Shall We Play a Game: Studying Human & Ransomware Interaction

Kevin Zhang
Department of Computer Science and Engineering
NYU Tandon School of Engineering
Brooklyn, NY
zhang.kevin@nyu.edu

Charles Thomas
Department of Computer Science and Engineering
NYU Tandon School of Engineering
Brooklyn, NY
cht327@nyu.edu

I. Problem Statement and Motivation

Ransomware has become endemic in the computer security world, opening up a new avenue for economic success as a cybercriminal. The Cybersecurity & Infrastructure Security Agency (CISA) has classified ransomware as a threat to both public and private entities, “causing data loss, privacy concerns, and costing billions of dollars a year” [1]. With weekly attacks on corporations, infrastructure, and the public, individuals cannot do much to stem the tide. CISA’s “Reduce the Risk of Ransomware” highlights mitigation techniques, but there is a need for greater understanding of the process of a ransomware attack from the human perspective. Fundamentally, a security breach is a human event, with real people following a forensic trail, discovering their services are off-line, and dealing with a hostile actor. While this may seem like an unimportant feature of an attack, understanding the human perspective of a ransomware attack process could be crucial in recovering lost data and acting as quickly as possible. Our problem, more succinctly stated, is as follows: What, if any, are the overlooked human-dependent features of a ransomware attack?

II. Approach

Our approach uses a game theoretic experiment with human subjects to analyze rational choices in the frame of a ransomware attack. The idea is to approach ransomware from a logical and economic perspective. Following similar theoretic studies involving ransomware and game theory, [3][4][5] we hope to open new dimensions by distilling the “order of operations” that comprise the lifecycle of an attack. This will heavily draw from the “hostage/kidnapping” example demonstrated in Li’s paper [2]. Ransomware can thus be examined in the lens of a collective action problem.

In our experiment, we will construct a multistage procedure, with a similar game played at each stage. The subject (known as the player) will serve as both the rational actor and defender. In this experiment, we will explore an asymmetric, sequential game, where the player initially has perfect information regarding their economic choices. However, when the “ransomware” event hits, the player will need to operate with imperfect/partial information (not knowing all the moves and payoffs). This will test the player’s ability to make choices given irrational circumstances.

The format of the game is in all essence a resource simulation. We have decided that the user is a CFO (business head) and COO (operations head) of the pizza chain Little Caligula’s, which serves several thousand customers with its online pizza ordering service. The subject will be a major decision maker in the company, so that they are capable of making both economic and operational decisions. Economic decision making will provide the player with an impetus and goal throughout the game, while the operational decision making covers actions post-ransomware attack. For the framework of this game, we thoroughly utilized a text-based mobile messaging platform called Twilio.

The Twilio Application Programming Interfaces (API) operates as a texting service with an input and an output. each “log” displayed in the system is either a confirmation that a text is sent to the user (displayed as “sent by” their phone number), or a computation of the user’s text (displayed as “sent by” the paired Twilio survey number, +1-352-645-3591). [6]

Twilio’s backend is structured as a set of discrete nodes. Within these nodes are "core" node texts that are sent out, each one requiring some kind of response. This response can range from something like okay (most often), yes/no, deny/accept, pay/negotiate/refuse, etc. After the user sends back a response, the text is processed by a computation node. This serves as the error checking during the game’s progress; it can either confirm the content of the node as fitting one of the correct responses or send a prompt text that directs the user to answer with one of the correct options. The system sends the last prompt text to the user so that they remain aware of their potential selections. If the response in question is correct and fits as an “accepted input,” then sends the next node in the tree. The game take place in a series of three steps:

1. “Distraction Phase” - A pre-ransomware phase of the game, the responses lead in a linear fashion along the decision tree. Each answer is recorded by Twilio’s backend, and can be exported to display a user’s “economic choice” for that particular prompt.
2. "Ransomware Event" - The user is given a ransomware prompt where it is implied that the work they had done is now held hostage. This serves as a shock to the user, as both the study description and prior portion of the game did not allude to a ransomware attack occurring.
3. "Decision-Making Phase” - This is the post-ransomware section, which pits the participants against a series of rational decisions with little information. The only information provided is “non-guaranteed” information (i.e. not necessarily rational or with perfect information, or information given with a chance to not be true). The participant must decide what to do to manage risk and retrieve their held hostage data.

III. Evaluation Approach

We will determine if the approach solves the problem if there is a relationship between the rationality of a user and the final choices that they make at the end of the game. A negative result would show that there is no relationship. In this case, a user’s rationality has no basis on what choices they made at the end of the game.

Furthermore, we would gain insight on the problem if there is any large aversion or attraction to a solution at the end. For example, even if the rationality has no effect on the final choices, it is possible that the majority of users would pick, for example CONTACT-NEGOTIATE. This would indicate that this choice is extremely attractive to the user given the context of the preceding questions.

While it is difficult to design an experiment that closely models reality, we have created an extensive pre-ransomware setup that provides significant mindset creation for the participant. There are a total of 27 mandatory nodes with explanatory text or business decisions, and there are 9 ransomware decision nodes. Each of the nodes requires at least thirty seconds to read, and there are a number of recurring characters that the user must keep track of while completing the game. We believe that this will model reality as closely as possible because the user becomes accustomed to maximizing company profits over time, and so they are more incentivized to model the decisions of a real life financial and operations officer.

IV. Related Work and Novelty

This paper is novel because it condenses a model into a rational problem for humans to solve. When reducing the ransomware phenomena into a game, we can more accurately examine human factors that influence choices.

There is research modeling ransomware as a kidnapping game [3][4][5], but these papers assume rational actors in a theoretical sense. Specifically, In Li's paper, the researchers noted that it may be rational to artificially self-restrict the decision set of an attacker, calling this move an 'irrational aggression' [2]. It could be insightful to incorporate negotiation as part of the experiment to see if the subject would play out this irrational aggression, or if the victim would dismiss it as an artificial construct. This would create a non-cooperative bargaining game where an economical equilibrium could be met between the player and the proctor. This study does not provide a real world study where human subjects are actively examined throughout the duration of a simulation. As conducting an actual ransomware on targets is illegal, impractical, and immoral, one of the few ways to study ransomware in a vacuum is to design a simulation that provides similar impetus and results as a ransomware would, without causing any unnecessary harm to the participants.

Our assumption is that people, and companies specifically, will not necessarily behave rationally. Performing an experiment with human subjects could reveal the ways in which irrational decisions might play a role. Potential avenues include time constraints, reputational damage, and imperfect knowledge. Public agencies (CISA) [7] and private cybersecurity firms (Crowdstrike) [8] indicate that backing up data and reporting to law enforcement are best practice. However, companies often neglect one or the other. In 2016, the FBI reported 2,673 ransomware incidents, but the true number of attacks is likely much higher [9]. We will examine the role rational choice plays in this phenomenon.

Using the information gleaned from our literature review and human-research training, we found that difficulty in studying ransomware is the inherent "knowledge" of an attack on the part of the subject. For this reason, we sought to "game-ify" the ransomware in the vehicle of a text-based adventure, while also indicating to the subjects that this was only a study for economic decision-making.

V. Results

Our data collection took place in three distinct parts (1. Candidacy form, 2. Text-based game, 3. Debrief/Exit Survey), it is important to distinguish between the phases and what important information was collected. All data was connected utilizing a central connecting datapoint - a phone number.

A. Candidacy Form

The Candidacy form was used namely to establish whether individuals were eligible or not to access this study. We had twenty-five (25) participants complete the candidate form. We required the potential participants to be over the age of 18, have a NYU NetID (and thus be affiliated with NYU), agreed to our study's consent form (included in Appendix 1.1), and have the ability to receive over 40 text messages and access to a phone with the country code +1. These questions were enacted to both control the population of this study and ensure that subjects were adequately protected as per IRB research ethicality. Additionally, the "40 text messages" question was used to logistically equalize the playing ground - we did not want to unnecessarily burden participants with the economic cost if they did not have an unlimited text plan.

As the candidacy form was used for vetting candidates, most parts of the form are not useful for the purposes of this study. However, one question in particular provides some demographic information as to the participants. The question: "Please indicate your academic status/affiliation at NYU," with the options 'Undergraduate - BA Candidate', 'Undergraduate - BS Candidate', 'Graduate - Masters' Candidate', 'Graduate - PhD Candidate', 'NYU Alumni', or 'NYU Faculty.' Surprisingly, close to three-quarters of the respondents indicated that they were NYU Alumni. This may be due to promotional volume and close relationships. Individuals who know the test proctors personally (Charlie and Kevin) were more likely to complete the entire study. Both of the proctors attended NYU while undergraduates and have NYU Alumni networks.

B. Text-based Game

The text-based game was used to analyze an individual's rational decision making and their responses before, during, and after the simulated ransomware attack. We had twenty-two (22) participants fully complete the text-based game. Four (4) participants began the text-based game but did not finish the prompts.

There are four potential paths that the participant could have chosen at the conclusion of the game. The first choice gives three possibilities:

1. Pay the attackers the full amount (five million dollars), and hope that the ransomware group will fulfill their promise.
2. Contact the FBI, this will potentially delay payment towards the hacking group if the FBI requires coordination. If the hacking group discovers coordination with law enforcement, they may retaliate.

3. Do not pay the hacking group. This will incur a cost on the service due to downtime, but there will be no loss in dollars from the ransom payment itself. The hacking group will most likely sell the stolen data.

If the user had chosen either option one or three, the game would finish. If the participant chose option two, the ransom payment would increase, and they would be asked if they would like to pay the ransom as it stands or negotiate further. We denote these paths as PAY, CONTACT-PAY, CONTACT-NEGOTIATE, and DENY. The results are shown in the following table:

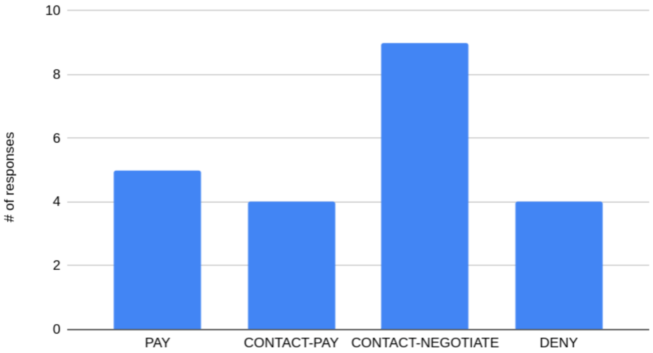


Figure 1 – Rationality Score Frequency

The majority of the participants chose to contact the FBI. This is likely the most risk averse strategy, and makes sense in the context of the game design.

Throughout the game, we had assigned a 'rationality' score to each of the set of questions that preceded the ransomware attack. This simulates the 'rationality' of the participant, i.e. how well they can make decisions in a business environment. While it is true that no decision is absolutely correct, we had designed the questions in mind such that there should be a more obviously correct answer. For each correct response the user's rationality score was incremented, and for each incorrect answer the score remained unchanged. The following chart is the rationality distribution:

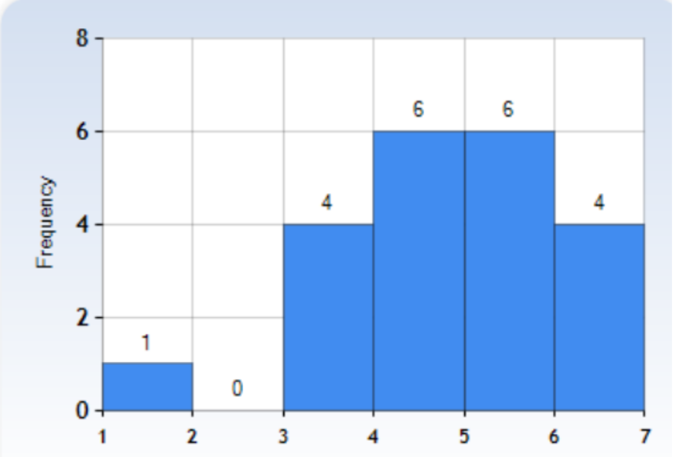


Figure 2 – Number of Responses Per Outcome

Only one participant scored a 1 or 2, and the majority of the participants scored either a four or a five.

Finally, we grouped the participants by outcome category, and calculated the average rationality score for each group. This is the result:

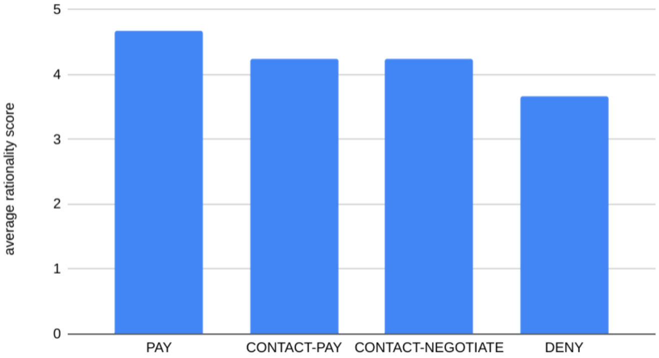


Figure 3 – Average Rationality Score for Each Outcome

From the above, the group with the highest rationality score chose to pay the attackers immediately, followed by contact-pay, contact-negotiation, and then finally deny. From the above, it's likely that the participants who would most want to maximize company profits would choose to immediately pay the attackers, and those who chose the less profitable decisions were more likely to immediately deny the attackers.

C. *Debrief Survey*

The Debrief form provides both usable data regarding sentiments during the text-based game and offers a chance to educate the participants on ransomware attacks, while elaborating why deception was necessary in the game. We had a total of nineteen (19) participants complete the debrief form.

Sentiment Questions:

In terms of the "game sentiment" questions, we attempted to see if there was any difference in strategy prior to the attack occurring, and strategy after the attack. Additionally, we asked them specifically to target which part of the attack may have motivated the change.

1. Describe as close as you can, your primary goal prior to the attack?

With this question, the major sentiment provided by the respondents was to expand the company and ensure financial success. Eleven (11) of the respondents indicated their primary goal as such, utilizing phrases such as "increase brand presence," "increase...cash flow," or "maximize future potential for…my pizza." Outliers within the survey are important, as one individual sought to "run Little Caligula's in the way that I would in the real world," and "avoid getting scammed."

2. Did this goal change after the attack? Which, if any, part of the attack might have motivated the change?

Ten (10) respondents indicated that their goals did change due to the ransomware attack - sentiments examined circled around protection of the company, recovery of lost data, and minimization of damage to the business. Of the eight (8) individuals who felt their goals did not change, the participants pointed to the fact that ransomware costs were fixed costs, no new deals were offered, and the idea that there would be no guaranteed data return.

Ease Questions:

Additionally, we utilized a set of "ease" questions to determine potential stress attitudes prior and after the ransomware attacks. The answers were scaled on a five-point Likert scale where a one (1) indicated "easy to answer", while a five (5) indicated "difficult to answer." The hope was to examine whether the perfect information/rationality pre-ransomware attack and the lack of information/irrationality after the ransomware attack had any effect on the ability to answer prompts. The results are provided below:

1. Please rate as closely as possible your ease of answering the text prompts, prior to the ransomware attack. Please note the x-axis is the scale (1-5), while the y-axis is the number of respondents :

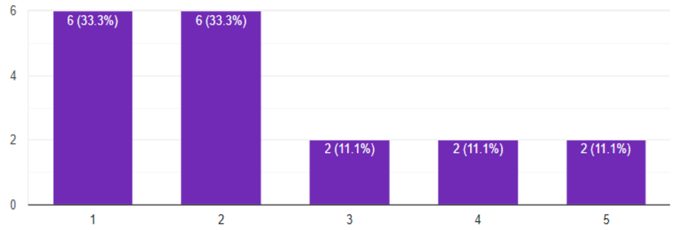


Figure 4 – Ease Answering Prompt Prior to Ransomware

2. Please rate as closely as possible your ease of answering the text prompts, after the ransomware attack. Please note the x-axis is the scale (1-5), while the y-axis is the number of respondents:

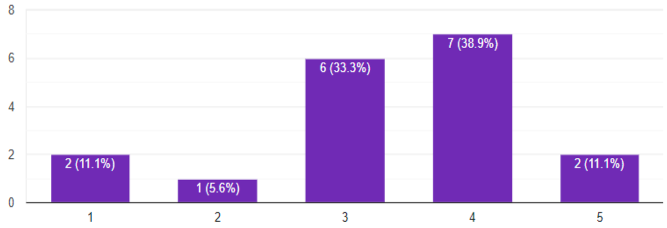


Figure 5 – Ease Answering Prompt After Ransomware Attack

As demonstrated by the aforementioned results, there was a general shift towards the harder side of the spectrum (e.g. 5). Taking a look at individual participants, there were three (3) participants who felt that the post-ransomware section was easier than the pre-ransomware prompts. Six (6) individuals' sentiments did not change - they answered the same level of ease regardless. However, the majority (nine participants) believed that the post-ransomware attack was harder to answer.

VI. Discussion

A. *Game Results*

While there are not enough participants to make a strong conclusion in any direction, there is enough evidence to show that the more rational a participant behaves in making business decisions, the more likely they are to pay the attackers, and further that they are more unlikely to immediately deny the attacker. This result matches that of the decisions that real business owners take when confronted with a ransomware attack. They are unlikely to deny the attack on the condition that they would lose profits.

We also found that users are most attracted to picking CONTACT-NEGOTIATE. This outcome is the 'safest' option, as contacting the FBI is the least likely (in the real world) to result in a highly negative profit outcome. Further, the option to negotiate after contacting the FBI indicates that the user is trying to minimize profit loss, and they are overriding the potential downside of raising the ransom in favor of the potential to lower it. While CONTACT-NEGOTIATE is the most common result, there is no strong preference among the other three results. PAY, CONTACT-PAY, and DENY all had a similar level of responses.

It is interesting that the attackers did not profit from only four participants. We had expected to see a higher number of people rejecting payment on ethical grounds. However, this result matches reality. Businesses are not likely to not pay attackers if it would be more profitable to pay the attackers, and ethical concerns regarding the support of hacking are only secondary to the business motivations.

B. *Debrief Results*

The Debrief section provided an interesting mix of both quantitative and qualitative analysis for ransomware attacks. The sentiment questions offered a snapshot of how participants interacted with the experiment and felt post-game. At the same time, the ease of answering questions allowed for a numerical representation of the change in stress attitudes due to the ransomware attack.

As part of the game design, we sought to distinguish the two sections clearly. Non-Player Characters (NPCs) were created to add emotional attachment to the economic decisions, while providing a degree of entertainment for the participant. An essential aspect of the study was the shift in rational to irrational decision making. This was made more apparent by the presence of a "recommendation." Pre-ransomware, the participants were introduced to a NPC, Alex, who served on the CFO Staff. This character acted as a guide and pointed the player towards options that would be considered "rational" (as indicated in the aforementioned rationality analysis). When the ransomware hits, Alex indicates that he will be "resigning" from his position, thus removing the perfect information from the participants' metaphorical inventory. As such, the respondent's sentiments echoed this, where after the goal they were no longer driven to make clear, economical decisions. One respondent actually indicated that they noticed the lack of recommendations.

In regards to ease of answering the prompts, we hypothesized that irrational decisions would be harder to make. One of our intended game design concepts was to organize the game where the majority would take place in the "Distraction" phase, making a large number of simple decisions. The "Decision Phase" was in contrast to that principle, as it was essentially a single/double complex decision. This was realized in our results.

C. *Ethical Considerations*

Institutional Review Board (IRB) ethical training was a vital part of both our literature review and training process to undertake this study. Both of the principal investigators conducted a New York University required Human Subjects Training Program [10] through the CITI program [11]. The specific course taken was , and served as a requirement for the course this research project was conducted under. For this study, we obtained approval from the instructor/faculty sponsor in line with IRB standards.

As this study involved human subjects, we needed to be thoroughly careful to measure the amount of impact our study might have on participants. Our interview questions and experiments are modeled so as not to cause undue stress to the participant. However, as there is some form of deception involved (i.e. participant is unaware that ransom will occur at some point). We included a consent form with our initial candidacy form that asked the participant for consent to deploy the study and use data gathered from their responses to write this paper. They were required to virtually sign and date prior to proceeding with the study. Within this consent form, we reiterated that participation in the study is entirely voluntary and at any point the participant could withdraw from the study. Please see Appendix 1.1 to see the full text of the consent form. Undue stress was mitigated post-game when conducting the debrief and providing some information on why deception was necessary and typically how Ransomware attacks play out. The debriefing also provides useful information regarding detecting, preventing, and responses to ransomware, as well as providing an area for feedback [12].

In regards to ethical concerns for information handling and privacy, redundant steps were taken to ensure data was thoroughly anonymized and handled appropriately. During the process of data collection, information was stored on either a 1) secure Google Drive shared only between the two principal investigators, and 2) the Twilio API. Within these two repositories, the only potential personal identifiable information (PII) connecting the human subjects to their responses were NetIDs, and Phone Numbers.

NetIDs are a New York University (NYU) universal identifying username which allows members within the NYU community to communicate with one another. These typically are a combination of alpha and numeric characters, generally the user's initials, followed by a random three to five digit number. Although these are connected to NYU's Google Suite and allow any NYU member to identify another NYU member, they are classified as low-risk private information by NYU's IT policy [13]. NetIDs serve also to authenticate participants as NYU community members, which are the target population for this study. After this purpose, they are no longer used as identifiers in the study.

Phone numbers are higher risk PII as they have a larger potential to affect subjects who take part in the survey if they were released to the public. This is a greater risk as phone numbers serve as our linking factor among all parts of the study (e.g. candidate form, text-based game, debrief form). The use of phone numbers to merge all three parts of the study is due to the fact that the Twilio API centers its output on phone numbers. We mitigate the risks of using this PII by assigning randomized "participant numbers" to each group of data immediately after merging the data sets. Additionally, we have thoroughly scrubbed our data analysis repositories of any lingering phone numbers.

D. *Limitations*

The subjects examined are all NYU affiliated individuals (whether current undergrads, graduates, or alumni), which may affect the final result (education level). We would like to see the results of the study deployed externally for different populations. There is a potential that individuals working may have more training and expertise than students. Furthermore, it's likely that students were under certain academic related pressures that may have decreased their focus and care in completing the game.

The total number of participants dropped when moving from the candidate form to the game, and then again from the game to the debrief form (i.e. 25 - 22 - 18). The length of the study may have played a role in this drop off, as there were over thirty text responses that each user had to respond to. In the future, it might be more beneficial to have a shorter game, or even modulate the length of the game in order to see if there is an effect on the final outcome of the participant.

The number of participants in the final debrief form are those who completed all three sections as the steps are sequential. Namely, to access the text-game, an individual must complete the initial candidate form and provide authentication that they had opened the game. In order to access the debrief form, a participant would need to play through the entire game and access the link contained on the final node.

Although we made the application is accessible to many, it does require the user to remain engaged and looking at their phone for 30 minutes from start to finish. WE also encountered an issue where users could not access the google form unless they had access to their NYU google suite accounts, which was a challenge for some Alumni.

Finally, our debrief offers a chance for participants to provide feedback regarding their experience during the experiment, as well as their relative satisfaction with the conclusion of the study. Many participants echoed the sentiments mentioned above.

VII. Conclusion

The metrics we examined are the ultimate choices made (paying, negotiating, or denying the ransomware group), as well as user rationality (making economic decisions) and user sentiments.

There is a clear relationship between the rationality of a participant and the likelihood that they are willing to pay the attackers. Participants who are the least business-rationale are the most likely to deny the attackers immediately. Participants are strongly attracted to contacting the FBI over immediately paying the ransom, or immediately denying the ransom.

There are a number of small improvements one could make for a future study. We did not include an exact income, cash reserve, and profit loss score over time. While we had several dollar figures interspersed, it may have been more effective to show the exact value to the user for every action that they take. This would have even more aligned their incentives with the real world, and likely would have made them more consider each option as they were presented. This was indicated in the feedback form in two answers. Further, it may have been easier to make the user choose a number as a response instead of a word like PAY or ACCEPT. A user indicated that this was a problem, and the data shows that a few users had mistyped responses. Using a number as a response would have cut down on this error.

Lastly, there are three unexplored avenues for experimental ransomware attacks with participants. The effect of the attacker's honor did not play a large role in this study, and a subsequent study could examine the effect of multiple attacks with a dishonorable attacker (one that does not keep promises). There is some research into the honorability of the attacker that could make use of an experiment based study [14]. The second avenue is the incorporation of anti-ransomware tools in business decision making [15]. These tools could be presented as an option before the attack occurs. The third avenue concerns the product pricing after the attack has occurred. There is research to indicate that ransomware actually increases the price, whereas malware decreases the price due to unintuitive economic incentives [16].

REFERENCES/BIBLIOGRAPHY

[1] Cybersecurity and Infrastructure Security Agency, CISA LAUNCHES CAMPAIGN TO REDUCE THE RISK OF RANSOMWARE, 16, Feb. 2021 [ONLINE] Available: https://www.cisa.gov/news/2021/01/21/cisa-launches-campaign-reduce-risk-ransomware [Accessed Oct. 4, 2021]

[2] Zhen Li and Qi Liao. 2020. Ransomware 2.0: to sell, or not to sell a game-theoretical model of data-selling Ransomware. In Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES '20). Association for Computing Machinery, New York, NY, USA, Article 59, 1–9. DOI:https://doi.org/10.1145/3407023.3409196

[3] Edward Cartwright, Julio Hernandez Castro, Anna Cartwright, To pay or not: game theoretic models of ransomware, Journal of Cybersecurity, Volume 5, Issue 1, 2019, tyz009, https://doi.org/10.1093/cybsec/tyz009

[4] Laszka A, Farhang S, Grossklags J. On the economics of ransomware. In: International Conference on Decision and Game Theory for Security. Springer, 2017, pp. 397-417.

[5] Caporusso N, Chea S, Abukhaled R. A game-theoretical model of ransomware. In: International Conference on Applied Human Factors and Ergonomics. Cham: Springer, 2018, pp. 69-78.M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[6] *SMS with Twilio programmable messaging: Send and receive texts in your app*. Twilio. (n.d.). Retrieved December 18, 2021, from https://www.twilio.com/docs/sms

[7] "CISA MS-ISAC Ransomware Guide," 30-Sep-2020. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf. [Accessed: 03-Oct-2021].

[8] K. Baker, "How to prevent ransomware," crowdstrike.com, 06-Jul-2021. [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/ransomware/how-to-prevent-ransomware/. [Accessed: 04-Oct-2021].

[9] C. Cimpanu, "FBI: Victims aren't reporting ransomware attacks," BleepingComputer, 23-Jun-2017. [Online]. Available: https://www.bleepingcomputer.com/news/security/fbi-victims-arent-reporting-ransomware-attacks/. [Accessed: 05-Oct-2021].

[10] Cartwright, Anna, and Edward Cartwright. 2019. "Ransomware and Reputation" Games 10, no. 2: 26. https://doi.org/10.3390/g10020026

[11] NYU Web Communications. (n.d.). Research with human subjects. NYU Research. Retrieved December 15, 2021, from https://www.nyu.edu/research/resources-and-support-offices/getting-started-withyourresearch/human-subjects-research.html

[12] Research, ethics, and compliance training. CITI Program. (n.d.). Retrieved December 19, 2021, from https://about.citiprogram.org/

[13] Office for Human Research Protections (OHRP). (2021, June 16). U.S. Department of Health & Human Services - 45 CFR 46. HHS.gov. Retrieved December 16, 2021, from https://www.hhs.gov/ohrp/regulations-and-policy/regulations/45-cfr-46/index.html#46.102

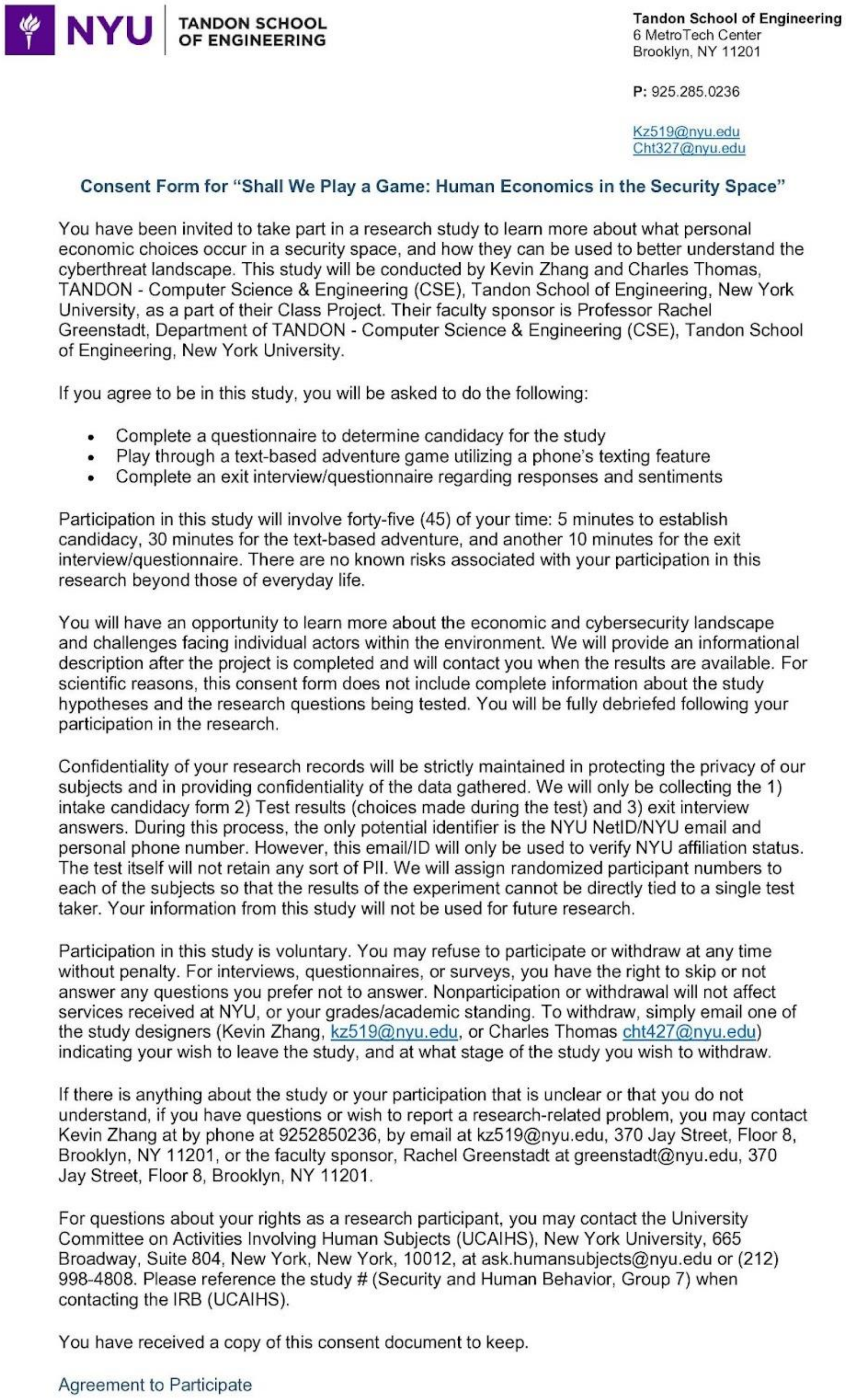
[14] NYU Web Communications. (n.d.). Electronic data and System Risk Classification Policy. NYU - University Policies and Guidelines. Retrieved December 15, 2021, from https://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/electronic-data-and-system-risk-classification.html

[15] Pont J., Abu Oun O., Brierley C., Arief B., Hernandez-Castro J. (2019) A Roadmap for Improving the Impact of Anti-ransomware Research. In: Askarov A., Hansen R., Rafnsson W. (eds) Secure IT Systems. NordSec 2019. Lecture Notes in Computer Science, vol 11875. Springer, Cham. https://doi.org/10.1007/978-3-030-35055-0_9

[16] August, Terrence and Dao, Duy and Dao, Duy and Niculescu, Marius Florin, Economics of Ransomware: Risk Interdependence and Large-Scale Attacks (November 5, 2021). Forthcoming in Management Science Earlier Version Presented at WISE 2017, CIST 2018, and WEIS 2019, Available at SSRN: https://ssrn.com/abstract=3351416 or http://dx.doi.org/10.2139/ssrn.3351416

APPENDIX

Figure 1.1 Consent Form



NYU | TANDON SCHOOL OF ENGINEERING

Tandon School of Engineering
6 MetroTech Center
Brooklyn, NY 11201

P: 925.285.0236

Kz519@nyu.edu
Cht327@nyu.edu

Consent Form for "Shall We Play a Game: Human Economics in the Security Space"

You have been invited to take part in a research study to learn more about what personal economic choices occur in a security space, and how they can be used to better understand the cyberthreat landscape. This study will be conducted by Kevin Zhang and Charles Thomas, TANDON - Computer Science & Engineering (CSE), Tandon School of Engineering, New York University, as a part of their Class Project. Their faculty sponsor is Professor Rachel Greenstadt, Department of TANDON - Computer Science & Engineering (CSE), Tandon School of Engineering, New York University.

If you agree to be in this study, you will be asked to do the following:

- Complete a questionnaire to determine candidacy for the study
- Play through a text-based adventure game utilizing a phone's texting feature
- Complete an exit interview/questionnaire regarding responses and sentiments

Participation in this study will involve forty-five (45) of your time: 5 minutes to establish candidacy, 30 minutes for the text-based adventure, and another 10 minutes for the exit interview/questionnaire. There are no known risks associated with your participation in this research beyond those of everyday life.

You will have an opportunity to learn more about the economic and cybersecurity landscape and challenges facing individual actors within the environment. We will provide an informational description after the project is completed and will contact you when the results are available. For scientific reasons, this consent form does not include complete information about the study hypotheses and the research questions being tested. You will be fully debriefed following your participation in the research.

Confidentiality of your research records will be strictly maintained in protecting the privacy of our subjects and in providing confidentiality of the data gathered. We will only be collecting the 1) intake candidacy form 2) Test results (choices made during the test) and 3) exit interview answers. During this process, the only potential identifier is the NYU NetID/NYU email and personal phone number. However, this email/ID will only be used to verify NYU affiliation status. The test itself will not retain any sort of PII. We will assign randomized participant numbers to each of the subjects so that the results of the experiment cannot be directly tied to a single test taker. Your information from this study will not be used for future research.

Participation in this study is voluntary. You may refuse to participate or withdraw at any time without penalty. For interviews, questionnaires, or surveys, you have the right to skip or not answer any questions you prefer not to answer. Nonparticipation or withdrawal will not affect services received at NYU, or your grades/academic standing. To withdraw, simply email one of the study designers (Kevin Zhang, kz519@nyu.edu, or Charles Thomas cht427@nyu.edu) indicating your wish to leave the study, and at what stage of the study you wish to withdraw.

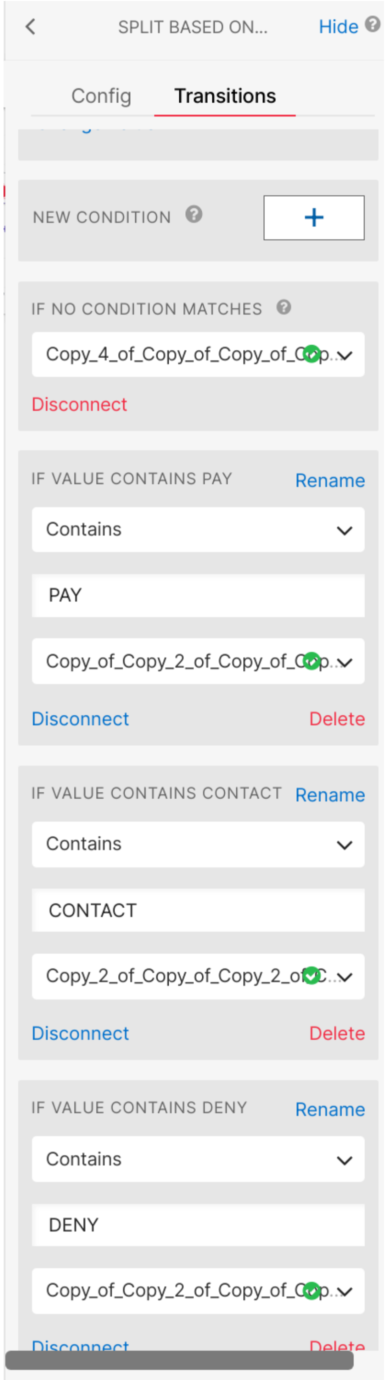
If there is anything about the study or your participation that is unclear or that you do not understand, if you have questions or wish to report a research-related problem, you may contact Kevin Zhang at by phone at 9252850236, by email at kz519@nyu.edu, 370 Jay Street, Floor 8, Brooklyn, NY 11201, or the faculty sponsor, Rachel Greenstadt at greenstadt@nyu.edu, 370 Jay Street, Floor 8, Brooklyn, NY 11201.

For questions about your rights as a research participant, you may contact the University Committee on Activities Involving Human Subjects (UCAIHS), New York University, 665 Broadway, Suite 804, New York, New York, 10012, at ask.humansubjects@nyu.edu or (212) 998-4808. Please reference the study # (Security and Human Behavior, Group 7) when contacting the IRB (UCAIHS).

You have received a copy of this consent document to keep.

Agreement to Participate

Figure 1.2 Twilio Decision Node Conditions



SPLIT BASED ON... Hide

Config Transitions

NEW CONDITION +

IF NO CONDITION MATCHES

Copy_4_of_Copy_of_Copy_of_Cop...

Disconnect

IF VALUE CONTAINS PAY Rename

Contains

PAY

Copy_of_Copy_2_of_Copy_of_Cop...

Disconnect Delete

IF VALUE CONTAINS CONTACT Rename

Contains

CONTACT

Copy_2_of_Copy_of_Copy_2_of_C...

Disconnect Delete

IF VALUE CONTAINS DENY Rename

Contains

DENY

Copy_of_Copy_2_of_Copy_of_Cop...

Disconnect Delete

Figure 1.3 Segment of Twilio Decision Tree

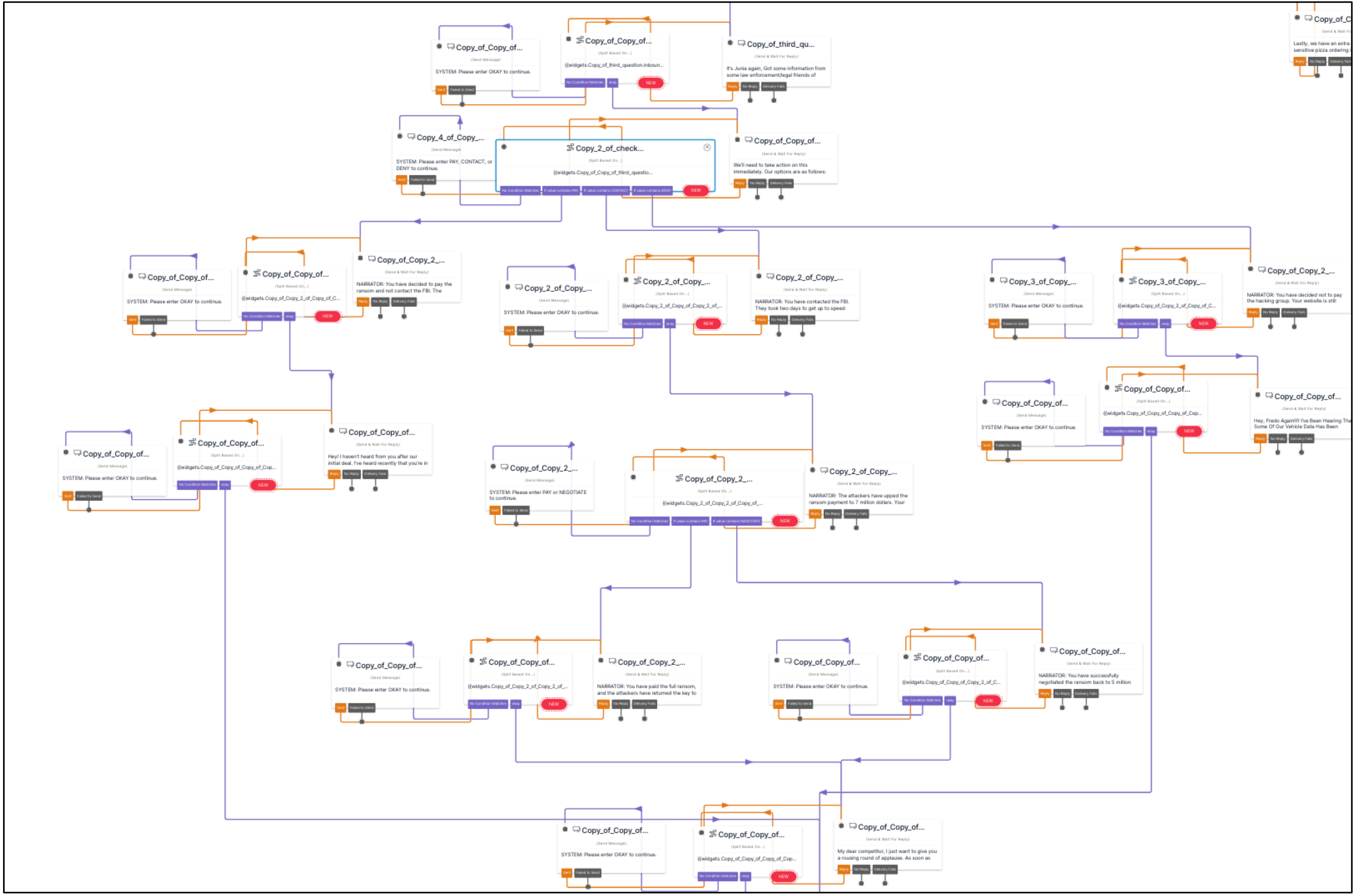
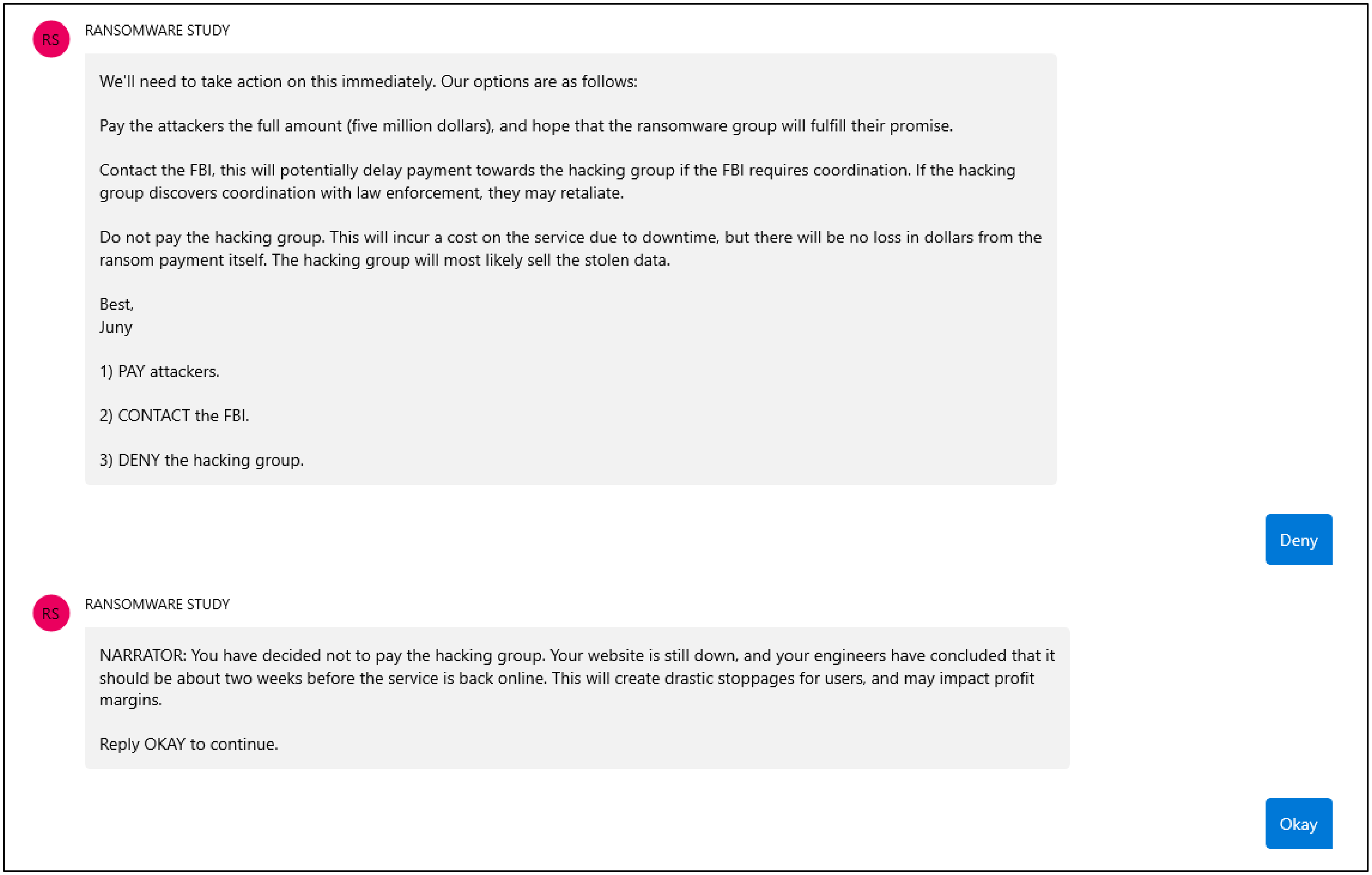

Copy_of_Copy_of...
(Send Message)
SYSTEM: Please enter OKAY to continue.
Sent
Failed to Send
Copy_of_Copy_of...
(Split Based On...)
{{widgets.Copy_of_third_question.inboun...
No Condition Matches
okay
NEW
Copy_of_third_qu...
(Send & Wait For Reply)
It's Junia again, Got some information from some law enforcement/legal friends of
Reply
No Reply
Delivery Fails
Copy_of_C
Lastly, we have an extra sensitive pizza ordering
Copy_4_of_Copy_...
(Send Message)
SYSTEM: Please enter PAY, CONTACT, or DENY to continue.
Copy_2_of_check...
(Split Based On...)
{{widgets.Copy_of_Copy_of_third_questio...
If value contains PAY
If value contains CONTACT
If value contains DENY
Copy_of_Copy_of...
(Send & Wait For Reply)
We'll need to take action on this immediately. Our options are as follows:
Copy_of_Copy_of...
(Send Message)
SYSTEM: Please enter OKAY to continue.
Copy_of_Copy_of...
(Split Based On...)
{{widgets.Copy_of_Copy_2_of_Copy_of_C...
Copy_of_Copy_2_...
(Send & Wait For Reply)
NARRATOR: You have decided to pay the ransom and not contact the FBI. The
Copy_2_of_Copy_...
(Send Message)
SYSTEM: Please enter OKAY to continue.
Copy_2_of_Copy_...
(Split Based On...)
{{widgets.Copy_2_of_Copy_of_Copy_2_of_...
Copy_2_of_Copy_...
(Send & Wait For Reply)
NARRATOR: You have contacted the FBI. They took two days to get up to speed
Copy_3_of_Copy_...
(Send Message)
SYSTEM: Please enter OKAY to continue.
Copy_3_of_Copy_...
(Split Based On...)
{{widgets.Copy_of_Copy_2_of_Copy_of_C...
Copy_of_Copy_2_...
(Send & Wait For Reply)
NARRATOR: You have decided not to pay the hacking group. Your website is still
Copy_of_Copy_of...
(Send Message)
SYSTEM: Please enter OKAY to continue.
Copy_of_Copy_of...
(Split Based On...)
{{widgets.Copy_of_Copy_of_Copy_of_Cop...
Copy_of_Copy_of...
(Send & Wait For Reply)
Hey, Fredo Again!!! I've Been Hearing Tha
Some Of Our Vehicle Data Has Been
Copy_of_Copy_of...
(Send Message)
SYSTEM: Please enter OKAY to continue.
Copy_of_Copy_of...
(Split Based On...)
{{widgets.Copy_of_Copy_of_Copy_of_Cop...
Copy_of_Copy_of...
(Send & Wait For Reply)
Hey! I haven't heard from you after our initial deal. I've heard recently that you're in
Copy_of_Copy_2_...
(Send Message)
SYSTEM: Please enter PAY or NEGOTIATE to continue.
Copy_of_Copy_2_...
(Split Based On...)
{{widgets.Copy_2_of_Copy_2_of_Copy_of_...
If value contains PAY
If value contains NEGOTIATE
Copy_2_of_Copy_...
(Send & Wait For Reply)
NARRATOR: The attackers have upped the ransom payment to 7 million dollars. Your
Copy_of_Copy_of...
(Send Message)
SYSTEM: Please enter OKAY to continue.
Copy_of_Copy_of...
(Split Based On...)
{{widgets.Copy_of_Copy_2_of_Copy_2_of_...
Copy_of_Copy_2_...
(Send & Wait For Reply)
NARRATOR: You have paid the full ransom, and the attackers have returned the key to
Copy_of_Copy_of...
(Send Message)
SYSTEM: Please enter OKAY to continue.
Copy_of_Copy_of...
(Split Based On...)
{{widgets.Copy_of_Copy_of_Copy_2_of_C...
Copy_of_Copy_of...
(Send & Wait For Reply)
NARRATOR: You have successfully negotiated the ransom back to 5 million
Copy_of_Copy_of...
(Send Message)
SYSTEM: Please enter OKAY to continue.
Copy_of_Copy_of...
(Split Based On...)
{{widgets.Copy_of_Copy_of_Copy_of_Cop...
Copy_of_Copy_of...
(Send & Wait For Reply)
My dear competitor, I just want to give you a rousing round of applause. As soon as

Figure 1.4 Screenshot of Texting Interface



We'll need to take action on this immediately. Our options are as follows:

Pay the attackers the full amount (five million dollars), and hope that the ransomware group will fulfill their promise.

Contact the FBI, this will potentially delay payment towards the hacking group if the FBI requires coordination. If the hacking group discovers coordination with law enforcement, they may retaliate.

Do not pay the hacking group. This will incur a cost on the service due to downtime, but there will be no loss in dollars from the ransom payment itself. The hacking group will most likely sell the stolen data.

Best,
Juny

1) PAY attackers.

2) CONTACT the FBI.

3) DENY the hacking group.

Deny

NARRATOR: You have decided not to pay the hacking group. Your website is still down, and your engineers have concluded that it should be about two weeks before the service is back online. This will create drastic stoppages for users, and may impact profit margins.

Reply OKAY to continue.

Okay