ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 12, Issue, 11, pp.14917-14922, November, 2020

DOI: https://doi.org/10.24941/ijcr.40253.11.2020

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

RESEARCH ARTICLE

RANSOMWARE ATTACK DETECTION AND PREVENTION

***Lama Alhathally and Emad Alsuwat**

Computer Science Department, School of Computer Science and Information Technology, Taif University

ARTICLE INFO

Article History:
Received 10th August, 2020
Received in revised form
27th September, 2020
Accepted 20th October, 2020
Published online 30th November, 2020

Key Words:
Ransomware,
Detection,
Preventation.

ABSTRACT

Nowadays, quite a lot of users became victims of cyberattacks campaigns especially those that depend on holding a document to get a ransom. In other words, users tend to save their vital documents on computers or on the cloud which makes these documents exposed to adversarial attackers. Ransomware is an emerging cyberattack and one of the toughest kinds of scareware to fight against. Moreover, it's not feasible to detect ransomware attacks with classical methods because suck attacks are evolving and reforming very quickly which makes it hard for antiviruses to detect such threats. There are three detection methods that can accurately detect this emerging attack. These detection methods are based on classifying and analyzing network traffic to extract abnormal behavior and thus detect ransomware. Moreover, it is possible to use machine learning techniques to erect a model for detecting this attack. Using honeypot to deceive the ransom ware and discover it a faster method for detecting ransomware attacks. There are effective preventing methods that can thwart this attack from happening, such as making an up-to-date backup and avoiding clicking on untrusted email links and attachments.

Citation: ***Lama Alhathally, Emad Alsuwat.*** **2020.** "Ransomware Attack Detection and Preventation", *International Journal of Current Research*, 12, (12), 14917-14922.

INTRODUCTION

Lately, several people who has been used the internet became a victimize to cyber-attacks movements that depend on blackmailing methods. Ransomware is considered the hardest type of scareware to prevent against (Sgandurra, 2016). Ransomware is type of malware which encode the target precious data and demand payment to decode these data. The demanding money usually is paid by bitcoin which is a currency that cannot be traced (Continella, 2016). Ransomware recognition and ending is a difficult mission for classical antivirus (AV) resolutions in order to two explanations. First, ransomware with ability to metamorphize and adjust itself, consequential lead to an execute with a dissimilar footprint or sign. Subsequently, that become impractical to retain a footprint directory of antivirus merchants updated (Akay, 2019). Second, ransomware main cryptography procedures such as key generating and encoding are famous techniques, which are achieved by harmless programs as web browsers, password administrators, office programs and zip services additionally to authentic cryptographical programs. Consequentially, restricted heuristic ability intensely rises the chances of untrue positive and destroy target knowledge.

***Corresponding author: Lama Alhathally,**
Computer Science Department, School of Computer Science and Information Technology Taif University.

Anti-malware resolutions can be advanced by a goal to handle precisely this malware risk (Akay, 2019). These tactics concentrate on nowadays alternatives, nevertheless, ransomware is becoming more advanced throw the time, as per it occurs with the other malicious program categories. Additionally, current methods for ransomware discovery are not enough to deal with the problematic owing to several restrictions, such as, key security being complex to mystification and behavior study being avoided by adjustive attack methods (Akay, 2019). The reminder of this survey paper is structured as follows. Section II will be a brief background about ransom ware attack and the infection factors. Section III explain several detection methods for ransomware attack. Section IV suggested some of a prevention technique to prevent people form got attacked by the ransomware. Section V is discussion and comparison between the three deducting methods. Section VI conclude the whole paper.

Background

- Ransomware is a kind of malware which is locked the system or files and require payment to unlock them. Ransomware classified into two sections depending on the used lock technique:
- **Computers locker:** this section closes the victim system processes by overloading system assets on the other hand the information will not be touched.

- **Crypto-virus:** encode the target information using high level of encoding method (Akay, 2019).

The ransomware procedure includes five stages

Infection: by implanting the ransomware into system. Frequently, the system gets infected by one of the infection methods such as phishing attack or click on harmful links usually by exploiting people unawareness about these attacks (Thomas *et al.,* 2019).

Distribution: in this stage the system starts to get infected by injecting an executive file. Moreover, this malware will emerge with the system and modified the register keys to make sure that the contagion will stay despite of rebooting the system. As a result, the information encoding going to happened based on the settled span (Thomas *et al.,* 2019).

Backup attack: If this attack succeeded it will restrict the target capability for recovery. In other words, this attack will force the target to pay the money to get back the system. During this stage losing information will happen (Thomas *et al.,* 2019).

Encoding: Information will be encoded then the encode keys will be created along with a different encoding period depends on many aspects for example, the amount of linked machines, folder size, and network architecture (Thomas *et al.,* 2019). user notice or announcement: Finally, announcement will appear to the target which contain the cost and guidance for paying the ransom (Thomas *et al.,* 2019).

There are different methods that attackers using to set up ransomware on target's PCs which is (Sgandurra, 2016):

- Phishing e-mails: usually contains links, or an attachment to a Phishing e-mails: usually contains links, or an attachment to a malicious file that have a communal name to attract the target to open it and the harmful software will be loading to the target Pc (Sgandurra, 2016).
- Exploit kits: Injecting fake ads to trusted websites these ads lead the victims to a harmful site that controlled by the adversary. In order to take advantage of the browser weaknesses by using the exploit kit to install the ransomware (Sgandurra, 2016).
- Downloader and Trojan Botnets: hiding malicious software in authentic files where the targets downloading it without knowing that these files contain a harmful software (Sgandurra, 2016).
- Social engineering strategies: deceive the targets to install a forged AV, by displaying the result of AV an examinations purportedly viewing malware on the target's PCs (Sgandurra, 2016)

Ransomware Deduction

Ransomware Data Classification: There are several deduction methods one of these methods is data extraction from suspicious badware earlier which means previous working or when it's already works. This method is used to classify the software to harmful or harmless. Based on data extracting analysis from ransomware events it can be classified to three groups (Berrueta, 2019):

- Passive: Extracting data from the binary of malicious software previous running and it could be found earlier post operating the software (Berrueta, 2019).
- Active: The information extracting happened during the working of the malware and depending on the activities that occurred on the affected system (Berrueta, 2019).
- Based on network: In this section the data is coming from the traffic in network which is formed from the working badware (Berrueta, 2019).

Passive Constant Data: Detecting algorithm that depends on constant variables can detect malicious software early before it's running. This algorithm is considered the most efficient to evade losing any information for the target. One of the popular methods that apply in commerce antiviruses programs is to get the constant variables from analyzing the binary of programs. Yet, several of ransomware family apply code encryption methods or various action that prevent the discovery of the malware. These constant data got from documents that is linked to text chains or operation claims (Berrueta, 2019).

Text chains: Popular chains can be in ransomware pairs are 'ransom', 'bitcoin', or 'encrypt'. Moreover, it could have well-known domains name or IP addresses. The antiviruses program could explore for the main words of phrase. Frequently it's completed through a deep study of constant and changing variables since the technique is like false positive alerts (Berrueta, 2019).

Operation claim: The most popular operation claim can be in ransomware malware are associated to cryptographic procedures (key peer group, encoding, besides decoding) also folder accesses. code check could spot a procedure on this suspicious operation claim. They are operating beginning at famous active systems library otherwise static connected collections (Berrueta, 2019).

Active changeable Data: Active variables can take out as soon as the malicious program is working. They show the drawback of the obligation to operate insecure programs. Nevertheless, active variables are hard to distract since the ransomware has no choice but to act. For instance, it could evade the use of system demands for key managing or using a recent encoding algorithm, yet it could not evade open, read, and write to file (Berrueta, 2019). Active data is statistics thus it needs gathering tester of ransomware activities in specific period. Throughout this time, the malicious program is unrestricted working and able to accomplish permanent damaging activities (Berrueta, 2019). Consequently, the information gathering stage should be limited, and stopping decision should be early before losing the data. Moreover, it should not be too brief because it will deliver inaccurate information to the detecting algorithm and as result, it will extract an incorrect decision. Disregarding actual malicious software (false negative) and stopping harmless software (false positive) should measure as deadly algorithm mistakes (Berrueta, 2019).

Active variables can be classified into three groups:

- **Data entry info:** They evaluate the ransomware activities that done on the target folders, not only what inside these folders but also how and when these folders were adjusted (Berrueta, 2019).

Table 1. Timeline of Ransomware attacks adapted from [1]

Name	Year	Main characteristics
PC Cyborg	1989	Spreading by floppy disks.
GPCoder	2005-2008	Distributed through emails; encodes a huge group of documents.
Archiveus	2006	Initial Ransomware to practice RSA encoding algorithm.
WinLock	2010	Block computers through showing a payment note
Reveton	2012	Alert pretended to be as of a regulation administration organization.
DirtyDecrypt	Summer of 2013	Encodes more that seven diverse file extentions.
CryptLocker	September 2013	Gets a public key from the C&C.
CryptoWall	November 2013	Needs TOR browser to do the payment.
Android Defender	2013	Initial Android locker-ransomware.
TorDroid	2014	Initial Android crypto ransomware.
Critroni	July. 2014	Analogous to CryptoWall
TorrentLocker	Augusts. 2014	sneakiness: cannot be recognize because it's identical to SSH connections
CTB-Locker	December 2014	Uses asymmetrical Curve Cryptography, TOR and Bitcoins
CryptoWall 3.0	January. 2015	Use only TOR to pay
TeslaCrypt	February. 2015	Improves the possibility to pay with PayPal My Cash Cards
Hidden Tear	Augusts. 2015	Open source ransomware distributed for educational purposes
Chimera	November. 2015	Threatening to disclose victims' secret files
CryptoWall 4.0	November. 2015	Encodes filenames as well
Linux.Encoder.1	November. 2015	Encodes Linux's home and site directories
DMA-Locker	January. 2016	Provide a special decoding built-in
PadCrypt	February. 2016	Supporting Live Chat
Locky Ransomware	February. 2016	Spread out via using a malicious macro in a Word document
CTB-Locker for WebSites	February. 2016	Targeted WordPress.
KeRanger	March. 2016	Initial ransomware for Apple's Mac computers
Cerber	March. 2016	Afford as RaaS (& quote in Latin)
Samas	March. 2016	Pen testing on JBOSS servers
Petya	April. 2016	Overwrite MBT by their carrier and encodes MFT.
Rokku	April. 2016	Using QR code for speeding and easing the payment.
Jigsaw	April. 2016	Force targets to pay the ransom
CryptXXX	May. 2016	Observe mouse actions and avoid sandboxed domain
Mischa	May. 2016	Created when PETYA failed to get supervisory permission.
RAA	June. 2016	Fully printed in JavaScript
Satana	June. 2016	Merge all characteristics of PETYA and MISCHA.
Stampado	July. 2016	Promoting via combative advertisement crusades taking place in the black net.
Fantom	Augusts. 2016	Use a forge Windows update screen
Cerber3	Augusts. 2016	Third repetition of the Cerber ransomware

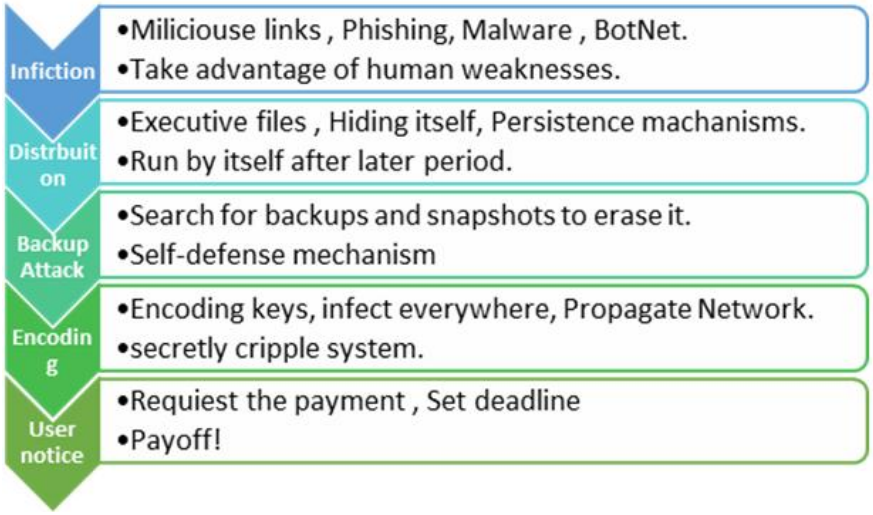

Figure 1. Ransomware procedure adapted from [4]

Method	Main Feature
RANSOMWARE DATA CLASSIFICATION	This scheme is used to categorize the software to damaging or inoffensive. Constructed on data mining investigation from ransomware actions and to perform it use detection algorithms.
MACHINE LEARNING MACHINE LEARNING (ML)	Comprises facts which forms in data to produce a model. This model can then deduction the result when fuel with new data. However, the problem with ML is discovering a right procedure to equivalent with a category of information and a vital outcome.
HONEYPOT	Honeypot comprises set up trick documents for the ransomware to attack. When these documents are entered, the ransomware could be recognized

- **Operation demands:** They evaluate the real library or system Operation demands by the suspicious procedure (Berrueta, 2019).

Data entry info: During the run of the malicious software, investigation program can excerpt info about how data in target folders are adjust and enter. This excerpted info is constructed on a detecting to recent encoded text (Berrueta, 2019).

Adjustment of magical bytes or folder type alteration: Mostly, the file type or extension could identify through a brief numeral byte in the start of a folder (magical bytes). The software which adapts the text in folder (for example, edit writing file) wouldn't alter the folder type. The software which encodes a folder is overwriting the above-mentioned text, altering the byte which characterize the folder type. The encoding act could detect through observing an alteration of an initial byte inside adapted folders. That method disposed in the direction of untrue positive since communal folder types adapt this folder text (Berrueta, 2019).

Entropy: Statistically, encoded information similar to unformal distribution random bytes. After a file is printed or overwritten, the newest content check for random values. This done by interrupting system demands that are used for file entree. Often use metrical is entropy. Equation no.1 illustrations a communal description of entropy in folder where PBn is the probability of bytes n appear in a folder, though additional choices happen (Berrueta, 2019).

$$e = \sum_{i=0}^{2} P_B \; l\iota \;\; {}_2 \frac{1}{P_B} \qquad (1)$$

There was not at all a definite entropy rate that distinguishes encoded on plain text. An impromptu beginning intended at entropy rate should be specified. Untrue positives alert might happen if this value is applied on ransomware detecting. That was not because the harmless encoding implements, but because of the many file formats that used compression methods. Compressed file might be statistical like to an encoded file and proceed to a wrong decision. Entropy calculation is depending on the investigation of the whole file, take a significant harm on CPU procedure. It also increases the pressure to the hard disk if the against malicious program investigates the contentment of entirely new adapted documents as a substitute of interrupting computer demands (Berrueta, 2019).

Folder Diversity: The encoded form of folder must not afford a little info about the unencoding information. After a folder was overwriting, a recent content compares to the previous content. This contrast needs interrupting the folder entree to computer demands. Uncertainty a folder was significantly altered, that will become a suspicious act because of a folder encoding. when ransomware is writing an encoded information to a diverse folder, that will be tough to compare reading information to writing information for contrast goal. Folder contrasts were disposed to activate untrue positives alert once a harmless software noticeably alters a file. These contrasts are united with entropy calculation since both variables need the investigation of file content (Berrueta, 2019).

FOLDER TYEP ALTERATION: Ransomware straining using a particular folder form to encoded documents. Ransomware family will make a novel file and rename the file, otherwise the ransomware overwritten the old folder and give it a new name otherwise alter a folder title form. The folder form will check by a record of identified extensions that used by ransomware. This is an easy process, not CPU exhaustive, and usually used by advertisement antiviruses programs. A folder title form considers as folder contain a data that describes the context of another value. they considered a folder title as data since it is unit of the data providing by the target at file construction and should be prevented opposite to ransomware activities. For instance, the file formation period is not dynamically providing by a target and frequently does not need prevention (Berrueta, 2019).

METADATA ENTREE EVIDENCE: entree to file metadata considers as any exploit that does not need file content. This info obtaining by interrupting file system demands, however it do not need to study the file data; consequently, fewer CPU period is essential for its calculation (Berrueta, 2019).

REGULARITY OF FILE SYSTEM DEMANDS: Most of analyzed ransomware chains try to encode a lot of files in limited period. They perform a form of common file system processes such as read, write, delete, or rename files. The time of these processes will obtain and analyze to differentiate the file entree form feature of ransomware activities (Berrueta, 2019). The study of this kind of data is popular to several anti-ransomware suggestions. The problem is the obligation of determining a regularity or form of file entree that differentiates between harmless and harmful software (Berrueta, 2019). This could be done by studying of preceding user file entree forms. In contrast, although that the popular user behavior might be diverse from the ransomware behavior, there is states somewhere in a limited time they might be alike. For instance, when users compressed a folder of files and eliminates the original files, the whole process may be considered as ransomware act from the behavior of occurrence of file processes and file removals (Berrueta, 2019).

AMOUNT OF OPENED DOCUMENTS: Ransomware attempts entering the whole target documents at the disk, otherwise minimum just the folders which has a file type specifies that are target files (for instance, a user will not make a payment to restore encoded functional program documents). The amount quantity of documents opened through the malicious software was huge in limited period. In contrast, operator activities were slow and do not change several documents in short amount of time. Yet, there are exemptions; for instance, a user might process a group of records used deletion program. Moreover, the exemptions to ransomware opening various documents in few minutes; for instance, if ransomware was encoding a huge folder otherwise the aforementioned tries to conceal its action via reducing their activities (Berrueta, 2019).

DIRECTORIES ACCESSED: Ransomware encodes target files from any folder and enters a huge number of routes. It usually starts by list the whole branch of files in a disk. It is rare that harmless software enters files from a huge amount of diverse folders; hence, this behavior distinguish between harmless and ransomware action (Berrueta, 2019).

CANARY FILES: Several of anti- malicious software erected documents at target folders. Those ‘‘canary’’ documents were observed via an observing means.

The target never supposed to enter those documents. If those documents were adapted, that because it's a consequence of damaging malicious software. accordingly, if the instrument recognizes the procedure that changed the file, it can alarm the target or stop the malicious software. To accomplish initial ransomware recognition, an anti- malicious software instrument will spread canary files through most of the folders including target files. Even though, it would not make just chaos to target folders, yet it needs observing the alteration of huge amount of files (Berrueta, 2019).

ROLE DEMANDS: The famous activities occupied in ransomware were connected to encoding and keys generating. System roles or library roles were intended for those functions. malware detecting program by monitoring a common usage that concerning a group of practical tasks in addition spot the procedure to undecided (Berrueta, 201). Cryptography secrets key is recognized in memory procedure due to its erection. Observing program could check procedure of disk search for key and notify the operator otherwise save a duplicate from it. The later choice is just beneficial in a situation where a idintical keys encoding otherwise shared keys encoding, where the decoding keys is existing in software. Use shared keys encoding, a secret keys is inaccessible to a target; consequently, even if a key might become placed in cash, and it might use for increase the alert, a decoding keys will never became accessible (Berrueta, 2019).

INFO PULL OUT FROM NET PACKITS OR TRANSIT: prevalent infected forms need Internet entry (electronic mail attaching documents and malevolent sites). Several ransomware examples have no need to extra net entree when contaminate a computer. Yet, furthermost ransomware series need Internet entree to work. They recover key from C&C servers, otherwise save local generating key in. Net Packets obtain at the affected computer or the locally net entry connection. Against-malicious programs analyze the traffics also distinguish ransomware act. If the act was preceding to info encoding stage, it could stop the ransomware earlier and the aforementioned would do a damaging activity. This is will be efficient if it stops the ransomware during that it will try to gain encoding keys in C&C servers to thwarts the malware from encoding documents. Afterward studying suggestions in works, they gathered a data that is found from traffic investigation to three sets. They also were built on studying of DNS inquiries, whereas the next includes huge quantity of variables that take out from net packets (Berrueta, 2019).

DISCOVERY OF DNS ENQUIRIES FOR CONSTANT TITLES

Ransomware programs could have or include the C&C server IP addresses in its binary; Yet, this was unusual action as it made it weak to net filters when those addresses were detected. An extra popular action is the active position of a C&C server built on the decision of a field name hard-cod in the ransomware binary. The title to address relative could be adjusted vigorously by an intruder to evade IP clarifying. This detecting method can stop ransomware earlier post it damaged files if the name resolve happens previous the encoding stage. Nevertheless, it needs to know the domain names to stop or prevent, that are pull out from the study of the ransomware acts in different servers or the study of its binary folder. So, it could not use in a zero-day situation(5).

Discovery of dns enquiries for vigorously produced tags: For ransomware families which practice a DGA (Domain Generator Algorithm), stopping the resolve of specific field tags is hopeless. The ransomware could try the resolve of loads of pseudo-random generator domain names previously, its discoveries a legal one. Nevertheless, the feature of transport a huge amount of DNS queries requesting for names that seems as a randomized batch of features which using to distinguish this kind of action. It is rare that an actual DNS tag will be random, since they are formed to be simply evoked by people. Statistics data is extracting from the domain names requests, and a grade of haphazardness in them could be distinguished. If the arbitrariness can be identified earlier post the ransomware resolutions a legal tag, after that it will stop previous it establishes eliminating documents. This could be a beneficial method in a zero-day situation since no need for removing data from an identified ransomware. Yet, this way seems the only method that is effective in contradiction of straining that use a DGA (Berrueta, 2019)).

Universal Traffic: A ransomware detecting algorithm could be used statistical data which pull out from net packets. Some means which consider a quantity of diverse IP addresses entered, the quantity of diverse server's port, and the quantity of period beginning of diverse applications layer rules. These variables could improve a verdict that is taking by a ML algorithm; nevertheless, they are does not use as the only input number. In business atmospheres, file depository is achieved through using network disk. various ransomware families are able of encoding files that kept on the links setted off dimensions in an infecting group. The net packets formed through read, write, besides destroy documents could use to ransomware discovery (Berrueta, 2019)).

Machine Learning Machine learning (ML): Contains knowledge the forms in information to generate a model. This model can then guess the result when fuel with new data. However, the struggle with ML is discovering a right procedure to equivalent with a category of information and a vital outcome. The good influence of ML is that it could precisely expect the result with suitable statistics. Trained statistics must be diverse with stable spreading of results to be expected. For the reason that ML includes knowledge of the form in the information, it is fewer likely to complication. The bad influence is to Find the right algorithm is frequently not clear and might need several rounds of experimental and mistake. Furthermore, biasing and over fitting might happen if suitable carefulness is not considered (Kok, 2019).

Honeypot: Honeypot includes set up trick documents for the ransomware to outbreak. When these documents are entered, the ransomware could be recognized. the advantage of the tricks or honeypot documents could be setting up, and then they just waited to be outbreak. Consequently, the method does not need care or process control from the system. The disadvantage is that there is no assurance that the honeypot documents going to be outbreak by a ransomware. As a result, it is vital to identify the features of documents that the ransomware going to outbreak (Kok, 2019).

PREVENTATION METHOD

Specialists give four commendations for people and organizations to thwart a ransomware infect and how to deal with it when it occurs (Richardson, 2017):

- **Back Up:** If the information is backing up, it's not necessary to make payment to restore information. As an alternative, it could be restored from the backups. Moreover, backups must to be up to date. Several ransomwares try to encode local linked backup systems, subsequently they must use one of these options making a cloud backup or a system that is just linked when the backup is made. In addition, it's a vital to retain various backups. In order to that ransomware is initial to postpone declaring itself. It encodes documents in the background, and those encoded documents are then substitute the recent backup, stopping that backup from actuality used to recover original documents (Richardson, 2017).

- **Evade Email Links and Attachments:** Phishing attacks are the popular method to distribute ransomware, thus evading click on links or open attachments in spam email will lead to avoid ransomware. Nevertheless, attackers initialized attack by compromising advertisement (adware) to distribute ransomware and its even targeting the most reliable websites. Ad stopper could defend versus adware. Closing Java and JavaScript it can be helpful too (Richardson, 2017).

- **Patch and Block:** Operating system, browsers, and safety software must keep patching and updated. Similarly, third-party plug-ins, such as Java and Flash, require keeping patching if they are permitted. Organizations system could depend on whitelist and limit operator privileges to decrease the fortuitous of a ransomware contagion. Furthermore, these phases will assistance to diminish different kinds of harmless software affections also. Regrettably, ransomware is continually developing to become step ahead of antiviruses software, because software by itself would not be enough to prevent an outbreak (Richardson, 2017).

- **Drop-and-Roll:** when first indicate of a contagion, the infested device must directly turn off to diminish the harm to documents. If it is linked to a network, admins must directly close the network to diminish the spread of the ransomware (Richardson, 2017).

DISCUSSION AND COMPARISON

There is no perfect way to detect the ransomware attack each way has its own characteristics and can be a huge help to discover this attack. Although that ransomware attack is always a step ahead in front of these ways but still it may detect it sooner or later. Most of these ways use data traffic monitoring such as the first two ways. Where is Ransomware Data Classification use traffic monitoring to observe the abnormal flow of data and catch the ransomware behavior to detect the attack. On the other hand, the ML use data mining to build a model that detect this attack. However, honeypot use a trick to deceive ransomware and discover it early.

Conclusion

These days a wide variety of users become a target of cyberattack movements, particularly that blackmailing users to get a ransom in exchange for their valuable files. To paraphrase it, users kept their vital documents in computers or clouds which makes these documents are weak to attackers exploitation. Ransomware is an attack where the attacker encodes the files or closes the system in exchange for payment which usually uses a bitcoin. Ransomware is one of the dangerous kinds of scareware to fight against. Moreover, it's tough to distinguish with classical means because it's developing very fast and changed continually which made it hard for antiviruses to realize it.

There are three recognition method can be precise to detect this outbreak which is organizing the network traffic and study it to excerpt the irregular behavior and extricate the ransomware. Furthermore, using machine learning methods to build a model for detecting this kind of attack is effective. Finally, using a honeypot to trick the ransomware and detect it earlier is one of the fastest ways. There are some thwarting techniques that can prevent this attack from occurring such as, making an up to date backups and evading clicking on email links and attachments.

REFERENCES

Akay, M. 2019. Detecting cryptographic ransomware by examining file system activity.

Alhawi, O.M., J. Baldwin, and A. Dehghantanha, 2018. Leveraging machine learning techniques for windows ransomware network traffic detection, in Cyber Threat Intelligence. Springer. p. 93-106.

Berrueta, E., *et al*., A Survey on Detection Techniques for Cryptographic Ransomware. IEEE Access, 2019. **7**: p. 144925-144944.

Continella, A., *et al*. ShieldFS: a self-healing, ransomware-aware filesystem. in Proceedings of the 32nd Annual Conference on Computer Security Applications. 2016.

Kok, S., *et al*., 2019. Ransomware, threat and detection techniques: A review. *Int. J. Computer Science and Network Security*, 19(2): p. 136.

Richardson, R. and M.M. North, Ransomware: Evolution, mitigation and prevention. *International Management Review*, 2017. 13(1): p. 10.

Scaife, N., *et al*. Cryptolock (and drop it): stopping ransomware attacks on user data. in 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS). 2016. IEEE.

Sgandurra, D. *et al*., Automated dynamic analysis of ransomware: Benefits, limitations and use for detection. arXiv preprint arXiv:1609.03020, 2016.

Thomas, J., *et al*. Enterprise Cybersecurity: Investigating and Detecting Ransomware Infections Using Digital Forensic Techniques. Thomas, JE, Galligher, RP, Thomas, ML, & Gallilgher, GC. 2019. Enterprise cybersecurity: Investigating and detecting ransomware infections using digital forensic techniques. Computer and Information Science, 2019. 12(3): p. 72-80.

****