RANSOMWARE: A SURVEY ON VARIOUS ATTACKS AND DEFENSE MECHANISMS

Gomathi S[1], K Anitha Kumari[2]
{mail2mathi86@gmail.com1, kak.it@psgtech.ac.in2}

Assistant Professor, CSE, Dr.N.G.P. Institute of Technology, Tamilnadu, India[1],Associate Professor, IT, PSG College of Technology, Tamilnadu, India[2]

Abstract. This paper examines various attacks and the techniques used in ransomware. Ransomware is a form of malicious software (malware) which make an alarm of revealing or denying access to the set of data or computer system, generally by encrypting them, waits till a ransom is paid by victim to the attacker. Ransomware attacks are all around normal nowadays. Cyber offenders attack an organization or a business or an individual those who come from all progress. Besides, a big part of the victims who pay the payment are probably going to experience the ill effects of rehash ransomware attacks, particularly in case it isn't cleaned from the framework. Ransomware was otherwise called "cryptoviral extortion," It is utilized to distinguish the weakness of the objective framework where there is the chance of malware attacks. Cryptowall-a ransomware attacker utilizes the methods ahead of time to penetrate PCs without knowing the person in question. The pernicious programming enters the PC by means of spam messages. Attackers have evolved progressively more innovative over time to time, demanding upgrades that are extremely impossible to track, which aids cybercriminals stay anonymous. In this paper, we look at the overall outline of various attacks and talked about the crypto-ware malware methodologies.

Keywords: Honeypots**,** Cryptoviral extortion**,** Crypto-ransomware, CryptoLocker, malware, malicious software.

1 Introduction

Ransomware is dangerous programming that makes the structure gets attacked and scramble the records set aside and keep them as a detainee. It is encryption, which uses keys to scramble and translate records. The assailants disclose private keys to hold the records, they make the private key open to the setback exactly when the result is paid [1]. Ransomware has transformed into a valuable business that has procured growing predominance among the aggressors. Even after the exclusion, ransomware seems to have an enduring effect that seems to be impossible to overcome the problem without the support of its creator. In any circumstance, the traveling cost and the initial expenses that businesses and individuals might pay as a down payment, such setbacks could lead to additional problems such as data loss, reputation, and maybe even death. [6].

Crypto-ransomware is a troublesome peril that calculates a customer's records while disguising the unscrambling key until a result is paid by the individual being referred to. This sort of malware is a beneficial business for cybercriminals, making an enormous number of

ICCAP 2021, December 07-08, Chennai, India

DOI 10.4108/eai.7-12-2021.2314607

dollars consistently [10]. The hole fills the detail and sets forward a novel ransomware scientific categorization, according to a few points of view. The elements that lead to a fruitful ransomware assault prior to talking about exhaustively the examination into checking ransomware, including investigation, counteraction, identification, and expectation arrangements [4].

Customary malware recognition strategies (e.g., measurable-based counteraction techniques) neglect to battle the developing Ransomware since they bring about a high level of bogus up-sides. To be sure, fostering a non-traditional, savvy strategy to defending against Ransomware is vital [18]. The crypto-ransomware encodes the loss' data, however, the capacity ransomware, locks the setback's PC, denying customers from getting to their structure [3]. SCADA works with the direction of remote access to real-time information and channels. It has an issue of robotized or driven administrative orders [13]. The control arrangement of most basic foundations like energy, force, water, fabricating plants, traffic signals, atomic plants is SCADA [14]. Looks at the security instruments that can be endeavored to perceive the ransomware practices on the site. If a phishing site is discovered, the detectives use honeypot testing to see if the target is a ransomware attack [19].

Ransomware identifying philosophy that is relying upon a developmental-based AI approach. The paired molecule swarm enhancement calculation, similarly highlight determination, has been used to adjust the hyperparameters of the arrangement data processing [18]. The absence of safety in gadgets associated with the IoT is making them hot focuses for digital crooks and the strength of botnet attacks has expanded radically. Botnets are the mechanical spines of innumerable attacks including Distributed Denial of Service (DDoS), SPAM, fraud, and authoritative spying [30]. Consistent ransomware attackers achieve to evade diverse security edges since its system relies upon the misleading of customers weakest spot in the security chain, which exhibit the clear planes of adequacy [12]. The life structures of ransomware are investigated from start to the end, as well as how they combine advancement with control, through well-considered planning, to meet their targets and compromise a considerable number of PCs [12]. Gatecrashers ought to be kept from such maltreatments of assets, and their malicious undertakings counterattacked. Among the least difficult strategies for holding intruders back from compromising servers and associations is the usage of standard security controls, similar to Interruption Anticipation Frameworks (IPS), firewalls, and against contaminations [16].

2 Malware Detection Methodology

Cryptoviral coercion is a covert kind of malware assault that catches the casualty's information by encoding it and undermining it by denying admittance to it until the casualty pays a payment. Casualties range from people to associations, government areas, makers, emergency clinics, and colleges [3]. Cryptoviral coercion first came in the extended period of 2005, later it was renamed "ransomware" by the media. The assault acquired worldwide VIP popularity in May 2017. When the malware WannaCry cryptoworm contaminated more than 200,000 laptops. Cryptoviral blackmail is seemingly the most pitched digital danger today [10].

Ali Shuja Siddiqui stated the collaboration of activities with the operational structure's Modifying interface (system calls) for malware requests is all that is considered in front malware recognition techniques. The author demonstrates that such methods are ineffective.

This study presents a point that is dismissed by the correct currently available approaches: Malware can interface to Windows and then provide the support needed to perform out all the appropriate action by replicating customer development [25]. In order to check against infection activities in Windows 10, a Phantom (ransomware exploits Customer copying for everything about malicious exercises) is written in C++. For testing purposes, various designers' programming is used. In any case, almost all failed. This dissertation explores the reasons why these activities failed, as well as the gauges that have been constructed against Specter Malware in perspective of the test results [27].

Crypto-ransomware isn't just encoded clients' documents, it endeavors to scramble any records situated on both planned and unmapped organization drives, making a solitary division or the whole association to a stop in the event that one framework gets tainted [29]. Above all, the article presents Customer Copying strategies for camouflaging malignant orders of malware as an imitated customer activity. The possibility of Spirit Malware will be exposed from that point forward: Customer Imitating is being used constantly by this malware to perform out all of its malicious activities [25].

Digital physical frameworks (CPS) are controlling various essential and tricky pieces of our real world while being perpetually introduced to advanced outbreaks. These structures typically have low level of execution, poor memory, and also have energy constraints, which limits their ability to perform the existing advanced malware protection, making them extremely difficult to get [29]. To address these issues, the above authors propose REMOTE, a more generous design for identifying malware by remotely seeing Electromagnetic (EM) signals are delivered by a device named electronic enrolling device (e.g., a chip) for running a known application, consistently and with low acknowledgment, and with little or no reasoned data on the malware [27].

Ransomware's impacts are permanent and difficult to solve even after malware have been removed from the system. REMOTE does not require any additional support or structure for the software's reliability, making it ideal for malware detection on resource-constrained systems such as embedded contraptions, CPSs, and Internet of Things (IoT) devices with limited technology and energy [29]. REMOTE's monitoring system is shown in Figure 1.

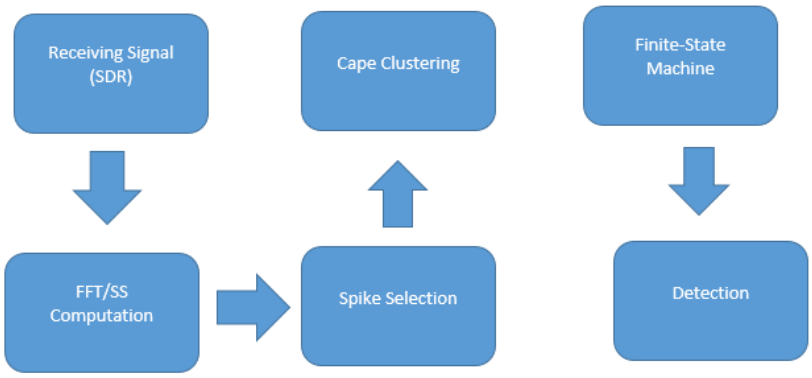

Figure 1: REMOTE's Monitoring system

Shell code-based DDoS and ransomware are designed to attack five distinct common programmes on an embedded system [27]. With an enormous extension in various flexible customers, compact perils are furthermore growing rapidly. Flexible malware can provoke a couple of organization insurance risks for instance taking fragile information, presenting optional entries, ransomware aggressors, and sending expense SMSs, etc [12].

Recent examinations have demonstrated that, due to the refinement of dangers and redesigned ways to avoid the region, only a small percentage of antivirus components are capable of identifying potential attacks. In any instance, by investigating traffic plans [30], Security layer gives an extra level on the association side which helps us to protect clients from high-level threats. A pair of controlled ML classifiers were developed in this employing educational records comprising named occurrences of association traffic characteristics caused by a couple of hazardous and damaging agents [1].

Because of the general gap in convenient malware and consumer popularity, this assessment's point of convergence is Android-based malware. Using the evaluation results, the model was capable of distinguishing between predictable and unpredictable threats with a precision of up to 99.4%. Traditional interference acknowledgement structures can also be used in this ML model to detect advanced threats and minimize false alarms [18].

3.Detection Techniques

Cryptowall is ransomware that utilizes diversion to encode records on a PC and requests that clients pay a payment to get access to an unscrambling key. Cryptowall enters a PC through a spam email, vindictive internet-based promotions, or one more type of malware. When executed, Cryptowall encodes all documents on the drive with explicit expansions and makes the records have a few directions of how to pay the payoff and get the decoding key. To prepare for Cryptowall, you need hostile to ransomware that can naturally keep clients from tapping on joins that may download the malware or opening connections that might contain malevolent code.

For encryption and decryption, the cryptographic methodology uses two distinct keys. The IDH collects large set of data from various sources alike Honeyfolder, SDN network and hosts, Audit Watch, and Firewall via CEP. The collected data is converted into several occurrences, which are later accessed by using aggregation rules for detecting malware activities, attack patterns, and respond fast. It is used to analyze and detect anonymous events received from complex datasets. For ransomware detection, a reliable IDH method is implemented. It exploits SoLA to implement the Honeyfolder for detecting ransomware activities with no subsequent data loss in post-attack circumstances. SoLA is the first algorithm to utilize a leopard's behaviour as a model. Which makes an efficient way of converting the data into variety of streams and consolidate them to learn about behaviour of ransomware. Designing multiple levels of security systems, like firewall, a honeypot (Dionaea), a honeyfolder, and an audit can help to make a proper decision.

Until now, a few examinations have been led to address this special, testing danger and have attempted to give discovery and avoidance arrangements. In any event, there is a lack of review publications that examine ransomware exploration initiatives and emphasize the problems and challenges addressed by existing approaches. It

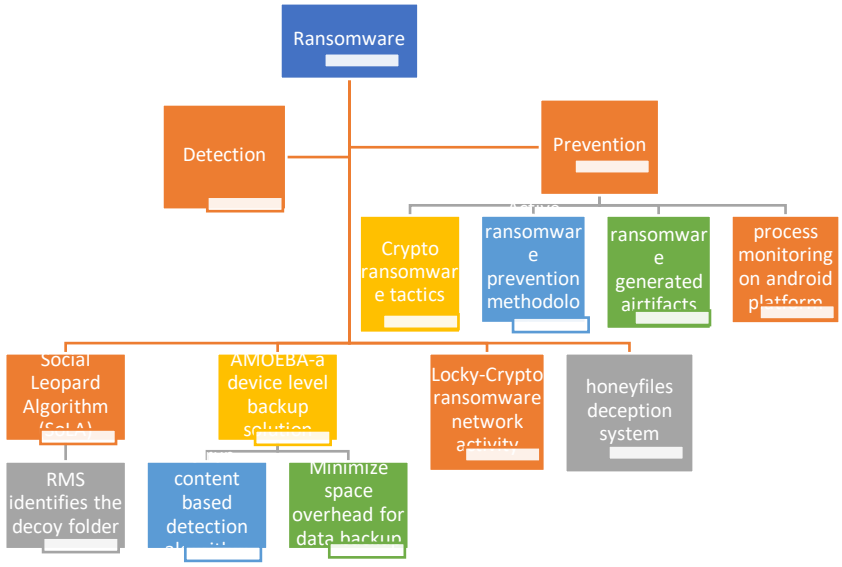

Fig 2. Ransomware prevention and detection strategies

addresses the gap by having a complete, up-to-date summary of the investigation into ransomware, its location, and mitigation. The review advances a novel ransomware scientific categorization, according to a few points of view. It then, at that point, expounds on the components that lead to fruitful ransomware attackers prior to talking about exhaustively the examination into checking ransomware, including investigation, avoidance, identification, and expectation arrangements. A review of ransomware prevention and detection strategies is shown in Figure 2. The review finishes up with a concise conversation on the open issues and potential exploration bearings soon.

The RARI module evaluates the risk of all pages and recommends whether or not to keep them in check. The NFA is graphically represented by states (Nodes) and state transition inputs (Edge). A free page's status transitions from OF to OV when it receives its first page write. Every overwrite request is analyzed by Amoeba's backup mechanism to make sure that the write request is in the method of a Read-After-Write design. Second, it examines if the current authorized page's RARI value exceeds the threshold value. Amoeba will treat it as a ransomware attack write request if both requirements are met (ransomware).

Scrambling malware is a ransomware that targets both small and large organisations, much like a typical home user. This author talks ransomware illness tactics, the innovation that supports them, and how they may be addressed with to avoid being the next victim. The efficiency with which a ransomware attack is been detected is highly dependent on how the actions are understood and how its characteristics are found.

4. Crypto-Ransomware Approach

Cryptowall is ransomware that utilizes diversion to encode records on a PC and requests that clients pay a payment to get access to an unscrambling key. Cryptowall enters a PC through a spam email, vindictive internet-based promotions, or one more type of malware. When executed, Cryptowall encodes all documents on the drive with explicit expansions and makes the records have a few directions of how to pay the payoff and get the decoding key. To prepare for Cryptowall, you need hostile to ransomware that can naturally keep clients from tapping on joins that may download the malware or opening connections that might contain malevolent code [3].Ransomware is sorted into a few kinds, the most destructive and forceful one as crypto-ransomware. The crypto-ransomware encodes the casualty's information, though the storage ransomware, locks the casualty's PC, denying clients from getting to their framework. Crypto ransomware isn't just encoded clients' documents, it endeavors to scramble any records situated on both planned and unmapped organization drives, making a solitary division or the whole association to a stop in the event that one framework gets tainted [1].

Hybrid Cryptosystem Ransomware scrambles the victim's documents with a gradually generated symmetric key and then encodes the symmetric key with a pre-stacked public key once it has been cleared from memory. Most current groups of crypto-ransomware utilize this strategy to exploit the two kinds of encryption [12]. The expansion of payment products that are based on predictability, for example, antivirus and hostile to malware, has demonstrated incapable of forestalling assaults. In this kind of assault, programmers introduce code on a phishing site that sidetracks to malignant destinations [19].

Current attackers are more forceful, they can sidestep most security devices. Servers are being compromised and records scrambled for emancipate. The use of a double-dealing framework based on honey files and honeytokens is presented to familiarize tiers of trickery frameworks with recognizing any interruption or ransomware attempting to access compromising sensitive records. One of the major deception methods offered to differentiate ransomware from gatecrashers is developed with a proof-of-concept execution [16].

Versatile malware can prompt a few network protection dangers for example taking delicate data, introducing secondary passages, ransomware attackers and sending premium SMSs and so on Past examinations have shown that because of the refinement of dangers and customized methods to stay away from the location, few out of every odd antivirus framework is equipped for distinguishing advance dangers [29]. The prevalence of ransomware is increasing as traditional recognition-based security, such as antivirus and anti-malware, has proven ineffective in preventing attacks. Furthermore, this form of virus is combining advanced encryption computations and expanding the range of document types it targets. Cybercriminals have discovered a lucrative industry, and no one is safe from being the next victim [10].

Ransomware attackers have found that the SCADA system is the most attractive and appealing target. The unsafe and malignant exercises of this malware are concentrated by breaking down the organization logs of the honeypot. In view of their properties and exercises, the malware is grouped. These groupings of malware and their conduct assist analysts with fostering a security system to keep an association from these sorts of destructive and pernicious exercises set off by the malware [26].

5. Ransomware Threat

Ransomware is malware that takes advantage of safety components, for example, cryptography to assume control over client records and related assets and requests cash in return for the locked information. Ransomware has also evolved into a profitable market with an increasing frequency among criminals. Ransomware is irreversible as it can be only removed by its developers. It gives the close watch of the files of an individual or an organization and encrypts them to make a hold of it. These may make the temporary or complete loss of data.

The review advances a novel ransomware scientific categorization, according to a few points of view. It then, at that point, expounds on the components that lead to fruitful ransomware attackers prior to talking about exhaustively the examination into checking ransomware, including investigation, avoidance, identification, and expectation arrangements. The review finishes up with a concise conversation on the open issues and potential exploration bearings soon.

6. Detection And Prevention Of Crypto-Ransomware

Crypto-ransomware is a difficult process which makes a client's records while screening the key until a ransom is paid by the person. Cyber attackers earn a large number of dollars every year in malware creation. The spread of malware leads to a normal security access, for example, antivirus and hostile to malware, has demonstrated insufficient forestalling assaults.

Attackers tracked down a many valuable markets in the industry and no individual are safe. Ransomware targets huge number of normal people and very low range of businesses and organizations. The author tells ransomware techniques for disease, innovation behind it, and how can be dealt with assistance, also investigates into most well-known kinds of crypto-ransomware, various techniques of infection, common crypto-ransomware behavior, strategies, how an attack happened, records that commonly focused on a victim's PC, and suggestions for avoidance and protections.

Steady ransomware attackers accomplish different security edges as the procedure depends on the clients most vulnerable security chain viability. It completely shows the life structures of ransomware and its innovation with control, design patterns. The recreations stages follow, passing an important rule of assessing the data with security, and then, generate approaches that lower the dangers of data loss.

7. Crypto-Ransomware Using Honeypot

Crypto ransomware is one of the difficult tasks which progress encryption calculations to hinder framework documents and request to decode the obstructed substance with the key. In this kind of assault, programmers introduce code on a phishing site that sidetracks to malignant destinations. The security instruments that can be attempted to recognize the ransomware exercises on the site. If there should arise an occurrence of a phishing site, the analysts try to find whether the goal is ransomware type of attack by using a honeypot examination. The test results give the achievability and improved execution in understanding ransomware exercises. Attacks occurred in different sectors is presented in Figure 3.

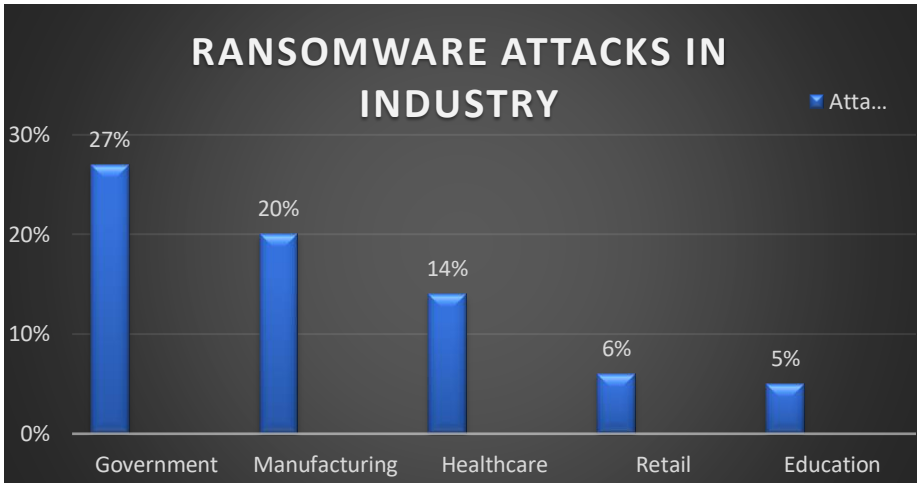

Fig 3. Ransomware attacks in Industry

The development of the web and clients has expanded dramatically and definitely in this decade. It offers types of assistance acquiring different advantages to the clients like web-based banking, advertising, purchasing/selling and different office the board administrations and so forth It draws in certain individuals to foster projects that perform different malignant exercises deliberately or unexpectedly like taking delicate data from PC, showing commercial, causing destructive, undesirable exercises. The vindictive programming alludes to malware, infections, worms, spyware, Trojans, adware and botnets are additionally malware.

The unsafe and malignant exercises of this malware are concentrated by breaking down the organization logs of the honeypot. In view of their properties and exercises, the malware is grouped. These groupings of malware and their conduct assist analysts with fostering a security system to keep an association from these sorts of destructive and pernicious exercises set off by the malware.

8. Conclusion

The crypto-ransomware encodes the loss data, however, the capacity ransomware,locks the setback's PC, denying customers from getting to their structure. It then explores into the components that contribute to an effective ransomware attack before persuading users to properly assess malware, including investigation, aversion, differentiating proof, and assuming game plans. Examining the widely recognized types of crypto-ransomware, how an attack happened and how it has been recorded. One of the major dishonesty techniques offered to identify ransomware and gatecrashers is put to the test in this proof of concept. Here it inspects the security instruments that can be endeavored to perceive the ransomware practices on the site. Results discussed in this work show that cryptographic keys can be found during encryption in the ransomware cycle memory for terms adequately long to work with complete data recuperation. It examines the reasons why these activities failed their methods, as well as the evaluations

that have been made about the Specter Malware in view of the test results. The authors set up a honeypot to catch zero-day attackers and malware.

The IDH utilizing CEP gathers a lot of information from different sources, for example, Honey folder, SDN organization and hosts, Firewall, Review Watch. It then converts the collected data into events and cycles the collected events in the CEP motor using the aggregation rules to find malware behaviour, how those collected events will be processed in the techniques of IDH utilizing methods. For ransomware detection, a powerful IDH is used. It uses SoLA to execute the Honey folder for detecting ransomware attacks, with no further loss of client data in post attack situations. According to a handful of viewpoints, the survey promotes a unique ransomware logical categorization.

References

[1] S.SibiChakkaravarthy, D.Sangeetha, Meenalosini Vimal Cruz, V.Vaidehi; Balasubramanian Raman, Member, IEEE, "Design of Intrusion Detection Honeypot Using Social Leopard Algorithm to Detect IoT Ransomware Attacks", September 14, 2020, IEEE Vol. 8, 2020.

[2] Adam L. Young; Moti Yung "On Ransomware and Envisioning the Enemy of Tomorrow", 09 November 2017, IEEE, Volume: 50, Issue: 11.

[3] Ahmad O. Almashhadani; Mustafa Kaiiali; Sakir Sezer; Philip O'Kane," A Multi-Classifier Network-Based Crypto-Ransomware Detection System: A Case Study of Locky Ransomware", 26 March 2019, IEEE, Volume: 7.

[4] Bander Ali SalehAl-rimyMohd AizainiMaarofSyed Zainudeen MohdShaid, "Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions", 10 January 2018, Elsevier, Volume 74, May 2018, Pages 144-166.

[5] Donghyun Min; Yung-woo Ko; Ryan Walker; Junghee Lee; Youngjae Kim, "A Content-based Ransomware Detection and Backup Solid-State Drive for Ransomware Defense",26 July 2021 IEEE.

[6] Muna Al-Hawawreh; Frank den Hartog; Elena Sitnikova, "Targeted Ransomware: A New Cyber Threat to Edge System of Brownfield Industrial Internet of Things", 01 May 2019, IEEE Volume: 6, Issue: 4, Aug. 2019.

[7] Bander Ali Saleh Al-Rimy; Mohd Aiziani Maarof; Mamoun Alazab; Fawaz Alsolami; Syed Zainudeen Mohd Shaid; Fuad A. Ghaleb. "A Pseudo Feedback-Based Annotated TF-IDF Technique for Dynamic Crypto-Ransomware Pre-Encryption Boundary Delineation and Features Extraction", 29 July 2020, IEEE Volume: 8.

[8] Donghyun Min; Donggyu Park; Jinwoo Ahn; Ryan Walker; Junghee Lee; Sungyong Park; Youngjae Kim Amoeba: "An Autonomous Backup and Recovery SSD for Ransomware Attack Defense", 28 November 2018, IEEE Volume: 17, Issue: 2, July-Dec. 1 2018.

[9] Nitin Naik; Paul Jenkins; Nick Savage, "A Ransomware Detection Method Using Fuzzy Hashing for Mitigating the Risk of Occlusion of Information Systems", Oct. 2019, IEEE.

[10] Daniel Gonzalez; Thaier Hayajneh, "Detection and prevention of crypto-ransomware", Oct. 2017, IEEE.

[11] Jaime Ibarra; Usman Javed Butt; Anh Do; Hamid Jahankhani; Arshad Jamal "Ransomware Impact to SCADA Systems and its Scope to Critical Infrastructure ", Jan. 2019, IEEE.

[12] Pablo L. Gallegos-Segovia; Jack F. Bravo-Torres; Víctor M. Larios-Rosillo; Paúl E. Vintimilla-Tapia; Iván F. Yuquilima-Albarado; Juan D, "Social engineering as an attack vector for ransomware", Oct. 2017, IEEE.

[13] Abdulrahman Alzahrani; Ali Alshehri; Hani Alshahrani; Raed Alharthi; Huirong Fu; Anyi Liu; Ye Zhu, "Randroid: Structural Similarity Approach for Detecting Ransomware Applications in Android Platform", May 2018, IEEE.

[14] Muna Al-Hawawreh; Elena Sitnikova, "Leveraging Deep Learning Models for Ransomware Detection in the Industrial Internet of Things Environment", Nov. 2019, IEEE.

[15] Manoj Basnet; Subash Poudyal; Mohd. Hasan Ali; Dipankar Dasgupta, “Ransomware Detection Using Deep Learning in the SCADA System of Electric Vehicle Charging Station”, Sept. 2021, IEEE.
[16] Ahmed El-Kosairy; Marianne A. Azer,” Intrusion and ransomware detection system”, April 2018, IEEE.
[17] Alfredo Cuzzocrea; Fabio Martinelli; Francesco Mercaldo, “A Novel Structural-Entropy-based Classification Technique for Supporting Android Ransomware Detection and Analysis”, July 2018, IEEE.
[18] Iman Almomani; Raneem Qaddoura; Maria Habib; Samah Alsoghyer; Alaa Al Khayer; Ibrahim Aljarah; Hossam Faris, “Android Ransomware Detection Based on a Hybrid Evolutionary Approach in the Context of Highly Imbalanced Data”, 07 April 2021, Volume: 9, IEEE.
[19] J. Venkatesh; V. Vetriselvi; Ranjani Parthasarathi; G. Subrahmanya V.R.K. Rao, “Identification and isolation of crypto-ransomware using honeypot”, Dec. 2018, IEEE.
[20] Meet Kanwal; Sanjeev Thakur, “An app based on static analysis for android ransomware”, May 2017, IEEE.
[21] Wanping Liu, “Modeling Ransomware Spreading by a Dynamic Node-Level Method”, 04 October 2019, Volume: 7, IEEE.
[22] Ankita; Shalli Rani, “Machine Learning and Deep Learning for Malware and Ransomware Attacks in 6G Network”, July 2021, IEEE.
[23] Pranshu Bajpai; Richard Enbody, “Memory Forensics against Ransomware”, June 2020, IEEE.
[24] Ali Shuja Siddiqui; Chia-Che Lee; Fareena Saqib, “Hardware-based protection against malware by PUF based access control mechanism”, Aug. 2017, IEEE.
[25] Tim Niklas Witte, “Phantom Malware: Conceal Malicious Actions from Malware Detection Techniques by Imitating User Activity”, 04 September 2020, Volume: 8, IEEE.
[26] Vasu Sethia; A Jeyasekar, “Malware Capturing and Analysis using Dionaea Honeypot”, Oct. 2019, IEEE.
[27] Nader Sehatbakhsh; Alireza Nazari; Monjur Alam; Frank Werner; Yuanda Zhu; Alenka Zajic; Milos Prvulovic, ”REMOTE: Robust External Malware Detection Framework by Using Electromagnetic Signals”, 07 October 2019, Volume: 69, Issue: 3, IEEE.
[28] S Mochamad Julian to; Rinaldi Munir, “Intrusion detection against unauthorized file modification by integrity checking and recovery with HW/SW platforms using programmable system-on-chip (SoC)”, March 2018, IEEE.
[29] Sanjay Kumar; Ari Viinikainen; Timo Hamalainen, “Machine learning classification model for Network-based Intrusion Detection System”, Dec. 2016, IEEE.
[30] Maryam Al-Janabi; Ahmad Mousa Altamimi, “A Comparative Analysis of Machine Learning Techniques for Classification and Detection of Malware”, Nov. 2020, IEEE.