Research Article

IoT Contact: A Strategy for Predicting Contagious IoT Nodes in Mitigating Ransomware Attacks

Mohammed Ibrahim[1], Mohd Taufik Abdullah[2], Azizol Abdullah[3], Thinagaran Perumal[4]

[1,2,3,4]Faculty of Computer Science and Information Technology, Universiti Putra Malaysia
[1]mibrahima47@gmail.com

Article History: Received: 10 November 2020; Revised: 12 January 2021; Accepted: 27 January 2021; Published online: 05 April 2021

Abstract: Although the emergence of the Internet of Things (IoT) can facilitate various aspects of people's lives, most IoT devices are vulnerable to ransomware attacks. Ransomware attacks in IoT networks can be more devastating due to its capability of affecting billions of interconnected devices. Ransomware can take control of compromised devices or an overall system and allow limited access to user interaction with IoT devices. Hence, there is a need for a strategy that can mitigate and predicts affected IoT devices to conduct in-depth forensic analysis in the event of a ransomware attack. This paper critically analyzes ransomware in IoT platforms and proposes IoT Contact. IoT Contact can formulate the mathematical model based on the interaction of multi hop IoT devices and its relationship with ransomware. Consequently, it is expected that IoT Contact can predict and classify affected IoT nodes into susceptible, compromise and resistible from the huge number of connected devices in the event of ransomware attacks. Therefore, the scope and the size of the object of forensic interest can be foreseen in preparation of an investigation.

Keywords: Internet of Things (IoT), Ransomware, Mathematical, Investigation.

1. Introduction

Advancement in sensing and hardware technologies have revolutionized computer systems to more easily perceive physical environment. Consequently, interconnection of embedded digital devices including smart objects into our physical environment bring about novelty in internet technology known as "Internet of Things" or IoT. IoT technology is accompanied with significant benefits, including among others, implanted medical devices, networked-cars and smart grids system. Although the emergence of IoT can facilitate various aspects of people's lives, most IoT devices are vulnerable to ransomware attacks (Yaqoob et al., 2017). As critically explained in their work, ransomware may take control of the overall user data or network system and provides limited access for users to interact with their devices (Yaqoob et al., 2017). In most ransomware attack, users data can be recovered after successful payment of ransom, otherwise the payment period or the ransom amount will be extended at the expense of the affected data (Nassi et al. 2017) and (Hussain et al., 2015).

Cases of ransomware are becoming worrisome, between 2005 to 2016, about 7600 ransomware cases were reported by Internet Crime Complaint Centre (IC3). Although ransomware cases are becoming a source of worry, the mode of its propagation was not on alarming. This is due to the fact that ransomware propagation relied on the number of connected devices. However, with the advancement in sensor technology and ever-increasing amount of connected IoT devices, the propagation of ransomware by hackers and attackers in IoT infrastructure will be alarming. Consequently, hackers and attackers can take advantage of billions of connected devices in IoT platform and launch ransomware attack (Yaqoob et al., 2017).

As part of suggestions to mitigate the menace of ransomware attacks, device users must be train to restart, switch off and upgrade device firmware. Another suggestion is the deployment of layered defense strategy, in which ransomware are to be scan at multiple layer of a network (Castilho et al., 2017), (Hussain et al 2020) and (Stewart et al., 2017). Also, a team of dedicated cyber security experts are required to periodically scan the entire IoT network traffic and perform in-depth forensic analysis (Yaqoob et al., 2017). All the aforementioned suggestions can provide a means of preventing ransomware attack; however, we argue that they are not sufficient to handle ransomware attacks in a large and dynamic network infrastructure like IoT.

Ransomware attacks differ in nature, similarly operations in IoT network is highly dynamic with no standardize network protocol. Also, the vulnerabilities of IoT devices are well pronounce compared to traditional network devices (S.V. Manikanthan et al, 2020). Therefore, attackers can devise a multiple approach for achieving a successful ransomware attack against IoT platform. As mentioned earlier, ransomware attack on IoT devices can be more devastating do to its capability of affecting large number of connected devices. Therefore, for in-depth forensic analysis and before the application of control strategy against ransomware in an IoT based infrastructure, it is important to predict not only the transmission rate of the ransomware and the number of

expected infected or compromised devices. But to develop a practical yet mathematical model that can model uncertainty to estimates key transmission parameters, gain insight to the contributions of different transmission pathways and generate long- and short-term forecasts of ransomware attack in an IoT based infrastructure. However, to the best of our knowledge, the existing studies does not consider key transmission parameters in modeling the transmission rate of ransomware attack as well as the number of expected devices that can be affected by the attack. The rest of the paper is organized as follows. section 2 discussed related work, while section 3 and 4 discussed threats of ransomware attacks and the ransomware penetration in IoT network respectively. Section 5 and 6 are the main contributions of this paper that discussed about the two objectives namely: IoT contact that describes the interaction among various parameters in an IoT multihop network environment and the mathematical model that consider key parameters in predicting the transmission rate of ransomware and forecasting the expected number of the affected devices respectively. Section 7 describes a case studies that justify the applicability of the model. The acknowledgement and conclusions close the article.

2. Related Works

Being a serious security issue, history of ransomware and general information is critically analysed by Gazet (2010) and its evolution between 2006 and 2014 was discussed in Kharraz et al., (2015). While information about ransomware remain important, Luo and Liao (2007) outlined some preventive measures against ransomware and how computer system will be protected from the threat of ransomware attack.

Ransomware threats also penetrate android and other mobile devices. Andronio et al., (2015) critically analyzed the properties of android ransomware and proposed a mobile-specific indicator for compromised android devices. Sgandurra et al., (2016) proposed Elderan which can be used in analyzing and distinguishing ransomware based on the set of executable actions of the applications in their installation phase. Mercaldo et al., (2016) approach ransomware family detection using three steps techniques in an android based application. However, weaknesses in evading static malware detection can similarly affect the three steps techniques.

With the emergence threat in IoT platform, Yaqoob et al., (2017) examined the rise and the basic working of ransomware within the context of IoT network. To detect ransomware attacks in IoT based applications, Azmoodeh et al., (2018) proposed machine learning technique that detects ransomware based on the pattern of power usage of an IoT nodes. The proposed technique divides device's power usage into sub-units, classifies them and aggregates outputs to enhance the detection rate of ransomware in an Android device.

The prevention of ransomware attack on the platform of IoT network was the focus of Koopman (2017). Koopman (2017) analyzed the infection and spreading of ransomware on IoT platform. The analysis involves attack vectors, computer worms and resources of IoT devices, building a proof of concept and creating a model of the number of infections overtime. However, we argue that the model should consider key transmission parameters and different transmission pathways.

In this paper, we proposed an IoT contact based on the concept of epidemiological concept that considers multihop IoT network and key transmission parameters in building model that can predict the susceptible, compromised and resistible IoT nodes along a connected path.

3. Ransomware Attack Threats to Iot Network

Whenever ransomware attack is mentioned, what usually comes to the mind of the users is the hijacking of user's data for the payment of money. However, in IoT platform, ransomware attacks can lead to the hijacking of both user's data and the device's functionality. In recent times, it has shown that IoT devices like thermostat was hacked by Tierney and Munro. The essence of hacking the thermostat was not for malicious or financial gain, it was just for the purpose of research. The researchers downloaded the exploitable ransomware bugs from an undisclosed bug in an IoT application and reported the vulnerability to the thermostat vendor (Yaqoob et al., 2017).

In 2015, security researchers of Trend Micro developed a Flocker, Flocker is a locker ransomware that penetrates smart TV systems. The ransomware was encapsulated in a fake movie screen application and install at the point of activation in a smart TV. The threats of Flocker doesn't stop at locking up the smart TV screen, it further denies users from using the factory reset options. Finally, Flocker demands the sum of $500 USD with a strict deadline of three days (Yaqoob et al., 2017).

In similar trends, cyber security researchers repackage an Android Simplocker within an Android wear

project. They findings shows that Android Simplocker can lock the display of android wearable device (Yaqoob et al., 2017).

In their work, Nassi et al., (2017) established a fact that ransomware can infiltrate business through the exploitation of IoT devices and office equipment. To proof their assertion, ransomware was injected into the organization network through light that was transmitted into flatbed scanner. The scanner was exploited as a covert channel that served as a gateway to convey the ransomware attacks. The attack was then performed in three stages: first, was the placing of laser device in a clear sight with the scanner. Second, the attackers used a drone to launch the attack using an onboard laser device. Finally, the internal smart bulb was hacked using an Android device from a nearby car.

Therefore, despite that the ransomware attack is not well prevail in an IoT platform, the proof of concept shows that ransomware can be brutal and silently control the entire IoT network in an organization (Yaqoob et al., 2017).

4. Penetration of Ransomware into IoT Network

Despite that ransomware attack differ in nature, the dynamic nature of IoT devices and its network will likewise force attackers to diversify their attack vectors. Attack vectors can be of the form of exploitation of weak or default password. For default password, it is mean that the device requires certain level of authentication, in this regard, connection has to be made to this device. Also, computer system traditional attack vectors can be exploit by hackers to transmit ransomware into IoT network. In this regard, traditional malware can penetrate computer system through:

4.1 Acceptance without Reading

Malware can be transmitted to computer system by deceiving users, a user can get prompt while browsing the internet or plug-in appear that must be run to view some file contents. If the user accepts the prompt, the computer system will automatically get infected. Such infection can transmit malware or ransomware to computer or IoT network in (Koopman, 2017)

4.2 Downloading infected Software

Cyber criminals usually deceive users by compromising their websites and provide them with fake updates. Although the user will be thought that the downloaded update is original but is malware or virus that can infect and lock user's data for ransom in (Koopman, 2017)

4.3 Wearable Malware

Wearable devices tend to connect to many devices since their travel along with users. Therefore, things like smart watches and glasses are highly vulnerable and can be exploit to spread malware in (Koopman, 2017).

4.4 Content Delivery Network and Malvertisement

Internet traffic can be exploited as a means of distributing massive ransomware when a malware is embedded in a multimedia internet traffic (Cabaj et al., 2018). Hackers can intercept CDN traffic from front-end of IoT devices and insert ransomware to hold the CDN traffic using back-end cache servers and onboard memory of IoT devices. Also, malvertisement can be used to trap IoT devices using CDN traffic. Attackers can advertise illegitimate material that contains malware through CDN traffic. If the users mistakenly install on their devices, it will automatically compromise the device and the user's data (Yaqoob et al., 2017).

4.5 Ransomware as-a-Services

Over dependency of IoT devices on applications services and data center give room for attackers to intercept device-cloud traffic and embed ransomware. For the device at the end, the traffic will transmit the ransomware as a subscribed service to the end IoT device. When the IoT device run the subscribed service with the content of the ransomware, the entire IoT network can be under the threat of ransomware attack.

However, in any case, for successful ransomware attack against IoT network, the dynamic nature of IoT network require attackers to know the controlling device that can be compromise and penetrate the entire

network (Yaqoob et al., 2017). Therefore, knowledge of the IoT network is essential for any successful attack, the higher the knowledge of the network by the attacker, the higher the probability of ransomware attack.

5. IoT Contact

IoT contact is a strategy developed in this paper to examine the preconditions elements in predicting the spreading of attacks in an IoT based infrastructure. The proposed IoT contact was inspired from contact tracing strategy widely used in predicting and controlling disease outbreak by public health practitioners (Clémençon et al., 2008). However, for the IoT network, once a specific IoT node identify as compromise, IoT contact will be employ to predict the remaining compromised nodes from the multihop IoT network. In a multihop IoT network, some nodes are considered powerful than the others and are referred to as trusted sources that store all available routing paths to the sink node Liu et al., 2018). For an attacker with the knowledge of the trusted or powerful devices in an IoT network, attacking such devices will jeopardize the entire IoT network.

Based on their work, Liu et al. (2018) consider trusted devices as those devices that periodically send sequence of probe messages to the sink node over many (or all) the available path to identify intermediate malicious nodes. A sink can be referred to as the destination node D of which in between, malicious nodes can be identify from the trusted source S (Liu et al., 2018). To identify malicious nodes, N is assumed to be the number of nodes assisting in multihop data transmission between S and D. To transmit data between S to D, there would be a multiple paths Np that contains various relay nodes with the assumption that each node has a communication range of radius r. For (1…N), $\exists R_i \in (1...N)$ such that if Ri is compromised, they will be a probability Pi that Ri will send a modified packets Mp to the remaining nodes. Since one of our aim is to determine the transmission rate of the attack Tr, Tr is given in Eq. [1] below:

$$T_r = \frac{Mp \times N_p}{N+(N \times r)} \quad [1]$$

Since we determined the transmission rate of the attack from equation [1], we will then determine the number of suspected and infected nodes (Ed). For S to communicate to D, multiple packets will be sent along multiple paths over a period of time (t). Along these paths, both modified packets (Mp) and unmodified packets (M'p) are send across multiple nodes (1…N) at a given time t. At any given node, there would be a probability Pi that the received packet is (Mp) or a probability P' = 1-Pi that the received packets is M'p or both.

5.1 Basic Assumption on IoT Contact

Given that the attacker has the knowledge of the trusted or controlling device R_i. If R_i is compromised, R_i will launch routing attack by sending modified packet M_p. Our assumption is as follows:

- All the connected nodes along the connected paths between the compromised node Ri to the destination node D are considered to be susceptible nodes(S). The probability of susceptible that will randomly get contact by a compromised node Ri is (S/N), they will likely turn the susceptible nodes into compromised node;
- Also, some susceptible nodes that are equipped with antivirus and other anti-malware can proof resistance against compromised nodes by destroying the modified packets Mp upon receive from compromised node R_i at a rate θ.

5.2 Mathematical Formulation

IoT Contact is aimed at modeling three classes of affected IoT devices. These classes include the following:

I. Susceptible IoT nodes
II. Compromised IoT nodes
III. Resistible IoT nodes

Susceptible nodes can be converted to compromise nodes when the probability (P) of contacting modified packets Mp received from compromised nodes Ri along a connected path (p) over a period of time t is successful. Also, susceptible nodes with strong antivirus can resist the attack using the antivirus parameter θ. this can be expressed in Eq. [2].

$$\frac{dS}{\partial t \partial P} = -PSR_i - \theta(S) \quad [2]$$

Compromised nodes consist of nodes that have undergone any of the methods described in section 3 or otherwise, these methods can be associated with a parameter (β) and any susceptible nodes that converted to a

compromised nodes along a connected path p over a period of time t. Mathematically, it can be expressed using Eq. [3].

$$\frac{dR_i}{\partial t \partial p} = -PSR_i + \beta(N - S) - \theta R_i \quad [3]$$

Resistible nodes (R) combine the susceptible nodes and any other nodes that are equipped with antivirus or any other security mechanisms that have resistance against Mp based on a given parameter(θ) as can be expressed in Eq. [4].

$$\frac{dR}{\partial t \partial P} = \theta(S + R_i) \quad [4]$$

Therefore, determining the parameters (Mp, β, θ), is a key factor to successful application of the mathematical models towards the mitigation of ransomware in an IoT platform.

5.3 IoT Contact: Application to Ransomware

Referring to the proof of concept in (Koopman, 2017), two virtual assistant runs on a Raspberry Pi and uses the Google Assistant API to answers questions. The method for spreading the ransomware is default password, this is due to the fact that virtual assistant toolkit doesn't require users to change the password. Therefore, virtual assistant being the most powerful device in which many IoT devices relied in a network, compromising virtual assistant has the capability of affecting the entire devices on the network. Hence our attack scenario can be outline as follows:

- Compromising powerful node (virtual assistant) Ri = virtual assistant, compromised by a parameter β = (default password). Then, chain of nodes connected to Ri are said to be susceptible nodes denoted by (S).
- Infecting susceptible nodes (other Pi): Being in contact with virtual assistant, susceptible nodes are prompt to get infected, based on the proof of concept, susceptible nodes can get infected by installing sshpass package. To install the sshpass package, the first line of the script will be modified by adding sshpass command and it will be automatically installed on other Pi device (Koopman, 2017) (therefore, modified packet (Mp) = sshpass).
- Resistible susceptible nodes(R): Resistible susceptible nodes are nodes that are equipped with strong authentication mechanism other than default password and with any intrusion detection system. These two security mechanisms can stop the spread of ransomware against other nodes. The parameter θ can be determine and evaluate based on the type of security mechanisms.
- Quantifying the parameters (Mp, β, θ): By taking the parameters as Mp, = sshpass, β = (default password) and θ = security mechanism. To quantify their respective values, fuzzy logic will be employed to determine how frequent sshpass and default passwords are exploited among other vulnerabilities to attack IoT devices. For θ, to determine its value, we ranked security mechanisms on the basis of its strength, the higher the strength the higher the value of θ vice versa. The values of these parameters are to be substituted into equation (2), (3) and (4) and the solution of the differential equations will be solved.

6. Expected Result

Obtaining the values of the parameters and determining the solution of Eq. [2], [3] and [4] will enable investigators to predict the compromised nodes, infer the susceptible nodes and determine the resistible nodes. Consequently, scope and the size of object of forensic (OOF) can be infer from the large number of devices connected to IoT infrastructure. Therefore, forensic investigators can conduct what is termed "search and seizure" within shortest period of time.

7. Conclusion

IoT devices are vulnerable to ransomware attacks and ransomware attacks in IoT network can be more devastating due to its capability of affecting billions of interconnected devices. Hence, there is need for strategy that can mitigates and predicts affected IoT devices in order to conduct in-depth forensic analysis at the event of ransomware attack. In this paper critical analysis of ransomware attack on IoT network is performed and IoT contact is proposed. IoT contact is a strategy that can formulate mathematical models and predicts susceptible, compromised and resistible IoT nodes at the occurrence of ransomware attack. Therefore, with the adoption of IoT contact as a strategy in mitigating malicious nodes in IoT platform, investigators can distinguish among various classes of nodes maliciously affected during the attack. It is expected that IoT contact will predict the susceptible, compromised and resistible nodes for in-depth forensic analysis.

8. Acknowledgment

We acknowledge that this research received support from the Faculty of Computer Science and Information Technology, Universiti Putra Malaysia and the Fundamental Research Grant Scheme FRGS/1/2019/ICT03/UPM/02/1 awarded by Malaysian Ministry of Education.

References

1. Andronio, N., S. Zanero, and F. Maggi. 2015. Heldroid: Dissecting and detecting mobile ransomware. in International Symposium on Recent Advances in Intrusion Detection. Springer.
2. Azmoodeh, A., A. Dehghantanha, M. Conti, and K.-K.R. Choo. 2018. Detecting crypto-ransomware in IoT networks based on energy consumption footprint. Journal of Ambient Intelligence and Humanized Computing, 9(4): 1141-1152.
3. Cabaj, K., M. Gregorczyk, and W. Mazurczyk. 2018. Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics. Computers & Electrical Engineering, Vol(66): 353-368.
4. Castilho, S.D., E.P. Godoy, T.W. Castilho, and F. Salmen. 2017. Proposed model to implement high-level information security in internet of things. In 2017 Second International Conference on Fog and Mobile Edge Computing (FMEC). IEEE, 165–170.
5. Clémençon, S., V. Chi Tran, and H. De Arazoza, 2008. A stochastic SIR model with contact-tracing: large population limits and statistical inference. Journal of Biological Dynamics, 2(4): 392-414.
6. Gazet, A. 2010. Comparative analysis of various ransomware virii. Journal in computer virology, 6(1): 77-90.
7. Hussain, A., Manikanthan, S.V., Padmapriya, T., Nagalingam, M. (2020). Genetic algorithm based adaptive offloading for improving IoT device communication efficiency. Wireless Networks, 26 (4), pp. 2329-2338.
8. Hussain, A., Abubakar, H.I., Hashim, N.B. (2015). Evaluating mobile banking application: Usability dimensions and measurements. Conference Proceedings - 6th International Conference on Information Technology and Multimedia. ICIMU 2014, art. no. 7066618, pp. 136-140.
9. Kharraz, A., W. Robertson, D. Balzarotti, L. Bilge, and E. Kirda. 2015. Cutting the gordian knot: A look under the hood of ransomware attacks. in International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. Springer.
10. Koopman, M. 2017. Preventing Ransomware on the Internet of Things. [Online]. Available: https://pdfs.semanticscholar.org/419f/ 8d22ba3eea1f4d9fbcd6b3b68d294504d276.pdf
11. Liu, X., M. Abdelhakim, P. Krishnamurthy, and D. Tipper. 2018. Identifying malicious nodes in multihop iot networks using diversity and unsupervised learning. In IEEE International Conference on Communications (ICC). IEEE. pp. 1-6.
12. Luo, X. and Q. Liao, Awareness education as the key to ransomware prevention. 2007. Information Systems Security, 16(4): 195-202.
13. Mercaldo, F., V. Nardone, A. Santone, and C.A. Visaggio. 2016. Ransomware steals your phone. formal methods rescue it. In International Conference on Formal Techniques for Distributed Objects, Components, and Systems. Springer, pp: 212-221
14. Nassi, B., A. Shamir, and Y. Elovici. 2017. Oops!... I think I scanned a malware. arXiv. https://arxiv.org/abs/1703.07751.
15. Sgandurra, D., L. Muñoz-González, R. Mohsen, and E.C. Lupu. 2016. Automated dynamic analysis of ransomware: Benefits, limitations and use for detection. arXiv preprint arXiv:1609.03020.
16. Stewart, C.E., A.M. Vasu, and E. Keller. 2017. Community Guard: A crowdsourced home cyber-security system. In Proceedings of the ACM International workshop on security in software defined networks & network function virtualization. ACM, pp: 1-6
17. S.V. Manikanthan, T. Padmapriya. An Efficient based Routing Protocols in Forecast Model for MANET – IoT. Solid State Technology. Vol. 63 No. 3 (2020).
18. Yaqoob, I., E. Ahmed, M.H. ur Rehman, A.I.A. Ahmed, M.A. Al-garadi, M. Imran, and M. Guizani. 2017. The rise of ransomware and emerging security challenges in the Internet of Things. Computer Networks, 129. pp: 444-458.