A Survey on Detection and Classification of Ransomware Bitcoin Transactions

Sabira Karim[1], Shemitha PA[2]
[1]*Computer science and Engineering, IES Engineering College under Kerala Technological University, Kerala, India*
[1]*Computer science and Engineering, IES Engineering College under Kerala Technological University, Kerala, India*

ABSTRACT

Ransomware transactions are widely used in crypto-currencies. Most modern ransomware use Bitcoin for payments. The Bitcoin transactions are permanently recorded and publicly available. Based on the collected ransomware related Bitcoin addresses, the researchers have employed advanced data analytics techniques to detect ransomware related transactions and malicious Bitcoin addresses automatically. The machine learning approaches are evaluated based on Bit-Heist Ransomware dataset which is publicly available. Various approaches are used for it. The machine learning approaches are evaluated based on the patterns differentiating such cybercrime operations from normal bit-coin transactions in order to identify and report attacks. Different experimental results show that this model achieved improved detection rate skill of the model in classification. A survey for all these techniques is in this paper for analyzing various algorithms and methods. This work would be the ultimate opportunity to expand and organize research efforts in future wok by applying some early preventions and strategies to defeat these kinds of malicious transactions.

Keyword : - *Block-chain, bit-coin, bit-heist, Machine learning, ransomware.*

1. INTRODUCTION

Bitcoin may be a cryptocurrency introducedby Satoshi Nakamoto in 2008. Bitoin was the primary application of Block chain. It had been introduced in 2009. Iit's a digital banking industry while not a physical banking central system with none specific country of origin. Bitcoin might be a suburbanized form of payment system wherever the general public ledger is correctly supported in a very distributed manner. The unknown anonymous members referred to as miners, capital punishment a protocol that maintains and extends a distributed public ledger that records bitcoin transactions is termed a block chain. Block chain is enforced as a series of blocks. Bitcoin is that the known crypto-currency business. The transactions of bitcoin area unit utterly digital and unknown to a good extent. This case has crystal rectifier several cyber-crime perpetuators to use bitcoin as a secure haven for misbr transactions like Ransomware payments. Ransomware is malicious code that affects the payments entry reciprocally of ransom that should be paid. Machine Learning approaches could also be utilized to pour over the previous transactions as coaching information inorder to properly predict the people or teams to whom Ransomware payments area unit being created. This paper tries to explore the efficaciousness of various machine learning approaches in police work such payments. Ransomware may be a form of malware that infects a victim's information and resources, and demands ransom to unleash them. In 2 main sorts, ransomware will lock access to resources or encipher their content. Ransomware will be delivered via email attachments or internet primarily based vulnerabilities. additional recently, ransomware are delivered via mass exploits. as an example, Crypto-Locker used Gameover ZeuS botnet to unfold through spam emails. Once the ransomware is put in, it communicates with a command and centre. though earlier ransomware used hard-coded IPs and domain names, newer variants could use namelessness networks, like TOR, to achieve a hidden command and management server. In the case of uneven cryptography, the cryptography secret is delivered to the victim's machine. In some variants, the cryptography secret is created on the victim's machine and delivered to the command center.

Once resources area unit latched or encrypted, the ransomware displays a message that asks a precise quantity of bitcoins to be sent to a bitcoin address. This quantity could rely on the amount and size of the encrypted resources. Once payment, a decipherment tool is delivered to the victim. However, in some cases, like with WannaCry, the ransomware contained a bug that created it not possible to spot World Health Organization paid a ransomware quantity.

2. LITERATURE SURVEY

There is a huge increase among the vary of on-line users investment and commerce bitcoin. However, the obscurity by the crypto-currencies were exploited by hackers or Ransomware operators. This paper aims to identify ransom payments in crypto-currencies, significantly in terms of bitcoins. I even have conducted several studies.

A ascendible data-driven Bitcoin dealings analytics framework that's well a lot of sensible in investigation ransomware payment connected addresses, compared to the prevailing heuristic primarily based approaches. Topological ransomware information analysis techniques to automatically ensure new malicious addresses at intervals the Ransomware family. The key thrust behind their planned approach is that the intrinsic capability to look at the whole block-chain graph and, as a result, to trace and analyze dynamics of the associated block-chain topological and geometrical properties at a multi resolution level. The authors have designed a bit-coin graph model as a directed weighted graph. New addresses happiness to the Ransomware family unit familiar supported the payments created to the legendary addresses of Ransomware family.

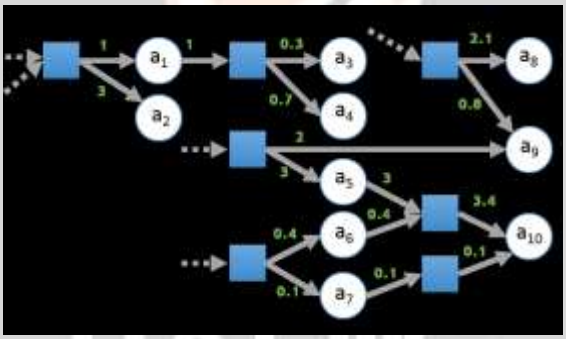

Fig1 -1: Bitcoin Transactions

In ransomware analysis, Montreal , Princeton and town studies have analyzed networks of cryptocurrency ransomware, and placed that hacker behavior can facilitate U.S.A. verify covert ransomware pay.

Feature extraction has been studied for ransomware detection in specific domains. In code code analysis, Cryptolock inspects ransomware programs and their activity for malicious characteristics.

Initially, the Ransomware addresses unit classified into twenty,000 groups. the following groups unit then analyzed for any relation between Ransomware families. every Topological information Analysis(TDA) still as DBSCAN clump rule unit utilised to find and predict Ransomware transactions

A framework that mechanically detects the ransom payments created to bitcoin address that belong to the CryptoLocker. The blockchain analysis and information sourced from the net forums like reddit and Bitcoin speak were utilised to create activity analysis on the info. The timestamps supported the ransom payments created by the victims area unit then extracted. victimisation this information analysis, the trends within the statistic ransom amounts were paid were analyzed.

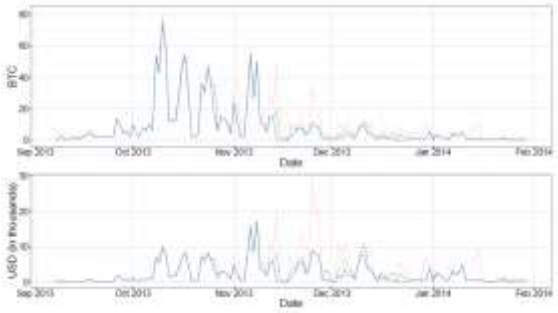

Fig -2: Trends in Transactions

Using data collected they generate a cluster of 968 Bitcoin addresses happiness to CryptoLocker. They provided a bound for CryptoLocker in Bitcoin and known 795 ransom payments total one,128.40 BTC ($310,472.38), however has shown that the payoff may are price upwards of $1.1 million at peak valuation. By analyzing ransom payment timestamps each lengthways across CryptoLocker in operation amount and transversally across times of day, we have a tendency to find changes in distributions and kind conjectures on CryptoLocker that corroborate data from previous efforts. to boot, we have a tendency to construct a constellation to detail CryptoLocker monetary infrastructure and procure further data on the CryptoLocker operation. Mainly, they found proof of that implies connections to in style Bitcoin services, like Bitcoin Fog and BTC-e, and delicate links to different cybercrimes close Bitcoin, like the Sheep Marketplace scam of 2013.

The safety and privacy issues in bitcoin shows how the veil of anonymity provided by the bitcoin ecosystem is encouraging the cyber criminals to resort to illegal and banned activities such as ransomware, tax evasion and money laundering. The transaction patterns of ransomware attacks. The patterns are analyzed to collect intelligence to counteract the Ransomware attacks. Ransomware seed addresses were used to model a target network for pattern analysis. Different graph algorithms were used to analyze the cash-in and cash-out patterns. The show distinguishable ways related to the input and output side of the Ransomware graphs.

The measurement analysis of Ransomware payment data including the details regarding the victims as well as operators. A cocmprehensive dataset from multiple data sources such as Ransomware binaries, victim telemetry as well as vast list of bitcoin addresses was formed. This data was used to bitcoin-trail right from when the victim aquires bitcoins to the point where the operators cashout the bitcoins. The results claim improved coverage and detection of the Ransomware when compared with existing algorithms.

Alhawi have proposed NetConverse which uses J48 primarily based decision-tree classifier to detect Ransomware samples from features that were derived from network traffic communications. Results show his approach returned better detection when compared to other conventional machine learning approaches such as Bayes Network, K-Nearest, Multi-layer perceptron, Random Forest and Logistic Model tree.

Poudyal have proposed a framework for investigating ransomware using machine learning techniques. Evaluation of the eight machine learning techniques has been conducted at two levels viz., assembly and dll programs. The results indicated that the ransomware detection rate of more than 90%.

The dataset for training the machine learning algorithms on the ransomware payments are from bitcoin network. The dataset was taken from the bitcoin transaction graph from 2009 January to 2018 Dec. Daily transactions from the network were extracted and therefore the network links having but zero less than 0.3 billion were filtered out as ransomware amounts were typically on top of this threshold. The dataset contains twenty four thousand four hundred eighty six addresses selected from 28 ransomware families. The “Bit Coin-Heist Ransomware Address Dataset “contains nine descriptive attributes and a decision attribute. A summary of the dataset is given in Figure 3.

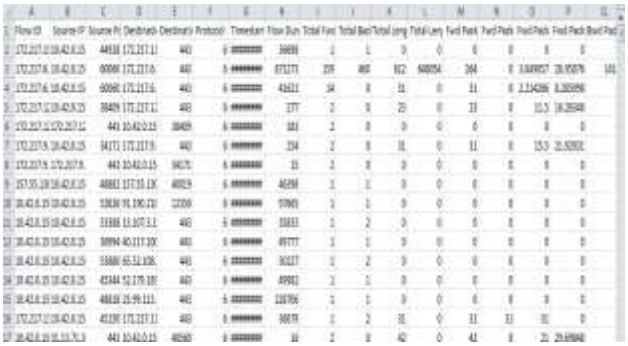

Fig -3: The BIT_HIEST dataset

The bitcoin transactions have been developed as a Bitcoin Graph model with the help of a directed acyclic graph (DAG). Along with the bitcoin address and its year and day time stamp, six other features also have been associated with the address. The attribute income is used to represent payment made in number of bitcoins. The attribute length is employed to identify the number of non-starter transactions on the longest chain.

Attribute Id	Attribute Name	Attribute Type	Category/Description
1	Address	String	Address of the transaction. The transaction could be ransomware or white.
2	Year	Integer	Year of transaction as integer
3	Day	Integer	1 is and 365 is last day of the year
4	Length	Integer	Number of non-starter transactions on its longest chain.
5	Weight	Float	Sum of fraction of coins that originate from starter transaction and end up reaching the address.
6	Count	Integer	Number of starter transactions connected to the address through a chain
7	Looped	Integer	Number of starter transactions connected to the address with more than one directed arc.
8	Neighbors	Integer	Number of transactions which have the address as output.
9	Income	Float	Total number of coins output to the address
10	Label	String	The class to which the transaction belongs to. either white (non-ransomware) or ransomware (one of the 27 ransomware families)

Table 1:- Description of the BitCoinHeistRansomware Address dataset

Fig -4: The labels of BitHiest

A starter-transaction is any one of the sooner transaction in a 24-hour window which did not receive any payments. The attribute weight corresponds to the fraction of coins originating from the starter transaction and ultimately ending up at the corresponding bitcoin address. The attribute length defines the quantity of non-starter transactions in its longest chain. The chain is enforced as a directed acyclic graph, originating from any starter transaction and ending at given address. Count attributes defines the quantity of starter transactions connected to the given address. Loop of an address is that the range of starter transactions connected to the address via more than one directed path.

Each of the transactions within the dataset are related to a label indicating whether the transaction is white (benign) or belongs to one of the 27 ransomware families. The dataset is a multiclass dataset which is extremely imbalanced in nature. A dataset is said to be imbalanced if the represeantations of various classesare roughly not equal.

The class distributions of the attribute label are represented in table2. The percentage of imbalance of the foremost frequent ransomware category viz., paduaCryptoWall with respect to the majority white class is 0.46%.

The representation of other less frequent ransomware families is almost negligible. Most of the conventional classifiers driven by accuracy-based evaluation metrics may fail in effectively predicting the ransomware attacks. This work focuses to study the effect of different classifiers in such extremely imbalanced data.

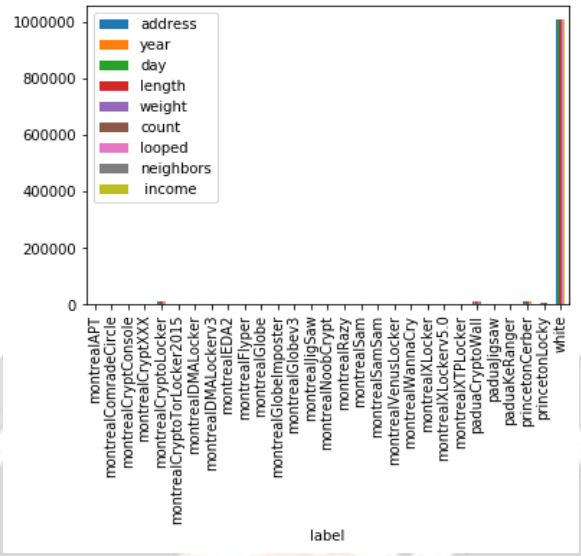

Fig-5: A histoplot of the ransomware classes

Class	Label	Frequency	Class	Label	Frequency
0	white	2875284	14	montrealWannaCry	20
1	paduaCryptoWall	12399	15	montrealRazy	15
2	montrealCryptoLocker	9315	16	montrealAPT	11
3	princetonCerber	8223	17	paduaKeRanger	10
4	princetonLocky	6625	18	montrealFlyper	9
5	montrealCryptXXX	2419	19	montrealXTPLocker	9
6	montrealNoobCrypt	683	20	montrealCryptConsole	7
7	montrealDMALockerv3	334	21	montrealVenusLocker	7
8	montrealDMALocker	231	22	montrealXLockerv5.0	7
9	montrealSamSam	82	23	montrealEDA2	6
10	montrealGlobeImposter	55	24	montrealFlyper	4
11	montrealCryptoTorLocker2015	33	25	paduajigsaw	2
12	montrealGlobev3	31	26	montrealJigSaw	1
13	montrealGlobe	22	27	montrealComradeCircle	1
			28	montrealXLocker	1

Fig -6: The class frequency table

As the part of preparation of data to this model, we can split the data using hold out method and bagging.

Then to build individual models and homogenous ensemble model for each machine learning algorithm. Finally tune the model performance. Machine Learning algorithms can build a heterogeneous ensemble with best performance. Then we will check for the variance in results using k-fold cross validation.

When creating appropriate training and testing splits for the classifiacation models using hold-out method, all the classification models using will be built by using 2 splits of data to check the variance and performance.

One set will be the main 75-25 split and other is 3 training and 1 testing dataset each with 25% of the data created using bagging with replacement. Cross-validation gives this model the opportunity to train on multiple train-test splits.

All the experiments were conducted on Intel Core i7-6500U CPU 2.5 GHZ PC with 16GB of RAM running 64 bit OS machine. The implementation is completed using Python Programming language on Jupyter Notebook. The experiments on "Bitcoin Heist Ransomware address dataset" are performed with randomly selected training data and validation data Machine Learning Approaches.

The machine learning approaches performed are for building the classification models to predict the Ransom attacks mainly used are TDA, Random Forest, SVM and k-Nearest Neighbor.

Random Forest (RF) is an ensemble classification model that is depends on the predictions from multiple single weak learners, so as to form a one unified accurate prediction. The ensemble approaches have been proven to perform greater than traditional classification approaches, and can ease the issues faced by the individual constituent classifiers. Random Forest approach creates a set of multiple decision trees. The constituent decision trees are fed the data by applying random subset sampling on the instances as well as features.

The predictions from these decision trees are aggregated to obtain the unified prediction.

The K-nearest neighbor (k-NN) is a lazy learning algorithm which is for generalizing the provided training dataset isn't prebuilt before examining the unknown instances. K-NN represents the provided training instances on the feature space in terms of similarity measures. K-number is user specified parameter which selects the k number of training instance "closely related" to a given unknown instance. The nearest neighbors are estimated using classical distance measures (Euclidean, Manhattan, or Minkowski) for continous variables and hamming distance for categorical variables. Consensus among these measures provides the predicted class label for a given unknown instance.

The classification algorithms recommended by the training algorithms cannot be deployed directly as models derived from active learners affects from the over-fitting drawback. The classification model is validated against a separate test dataset. Once the evaluation of parameters for classification model are based on the confusion matrix. Confusion matrix is comprised of TP (True-Positive), TN (True-Negative), FP (False-Positive), FN (False - Negative).

The most analysis metrics evaluated are Accuracy, Precision, Recall and F1-Measures. Accuracy is outlined as proportion of total number of prediction made that is correct. True Positive Rate is measured as the ratio of correctly classified positive examples to the total number of positive examples. Precision is another widely used metric in information retrieval which estimates the percentage amount of relevant objects out of the retrieved ones. Recall corresponds to the number of relevant instances retrieved out of all the relevant ones. F1-measure is the harmonic mean of Precision and Recall. Accuracy has been shown in many studies is biased towards majority class. In case of the bit-coin dataset which is extremely skewed in nature, accuracy may not be considered a sa good evaluation metric. Hence the results were drawn on the testing dataset for Precision, recall and F-measure values.

Of the validation dataset corresponds to 10% of the randomly sub-sampled instances from the Bitcoin Ransomware dataset. The addresses are well as the class label attributes of the entire dataset have to be transformed using Label encoding process for some classification algorithms to begin modeling data. The resulting class label and the frequency counts of individual class labels are provided in the result tables for clear understanding. The validation dataset also can be noticed as extremely imbalanced in nature. The result is in terms of Accuracy, Precision, Recall and F1-measure.

Naïve Bayes Classifier did not perform well on the dataset whereas other classifiers return good values. The k-nearest neighbor algorithm was able to correctly identify instances belonging to the minority classes. K-nn is a lazy

classifier which postpones the classification task until the unknown instance is provided. The prediction is based on the consensus from 'k' similar training instances. It may be observed that k-NN correctly identifies fraud classes better than naive Bayes classifiers.

Random Forest is an ensemble formed from base classifier of decision trees. The weak learners are trained on the data obtained by applying random subset sampling on the set of instances and features as well. This process ensures least correlation among the constituent decision trees.

The class imbalance did not have as much effect on Random Forest as it did on Naïve Bayes and k-NN algorithms.

3. DISCUSSIONS AND REMARKS

This paper investigates the many effects of various supervised machine learning approaches for effective identification of Bitcoin payments for Ransomware perpetuators. Dataset thought-about could be a multi-class extraordinarily imbalances in nature. Results on completely different analysis metrics indicate that the Random Forest with k-fold cross validation rule may properly know additional of the attack categories.

The findings of the algorithms want any exploration on the datasets having extreme category imbalances also. additional stress may be provided to classifiers that think about the representatives of the minority categories from the coaching knowledge for creating higher reductions. Future work may be done to validate the results on more moderen spurious bitcoin transactions involving crime like ransomware payments and cash launder.

4. ACKNOWLEDGEMENT

This paper and the research behind it would not have been possible without the exceptional support of my supervisor, Shemitha PA. I am also grateful for the insightful comments offered by my colleagues allowed me to continue my research with the book much longer than I could have hoped. Finally I would like to thank my college and university for the unconditional support for completing this work.

6. REFERENCES

[1]. Cuneyt G Akcora, Yitao Li, Yulia R. Gel, Murat Kantarcioglu (2020). BitcoinHeist : Topological Data Analysis for Ransomware Prediction on the Bitcoin Blockchain.

[2]. Jitti Annie Abraham, Susan M George: "A Survey on Preventing Crypto Ransomware using Machine Learning" , 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)

[3]. Firoz khan, CorneusNcube: "A digital DNA Sequencing Engine for Ransomware Detection Using Machine Learning", IEEE Access Special section on Deep Learning Algorithms for Internet of Medical Things June 19,2020.

[4]. Umaru Adamu, Irfan Awin, "Ransomware Prediction using Supervised Learning Algorithms", 2019 7th International Conference on Internet of Things and Cloud.

[5]. Seong II Bae, Gyu Bin Lee, "Ransomware detection using Macine Learning algorithms", WILEY Special Issue 8th MAY 2019.

[6]. Eduardo Berrueta, Daniel Morato, "A Survey on Detection Tehniques for Cryptographic Ransomware", IEEE ACCESS 25th September 2019.

[7]. K. Liao, Z. Zhao, A. Doupe and G. Ahn,"Behind closed doors: measurement and analysis of CryptoLocker ransoms in Bitcoin", 2016 APWG Symposium onElecronic Crime esearch , Toronto,ON, 2016, pp. 1-13, doi:10.1109/ECRIME.2016.7487938. K. Elissa, "Title of paper if known", unpublished.

[8]. M.Conti, E. Sandeep Kumar, C. Lal and S. Ruj, (2018).(2016). "A Survey on Security and Privacy Issues of Bitcoin", in IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3416-3452, Fourthquarter 2018, doi:10.1109/COMST.2018.2842460.

[9]. Turner, A>B., McCombie, S. and Uhlmann, A.J. (2020) "Discerning payments patterns in Bitcoin from ransomware attacks", Journal of Money Laundering Control, Vol. ahead –of-print No. ahead-of-print. https://doi.org/10.1108/JMLC-02-2020-0012.M. Young, The Technical writer's Handbook. Mill Valley, C A: University Science, 1989.

[10]. D.Y. Huang et al., "Tracking Ransomware End-to-End", (2018).2018 IEEE Symposium on Security and Privacy(SP), San Francisco, CA, 2018, pp.618-631, doi: 10.1109/SP.2018.00047.

[11]. Alhawi O.M.K., Baldwin J., Dehghantanha A. (2018) Leveraging Machine Learning Techniques for Windows Ransomware Network Traffic Detection. In: Dehghantanha A., Conti M., Dargahi T. (eds) Cyber Threat Intelligence. Advances in Information Security, col 70. Springer, Cham. Doi: 10.1007/978-3-319-73951-9_5

[12]. S.Poudyal, K.P. Subedi and D. Dasgupta, "A Framework for Analyzing Ransomware using Machine Learning," 2018 IEEE Symposium Series on Computational Intelligence (SSCI), Bangalore, India, 2018, pp. 1692-1699,doi: 10.1109/SSCI.2018.8628743.