Computers & Security 116 (2022) 102644

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Preventive portfolio against data-selling ransomware—A game theory of encryption and deception

Zhen Li[a], Qi Liao[b,*]

[a] Department of Economics & Management, Albion College, USA
[b] Department of Computer Science, Central Michigan University, USA

ARTICLE INFO

Article history:
Received 14 April 2021
Revised 5 January 2022
Accepted 7 February 2022
Available online 9 February 2022

Keywords:
Computer and network security
Cybersecurity
Data-selling ransomware
Preventive portfolio
Encryption
Deception
Game theory
Economics

ABSTRACT

Ransomware has risen to be among the top cyber threats in recent years. There is an alarming trend of ransomware stealing data in addition to locking files. Compared to traditional ransomware, this new data-selling ransomware can be more harmful to the victims facing the data leakage threat. Traditional wisdom of defensive measures such as data backup is less effective in preventing the attacker from making money by selling data. We propose two preventive measures designed to defend against the data-selling ransomware, i.e., preventive data encryption and preventive data deception. Users may form a preventive portfolio made up of the two preventive measures. We contribute a novel game theoretical model of the data-selling ransomware to study the equilibrium strategies of the attacker and victims. The equilibrium solution of the portfolio and tradeoff analysis of both data encryption and deception are particularly useful for the users to optimize their system to defend against ransomware attacks. Simulation studies demonstrate the effectiveness of the preventive portfolio, which maximizes user utility while significantly reducing the profit of the attacker.

1. Introduction

Ransomware is a particular malware that locks a victim's computer systems and files through encryption via either software vulnerabilities or social engineering. These deny-of-access attacks typically infect high-value machines containing sensitive files such as login credentials, important financial data, business records, hospital patient records, government documents, etc. Victims are then asked a ransom payment in return for the key to decrypt their data and systems.

Since the malware gains full access to user data, it can potentially collect sensitive information from the target machines and use the information to blackmail the victims. We believe one of the most detrimental types of ransomware is the one that not only encrypts files, but also steals information in each of the targeted applications (Cyware, 2020). Ransomware attackers have threatened to publicly release the stolen data if the victims choose not to respond to their ransom demands (Cyware, 2020), e.g., the Maze ransomware (Whitwam, 2019), and the trend is likely to continue (Mathews, 2020).

Ransomware is believed to be highly lucrative (Simoiu et al., 2019). Traditionally, all ransomware profits come from ransom payment. A hypothetical, new ransomware model, i.e. Ransomeware 2.0 (Li and Liao, 2020), has been proposed by considering an additional revenue source to the attacker, i.e., data selling capability. We believe this new data-selling ransomware is not only imminent but also is much harder to defend compared with traditional ransomware. For example, victims with a full data backup may still be motivated to pay ransom to prevent attackers from selling their sensitive data.

To that end, we propose, study and evaluate two preventive measures targeting the data-selling ransomware, i.e., preventive data encryption and preventive data deception. Preventive data encryption may be achieved by encrypting either the partial or whole system drive enabled by technologies such as trusted platform module (TPM) or as simple as via password-protected data files. While traditional ransomare prevents victims from accessing their system and data through encryption, we note that preventive encryption prevents attackers from accessing victims' data.

Preventive data deception is another interesting measure that is supported by fake information or data. In this scheme, a percentage of data unknown to the attacker may be artificially generated and does not reflect the real data actually used by the users. Intuitively, the *uncertainty* of fake information deteriorates the quality

* Corresponding author.
E-mail address: liao1q@cmich.edu (Q. Liao).

https://doi.org/10.1016/j.cose.2022.102644
0167-4048/

of data stolen from users and waters down the market value of data.

To study the proposed preventive measures, we build a novel game-theoretical model of the data-selling ransomware at the presence of proposed preventive measures. In this model, attackers consider factors such as how much ransom to ask, whether to keep reputation to unlock user's data once ransom is paid, and whether to sell the data based on the ransom. Users, on the other hand, decide on the composition of preventive portfolio (i.e., percentages of data encryption and deception) to maximize their utilities based on their cost constraints. We derive the equilibrium strategies for both the attacker and the users/victims. Through extensive simulation studies, we analyze the complex relationships among the preventive measures, user utility, and ransomware profit. The results suggest the proposed preventive measures effectively defend against data-selling ransomware and significantly reduce the attackers' profit.

Our major contributions of the paper include

1. We proposed an interesting concept of preventative portfolio using a combination of both data encryption and data deception to defend against the data-selling ransomware, which we perceive as the emerging variant of ransomware attacks.
2. We developed a novel game theoretic model for the new data-selling ransomware to analyze the complex relationships between attackers and users/victims by considering multiple decision variables. We were able to derive the optimal strategies, and ultimately, equilibrium / optimal solutions for both attackers and victims.
3. We conducted an extensive simulation study to compare the complex relationships between various decision variables imbedded in equilibrium solutions, for example, how various rates of encrypted and fake data affect user utility and attacker profit. We derived other insights for the security practitioners and ransomware market.

It is worthwhile to note several derivatives from our study. First, the proposed preventive measures also have positive externality, i.e., they protect not only the victims who adopt them, but also others who may not use preventive measures or for whom low prevention is optimal. In addition, preventive measures may motivate the attacker to improve credibility. Second, other market-based defensive measures may be explored as well, e.g., the victims and defensive buyers (Li and Liao, 2018) may participate in the data market, to increase the transaction costs of the attacker, lower the transaction price, and/or track down the sellers.

The rest of the paper is organized as follows. Section 2 reviews related literature. Section 3 performs the game theoretical analysis of the data-selling ransomware at the presence of preventive portfolio composed of preventive encryption and preventive deception. Optimal strategies of the victims and the attacker are derived. Based on the theoretical analysis, Section 4 presents simulation results that illustrate how individual users choose the composition of their preventive portfolio, and how the presence of preventive portfolio affects the expected payoffs of the victims and the attacker. Section 5 concludes the paper.

2. Related works

Ransomware has recently become the top cyber threats and one of the most widespread cybercrimes (CyberEdge, 2020). Often, we hear the news report on ransomware attacks on businesses, government agencies, or even hospitals, forcing them to shut down their daily operations. Healthcare systems and financial systems are being attacked with ransomware through COVID-related content (Hakak et al., 2020). Recent attacks on vast number of organizations post enormous burden in terms of monetary and reputation loss involved in those attacks (Aldaraani and Begum, 2018; Simoiu et al., 2019).

To reduce the risk of ransomware, various cyber security strategies and practices are recommended (Silva et al., 2019), and research on ransomware and its detection and prevention techniques has been reviewed (Al-rimy et al., 2018). For example, zero-day ransomware attacks may be detected via monitoring file system activities for I/O requests and protecting Master File Table (Kharraz et al., 2015). Botnets may be traced for the distribution paths of ransomware or to exploit vulnerabilities to deliver malware.

General preventive measures, such as user education and network management, apply to most malware including ransomware. Users are recommended to take preventive measures to avoid ransomware (Mohurle and Patil, 2017). A common advice of ransomware literature is mitigation such as backup technologies (Laszka et al., 2017). Data backup is considered the most effective strategy to mitigate the loss of ransomware (Ali, 2017; Anghel and Racautanu, 2019; Subedi et al., 2017). Although sufficient data backup has the potential to defeat traditional ransomware, it has no effect on preventing the new data-selling ransomware (Li and Liao, 2020; 2021). Are there any effective preventive measures against this data-selling ransomware? This leads to our research in this paper.

The problem of ransomware needs to be addressed from the perspective of multiple disciplines (Wolf and Goff, 2018). In addition to technical approaches, there has been recent research that uses economics and game theory to study specific aspects of ransomware. For example, economic analysis of ransomware (Hernandez-Castro et al., 2020) reveals the impact of different price discrimination strategies for estimating an optimal ransom value. A theoretical model of ransomware based on standard economic pricing models was implemented to explore strategies criminals could use to extract illegal gains from ransomware (Hernandez-Castro et al., 2020). Game theory can model the strategic playing by ransomware criminals and victims (Caporusso et al., 2018). A repeated game setting was developed to explicitly model reputation of the criminals in ransomware attacks (Cartwright and Cartwright, 2019). For businesses, the relationship of investment in backup technologies and deterrent for ransomware attacks is analyzed in a game-theoretical model of the ransomware ecosystem (Laszka et al., 2017).

Since existing game theoretic works are almost entirely on traditional ransomware that demands ransom payment with no data leakage threat, we conduct the first game theoretical analysis of the data-selling ransomware by focusing on two preventive measures, i.e., preventive data encryption and preventive data deception. The equilibrium solutions derived from the game theory model provide the rules users may follow to construct their optimal preventive portfolio against the data-selling ransomware.

Defense against data-selling ransomware is related to defense against data theft and data protection. In such case data encryption has been used (and sometimes required by law) to protect customer databases kept by organizations against data theft. We note that the setting of data-selling ransomware is different from traditional data theft. While it may be possible for organizations to encrypt the entire databases on a server to protect against conventional data theft, in a ransomware attack, the victims are often end users whose system and user files on the local machines get locked (encrypted) and/or stolen by the malware. For practical purpose, it may not be possible for the end user systems to be 100% encrypted while users are using their machines. Therefore, preventive encryption in the paper (ranging from full disk encryption to partial on-demand encryption based on file/directory access) is to protect private data of end users against data-selling ransomware. While data encryption may be better than data deception for trac-

tional data theft, data deception (in addition to data encryption) is a valuable alternative in defense against data-selling ransomware.

The practice of data deception proposed in the paper is also related to but not entirely the same as a practice known as security-by-obscurity. Traditionally, security-by-obscurity/secrecy means that the technical details of a system are kept secret in a hope that such system will not be easily compromised if no one knows how it works. For example, a software company may not want to make their source code public, making it hard to identify potential vulnerabilities in their software. We, on the other hand, are not hiding the fact of using fake data. Actually, we argue the benefit of advertising to the public including attackers that data deception policy is enforced in a protected organization.

It is generally agreed in security community that security-by-obscurity "*alone*" may not be a good idea. However, good security is always layered. When used as an independent layer, obscurity is considered a valid security tool (Climek et al., 2016). In recent years, security through obscurity has gained support as a methodology in cybersecurity through Moving Target Defense and Cyber Deception from both military and civilian contexts such as AFRL cyber agility program, DoD, and DHS. NIST's cyber-resiliency framework includes deception as an integral part of a resilient and secure computing environment (Ross et al., 2021). The data deception component suggested in the paper is not intended to replace existing security mechanisms against cyber-attacks. Things such as firewalls, intrusion detection/prevention systems, spam filters, multi-factor authentications, encryptions, data backup/recovery procedures, user educations, etc. are still in place. The additional independent layer of preventive portfolio (i.e., a combination of data encryption and data deception) suggested in the paper is a complementary part of the entire secure ecosystem. In the case that ransomware attacks still succeed despite of these existing security mechanisms, the preventive strategies at least lower the market value of the data and reduce the economic incentives of data-selling ransomware attackers.

3. Game theoretic model of preventive portfolio against data-selling ransomware

In this section we lay out a game theoretic framework to model a preventive portfolio against the data-selling ransomware and derive the game outcomes. The portfolio is made up of two preventive measures: preventive data encryption and preventive data deception.

3.1. Preventive data encryption and preventive data deception

Compared to traditional ransomware, the data-selling ransomware imposes additional data leakage threat on the victims. We aim to design preventive mechanisms that target in particular the data-selling feature of the ransomware. We propose two preventive measures called preventive data encryption and preventive data deception.

Preventive data encryption can be used to protect data from being disclosed to unauthorized access. The term preventive refers to users encrypting their data before possible ransom attacks. If a ransomware attack does occur, while the attacker will still be able to encrypt the victims' systems to prevent the victims from using their computers or accessing their data, the attacker will not be able to steal or access the victims' data. In other words, if data is encrypted with one key, one may encrypt the already encrypted data again with another key, but double encryption will not reveal the original data.

The rationale for preventive data deception is that the profit of data-selling ransomware largely depends on the market value of data and/or the transaction cost of selling data. We propose to create fake information/data to water down the true information/data. When the stolen data is a mix of true and fake data, the market price of data must go down as the data quality deteriorates. The transaction cost may go up because of the increased uncertainty.

3.2. Game players' strategy space

There are two types of players in the data-selling ransomware game: attackers and users/victims. To prevent the possible loss of data leakage, the users construct a preventive portfolio made up of preventive data encryption and preventive data deception. Let $\delta_e \in [0, 1]$ be the percentage of data that is pre-encrypted and $\delta_f \in [0, 1]$ be the percentage of fake data. An existing preventive portfolio at the moment of attack is the actual level of protection the portfolio provides to the users.

Once a data-selling ransomware attack succeeds, the users become the victims, who face dual threats: losing access to data and data leakage. The attacker demands an equalized ransom payment $R > 0$ on all the victims, and the victims decide whether to pay the ransom or not. Let p be the victims' choice of ransom payment that is binary, i.e., $p = 1$ if choosing to pay, and $p = 0$ otherwise. Upon observing the victims' action on ransom payment, the attacker chooses whether to return files and/or to sell data. It is reasonable to assume that the attacker would not return files and would sell data with no ransom payment. However, when a victim chooses to pay the ransom, there is no guarantee that the attacker would always return the files and/or not to sell the data. We use β_r for the attacker's probability of returning files with ransom payment, and β_s for the attacker's probability of selling data with ransom payment.

Therefore, the users/victims' strategy space is the choice of (δ_e, δ_f, p), and the attacker's strategy space is the choice of (R, β_r, β_s). The combination of δ_e and δ_f is defined as the structure of the preventive portfolio composed of preventive data encryption and preventive data deception. The after-attack scenario fits a Stackelberg game with asymmetric information: the attacker moves first by demanding a uniform ransom based on incomplete information of the victims' willingness to pay and preventive portfolio; the victims follow by choosing ransom payment strategy based on incomplete information about the attacker's reputation. The equilibrium solution of the game is the strategy profile that serves best each player, given the expected strategies of the other player.

Table 1 lists the major symbols and definitions used in the model. We use the phrase "returning files" or "unlock data" interchangeably to refer to the situation in which the attacker delivers decryption keys to remove restrictions to a victims' computing resources and files. We use the phrase "selling data" to refer to the situation in which the attacker sells the stolen data to a third party or in a market place. We also use the terms "pre-encrypted files" and "preventive data encryption" interchangeably, and "fake data/information" and "preventive data deception" interchangeably. We assume all the game players are rational, i.e., they choose strategies to reach a game outcome that maximizes their expected payoffs. In the following sections, we will derive the equilibrium solution of the game by analyzing the optimization problems of the game players.

3.3. Victims' expected payoff

The victims' expected payoff (or user utility) at the presence of preventive portfolio is

$$u = -pR - (1 - p\beta_r)V - (1 - p(1 - \beta_s))(1 - \delta_e)h(\delta_f)D \\ -C(\delta_e) - C(\delta_f) \quad (1)$$

Table 1
Symbols/variables and definitions.

Symbol/variable	Definition
R	ransom request
M	market value of data
V	victims' self-valuation of cost from losing access to data
D	data leakage damage to victims
A	attacker's profit of selling data (data profit)
β_r	probability of returning/unlocking files with ransom payment
β_s	probability of selling data with ransom payment
C_r	cost of returning/unlocking files to victims
C_s	transaction cost of selling data
δ_e	percentage of encrypted files
δ_f	percentage of fake data
$C(\delta_e)$	cost of preventive encryption
$C(\delta_f)$	cost of preventive deception
$h(\delta_f)$	fraction of data value remained at the presence of fake data
p	binary variable measuring victims' ransom payment choice
N	number of users/victims
n	number of victims choosing to pay ransom
u	(individual) user utility
π	ransomware profit from an individual victim
Π	ransomware profit from all victims

Table 2
Victims' expected payoff.

Case	Victims' choice	Victims' expected payoff
I	$p=0,\ \delta_e=\delta_f=0$	$-V-D$
II	$p=1,\ \delta_e=\delta_f=0$	$-R-(1-\beta_r)V-\beta_s D$
III	$p=0,\ \delta_f=0,\ 0<\delta_e\le 1$	$-V-(1-\delta_e)D-C(\delta_e)$
IV	$p=1,\ \delta_f=0, 0<\delta_e\le 1$	$-R-(1-\beta_r)V-\beta_s(1-\delta_e)D-C(\delta_e)$
V	$p=0,\ \delta_e=0,\ 0<\delta_f\le 1$	$-V-h(\delta_f)D-C(\delta_f)$
VI	$p=1,\ \delta_e=0,\ 0<\delta_f\le 1$	$-R-(1-\beta_r)V-\beta_s h(\delta_f)D-C(\delta_f)$
VII	$p=0,\ 0<\delta_e\le 1,\ 0<\delta_f\le 1$	$-V-(1-\delta_e)h(\delta_f)D-C(\delta_e)-C(\delta_f)$
VIII	$p=1,\ 0<\delta_e\le 1,\ 0<\delta_f\le 1$	$-R-(1-\beta_r)V-\beta_s(1-\delta_e)h(\delta_f)D-C(\delta_e)-C(\delta_f)$

where V is the victims' self-valuation of the locked files that measures the victims' loss of losing access to the files, including but not limited to the recovery costs to restore the operations back to normal and longer-term impacts of permanent loss of data; D is the victims' data leakage loss; $C(\delta_e)$ is the cost of preventive encryption; and $C(\delta_f)$ is the cost of preventive data deception.

It is reasonable to assume there are costs associated with preventive measures. For example, preventive encryption may require extra CPU cycles and reduce quality of experience (QoE). Preventive deception may require extra storage for storing fake data. Moving targets may cause user confusion and extra maintenance overhead. If there are no preventive measures taken, there is obviously no prevention cost, i.e., $C(\delta_e)=0$ at $\delta_e=0$ and $C(\delta_f)=0$ at $\delta_f=0$. Prevention costs increase as the level of prevention increases, i.e., $C'(\delta_e)>0$ and $C'(\delta_f)>0$.

All terms in Eq. (1) have negative signs, meaning the victims are absolutely harmed by the data-selling ransomware attack. Preventive portfolios help reduce the data leakage loss of the victims but do not affect the loss of the victims when they are denied access to the data locked in the attack. The decrease in the victims' data leakage loss is proportional to the level of preventive encryption while the protection of preventive deception is not necessarily linear. In Eq. (1), $h(\delta_f)\in[0,1]$ measures the potential impact of fake data on camouflaging real data. At $\delta_f=0$, $h(\delta_f)=1$. As the percentage of fake data increases, $h(\delta_f)$ decreases and $h(\delta_f)D$ decreases, i.e., $h'(\delta_f)<0$.

The victims' expected payoffs in various cases of the victims' strategy choice are listed in Table 2.

3.4. Victims' optimal strategy

The users need to determine the composition of the preventive portfolio before the attack and whether to comply with the ransom request after the attack. They choose their optimal strategy $(\delta_e^*, \delta_f^*, p^*)$ to maximize their expected payoff. The optimal choice of preventive portfolio δ_e^* and δ_f^* depends on the comparison of expected benefit and preventive cost that solve the following two first-order conditions of Eq. (1):

$$(1-p(1-\beta_s))h(\delta_f^*)D=C'(\delta_e^*) \tag{2}$$

and

$$-(1-p(1-\beta_s))(1-\delta_e^*)h'(\delta_f^*)D=C'(\delta_f^*) \tag{3}$$

In Eqs. (2) and (3), the left-hand-side is the marginal benefit of the preventive measures in terms of the marginal decrease in data leakage loss, and the right-hand-side is the marginal cost of taking the preventive measures. The optimal level of prevention corresponds to the point where the marginal benefit and the marginal cost are equal.

These two equations are what the users shall follow to construct the preventive portfolio before the attack. At the time of forming the portfolio, the users evaluate their data (how much the data is worth to them) and cost structure of preventive measures. What is unknown to the users is the attacker's credibility and the ransom request that would affect the users' ransom payment choice. The users would have to set up the preventive portfolio based on the expected values of the attacker's control variables.

When an attack actually occurs, the existing level of prevention is what the victims take as given to choose their optimal compliance strategy. The actual ransom demand will become known. The victims incorporate the new information into their decision-making to choose whether to pay ransom. Cases VII and VIII in Table 2 are the victims' expected payoff when they either refuse to pay the ransom or choose to pay at the presence of preventive portfolio. The victims choose to pay the ransom ($p = 1$) if the expected payoff in Case VIII is no less than the expected payoff in Case VII. Therefore, the victims' optimal choice of ransom payment given the pre-determined optimal preventive portfolio (δ_e^*, δ_f^*) is

$$p^* = \begin{cases} 1, & \text{if } \beta_r V + (1-\beta_s)(1-\delta_e^*)h(\delta_f^*)D \geq R, \\ 0, & \text{if } \beta_r V + (1-\beta_s)(1-\delta_e^*))h(\delta_f^*)D < R. \end{cases} \tag{4}$$

where $\beta_r V + (1-\beta_s)(1-\delta_e^*)h(\delta_f^*)D$ defines the victims' williness to pay, i.e., the highest ransom the victims may accept in exchange for unlocking data and not leaking data. The victims would only choose to pay the ransom if the ransom request is no higher than their willingness to pay. Eqs. (2)–(4) combined specify the victims' optimal strategy.

The key factors determining the victims' willingness to pay include the victims' valuation of the locked files (V), the data leakage loss to the victims (D), the level of prevention (δ_e and δ_f), and the attacker's reputation (β_r and β_s). Of the factors, V and D are given. The preventive portfolio is also given at the time of attack. The attacker's reputation matters since the victims' willingness to pay increases when the attacker is more likely to keep the promise with ransom payment.

3.5. Ransomware profit

The data-selling ransomware attacker receives the following profit from victim i,

$$\pi_i = p_i R - p_i \beta_r C_r + (1 - p_i(1-\beta_s))A_i \tag{5}$$

where C_r is the cost of returning files, and A_i is the data profit received from victim i. The attacker sells the victim's data if doing so is profitable, i.e.,

$$A_i = \begin{cases} (1-\delta_{e,i})h(\delta_{f,i})M_i - C_s, & \text{if}(1-\delta_{e,i})h(\delta_{f,i})M_i \geq C_s, \\ 0, & \text{if}(1-\delta_{e,i})h(\delta_{f,i})M_i < C_s. \end{cases} \tag{6}$$

where C_s is the cost of selling data, and M_i is the market value of the victims' data in absence of preventive measures.

From Eq. (5), the attacker receives a profit of A_i if victim i chooses not to pay the ransom ($p_i = 0$). The attacker's profit is $R - \beta_r C_r + \beta_s A_i$ if victim i chooses to pay ($p_i = 1$).

Combining all N victims, the total profit of the attacker is

$$\Pi = n(R - \beta_r C_r) + \beta_s \sum_{i=1}^{n} A_i + \sum_{i=n+1}^{N} A_i \tag{7}$$

where $n = \{i \in N | \beta_r V_i + (1-\beta_s)(1-\delta_{e,i})h(\delta_{f,i})D_i \geq R\}$.

The attacker receives both ransom profit and data profit from the n victims who pay the ransom. Of which, the per-victim ransom profit is $R - \beta_r C_r$, and the per-victim data profit is $\beta_s A_i$. For the $N - n$ victims who do not pay, the attacker receives zero ransom profit but A_i individual data profit.

3.6. Attacker's optimal strategy

The goal of the attacker is to choose ransom R and the probabilities of returning and selling users' data β_r and β_s to maximize profit. Had the attacker had perfect information on each victim's willingness to pay, the attacker would differentiate the ransom request to demand an individualized ransom $\beta_r V_i + (1-\beta_s)(1-\delta_{e,i})h(\delta_{f,i})D_i$ on victim i, which is the maximum ransom victim i can accept. Then the attacker would set $\beta_r = 1$ if $\beta_r V_i \geq C_r$, and $\beta_s = 0$ if $(1-\beta_s)(1-\delta_{e,i})h(\delta_{f,i})D_i \geq (1-\delta_{e,i})h(\delta_{f,i})M_i - C_s$. Lacking perfect information, the attacker may group the victims by estimating their willingness to pay and demand a tailored ransom to each individual group. When hacking companies, the attacker may request individual ransoms depending on company size and revenue. Nevertheless, the attacker would not perfectly price differentiate the victims, especially when the attacker faces a large number of unknown victims. In this case, knowing the distribution of users' willingness-to-pay within the population is the key. When the willingness to pay is uniformly distributed, the profit-maximizing ransom would be the mean of all the victims' willingness to pay (Li and Liao, 2020). That is

$$R^* = \frac{1}{N}\sum_{i=1}^{N}\{\beta_r V_i + (1-\beta_s)(1-\delta_{e,i})h(\delta_{f,i})D_i\} \tag{8}$$

β_r and β_s gauge the reputation of the attacker. The attacker's promise is more credible as β_r increases and/or β_s decreases. The attacker's likelihood of default depends on the tradeoff between ransom revenue and gains from default. Choosing a high probability of returning files and a low probability of selling data with ransom payment increases the victims' willingness to pay, hence generating more ransom revenue, but at the cost of foregone data-selling income.

The attacker is not granted reputation but has to gain reputation by building records. The victims estimate the credibility of the attacker by collecting information on the past records of the attacker. Unfortunately, the currently available information is largely on a population mean rather than on a particular attacker, and the population mean changes from survey to survey. For example, it is reported in 2019 about 60% victims who pay the ransom recovered their files (CyberEdge, 2020). In a 2021 global survey, 32% of those organizations whose data was encrypted decide to pay the ransom but only 8% of them got all their data back (Sophos, 2021). The percentage changes over time and across ransomware and attackers. In this game the attacker sets $\beta_r = 0$ and $\beta_s = 1$ for the $(N - n)$ victims who do not pay. The attacker returns files to n_r of the n victims who pay the ransom ($\beta_r = \frac{n_r}{n}$), and sells the data of n_s of the n victims who pay the ransom ($\beta_s = \frac{n_s}{n}$).

Indeed, there are two β_r's and two β_s's, ex ante and ex post, depending on the timing. The β_r and β_s determining the victims' optimal preventive portfolio and willingness to pay are ex ante or expected, based on the historic record of the attacker, likely to be a mixed result of the attacker's optimal choice, random acts, technical errors, and incomplete records. The β_r and β_s in equations $\beta_r = \frac{n_r}{n}$ and $\beta_s = \frac{n_s}{n}$ are ex post or realized. For simplicity, we assume the ex ante and ex post β_r and β_s have no significant difference. This would be true if the distribution of V and D were not significantly different between previous victims and current victims of ransomware.

Applying marginal analysis, the attacker shall compare the additional benefit (i.e., marginal benefit) of a small change in β_r or β_s to the additional cost (i.e., marginal cost) of the change. The change would be profit improving if the marginal benefit of the change exceeds the marginal cost.

Holding β_s constant, we study the marginal effect of β_r on ransomware profit. When the attacker increases the probability of returning files, i.e., when β_r increases, n increases as more victims choose to pay the ransom hence the ransom profit increases for the attacker. In the meantime, data profit decreases from the victims who change their ransom payment choice in response to changing β_r. Let β_r change by $\Delta\beta_r$. The corresponding change in data profit is $-(1-\beta_s)\sum_{i=1}^{\Delta n} A_i$. The corresponding change in

ransom profit is $(n+\Delta n)(R-(\beta_r+\Delta\beta_r)C_r)-n(R-\beta_r C_r)$, which simplifies to $\Delta n(R-(\beta_r+\Delta\beta_r)C_r)-n\Delta\beta_r C_r$.

The net change in ransomware profit is hence

$$\Delta\Pi=\Delta n(R-(\beta_r+\Delta\beta_r)C_r)-n\Delta\beta_r C_r-(1-\beta_s)\sum_{i=1}^{\Delta n}A_i \tag{9}$$

In Eq. (9), the first term $\Delta n(R-(\beta_r+\Delta\beta_r)C_r)$ is the increase in ransomware profit generated by the Δn victims who switch from no pay to pay. The second term $n\Delta\beta_r C_r$ is the decrease in ransom profit as the cost of returning files increases for the original n victims who pay the ransom, and the last term $(1-\beta_s)\sum_{i=1}^{\Delta n}A_i$ is the decrease in data profit.

For marginal analysis, the first term in Eq. (9) is the marginal benefit of the incremental change in β_r, and the sum of the last two terms is the marginal cost of the change. The attacker shall increase β_r when the marginal benefit is bigger and decrease β_r when the marginal cost is bigger. The profit-maximizing β_r^* satisfies

$$\lim_{\Delta\beta_r\to 0}\Delta n(R-(\beta_r^*+\Delta\beta_r)C_r)=\lim_{\Delta\beta_r\to 0}n\Delta\beta_r C_r+(1-\beta_s)\sum_{i=1}^{\Delta n}A_i$$

Or,

$$\beta_r^*=\lim_{\Delta\beta_r\to 0}\frac{1}{C_r}\{R-\frac{\Delta\beta_r C_r(n+\Delta n)+(1-\beta_s)\sum_{i=1}^{\Delta n}A_i}{\Delta n}\} \tag{10}$$

Similarly, we can derive the profit-maximizing β_s by comparing the marginal benefit and the marginal cost of changing β_s by holding β_r constant. When the attacker's probability of selling data decreases from β_s to $\beta_s-\Delta\beta_s$, the number of victims choosing to pay the ransom increases. The corresponding change in ransom profit is $\Delta n(R-\beta_r C_r)$, and the corresponding change in data profit is $-\Delta\beta_s\sum_{i=1}^{n}A_i-(1-\beta_s+\Delta\beta_s)\sum_{i=1}^{\Delta n}A_i$. The former is the marginal benefit of the decrease in β_s and the latter is the marginal cost. The attacker shall decrease β_s if the marginal benefit is bigger and increase β_s otherwise. The profit-maximizing β_s^* satisfies

$$\lim_{\Delta\beta_s\to 0}\Delta n(R-\beta_r C_r)=\lim_{\Delta\beta_s\to 0}\Delta\beta_s\sum_{i=1}^{n}A_i+(1-\beta_s^*+\Delta\beta_s)\sum_{i=1}^{\Delta n}A_i$$

Or,

$$\beta_s^*=1-\lim_{\Delta\beta_s\to 0}\{\frac{\Delta n(R-\beta_r C_r)-\Delta\beta_s\sum_{i=1}^{n}A_i}{\sum_{i=1}^{\Delta n}A_i}-\Delta\beta_s\} \tag{11}$$

Combining Eqs. (8), (10), and (11), $\{R^*,\beta_r^*,\beta_s^*\}$ is the attacker's optimal strategy to maximize ransomware profit that balances ransom profit and data profit, dependent on the victims' valuation of locked files and stolen data that affect n.

The equilibrium solution provides the guidelines the attacker may follow to increase profit. For example, the attacker shall decrease the probability of returning files if the cost of returning files increases, while increasing the probability of returning files if demanding a high ransom. The attacker shall increase the probability of selling data if more victims are of high value. It would be difficult for the attacker to fulfill the optimal strategy due to incomplete information. The best practice could be to choose β_r and β_s consistent with the victims' perception. Since the victims' perception is consistent with past records of ransomware attacks, the practice can be self-reinforcing, leading to a steady state of the two probabilities that helps control uncertainty.

3.7. Effects of preventive measures

3.7.1. Preventive measures reduce victims' willingness to pay

Cases I and II in Table 2 are the victims' expected payoffs in absence of preventive measures. Cases III and IV are the victims' expected payoffs when preventive data encryption is the only preventive measure used while Cases V and VI are the victims' expected payoffs when preventive data deception is the only preventive measure used. In any case of preventive portfolio, the victims would choose to pay the ransom if doing so generates a larger expected payoff than declining the ransom demand. We derive the victims' willingness to pay in all cases as in Table 3.

Table 3
Victims' willingness to pay.

Preventive portfolio	Victims' willingness to pay
$\delta_e=\delta_f=0$	$\beta_r V+(1-\beta_s)D$
$\delta_f=0,\ 0<\delta_e\le 1$	$\beta_r V+(1-\beta_s)(1-\delta_e)D$
$\delta_e=0,\ 0<\delta_f\le 1$	$\beta_r V+(1-\beta_s)h(\delta_f)D$
$0<\delta_e\le 1,\ 0<\delta_f\le 1$	$\beta_r V+(1-\beta_s)(1-\delta_e)h(\delta_f)D$

As shown, the existence of preventive measures decreases the victims' willingness to pay. While preventive portfolio would not help reduce the victims' loss from losing access to the locked data, preventive portfolio would help reduce the loss of data leakage. In the case of sufficiently large preventive encryption ($\delta_e=1$) and/or preventive deception ($h(\delta_f)=0$), the data-selling ransomware profit would be equal to the profit of traditional ransomware when data profit is zero and victims' willingness to pay ransom is completely determined by their valuation of locked files ($\beta_r V$).

3.7.2. Preventive measures induce higher credibility of attacker

The attacker's optimal strategy of returning files and selling data are in response to the victims' preventive portfolio choice. As in Eqs. (10) and (11), the values of β_r^* and β_s^* depend on the value of A^* that changes with the victims' preventive portfolio structure, δ_e^* and δ_f^*.

Since $\delta_e^*\in(0,1)$, the attacker's probability of returning files (β_r^*) increases in the presence of preventive encryption. Such change induces more victims choosing to pay the ransom, increasing ransom profit to compensate for the lost data profit.

The attacker's probability of selling data (β_s^*) decreases as well in the presence of preventive measures. The deteriorated quality of data decreases the marketability of the stolen data, thus giving ransom profit more weight over data profit.

3.7.3. Preventive measures decrease ransomware profit

As in Eq. (7), there are two components of profit of the data-selling ransomware: ransom profit and data profit. Both preventive encryption and preventive deception decrease data profit of the attacker. They can also decrease ransom profit of the attacker by decreasing the victims' willingness to pay, thus reducing the ransom demand and the number of victims choosing to pay the ransom.

In absence of preventive measures, the data-selling ransomware profit has the same format as in Eq. (7) with a different number of victims choosing to pay the ransom as $n=\{i\in N|\beta_r V_i+(1-\beta_s)D_i\ge R\}$ and different individual data profit as

$$A_i=\begin{cases}M_i-C_s, & \text{if} M_i\ge C_s,\\ 0, & \text{if} M_i<C_s.\end{cases} \tag{12}$$

In absence of preventive measures, the attacker would receive both higher ransom profit and data profit, and hence total higher ransomware profit. Comparing ransomware profit in Eq. (7) at various levels of preventive encryption and preventive deception, we can see that the number of victims paying the ransom (n) decreases as δ_e increases, thus reducing ransom profit. Data profit decreases as well as the attacker cannot sell the data stored in the pre-encrypted files. Since both components of ransomware profit decrease, the data-selling ransomware becomes less profitable. The higher δ_e is, the bigger is the decrease in ransomware profit.

4. Simulation results

The game theoretic analysis suggests how both users and attackers choose their optimal strategies, especially how the users shall form their optimal preventive portfolio including preventive data encryption and preventive data deception to defend against the data-selling ransomware attack. In this section, we conduct simulations to systematically study how users choose optimal preventive portfolio and how the presence of preventive portfolio affects the expected payoffs of both users/victims and attackers.

4.1. Simulation parameters

The number of users/victims is set at $N = 30$. The victims' self-valuation of files and the market value of data are both randomly generated in the range of $0 \sim 50$. Without loss of generality, the following parameters are set: $C_r = C_s = 0$, $D = M$. The simplifications will not affect the insights we shall derive from the simulations.

The relationship between the fake data rate and the decrease in the market value of data is set as $h(\delta_f) = 1 - (\delta_f)^{\frac{1}{2}}$. At $\delta_f = 0$, $h(\delta_f) = 1$. At $\delta_f = 1$, $h(\delta_f) = 0$.

The preventive encryption cost function has the increasing marginal cost, $C(\delta_e) = \delta_e^2$. The cost function of preventive deception also has the increasing marginal cost, $C(\delta_f) = \delta_f^2$.

Eqs. (2) and (3) are used to solve for the users' optimal choice of preventive portfolio $(\delta_{e,i}^*, \delta_{f,i}^*)$, where i in the following two equations denotes those victim-specific variables,

$$\delta_{e,i}^* = \frac{(1 - p_i(1 - \beta_s))(1 - (\delta_{f,i}^*)^{\frac{1}{2}})D_i}{2} \tag{13}$$

and

$$1 - \frac{(1 - p_i(1 - \beta_s))(1 - (\delta_{f,i}^*)^{\frac{1}{2}})D_i}{2} = \frac{4(\delta_{f,i}^*)^{\frac{3}{2}}}{(1 - p_i(1 - \beta_s))D_i} \tag{14}$$

Besides p that depends on the comparison of ransom demand and the victims' willingness to pay, the optimal preventive portfolio depends on three key factors: the potential data loss to the victims, the cost of preventive measures, and the attacker's probability of selling data with ransom payment. Throughout the simulations we hold the attacker's probability of returning files with ransom payment constant at $\beta_r = 0.6$ because the variable does not affect the choice of preventive measures.

The optimal ransom is as defined in Eq. (8). The following equation is used to calculate the ransom used in each simulation,

$$R^* = \beta_r \overline{V} + (1 - \beta_s)\left(1 - \overline{\delta_e}\right)\left(1 - \overline{(\delta_f)}^{\frac{1}{2}}\right)\overline{D} \tag{15}$$

where the variables with an upper-bar are the estimated means of individual values of the victims.

4.2. Users' optimal preventive portfolio

Users follow Eqs. (13) and (14) to choose their optimal preventive portfolio to maximize utility. The maximized utility is as in Eq. (1) where both the encryption rate and the fake data rate take their optimal values. Since the first two terms in the equation do not depend on the preventive portfolio, only the part of user utility that depends on the choice of preventive portfolio is calculated,

$$u_{e,f,i}^* = -\beta_s(1 - \delta_{e,i}^*)(1 - (\delta_{f,i}^*)^{\frac{1}{2}})D_i - (\delta_{e,i}^*)^2 - (\delta_{f,i}^*)^2 \tag{16}$$

where $u_{e,f,i}^*$ represents the part of user i's utility that depends on the user's choice of preventive portfolio.

For illustration purpose we pick a representative victim whose optimal portfolio is $\delta_{e,i}^* = 15.4\%$ and $\delta_{f,i}^* = 26.1\%$ at $\beta_s = 0.1$, and $u_{e,f,i}^* = -0.3521$ from Eq. (16).

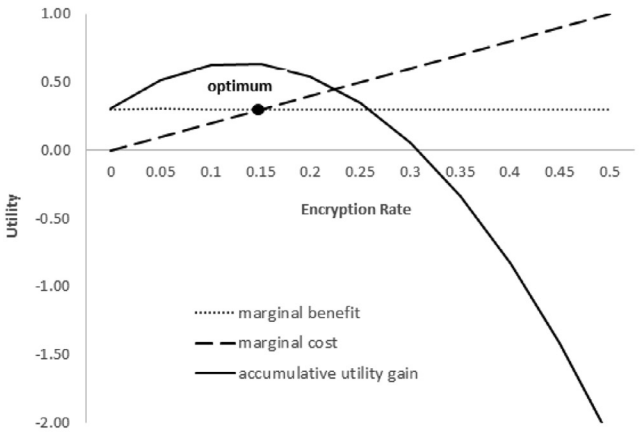
Fig. 1. Heatmap of user utility with combinations of encryption rate (δ_e) and fake data rate (δ_f). The optimal portfolio commination with highest utility is highlighted at −0.356.

The heatmap in Fig. 1 shows the value of $u_{e,f,i}$ at various combinations of $\delta_{e,i}$ and $\delta_{f,i}$ where both $\delta_{e,i}$ and $\delta_{f,i}$ take 10 discrete values between 0 and 1. As shown, the worst case occurs at full preventive portfolio. The maximized user utility occurs at $\delta_{e,i}^* \approx 0.1$ and $\delta_{f,i}^* \approx 0.3$, consistent with the mathematical model using Eqs. (13) and (14). The visualization is also useful in such cases that suboptimal solutions may be desirable by moving away from the optimal solution when users' constraints evolve in dynamic environment.

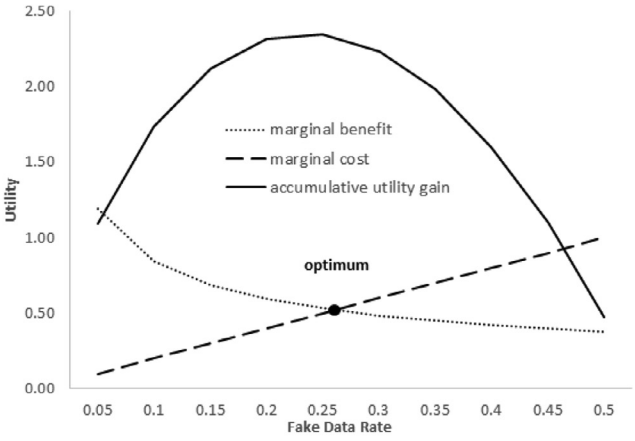
Fig. 2 further illustrates how users choose their optimal preventive portfolio with marginal analysis specified by Eqs. (2) and (3). The curve of accumulative utility gain measures the accumulative change in utility as the user continues to increase the rate of encryption or the fake data, holding the other rate constant at the optimal level. The intersection of the marginal cost and the marginal benefit curves is the optimum point where the accumulative gain in utility reaches the maximum. In this case, the utility-maximizing rates of encryption and fake data are approximately 15% and 26%, respectively.

Fig. 3 shows individual users' optimal preventive portfolio at various probabilities of selling data (β_s). Three representative users are chosen with low, medium, and high market value of data. Simulation results generally match Eq. (13) since both preventive encryption and preventive deception reduce data leakage loss. It appears that when the chance of data leakage is low and/or the data has limited market value, users prioritize the utilization of data deception. Increasing fake content may lower the needs of data encryption. Users have the option to substitute one preventive measure for the other. When the attacker has a high probability of selling data and/or the market value of data is high, users may increase the rates of both preventive measures.

Market value of data is the most important factor affecting the users' choice of optimal preventive portfolio. Fig. 4 shows individual users' optimal rates of encryption and fake data at various β_s. The simulation results suggest that overall the optimal prevention rates are increasing in the market value of data, and users tend to increase both preventive measures when the attacker has a high probability of selling data. Nevertheless, the positive relationship is less clear at low β_s. At $\beta_s = 0.1$, both encryption and fake data rates increase initially as the market value of data increases. Users adopt more deception than encryption because the



(a) Optimal encryption rate with maximum utility gain



(b) Optimal fake data rate with maximum utility gain

Fig. 2. Marginal analysis of choosing optimal preventive portfolio composed of encryption and fake data. The intersections of marginal cost and marginal benefit curves determine the optimal rates of encryption or fake data, where the accumulative gains in utility reach the maximum.

functional form of $h(\delta_f)$ used in the simulation determines deception provides more protection effects than encryption at low level of fake content. When fake data rate reaches a threshold, users adjust optimal preventive portfolio to use encryption to substitute for fake data. As β_s increases, users have to increase both the encryption rate and fake data rate to prevent data loss. The findings are consistent with Fig. 3.

4.3. Effect of preventive portfolio on user utility

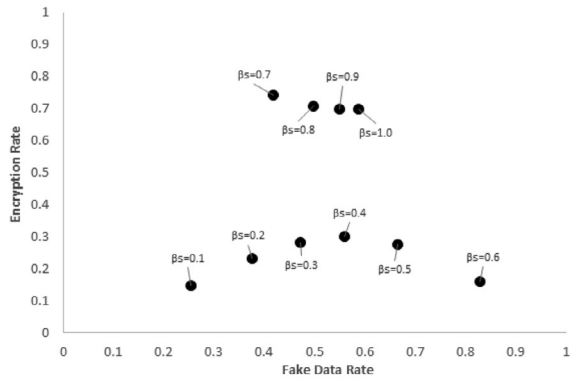
In this simulation, we study the effect of prevention portfolio on the expected payoff of the users/victims. In particular, we compare the users' expected payoff when they use the optimal preventive portfolio and the expected payoff when no preventive measure is used. The expected payoffs in various cases are listed in Table 2.

We compare user utility with and without preventive portfolio at various β_s. Individual users' composition of optimal preventive portfolio is as shown in Fig. 3. With preventive portfolio, the expected payoff for the victims choosing $p = 1$ is

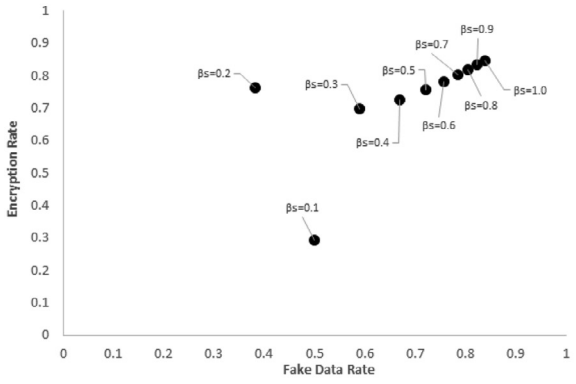
$$u^* = -R - 0.4V - \beta_s(1-\delta_e^*)(1-(\delta_f^*)^{\frac{1}{2}})D - (\delta_e^*)^2 - (\delta_f^*)^2$$

and the expected payoff for the victims choosing $p = 0$ is

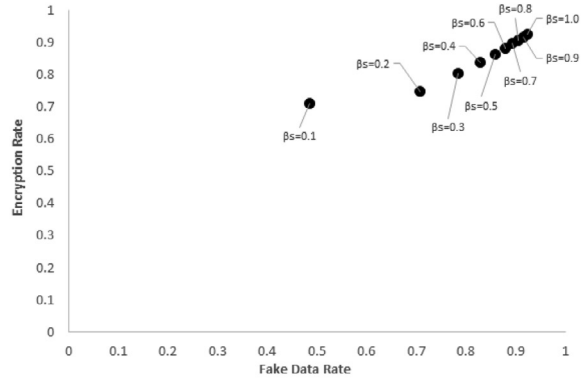
$$u^* = -V - (1-\delta_e^*)(1-(\delta_f^*)^{\frac{1}{2}})D - (\delta_e^*)^2 - (\delta_f^*)^2$$



(a) User 1 (D=6)



(b) User 2 (D=20)



(c) User 3 (D=47)

Fig. 3. Optimal preventive portfolio of encryption and fake data of representative users (with low, medium and high market value of data). The users may use one preventive measure to substitute for the other at low β_s and/or low market value of data, and may increase the rate of both preventive measures at high β_s and/or high market value of data.

In absence of preventive measures, the expected payoff for the victims choosing $p = 1$ is

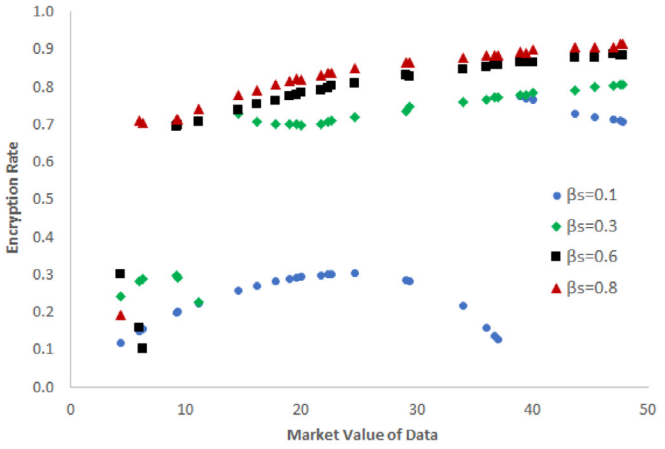
$$u = -R - 0.4V - \beta_s D$$

and the expected payoff for the victims choosing $p = 0$ is

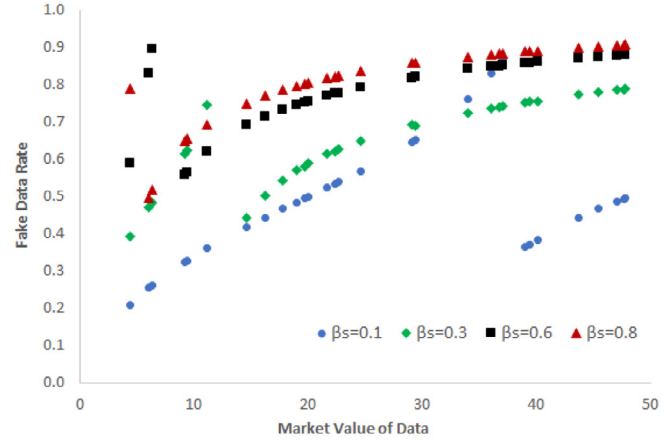
$$u = -V - D$$

The ransom demand in each case is equal to the mean of all victims' willingness to pay.

Fig. 5 illustrates individual users' utility gain that is equal to the difference between optimal user utility with and without preven-



(a) market value vs. encryption rate



(b) market value vs. fake data

Fig. 4. Relationship between the market value of data and individual users' optimal choice of rates of encryption and fake data at various β_s. Overall, fake data rate and encryption rate are increasing in market value of data. At lower β_s, users have a choice to lowering one preventive measure by increasing the other.

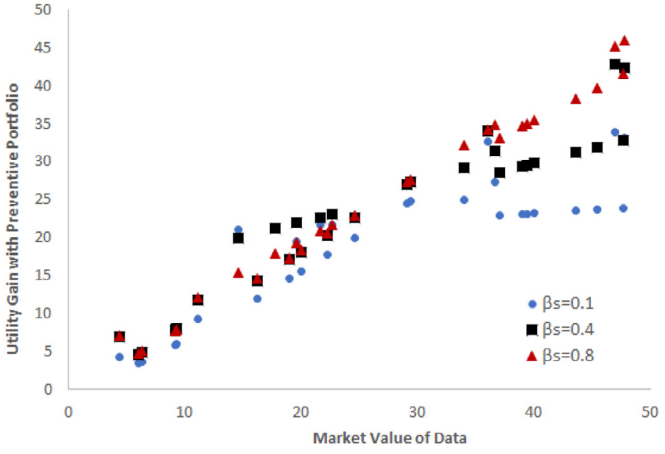


Fig. 5. Relationship between market value of data and users' utility gain (i.e., utility with preventive portfolio minus utility without preventive portfolio). In all cases, users are better off with preventive portfolio. Overall, utility gain is increasing in the market value of data at high β_s.

tive portfolio at $\beta_s = 0.1$, $\beta_s = 0.4$, and $\beta_s = 0.8$, respectively, in relation to the market value of data. The preventive portfolio benefits all users, and the gain in expected utility is overall increasing in the market value of data, especially at high β_s. That is, preventive measures benefit more the users with valuable data. Nevertheless, utility gain levels off at certain market value of data at low β_s. The marginal gain in utility tends to increase in β_s as the curve becomes steeper with rising β_s.

Although the optimal composition of preventive portfolio changes with β_s, at any β_s, the victims receive a higher expected payoff (or lower expected loss) when protected by the preventive portfolio. The presence of preventive measures benefit the users/victims. This is true for every individual user, even those who choose low (or even zero) level of prevention. Those are the users for whom the costs of preventive measures exceed the benefits. They are better off as well when other users use preventive portfolio. The presence of preventive measures generates positive externality that provides social prevention insurance protecting all the users. The effectiveness of preventive measures and mutual insurance requires effective communication. It can become a general practice for users to publicly announce the adoption of preventive measures, thus to form a common knowledge that user files may be encrypted and data may be fake. The uncertainty would discourage ransomware attackers and data buyers.

4.4. Effect of preventive measures on ransomware profit

The ransomware profit at the presence of preventive portfolio can be written as

$$\Pi_1 = R_1 * n_1 + \beta_s \sum_{i=1}^{n_1} (1-\delta_e)(1-\delta_f^{\frac{1}{2}})D_i + \sum_{i=n_1+1}^{N} (1-\delta_e)(1-\delta_f^{\frac{1}{2}})D_i$$

where the first term is the ransom profit, the last two terms measure the data profit, R_1 is the optimal ransom request, and n_1 is the number of victims choosing to pay the ransom at the presence of preventive portfolio.

With no preventive measures the ransomware profit is

$$\Pi_2 = R_2 * n_2 + \beta_s \sum_{i=1}^{n_2} D_i + \sum_{i=n_2+1}^{N} D_i$$

where R_2 is the optimal ransom request and n_2 is the number of victims choosing to pay the ransom in absence of preventive portfolio.

We choose a representative victim and compare how ransom profit, data profit, and total ransomware profit the attacker may receive from the victim change with the victim's use of preventive portfolio. The comparison in Fig. 6 suggests that as the encryption and fake data increase, both data profit and ransom profit of the attacker drop. At the presence of preventive portfolio, the overall ransomware profit decreases significantly.

Fig. 7 analyzes the relationship between ransomware profit and the data-selling rate with and without preventive portfolio. Without preventive portfolio, total ransomware profit increases as the data-selling rate β_s increases. With preventive portfolio, however, overall ransomware profit is reduced by more than two-thirds (Fig. 7a), and the reduction is even more significant as the data-selling rate β_s increases. The profit reduction of ransom component decreases as the data-selling rate increases due to victims' decreasing willingness to pay (Fig. 7b). Ransom request is much lower than the no-prevention case as the attacker can no longer use data as much as valid threat. Notably, the profit reduction in the data component is the most significant, over 90% reduction as

δ_s/δ_r	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1
1	13.71	13.71	13.71	13.71	13.71	13.71	13.71	13.71	13.71	13.71	13.71
0.9	17.11	16.03	15.59	15.25	14.96	14.71	14.48	14.27	14.07	13.88	13.71
0.8	20.51	18.36	17.47	16.79	16.21	15.70	15.24	14.82	14.43	14.06	13.71
0.7	23.91	20.68	19.35	18.32	17.46	16.70	16.01	15.38	14.79	14.23	13.71
0.6	27.31	23.01	21.23	19.86	18.71	17.69	16.78	15.93	15.15	14.41	13.71
0.5	30.71	25.33	23.11	21.40	19.96	18.69	17.54	16.49	15.50	14.58	13.71
0.4	34.11	27.66	24.99	22.94	21.21	19.69	18.31	17.04	15.86	14.76	13.71
0.3	37.51	29.98	26.87	24.47	22.46	20.68	19.07	17.60	16.22	14.93	13.71
0.2	40.91	32.31	28.75	26.01	23.71	21.68	19.84	18.15	16.58	15.11	13.71
0.1	44.31	34.63	30.63	27.55	24.96	22.67	20.61	18.71	16.94	15.28	13.71
0	47.71	36.96	32.50	29.09	26.21	23.67	21.37	19.26	17.30	15.45	13.71

(a) Total Ransomware Profit

δ_s/δ_r	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1
1	13.71	13.71	13.71	13.71	13.71	13.71	13.71	13.71	13.71	13.71	13.71
0.9	16.77	15.80	15.40	15.09	14.83	14.61	14.40	14.21	14.03	13.87	13.71
0.8	19.83	17.89	17.09	16.48	15.96	15.50	15.09	14.71	14.36	14.02	13.71
0.7	22.89	19.99	18.78	17.86	17.08	16.40	15.78	15.21	14.68	14.18	13.71
0.6	25.95	22.08	20.48	19.25	18.21	17.30	16.47	15.71	15.00	14.34	13.71
0.5	29.01	24.17	22.17	20.63	19.33	18.19	17.16	16.21	15.33	14.50	13.71
0.4	32.07	26.26	23.86	22.01	20.46	19.09	17.85	16.71	15.65	14.65	13.71
0.3	35.13	28.36	25.55	23.40	21.58	19.98	18.54	17.21	15.97	14.81	13.71
0.2	38.19	30.45	27.24	24.78	22.71	20.88	19.23	17.71	16.29	14.97	13.71
0.1	41.25	32.54	28.93	26.17	23.83	21.78	19.92	18.21	16.62	15.12	13.71
0	44.31	34.63	30.63	27.55	24.96	22.67	20.61	18.71	16.94	15.28	13.71

(b) Ransom Profit

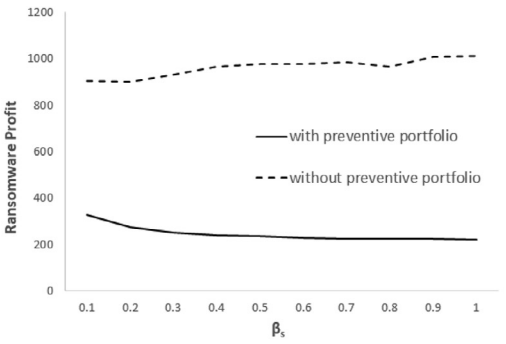
δ_s/δ_r	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1
1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
0.9	0.34	0.23	0.19	0.15	0.12	0.10	0.08	0.06	0.04	0.02	0.00
0.8	0.68	0.46	0.38	0.31	0.25	0.20	0.15	0.11	0.07	0.03	0.00
0.7	1.02	0.70	0.56	0.46	0.37	0.30	0.23	0.17	0.11	0.05	0.00
0.6	1.36	0.93	0.75	0.62	0.50	0.40	0.31	0.22	0.14	0.07	0.00
0.5	1.70	1.16	0.94	0.77	0.62	0.50	0.38	0.28	0.18	0.09	0.00
0.4	2.04	1.39	1.13	0.92	0.75	0.60	0.46	0.33	0.22	0.10	0.00
0.3	2.38	1.63	1.32	1.08	0.87	0.70	0.54	0.39	0.25	0.12	0.00
0.2	2.72	1.86	1.50	1.23	1.00	0.80	0.61	0.44	0.29	0.14	0.00
0.1	3.06	2.09	1.69	1.38	1.12	0.90	0.69	0.50	0.32	0.16	0.00
0	3.40	2.32	1.88	1.54	1.25	1.00	0.77	0.56	0.36	0.17	0.00

(c) Data-selling Profit

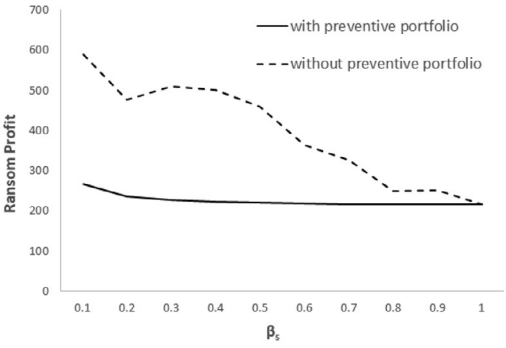
Fig. 6. Attacker's ransomware profit received from a representative victim in response to the victim's changing composition of preventive portfolio. Presence of encryption and deception not only reduces data profit, but also reduces ransom profit, thus reducing overall ransomware profit significantly.

data-selling rate increases. With preventive portfolio, both ransom profit and data profit (and thus total ransomware profit) decrease as β_s increases. Overall, the ransomware profit reduction (between with and without preventive portfolio) widens as β_s increases.

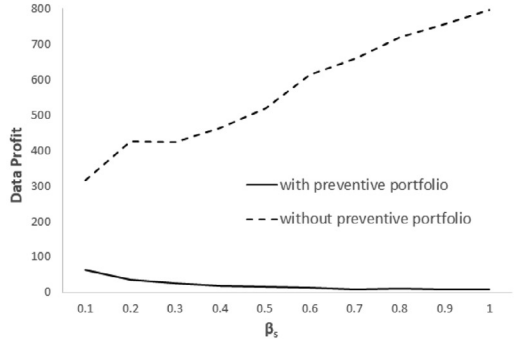
Finally, Fig. 8 further compares side-by-side the profitability of ransomware (together with ransom and data component profit) at various data-selling rate ($\beta_s = 0.3$, $\beta_s = 0.6$, and $\beta_s = 0.8$). Taking



(a) Total Ransomware Profit



(b) Ransom Profit



(c) Data-selling Profit

Fig. 7. Analysis of ransomware profit components (data and ransom) with and without preventive portfolio at various data-selling rate β_s. Preventive measures flatten the curves and lower the ransomware profits. The decrease in data profit is most significant.

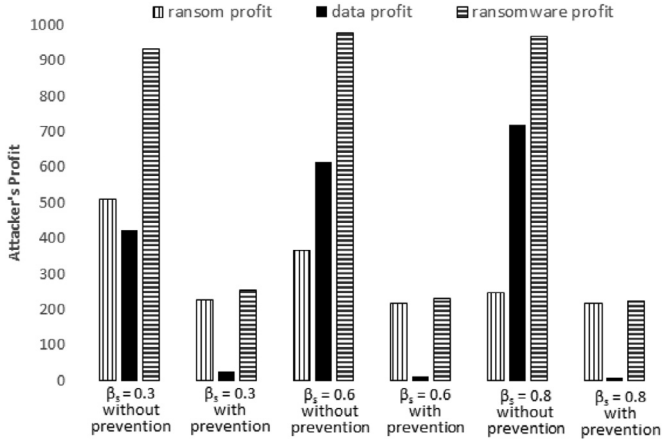


Fig. 8. Profitability of ransomware with preventive portfolio decreases as compared to the profitability without prevention at all data-selling rate β_s.

$\beta_s = 0.6$ for example, all three profits (ransom, data, ransomware) decrease dramatically with preventive portfolio, with data profit reduction being most significant. In absence of preventive measures, the attacker faces a tradeoff between ransom profit and data profit, i.e., while data profit increases, ransom profit decreases, hence total ransomware profit may go up and down when β_s changes. At the presence of preventive measures, however, both ransom profit and data profit decrease as β_s increases, hence total ransomware profit is always decreasing in β_s.

5. Conclusion

More research is needed for the inevitable data-selling ransomware which is harder to defend than traditional ransomware. In this paper, we proposed a preventive portfolio that consists of two preventive measures, i.e., preventive data encryption and preventive data deception against the data-selling ransomware. Through both game-theoretical modelings and extensive simulation studies, we discovered the complex relationships between users/victims and attackers considering various decision variables, expected payoffs, strategy space and other parameters. The results suggest the preventive portfolio is effective against data-selling ransomware in that it can significantly decrease the profit of the data-selling ransomware and increase the expected payoff of the victims. Preventive portfolio not only dramatically decreases data profit but ransom profit as well by decreasing the victims' willingness to pay thus reducing the ransom demand. Preventive measures have positive externality in the sense that some adoption of preventive measures benefits all users. The practice also reduces uncertainty and provides financial incentives for the attacker to increase credibility or reputation. Our future work is to explore other market-based solutions involving defensive buyers against the data-selling ransomware.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Zhen Li: Formal analysis, Validation, Writing – original draft. **Qi Liao:** Conceptualization, Methodology, Writing – review & editing.

References

Al-rimy, B.A.S., Maarof, M.A., Shaid, S.Z.M., 2018. Ransomware threat success factors, taxonomy, and countermeasures: a survey and research directions. Comput. Secur. 74, 144–166.

Aldaraani, N., Begum, Z., 2018. Understanding the impact of ransomware: a survey on its evolution, mitigation and prevention techniques. In: Proceedings of the 21st Saudi Computer Society National Computer Conference (NCC), Riyadh, Saudi Arabia, pp. 1–5.

Ali, A., 2017. Ransomware: a research and a personal case study of dealing with this nasty malware. Issues Informing Sci. Inf. Technol. 14, 87–99.

Anghel, M., Racautanu, A., 2019. A Note on Different Types of Ransomware Attacks. IACR Cryptology ePrint Archive, p. 605.

Caporusso, N., Chea, S., Abukhaled, R., 2018. A game-theoretical model of ransomware. In: Proceedings of the International Conference on Applied Human Factors and Ergonomics, Orlando, FL, pp. 69–78.

Cartwright, A., Cartwright, E., 2019. Ransomware and reputation. Games, MDPI, Open Access J. 10 (2), 1–14.

Climek, D., Macera, A., Tirenin, W., 2016. Cyber deception. Cybersecur. Inf. Syst. Inf. Anal. Center (CSIAC) 4 (1), 1–2. https://csiac.org/articles/cyber-deception/2/.

CyberEdge, 2020. Cyberthreat defense report.

Cyware, 2020. Ftcode Ransomware Returns with Credential-Stealing Capabilities. Cyware Hacker News.

Cyware, 2020. Ransomware Operators Turn Evil for Late Reposnders and Non-Paying Victims. Cyware Hacker News.

Hakak, S., Khan, W.Z., Imran, M., Choo, K.-K.R., Shoaib, M., 2020. Have you been a victim of COVID-19-related cyber incidents? Survey, taxonomy, and mitigation strategies. IEEE Access 8, 124134–124144.

Hernandez-Castro, J., Cartwright, A., Cartwright, E., 2020. An economic analysis of ransomware and its welfare consequences. R. Soc. Open Sci. 7 (3), 1–14.

Hernandez-Castro, J., Cartwright, E., Stepanova, A., 2020. Economic analysis of ransomware. SSRN Electronic Journal 1–14. https://royalsocietypublishing.org/doi/10.1098/rsos.190023.

Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., Kirda, E., 2015. Cutting the Gordian knot: a look under the hood of ransomware attacks. In: Proceedings of the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA 2015), pp. 3–24.

Laszka, A., Farhang, S., Grossklags, J., 2017. On the economics of ransomware. In: Proceedings of the 8th Conference on Decision and Game Theory for Security (GameSec 2017), pp. 397–417.

Li, Z., Liao, Q., 2018. Economic solutions to improve cybersecurity of governments and smart cities via vulnerability markets. Gov. Inf. Q. 35(1), 151–160.

Li, Z., Liao, Q., 2020. Ransomware 2.0: to sell, or not to sell. Agame-theoretical model of data-selling ransomware. In: ACM Proceedings of 9th International Workshop on Cyber Crime (IWCC) at the 15th International Conference on Availability, Reliability and Security (ARES), Dublin, Ireland.

Li, Z., Liao, Q., 2021. Game theory of data-selling ransomware. J. Cyber Secur. Mobil. 10 (1), 65–96.

Mathews, L., 2020. Another Ransomware Campaign Threatens to Expose Victims' Data. Forbes.

Mohurle, S., Patil, M.R., 2017. A brief study of wannacry threat: ransomware attack 2017. Int. J. Adv. Res. Comput. Sci. 8 (5), 1938–1940. http://www.ijarcs.info/index.php/Ijarcs/article/view/4021.

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., McQuaid, R., 2021. Developing cyber-resilient systems: a systems security engineering approach. NIST Spec. Publ. 800-160 2 (Revision 1), 1–310.

Silva, J.A.H., Barona, L., Valdivieso, L., Alvarez, M., 2019. A survey on situational awareness of ransomware attacks – detection and prevention parameters. Remote Sensing 11, 1168.

Simoiu, C., Gates, C., Bonneau, J., Goel, S., 2019. "I was told to buy a software or lose my computer. I ignored it": a study of ransomware. Proceedings of the Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019), Santa Clara, CA, pp. 155–174.

Sophos, 2021. The state of ransomware 2021.

Subedi, K., Budhathoki, D.R., Chen, B., Dasgupta, D., 2017. RDS3: ransomware defense strategy by using stealthily spare space. In: Proceedinds of 2017 IEEE Symposium Series on Computational Intelligence (SSCI), Honolulu, HI, pp. 1–8.

Whitwam, R., 2019. Ransomware Groups Now Threatening to Release Stolen Data if Businesses don't Pay. ExtremeTech.

Wolf, D.G., Goff, D.L., 2018. A ransomware research framework: poster. In: Proceedings of the 5th Annual Symposium and Bootcamp on Hot Topics in the Science of Security (HoTSoS), pp. 1–2.

Zhen Li is currently an E. Maynard Aris Endowed Professor of Economics in the Department of Economics and Management at Albion College. She received her Master's Degree and Ph.D. in Economics from Princeton University under the direction of Dr. Michael Woodford. She graduated with her Bachelor's Degree in International Economics from Peking University. Dr. Li conducted research on applied macroeconomics and international finance, in particular on international financial integrity and related policy issues. Dr. Li's recent research interests include inter-disciplinary research study on economics and game theory of computer networks and information security.

Qi Liao is currently a Professor of Computer Science at Central Michigan University (CMU). He received his M.S. and Ph.D. in Computer Science and Engineering (CSE) from the University of Notre Dame, and a B.S. and departmental distinction in Computer Science (minor in Mathematics) from Hartwick College, New York. Dr. Liao's research interests include computer security, machine learning, visual analytics, and economics/game theory at the intersection of network usage and cybersecurity. He received best paper awards at USENIX LISA, IEEE ICCCBDA, Emerald Literati Awards for Excellence for Information and Computer Security, IEEE VAST Challenge Award, winner of National Security Innovation Competition, Center for Research Computing Award for Computational Sciences and Visualization, and CMU College of Science & Engineering Award for Outstanding Research. Dr. Liao was a visiting research scientist at IBM Research, Argonne National Lab, and ASEE Fellow at U.S. Air Force Research Lab.