and victims, including ransom demands, discount negotiations, emotional appeals, threats, and settlement discussions.

Coding was conducted using Atlas.ti, a qualitative data analysis software that facilitated systematic annotation, categorization, and retrieval of coded messages. Throughout the coding process, an original codebook was developed, containing codes representing distinct negotiation tactics identified in the dataset. All data were stored securely and analyzed offline to maintain confidentiality and data integrity.

Procedure

Access to ransomware negotiation logs was granted through the public GitHub website. Two bachelor students initially included all available logs from several ransomware groups (e.g., Akira, Conti, Hive, Avaddon, Darkside, BlackMatter, BlackBasta, Babuk, and Avos), without pre-screening their content.

To begin the analysis, the researchers (myself and another bachelor student) independently coded three practice logs to identify recurring communication strategies and evaluate initial coding consistency. Based on the discussion of these logs, a shared codebook (Appendix A) was developed. Training on the practice logs took 3-4 hours and the discussion of those logs took 4 hours, therefore the whole training process took 7-8 hours. The researchers then independently coded 24 additional logs to test the usability of the codebook before proceeding to the full dataset.

All remaining logs were then coded independently using the finalized codebook. During the coding process, some logs were identified as unsuitable for analysis - either because they lacked victim-side messages, did not include sufficient negotiation content, was in a language that the researcher could not read, had an unclear outcome or got their data or decryption for free. In total, 23 logs were excluded on these grounds, resulting in a final dataset of 134 coded negotiation logs.

After independent coding, the researchers reviewed all 134 logs together, marking agreement and disagreement rates in coding decisions and then discussing the coding results. All the disagreements in quotation incidents and code usage were noted down and later used to calculate Cohen's Kappa to evaluate inter-coder reliability. The average Cohen's Kappa across the dataset was 0.71, indicating substantial coding agreement. When discussing the present disagreements, the researchers settled what presented a solid representation of a code, rather than simple implementation of the code meaning.

Data Analysis

To analyze the relationships between the codes, code groups and negotiation outcomes, quantitative and qualitative analyses were conducted. Qualitative analysis involved going through negotiation log transcriptions and coding literary quotes. Each new message in the log served as a new unit of analysis. Researchers read through the full log and looked for units that represented a tonal expression or a method to argument against ransomware group. When an expression or method was used more than once it was quoted more than once within the same log. Quotations included simple words, phrases, sentences and whole paragraphs. After coding all the logs, code groups were formed based on two indicators – level of power and level of emotion. Three combinations were formed from the possible high/low labels of each indicator: *high power + high emotion*, *high power + low emotion*, *low power + high emotion*. Then, looking at the strengths of the emotions that each code carried and level of power that the victim showed, each code was placed in their respective groups.

Each group contained two-three codes. *High power + high emotion* had two codes: *Aggressive response* and *Demand of Quality*. This group had a very aggressive and loud tone. *Aggressive response* directly describes verbal aggression from the victim towards the ransomware group, signifying massive distress and dislike for their actions or behaviors: "*You sons of bitches*". *Demand of Quality* encompasses all the requests from the victim where they demand to see the quality of the services that the ransomware group provides: "*What guarantees do I have that my system will start working after I do what you ask for?*" (see Appendix B for more quotation exemplars).

High power + low emotion had three codes: *Assertive pushback*, *Strategic politeness* and *Readiness to negotiate*. This tone is characterized by a calm and controlled style. *Assertive pushback* describes any opposition from the victim that is done in a calm matter: "*I'm here and after intense conversations and internal consultations as you might imagine. Please refrain from hostile language. I will appreciate it. I was instruct to further elaborate with you couple of points, obviously after I did my own research about you and your highly* *professional capability and status.*". *Strategic politeness* refers to the polite tones and polite phrases that the victim uses to maintain a calm conversation: "*Thank you again for your continued willingness to work with us and understanding of our situation.*". *Readiness to negotiate* usually appears in the very beginning of the logs and shows that the victim is here to negotiate and want their data back: "*Can we discuss this price then?*".

Low power + high emotion also had three codes: *Emotional plea*, *Discount request by victim* and *Financial constraint appeal*. This tonal group adopted an emotional and pleading tone. *Emotional plea* encompasses any type of emotional call that is made towards the ransomware group from the victim: "*It is our existence... please please help us*". *Discount request by the victim* is a direct code that reflects whether the victim has asked for a discount to the initial price: "*Please show us a good discount.*". *Financial constraint appeal* describes a plea by the victim that in some form tells that the company does not have the financial capabilities to pay the ransom amount: "*We are a small business, we have been hit hard due to the economic downturn, and the pandemic.*".

Qualitative analysis involved calculating various likelihoods of payments, as well as conducting a binary regression analysis. For this data, likelihoods of payment were calculated with two predictors – number of counteroffers and formed code groups. Per log, it was noted how many, if any, counteroffers were made and what type of tonal group was used in the log, as well as whether the log was paid or not. For the payment likelihood based on number of counteroffers, the number of counteroffers and the payment outcome were used. Afterwards, for the payment likelihood based on the tonal group, the group type and the payment outcome were used.

A binary regression was calculated in order to understand whether the relationship between the outcomes (i.e. paid and unpaid) and the predictors (i.e. tonal group and number of counteroffers) have statistical significance. Using RStudio, the binary regression was conducted, where: tonal groups represented the primary independent variable, the number of counteroffers represented the secondary independent variable, the payment outcomes represented the dependent variable as a binary value – 1 (paid) and 0 (unpaid).

Results

Tonal group usage

To provide context for the subsequent analyses, the distribution of tonal groups across the 134 negotiation logs was examined.

"*High power and high emotion*" presents the strongest tone. High power refers to the ability of the victim to take control through powerful language or strong demands from the ransomware group (Staff, 2025). High emotion signifies that the victim is not controlled, but rather acting on powerful emotions (Mooser, 2025). In this group there are two codes – '*Aggressive response*' and '*Demand of Quality*'. *Aggressive response* was quoted in 33.58% throughout all negotiation logs, approximately a third of the sample. *Demand of Quality* was quoted in 35.82% throughout all negotiation logs, which is also roughly a third of the sample.

"*High power and low emotion*" presents the calmest tone. Just as in the first group, high power refers to the victim being able to gain control within the negotiations. Low emotion presents a new angle – a composed and calm tone that the victim uses. Low emotion can present itself as just being calm, talking without any offences or pleads, as well as being able to push back against the ransomware group and regain control. This group contains three codes – '*Assertive pushback*', '*Strategic politeness*' and '*Readiness to negotiate*'. Among the various negotiation techniques, *Assertive pushback* stood out, appearing on average more than twice per negotiation log, highlighting it as the most commonly used recurring technique. This also reflects it as the most common tendency among victims to keep a calm tone during negotiations. Similarly, *Strategic politeness* stood out, occurring more than once per negotiation log. This highlights it as another commonly used recurring negotiation technique. *Readiness to negotiate* was quoted in 55.22% throughout all negotiation logs, appearing in more than half of the logs.

"*Low power and high emotion*" presents the most emotional tone. This group contains codes that show the victim's reliability onto emotion in order to reach a certain goal. In these cases, the emotion that is being displayed by the victim is vulnerable or anxious, sometimes sad or upset. It is a strong emotion, but it does not allow the victim to stay in the position of power. The victim is metaphorically below the ransomware group, pleading and begging them for understanding. The group contains three codes – '*Emotional plea*', '*Discount request by victim*' and '*Financial constraint appeal*'. *Emotional plea* was quoted in 88.06% throughout all negotiation logs, indicating this code was present in a vast majority of logs. *Discount request by victim* was quoted in 29.10% throughout all negotiation logs, appearing in under a third of the logs. *Financial constraint appeal* was quoted in 78.36% throughout all negotiation logs, appearing in three-thirds of the logs.

Two additional codes were identified and coded for – '*Initial price*' and '*Counteroffer from the victim*'. These codes represent the general picture of the trajectory of the negotiations, as the initial price states what the starting price was for the victim and the counteroffer shows how much the victim was willing to offer and how many times they were willing to increase their price. *Initial price* was present in all 134 logs, as each ransomware negotiation conversation had a starting price. *Counteroffer price from the victim* was coded 205 times in 134 negotiation logs, but was not used in every log. The lowest amount of counteroffers made by the victim is zero and the maximum amount is eight.

Likelihoods

From the 134 negotiation logs that were analyzed 48 were logs where the victim paid and 86 logs where the victim did not pay. Based on this binary statistic, it can be said that in the collected sample, victims paid the ransom in roughly one in three negotiations.

It was important to examine whether the presence or absence of a counteroffer had an effect on the likelihood of payment. Since not all victims attempted to make a counteroffer, this variable needed to be explored more. As shown in Table 1, negotiations without any counteroffers resulted in a low payment likelihood of 10.0%, while making a counteroffer had a significantly higher likelihood of payment – 51.3%.

Table 1.

Likelihood of Payment based on Counteroffer Presence

Counteroffer Presence	Likelihood of Payment
No	10.0%
Yes	51.3%

Seeing that making just one counteroffer increases the likelihood of payment, it was essential to observed how the likelihood would change based on the number of counteroffers that a victim makes. As stated before, not every victim has made an attempt to make a new price, while some other victims have made eight attempts. Table 2 shows all the likelihoods per number of counteroffers made. The overall payment likelihood is 36.8% and the average number of counteroffers made per log is 1.50. Although the average shows that on average there is a counteroffer present in each log, this figure is influenced by negotiations with multiple counteroffers, while others had none at all.

Table 2.

Likelihood of Payment based on Number of Counteroffers

Number of Counteroffers	Likelihood of Payment	Case Instance
0	11.4%	53
1	21.1%	20
2	56.0%	27
3	61.1%	21
4	100.0%	7
5	33.3%	4
6	100.0%	1
8	100.0%	1

The likelihood of payment was also calculated based on the groupings of the codes. From Table 3 we can see the group type, the likelihood each group had and how many negotiation logs belonged to each group. *High power + high emotion* was the least used group during negotiations. Although, this group had an intermediary likelihood of payment – 42.5%. *High power + low emotion* was the most used group, but it unexpectedly had the lowest likelihood of payment – 37.1%. *Low power + high emotion* was another underused group. This presents a further variation – this group had the highest likelihood of payment of 51.7%. This highlights a contrast between frequency of use and payment likelihood across the tone groups.

Table 3.

Likelihood of Payment based on the Group

Group	Likelihood of Payment	Log Count per Group
High power + high emotion	42.5%	11
High power + low emotion	37.1%	90
Low power + high emotion	51.7%	33

Binary regression

Having calculated the likelihoods of payments, it was also significant to look whether or not the correlations have a statistical value, as well as combine the effects of group type and number of counteroffers. In order to do that, I have conducted a binary regression, with the three groups representing the primary independent variables, number of counteroffers representing the secondary independent variable and the paid and unpaid outcome representing the dependent variable. For the analysis, the "*High power + high emotion*" group was used as a reference group. This would showcase whether or not the previously found correlations have a statistical value, as well as combine the effects of group type and number of counteroffers.

Table 4 presents all the results from the binary regression. *High power + low emotion* group was 1.31 times more likely to pay than the reference group. *Low power + high emotion* group was 2.57 times more likely to pay than the reference group. Additionally, we can observe the p-values of each group. Both of them are >0.05, showing that it cannot be confidently said that the effects didn't occur accidentally. From this analysis, it can be seen that counteroffers are a statistically significant predictor of payment. The odds ratio of the counteroffers show that each new counteroffer doubles the odds of payment, which is very significant. Additionally, counteroffers have an absolute p-value – 0.000, which also highlights the statistical significance of this predictor.

Table 4.

Binary Regression Presenting Payment Outcome Based on Counteroffers and Power–Emotion Conditions

Predictor	Coefficient	Std. error	Odds ratio	p-value	95% CI
Intercept	-1.099	0.691	-	0.099	0.06 - 0.94

Counteroffers	+0.790	0.168	2.20	0.000	1.58 - 3.06
High power + low emotion	0.269	0.791	1.31	0.704	0.09 - 1.97
Low power + high emotion	0.944	0.809	2.57	0.202	0.20 - 4.68

Based on the conducted analyses, conclusions can be drawn regarding the hypotheses. Hypothesis 1 was supported, as the likelihood of payment for victims who made a counteroffer is significantly higher (see Table 1). Hypothesis 2 was not supported, as victims using a calm tone had the lowest likelihood of payment (see Table 3). Hypothesis 3 was supported, as victims who made more than one counteroffer did have a higher likelihood of payment (see Table 2 for descriptive statistics and Table 4 for regression results).

Discussion

This study aimed to explore communication tones and counteroffer strategy used by ransomware victims during negotiations and how each influenced payment outcomes. Using a mixed-methods, exploratory approach, the study identified three tone groups – aggressive, calm and emotional – and explored how these tones, along with the number of counteroffers made by the victims, influenced the negotiation process. The findings suggest that tone and persistence are both important, but in different ways and degrees. Contrary to expectations, calm and controlled tones had no significant effect, while emotional approaches were more often associated with ransom payment. The most significant predictor was the number of counteroffers – victims who made multiple counteroffers were significantly more likely to reach payment agreement. These findings indicate that active and persistent engagement may be more influential than tone alone in determining negotiation outcomes.

To better understand how tone and number of counteroffers influence the outcomes, the following sections explore each tone group in detail, followed by a discussion of payment likelihoods based on tone and counteroffer behavior, and statistical findings.

Negotiation tone appliance

Building on the findings observed in the results, the use of tonal groups during negotiations reveals their role in the negotiation dynamics.

High power + high emotion codes have been used relatively infrequently throughout all negotiation logs. This suggest that victims generally refrain using aggressive or loud tones during negotiations. An aggressive tone could have been avoided by the victims in order to prevent an emotional backfire from the attacker – answering aggression with more aggression. This tendency reflects principles from Communication Accommodation Theory, which suggests that individuals often adjust their communication styles to reduce social distance and avoid conflict escalation (Giles, 1973).

High power + low emotion codes have a more variable frequency. *Assertive pushback* was used very frequently in all negotiation logs, showing that there is an abundant use of resilient and controlled, but calm language. *Strategic politeness* also has a high frequency rin all negotiation logs, which also suggests that politeness is used a lot by the victims. This high frequency suggests that politeness may serve as a functional role in maintaining dialogue with the ransomware group, deescalating tension and showing cooperation without giving up power. In contrast, *Readiness to negotiate* was less frequently used. As suggested by the power asymmetry theory, the less powerful side often feels disadvantaged and hesitant to engage in negotiations. Such frequency could reflect a perceived power imbalance, as suggested by Rubin & Zartman (1995) victims can feel that they have less power or lack the confidence to negotiate first.

Low power + high emotion codes are also variable in their usability. *Emotional plea* and *Financial constraint appeal* were relatively common techniques used by victims throughout negotiation logs. *Discount request by victim* has not been used as much – it was noticeably less frequent compared to all the other codes, making it the least used technique overall. This could suggest that victims refrain from asking for discounts due to fearing it could offend the ransomware group and risk higher ransom demand (Brown & Levinson, 1987).

Payment likelihood by predictor

Effect of counteroffers

The act of making counteroffers has shown to significantly influence the likelihood of ransom payment As shown in Table 1, the likelihood of payment increases substantially when a counteroffer is made, compared to when no counteroffer is made. This substantial difference suggests that victims who actively engage in negotiations are perceived as more willing participants prompting the ransomware group to remain involved in the conversation. A counteroffer may serve as a cue to the ransomware group – the victim is not plainly refusing the ransom demand. By making a counteroffer, the victims indicates openness to dialogue, which can encourage the ransomware group to engage.

Evaluating the number of counteroffers more closely, more information can be obtained. As shown in Table 2, a pattern can be seen: victims who made no counteroffers, essentially refraining from engaging in price negotiation, had a low payment success rate of just one in ten. This suggests that when victims don’t fight back or try to negotiate, the ransomware group may think that the victim is not serious about paying or not in a hurry to resolve the situation. Notably, just a single counteroffer doubled the likelihood of payment, raising it to roughly to one in five. But the biggest shift occurred between one and two counteroffers – likelihood went to more than half of analyzed negotiations. This big increase indicates that early signs of active negotiation may signal to the ransomware group that the victim is willing to cooperate, but also to negotiate the price, fostering a dynamic process.

Strikingly, when victims made four counteroffers, payment was successful in every observed case, indicating a possible ‘optimal point’ in negotiating persistence. However, this conclusion should be interpreted cautiously, as only seven victims made four counteroffers, all with the same outcome. A noticeable decline at five counteroffers follows, which might suggest negotiation fatigue from the side of the ransomware group, though this remains speculative, as it was not statistically confirmed. Outlier cases – such as victims making six or eight counteroffers, which resulted in successful payments – should be interpreted cautiously due the limited occurrence of such instances. Although, their appearance does suggest that extreme persistence may occasionally lead to success.

Overall, the data implies that victims who actively participate in the negotiation process ad make multiple counteroffers may increase their chances of reaching consensus, especially when the effort is perceived as collaborative between the ransomware group and the victim. The process appears to encourage logical persistence, where victims strive for a mutually acceptable price rather than submit to demands or reject them.

Effect of tonal groups

When examining likelihoods of payment cross tonal groups, multiple interpretations can be made. Victims using a *Low power + high emotion* tone demonstrated the highest likelihood of payment, with a successful outcome appearing in just over half of the negotiations. A pleading expression may prompt empathy, remorse or pity from the ransomware group, potentially leading them to lower their demands or settle quicker. This suggest that emotional vulnerability can be used as a form of persuasion within the negotiation dynamic.

High power + low emotion tone, despite being the most frequently used tone, had the lowest payment likelihood compared to other tones. While this approach can project control and rationality, it can also increase tensions or be perceived as resistance, resulting in more argumentative exchanges and less successful outcomes. Victims in this category often challenge threats or huge price demands without emotionality, showing awareness and firm boundaries, which may reduce the ransomware group's willingness to compromise and cooperate.

High power + high emotion tone had an intermediary likelihood, with successful outcomes appearing in just under a half of the negotiation logs. Although this tone was the least frequently used, its relatively higher success rate compared to the most common tone group suggests that combining assertiveness with emotional expression – like anger and frustration – might create pressure that motivates consensus. This tactic may strike a balance between resistance and urgency, increasing the likelihood of a successful outcome.

H2 aimed to find out whether victims using a calm tone have a greater likelihood of payment of the ransom. Contrary to expectations, a calm and controlled tone did not increase the likelihood of payment; in fact, it was associated with the lowest payment rate among the three tone groups. The *High power + low emotion* tone may indicate that the victim is attempting to take back control over the situation. By remaining composed and emotionally detached, the victim could be strategically positioning themselves to resist pressure, minimize urgency and shift the power dynamic of the negotiation. Rather than succumbing to fear or anxiety, such behavior might be aimed at reducing the perceived power of the ransomware group and probing for concessions – suggesting that calmness serves more as resistance than a cooperation.

Binary regression findings

While payment likelihoods were initially analyzed separately, it was crucial to assess whether these factors had equal influence and whether the observed differences were statistically significant. The groups *High power + high emotion* and *Low power + high emotion* exhibited almost identical payment likelihoods, with differences too small to be considered statistically significant. *High power + low emotion* group showed a notably lower likelihood of payment compared to the reference group, but this difference also did not have statistical significance. Overall, these findings suggest that tonal groups alone may not be a strong or statistically significant predictor of whether a ransom payment occurs.

In stark contrast, the number of counteroffers emerged as the strongest and statistically significant predictor of payment likelihood. Each additional counteroffer made by the victim doubled the likelihood of payment, highlighting the important role of persistent negotiation efforts. This finding aligns with the concept of Multiple Equivalent Simultaneous Offers (MESOs) in negotiation theory, which states that presenting several counteroffers to the opposing group increases the likelihood of agreement (Heller, 2013). Such behavior demonstrates the victims flexibility and a willingness to collaborate, as the victim repeatedly offers new counteroffers that would suit both parties.

The statistical significance of the counteroffers (see Table 4) is clearly demonstrated, suggesting that the result is extremely unlikely to be due to chance. Moreover, when controlling for the number of counteroffers, the effect of tonal groups on payment likelihood becomes statistically insignificant. This pattern indicates that differences previously attributed to tone may be better explained by the victim's negotiation persistence. Overall, the data suggests that active engagement and effort in the negotiation process play a more determining role in successful payment outcomes than the emotional tone adopted by victims.

H1 and H3 aimed to explore whether engaging in counteroffer exchanges and the number of counteroffers influence the likelihood of ransom payment. The descriptive analysis showed that victims who made a counteroffer were more likely to pay the ransom compared to those who did not make any. This finding supports H1, suggesting that engaging in the negotiating process, rather than not, is associated with a higher chance of payment.

Furthermore, the data revealed an upward trend – as the number of counteroffers increased, so did the likelihood of payment. From the binary regression we can see that an additional counteroffer doubled the odds of payment. These findings strongly support H3, indicating that more than one counteroffer is not only more common in paid negotiations, but also statistically predictive of payment. This pattern suggests that persistence in negotiation through repeated attempts to reduce the ransom increases the likelihood of reaching a mutually acceptable agreement. This could also suggest to the ransomware group that the victim is potentially cooperative, increasing the chances of a price reduction being accepted.

Implications

These findings have several implications for practice. They suggest that ransomware victim can hold power during negotiations. While tone plays a role in forming the dynamic of the conversation, it is the persistence and effort of the victim that appears to be most influential in influencing payment outcomes. This insight ca inform organizations how they can prepare for and how to respond during ransomware attacks, putting a lot of emphasis on the importance of negotiation training. Although different tone lead to different psychological approaches, the findings imply that behavior of the victims has a greater impact on resolution of negotiations, rather than their tonal projection.

While the descriptive statistics show that both predictors influence payment outcomes, only the number of counteroffers is a statistically significant predictor. This suggests that the effort victims put in negotiating is more critical than their tone – a finding with relevance for future research.

Limitations and Future research

There are a few limitations present in this research. One of them is the fact that it is hard to say with confidence whether all the labelled or quoted phrases or words are what we believe they are. When an emotion is strong, you can confidently hypothesize that a victim is angry or sad, but not with all the calm or resilient emotions. We are not able to know exactly on what emotion was the victim acting on – while they might appear calm on text, they might be really panicked in real life. The coding process is subjective, which adds another limitation. Some phrases were sometimes coded or coded differently by one of the researchers, showing that sometimes it is hard to say definitively, what emotion or tone is being displayed. In some cases, disagreements arose regarding the degree to which a particular code was expressed. For example, explicitly stating a financial constraint versus merely implying financial difficulties led to differing interpretations, with one researcher coding it as a definitive instance and the other not.

There are plausible suggestions for future researching appearing from this study. It was noticed that some logs victims use a combination of different tones, sometimes starting very angry and aggressive and then becoming really anxious and pleading for help. Researching whether these combinations of tone groups have a different outcome of payment rather than just using one tone group is beneficial, as this opens new insights into negotiation behavior. It would also be interesting to add ransomware group behavior into the study – combine victim behavior with ransomware group behavior. Actions of victims can be reflective or defensive, therefore adding the tone of the ransomware group would provide necessary context to the analysis and also provide new insights into how they direct the negotiations. It could be that the attitude of the ransomware group (ex. being offensive and aggressive towards the victim) influenced whether the victim wants to continue talking or pay the ransom.

Conclusion

This study highlights the active role victims can play in shaping the outcomes of ransomware negotiations. Ransomware victims are not passive, they demonstrate varying degrees of agency: victims swore, pleaded, bargained, threatened, counterargued and reasoned. While emotional appeals may elicit cooperation and calm reasoning offers composure, the findings indicate that sustained engagement is the most significant predictor of resolution. These results suggest that successful negotiation outcomes are more influenced by the victim's effort than their emotional tone alone.

By analyzing real-world negotiation transcripts, this research aimed to understand how victims influence ransomware negotiations and contributes a unique perspective on victim effect. As ransomware continues to present ethical, operational, and psychological challenges to organizations, a deeper understanding of how victims can actively participate in negotiation processes becomes increasingly important. Recognizing that victims have the ability to influence these interactions adds to the understanding about the power dynamics during cyberattacks. Future research in this area can provide further insight into the complex system of negotiations and inform more effective methods for victims involved in such difficult situations.

References

Amann, A., Healy, S., Fokker, J., & Ryan, P. (2022). Dynamics of targeted ransomware negotiation. *IEEE Security & Privacy*, 20(2), 24–31. https://doi.org/10.1109/MSEC.2021.3135953

Boticiu, S., & Teichmann, F. (2023). How does one negotiate with ransomware attackers? *International Cybersecurity Law Review*, *5*(1), 55–65. https://doi.org/10.1365/s43439-023-00106-w

Brown, P., & Levinson, S. C. (1987). *Politeness: Some universals in language usage* (Vol. 4). Cambridge University Press.

Druckman, D., & Olekalns, M. (2008). Emotions in negotiation. *Group decision and negotiation, 17 (1)*, 1-11.

Galinsky, A. D., & Mussweiler, T. (2001). "First offers as anchors: The role of perspective-taking in negotiations." *Administrative Science Quarterly, 46(4)*, 718-744.

Gawazah, L., Rondla, A., & Balhareth, M. S. A. (2024). *To pay or not to pay: The US Colonial Pipeline ransomware attack* [Unpublished manuscript]. Thunderbird School of Global Management. https://www.researchgate.net/publication/383206534

Giles, H. (1973). Accent mobility: A model and some data. Anthropological Linguistics, 15(2), 87-105.

Heller, R. E. (2013). Negotiating for more: the multiple equivalent simultaneous offer. *Journal of the American College of Radiology*, *11*(2), 153–155. https://doi.org/10.1016/j.jacr.2013.06.004

Mattern, D. (2024, May 9). The importance of maintaining composure in a negotiation. *Advanced Purchasing Dynamics*. https://apurchasingd.com/the-importance-of-maintaining-composure-in-a-negotiation/

Mooser, A. P. E. (2025, January 14). *Emotions in negotiations: Friends or foes? - Frontline Negotiations*. Frontline Negotiations. https://frontline-negotiations.org/blog/blog-emotions-in-negotiations/

National Cyber Security Center. (2020, June). *Ransomware: Measures for preventing, limiting and recovering from a ransomware attack* (NCSC Factsheet).

Rubin, J. Z., & Zartman, I. W. (1995). Asymmetrical negotiations: Some survey results that may surprise. *Negotiation Journal*, 11(3), 221–229. https://doi.org/10.1111/j.1571-9979.1995.tb00751.x

Schneider, A., & Arnold, C. (2019, July 22). Equifax to pay up to $700 million in data breach settlement. *NPR*. https://www.npr.org/2019/07/22/744050565/equifax-to-pay-up-to-700-million-in-data-breach-settlement

Singh, S., & Kumar, S. (2020). The times of cyber attacks. *Acta Technica Corviniensis-Bulletin of Engineering*, 13(3), 133-137.

Staff, P. (2025, May 29). Power in negotiation: The impact on negotiators and the negotiation process. *Program on Negotiation at Harvard Law School*. https://www.pon.harvard.edu/daily/negotiation-skills-daily/how-power-affects-negotiators/

Steinberg, S., Stepan, A., Neary, K., Picker Center Digital Education Group, & Columbia School of International and Public Affairs. (2021). *The hacking of Sony Pictures: A Columbia University case study* (pp. 1–3). SIPA. https://www.sipa.columbia.edu/sites/default/files/2022-11/Sony%20-%20Written%20Case.pdf

Appendix: AI Use

During the preparation of this work the author used ChatGPT in order to fix grammar mistakes and improve sentence syntax. After using this tool/service, the author reviewed and edited the content as needed and take(s) full responsibility for the content of the work.

Appendix A

Codebook

Codes:	Definitions:
Initial Offer	The initial offer that the ransomware groups makes to the victim.
Assertive Pushback	The victim stands their ground or fights back.
Counteroffer by Victim	A counteroffer that the victim makes to the ransomware group.
Discount Request by Victim	The victim requests a discount for the initial price.
Financial Constraint	The victim tells the ransomware group that their company is struggling with money due to issues.

Emotional Plea	The victim uses strong emotional phrases to appeal to the ransomware group.
Information Seeking	The victim asks questions to understand what’s happening or the process of ransomware.
Readiness to Negotiate	The victim shows readiness to negotiate with the ransomware through showing initiative in the dialog.
Demand of Quality	The victim demands to see proof of quality from products of the ransomware group.
Strategic Politeness	The victim is polite in order to achieve consensus with ransomware group.
Strategic Delay	The victim delays the covnersation in order to gain more time.

Aggressive Response	The victim aggressively responds to the ransomware group.

Appendix B

Exemplar quotations per code

Codes:	Quotes:
Assertive Pushback	“I'm here and after intense conversations and internal consultations as you might imagine. Please refrain from hostile language. I will appreciate it. I was instruct to further elaborate with you couple of points, obviously after I did my own research about you and your highly professional capability and status.” “We had 70% back up and i was able to hire IT guys to build me a new system and restore 70% of my data. I spent 12,250.00 for this and I don't have anymore the 35,000.00 I am willing to pay the balance to you to get the remaining data so I can continue with my life.” “We appreciate your response, yet our "concerns" persist. Post-payment, we're left without any recourse should your service fail to decrypt what has been encrypted. In an effort to push this conversation forward and mitigate our hesitations about proceeding with payment, we require further clarity. Specifically, we need reassurance about your

	capability to decrypt a critical piece of our infrastructure <…>. This file is crucial to our negotiation. Gaining assurances from your team that we could expect this DB to be decrypted will help us move forward with a decision.”
Discount Request by Victim	“Do you allow any kind of discount for payment?” “Please show us a good discount.”
Financial Constraint	“We are a small business, we have been hit hard due to the economic downturn, and the pandemic.” “You will find if you search us, that we went bankrupt 2 years ago and have been on the losing side since.” “We're a non-profit organization with the majority of services covered by tax payers/state government. We help treat a variety of patients from cancer to mental health. It's very important we get our systems back quickly.”

	“We are a small company with not many people and all my family members work here. you didnt hack a big company. this situation is very bad for us and to be honest we dont have much money because work is not going good.”
Emotional Plea	“We try to survive from day to day...” “Everything is shut down, we can't help our patients. Everyday we are down, the worse off we are.” “It is our existence... please please help us”
Readiness to Negotiate	“What will be the discount if we pay quickly to you today?” “Can we discuss this price then?”
Demand of Quality	“What guarantees do I have that my system will start working after I do what you ask for?” “How are we supposed to trust this process?”
Strategic Politeness	“A 50% discount, approximately $300,000 USD is very helpful.”

	“Thank you again for your continued willingness to work with us and understanding of our situation.” “As I understand we cannot work together. So we will see what we can recover with manual work in the following days. Your service would help me a lot save time if it is fast but you are very expensive for me.”
Aggressive Response	“You made this problem for me.” “If you do not want to cooperate, then I will pass this information on to the customer and the media to make it obvious that BlackMatter are a group of crooks.” “You sons of bitches.” “Absolutely not. You posted us when I explained to you that we might increase our number. Remove the fucking post and I will try to save this on Monday but I am literally not promising anything. It is your choice.” “Are you kidding me?!?! That's a crazy amount of money.”