Detection and Avoidance of Ransomware

[1]S.Mahmudha Fasheem, [2]P.Kanimozhi, [3]B.AkoraMurthy
[1]UG scholar, [2]Associate Professor, [3]Assistant Professor, Department of Computer Science and Engineering
IFET College of Engineering, Villupuram, India

***Abstract*—Ransomware is a type of malware that stops or limits users from accessing their system, either by securing the system's screen or by locking the users' files unless a ransom is paid. Further present ransomware families, collectively characterized as crypto-ransomware, encode certain file types on infected systems and forces users to pay the ransom through certain online payment methods to get the key for decryption. Hindering of ransomware is necessary in order to save the user's file. This paper proposes the automatic test packet generation (ATPG) .ATPG is a model which is used to produce a minimum set of test packs to exercise each link in the network. Test packets are sent occasionally, and detected failures prompt a distinct mechanism to localize the fault. ATPG reads router configurations and creates a device-independent model. This method prevents the ransomware from entering the system.**

***Index Terms*— Ransomware, Automatic Test Packet Generation (ATPG), Fault detection.**

I. INTRODUCTION

It seems nowadays that getting your computer infected with malware (or virus) is inevitable. Though we are very careful while working with computers such as downloading or browsing , sometimes our system may get infected without our knowledge. Therefore precautionary steps may help mitigate the possibility of downloading malwares but, nevertheless, getting infected with malware seems unavoidable. One of the most risky malware that is widely spreading among computers and upsetting the work of many is called "ransomware".

Ransomware has emerged as one of the most difficult malware which encrypts the files once it enters the system. There are two types of ransomware: the first one is the locker-ransomware. This typically takes the form of locking the computer's or device and then asking the user to pay a fee in order to restore access to it. The computers which get locked will often be left with partial capabilities, such as only allowing the user to interact with the ransomware and pay the ransom. Locker ransomware can predominantly be effective on devices that have limited options for users to interact with. This problem is likely to be affected in wearable devices and Internet of Things, where millions of connected devices could potentially be at risk from this type of ransomware.

The second type is the crypto-ransomware which encrypts the victim's personal files thus making them inaccessible to it. This type of ransomware is designed to find and encode valuable data stored on the computer, making the data useless unless the user obtains the decryption key. In these two cases users are forced to pay the ransom money to decrypt the files. Therefore attacked files are useless until a ransom is paid and decryption key is obtained. The use of ransomware has grown internationally, wide ranging attacks involving encryption-based ransomware began to increase through Trojans such as Crypto locker. The Mcafee labs analyzed that the Ransomware attacks could occur through the wearables as these may contain personal information. They also reported that there will be an increase in the cyber-criminals through the ransomware attacks. Because of its stealthy nature and disastrous effects (i.e., losing your data forever, or worse, having it leaked publicly) ransomware is perceived by many as a refined, hard-to-prevent attack. There are many paths that can lead to a ransomware infection. Some of it includes Traffic Distribution System, Malvertisement, Spam email, Downloaders and botnets, Social Engineering and self- propagation.

Some of the common types of Ransomware include:

CryptoLocker: For the past two decades, Ransomware has been in and around but it really came to existence in 2013 with CryptoLocker. The original CryptoLocker botnet was blackout in May 2014, but not before the hackers behind it extracted nearly $3 million from victims. Since then, the CryptoLocker approach has been widely copied, but the variants are not directly linked to the original. The cryptolocker word seems like Xerox and Kleenex and it has become almost synonymous with Ransomware.

CryptoWall: After the downfall of CryptoLocker, the CryptoWall had gained its importance. Earlier it had appeared first in 2014 and its variants with a variety of names, including Cryptobit, CryptoDefense, CryptoWall 2.0 and CryptoWall 3.0, among others. Like CryptoLocker, CryptoWall is distributed via spam or exploit kits.

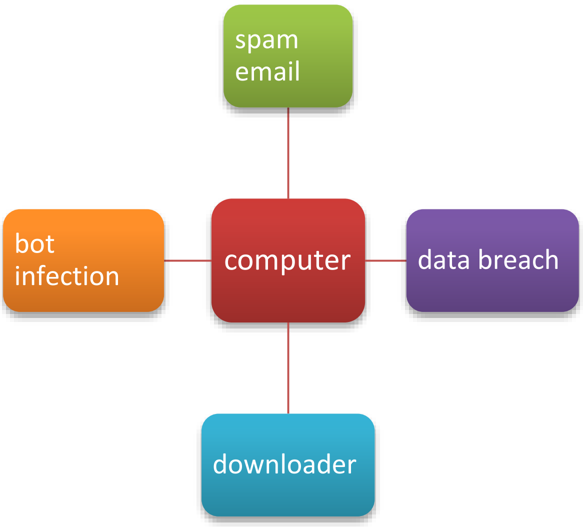

Fig.1. Routes for ransomware to arrive on a computer

Locky: Locky having a familiar approach like the other,is said to be new type of Ransomware. The malware gets spread using spam in the form of an email messages containing malicious links and it is disguised as an invoice. When user opens it, the invoice is scrambled, and the victim is instructed to enable macros to read the document. When macros are enabled, Locky Ransomware begins to encrypt a large array of file types using AES encryption. Bitcoin ransom is demanded when encryption is complete.

TeslaCrypt: TeslaCrypt is another new type of ransomware on the scene. Like other type of Ransomware, it uses an AES algorithm to encrypt files. It is typically disseminated via the Angler exploit kit specifically attacking Adobe vulnerabilities. Once vulnerability is exploited, TeslaCrypt installs itself in the Microsoft temp folder.

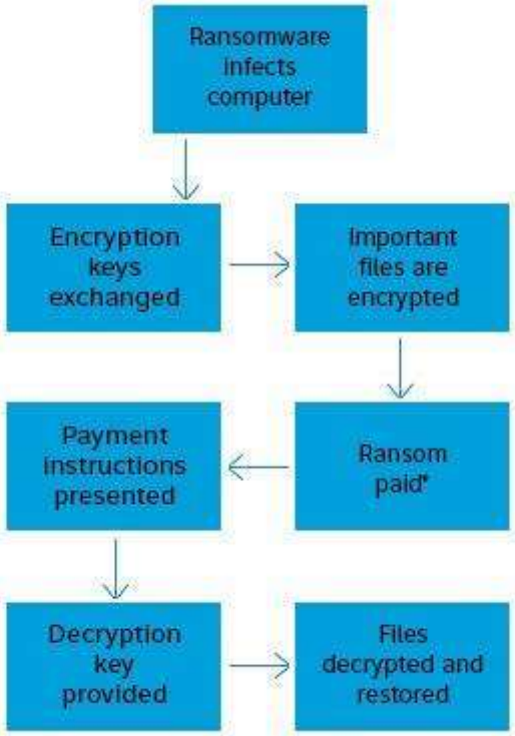
Ransomware infects computer
Encryption keys exchanged
Important files are encrypted
Payment instructions presented
Ransom paid*
Decryption key provided
Files decrypted and restored

Fig.2. Ransomware process

The ransom money is paid in terms of bitcoins. Bitcoin is digital currency that lets you anonymously buy goods and services. The victims can send bitcoins digitally using a mobile phone app or computer. It's as easy as swiping a credit card. Each bitcoin transaction is on a public log. Names of buyers and sellers are anonymous – only their wallets IDs are exposed. And it allows buyers or sellers do business without easily tracing it back to them. As a result, it's become a popular choice for cybercriminals to choose bitcoin as a form of payment. To make a bitcoin payment, victims are often alerted to download anonymous browsers, such as Tor2web or Tor project, in order to visit a URL hosted on anonymous servers. Thus eradication of ransomware is very essential.

This paper presents the automatic test packet generation technique for detecting and preventing the ransomware from entering the system. A ransomware is created using the AES encryption algorithm and it can be decrypted using the same.

II. RELATED WORK

North eastern University's latest ransomware research paper, "cutting *the Gordian knot: A Look under the Hood of Ransomware Attacks"* offers a different perspective. Between 2006 and 2014, this research team analyzed 1,359 ransomware samples [3] and found that a close examination on the file system activities of multiple ransomware samples suggests that Master File Table (MFT) in the NTFS file system has to be protected; it is possible to detect and prevent a significant number of zero-day ransomware attacks.

In the "network analysis of crypto wall ransomware" by Krzysztof, Piotr, Konrad, Dawid mentions about the Honeypot techniques[4] and the automatic run-time malware analytical system called Maltester were used. In this paper, the dynamic analysis concept is being used to find out the network analysis of crypto wall ransomware in the maltester environment which identifies the infected proxy machines that were playing an important role in the complex crypto wall's infrastructure. They also investigated that, in a single month the honey proxy has identified about 1587 machines.

Krzysztof Cabaj, Marcin Gregorczyk and Wojciech Mazurczyk in their work "Software-Defined Networking-based Crypto Ransomware Detection Using HTTP Traffic Characteristics" reports about the network communication of the two ransomware families namely crypto wall and locky [5] and concluded that analysis of the HTTP messages' sequences and their respective content sizes is enough to detect such threats. When the machine is infected, it contacts the C&C (command and control) server through the multiple proxy servers. They focused mainly on the crypto ransomware that utilizes the asymmetric cryptography. They observed that a promising approach would be to detect malicious communication between an infected host and attacker C&C server using the HTTP traffic characteristics. They were able to achieve detection rate of 97-98% with 1-2% or 4-5% false positives when relaying on domains or POST triples respectively.

In the paper "automatic test packet generation" proposed by Hongyi Zeng, Peyman Kazemian,, George Varghese, ,Fellow, ACM, and Nick McKeown, proposed about the working of the ATPG techniques[2] for testing and debugging networks This method generates a minimum number of dummy nodes or test packets to check every link in the network. Our implementation also augments testing with a simple fault localization scheme also constructed using the header space framework. Thus the liveness of the network is tested.

The work by Nolen Scaife, Henry Carter, Patrick Traynor, Kevin R.B.Butler "Cryptolock(drop it): Stopping Ransomware attacks on user data" explains about the CryptoDrop,[1] an early warning detection system that alerts user during suspicious file activity. It focuses on detecting Ransomware through monitoring the real time change of user data. Indicators have been used to track the suspiciousness. By tracking these, they develop a reputation score, which alerts the user and suspends the suspicious process.

Analyzing the work of five, it is noted that methods are implemented to detect the ransomware but still there is no prevention is provided. Hence the proposed system imports a method to prevent the malware from dangerous attacks.

III. METHODOLOGY

In the proposed approach, the automatic test packet generation (ATPG) is used to detect the faults in the network. This approach gets router configurations and generates a device independent model. ATPG is a model which produces the test packets to find all the link in the network. Test packets are dispatched frequently and it detect failures to localize the fault. ATPG can detect both functional and performance (throughput, latency) problems.

Established on the network model, ATPG generates the minimum number of test packets so that every link in the network is exercised and enclosed by at least one test packet. When there occurs a possibility for error detection, ATPG uses a fault localization algorithm to determine the failing routes or links.

When sending the file System will send test packets first through each and every link and the receiver end checks the packet whether it is affected by Ransomware attack or not. If the file is affected the acknowledge will be directed with node details where file get affected and sender sends the file based on the acknowledgement.

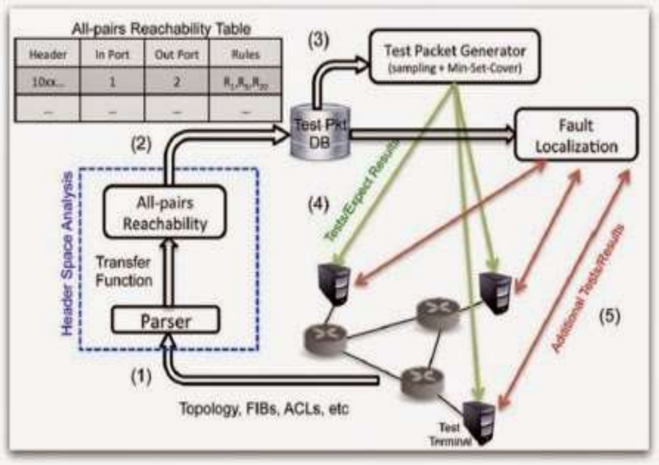

Fig.3. ATPG model

***1. Sender*:**

The sender sends the file to the multipath node in different capacity to the certain user. The intermediate nodes are used to send the file in different capacity.

2. File Send, Shuffle and Encode:

The original message m is alienated into (n - 1) shares; each of them has a unique identifier. The protocol makes a path numbers of which suitable messages are to be sent on the signaling channel. The path numbers assigned for the message parts are selected subjectively and sent at appropriate paths of multi-path routing protocol. When the message transmission is succeeding various paths are used for the parted messages that are created through pseudo random model. The message share will be transmitted in plain text. The concluding part is sent in plain text on one of the n paths. It will be the starting point for receiver to find other parts. Based on the manner of dividing messages, a Channel coding approach called Diversity Coding is used to improve from link failures.

Finally combine, the n - 1 parts of m in pairs using pseudo random process related to final path. On the nth link, which is measured as signaling channel, send values of pseudo random number and number of path in which message parts are transmitted.

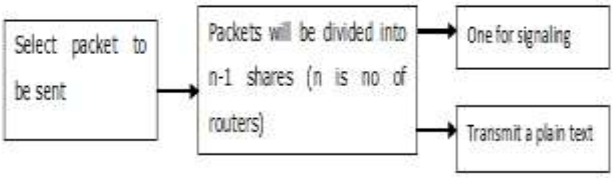

Fig.4. Dividing the packets

3. Receiver:

The receiver downloads the file from the intermediate nodes from the sender from the multipath. The files which are splitted while sending will get merged when it reaches the receiver.

***4. Test packet*:**

First test packet is generated whenever sender sends a file it is transmitted to receiver and later original packets are transmitted and the test packet identifies the fault tolerance and sends files.

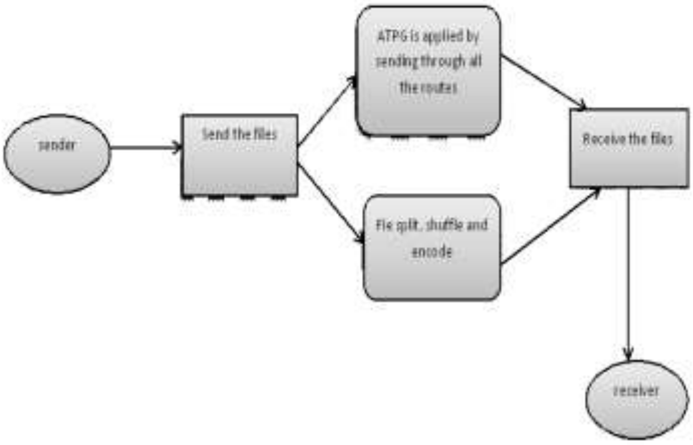
sender
Send the files
ATPG is applied by sending through all the routes
File split, shuffle and encode
Receive the files
receiver

Fig.5. ATPG for ransomware

By using this method, the malicious ransomware can be detected. The test packets are sent across each link in the network. The files are encrypted while sending. The receiver end receives the multiple test packets; the packets which are received as sent can be concluded that the link does not have any ransomware present. If any of the received packets is corrupted, then it is noted that the ransomware is present. So the particular link in the network can be avoided. And also we can detect the presence of Ransomware on our network by two ways: by watching out the file extensions and the other method is by identifying the increment in the file extensions.

Further, it is noted that most of the ransomware types are created using the AES algorithm. Thus a ransomware is created using the AES encryption algorithm and it can be decrypted using the same when it asks for the ransom money. AES is a symmetric encryption algorithm. It has the block length of 128 bits and key length of 128, 192, 256 bits. By implementing this, we can able to provide the solution to the affected system.

IV. CONCLUSION

This paper is designed to detect and prevent the ransomware by using the automatic test packet generation (ATPG). In proposed system two things are absorbed one is to prevent ransomware and second is the detection of the ransomware and to recover the affected file or unblock the access control. The link in which the ransomware is present can be recognized and it can be avoided. This helps in avoiding the early detection of ransomware and it can be disallowed by entering into the system. By using the AES encryption the ransomware is created. By this the files affected by ransomware can be evaded and the key for the decryption can be obtained.

V. REFERENCES

[1] P. T. N, Scaife, H, Carter, K. R. Butler, Cryptolock (and drop it): Stopping ransomware attacks on user data. In 2016 IEEE 36th International Conference on Distributed Computing Systems, pp. 303-312, 2016.

[2] Zeng, Kazemian, Varghese,and Nick “Automatic Test Packet Generation”,VOL. 22, NO. 2, APRIL, 2014.

[3] Kharraz, W. Robertson, D. Balzarotti, L. Bilge, E. Kirda, “Cutting the gordian knot: A look under the hood of ransomware attacks”,12th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2015), July 9-10, 2015, Milan, Italy.

[4] K. Cabaj, P. Gawkowski, K. Grochowski, D. Osojca, “Network activity analysis of CryptoWall ransomware”, Przeglad Elektrotechniczny, vol. 91, nr 11, 2015, ss. 201-204, URL: http://pe.org.pl/articles/2015/11/48.pdf .

[5] Krzysztof Cabaj, Marcin Gregorczyk and Wojciech Mazurczyk, “Software-defined Networking-based Crypto Ransomware detection using HTTP traffic characteristics”,URL:https://arxiv.org/pdf/1611.08294.

[6] Moore, Chris. "Detecting Ransomware with Honeypot Techniques. "*Cybersecurity and Cyberforensics Conference (CCC), 2016*. IEEE, 2016.

[7] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf

[8] Ali, Azad, Raj Murthy, and Frederick Kohun. "Recovering from the nightmare of ransomware- how savvy users get hit with viruses and malware: a personal case study.” *Issues in Information Systems* 17.4 (2016).

[9] Mercaldo, Francesco, Vittoria Nardone, and Antonella Santone. "Ransomware Inside Out." *Availability, Reliability and Security (ARES), 2016 11th International Conference on*. IEEE, 2016.

[10] URL: https://heimdalsecurity.com/blog/what-is-ransomware-protection/

[11] Bhardwaj, Akashdeep, et al. "Ransomware Digital Extortion: A Rising New Age Threat." *Indian Journal of Science and Technology* 9 (2016): 14.

[12]www.symantec.com/content/en/us/.../ISTR2016_Ransomware_and_Businesses.pdf.

[13] Kharraz, Amin, et al. "UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware." *25th USENIX Security Symposium (USENIX Security 16)*. 2016.

[14] D. Sgandurra, L. Muñoz-González, R. Mohsen, E. C. Lupu, Automated Dynamic Analysis of Ransomware: Benefits, Limitations and use for Detection, In: Computing Research Repository (CoRR), abs/ 1609.03020, arXiv.org E-print Archive, Cornell University, Ithaca, NY (USA), September 2016