A Secured Framework to Identify and Mitigate Attack

Lingala Thirupathi, Venkata Nageswara Rao Padmanabhuni

Abstract: Nowadays security is major concern for any user connected to the internet. Various types of attacks are to be performed by intruders to obtaining user information as man-in-middle attack, denial of service, malware attacks etc. Malware attacks specifically ransomware attack become very famous recently. Ransomware attack threaten the users by encrypting their most valuable data, lock the user screen, play some random videos and by various more means. Finally attacker takes benefits by users through paid ransom. In this paper, we propose a framework which prevents the ransomware attack more appropriately using various techniques as block chain, honeypot, cloud & edge computing. This framework is analyzed mainly through the IoT devices and generalized to the any malware attack.

Keywords: Ransomware attack, Malware attack, Block chain, IoT Device, Cloud & Edge Computing, Honeypot.

1 INTRODUCTION

There are lots of malware attack happen today but ransomware is one of the most dangerous one that threaten its victim. There are various types of ransomware as Lock-type ransomware, Crypto-ransomware etc. It usually install by as some another malware through malicious e-mail attachments or links, infected software applications or websites and via some connected external storage systems. Then check the vulnerabilities of the system by which make a connection to the C & C server and encrypt user’s important data or lock the screen of the users. Finally attackers demand the payment as crypto currency or threaten the users till they are not satisfied and delete or hide their traces so that no one can easily track them. There are various approaches mentioned in literature for detecting and preventing this attack as signature based and anomaly based techniques which takes various parameters as input- open ports, various system calls, registry editing, accessing of files and folders, file entropy changes etc. and make prediction of attack. Some of them use sandboxing methods and use cloud storage for backup purpose. But all of them have some weaknesses as need large storage for signatures, not predicting zero day attacks, high false alarm rate, new advanced ransomware evading from sandbox by sleep mode at earlier time, only for the user mode but what if- when root is compromised, training database or machine learning or deep learning algorithms are compromised. These above limitations motivate us to develop a new framework which can efficiently detect and mitigate this attack.

In computer networks, security breaches can occur when vulnerability in network or connection is used to damage/sabotage or do some kind of harm to the user. Attacks are mainly of two types, active attacks, and passive attacks. These act either actively, or inactively to steal data, identity or money by using various methods and mechanisms. Examples are snooping, masquerading, replaying, DOS etc. [2] [3] [4]. Malware is an abbreviated term for “Malicious Soft- ware”. Such software programs are specifically designed to gain access or damage victim’s computer.
A lot of malware is created today for profit through forced advertising (adware), stealing information (spyware), spreading spam emails or child pornography (zombie computer) or to extort money (ransomware) [5]. Ransomware is a type of malicious software that hinders working of a computer or user access to data and certain programs till a demand is fulfilled [6]. Ransomware has evolved since 2005 and there are several types of ransomware which are constantly being developed by attackers. Figure 2 shows the percentage of new families of fake AVs, misleading apps, lockers and crypto-ransomware identified between 2005 and 2015 [7]. The figure has a varying number of the families. It can be noted that initially only crypto-ransomware and misleading applications were found. Misleading applications mostly made use of phishing and other such activities. Crypto-ransomware could not survive in that time due to antivirus applications analyzing and identifying such malware. By 2009, the misleading applications were replaced by fake antivirus software programs. They would tell the user that some virus has been detected or some problem has occurred. To rectify the same premium version of a paid solution is to be purchased. Threatened for security, victims would pay the same.

![Figure 2: Percentage of new families of fake AVs, misleading apps, lockers and crypto-ransomware identified between 2005 and 2015 [8]](image)

### II PROPOSED FRAMEWORK

In our proposed method (figure 3), we take a example of a smart home environment in which various smart heterogeneous (both resource constrained and high resource power) IoT devices are to be vulnerable from this attack.

We create a database using block chain smart contract in which authentication, access control of IoT devices are to be stored for removing the risk of external device attack. This smart contract also contains the valuable system call functions as registry editing functions, root access functions, cryptographic encryption functions, port assessing functions, desktop controlling functions, file read or write functions, folder deleting functions etc. These calls are included in the basic steps of ransomware attack, when intruder performs sequence of operations as fingerprinting, port scanning, connection to the C & C server, accessing of important data, encrypting the important documents, lock the user screen, demand for the payment and delete the backup data along with traces of intruders. Some of the calls same as the normal operations and others are not but it makes difference when executed in sequence of ransomware attack.

But due to the complex nature of block chain operations (mining and storage), it cannot be stored at every IoT devices specifically resource constrained devices. That’s why we use edge computing here, means take high power IoT devices at edges which compute all block chain operations and data analysis. For security reason key management and generation are to be done at particular device itself.

We also take some honeypot devices (very high power devices) for proper evaluation of this attack before that attack is performed on the actual device. For backup data of these IoT devices, we use cloud architecture which is also decentralized, distributed in nature mean managed by block chain. Both of the block chain managed by the load balancer devices or software for handling incoming request messages. For additional security, the smart home gateway includes the firewall for filtering malicious ports, IP addresses, file extensions etc. to preventing ransomware attack.

### III WORKING PROCESS

Any ransomware or software comes to the smart home infrastructure either via network or through physical devices. For network attack, it first go through the gateway that include first line of defense as firewall which filter malicious ports, IP addresses, file extensions etc. But advanced malware can
Easily by pass it. Following steps are same for both (device and network attack). This software or malware runs at two environments simultaneously-first one at that device which they want to access and second one on the honeypot devices. Block chain smart contract check the various sequences of system call run by that software and also check the authenticity and access control of that external device. If that software check for searching of a file, read/write of files, need admin privilege, edit log and registry events etc. Then this software behavior is same as normal user behavior. But when it wants to access network information as open ports, open sessions, read the user’s browsing history and bookmarks and read kernel level information then that smart contract alert the user because it may be the malware and require the user permission for execute it. After some time, if that software call any encryption function, call to make a new network connection using for browser, call to disable key guard and need the control over the desktop, then our block chain stop this software processing at all devices except the honeypot nodes before that functions are executed and wait till software execution end up at that honeypot devices, if that software demand the ransom then it is a ransomware attack. Uninstall that software at all the devices and check honeypot devices for some new rules given as feedback to the addition of block chain rules for more efficient detection of attacks. For secure backup data of these IoT devices, we use block chain cloud infrastructure with load balancer (schedulers) and various workstations. All block chain operations are to be maintained at cloud but key management is done at devices themselves for providing end point security.

IV THEORETICAL ANALYSIS

We perform the theoretical analysis for validation of our work. Some of the observations are as: By the use of ransomware block chain, attacker cannot compromise our data analysis algorithms or methods.

Figure 3: Proposed Framework for Preventing Ransomware Attack

1) Zero day attacks are prevented by the honeypot devices and new attacks rules are to be added at blockchain for more efficient detection of attacks.
2) All IoT devices authenticate by the block chain so that no external device attack in the network.
3) Basic firewall rules are applied at gateway for novice intruder.
4) For backup data securely, cloud block chain is used.
5) For end point security, key management is to be done at devices themselves for both of the blockchain.
6) or complex operations of block chain, edge and cloud infrastructure are to be used along with load balancer (hardware or software) for handling incoming requests.

V CONCLUSION AND FUTURE WORK

Nowadays ransomware attack is one of the most dangerous attacks. It can very easily spread to any vulnerable system or device and demand the ransom from users. Various techniques are available in literature for mitigating this attack but every solution has problem as handling zero day attack, high false alarm rates, security of machine learning data and methods etc.

So, for overcoming to these limitations we propose a new secured method which includes block chain, honeypot, edge or cloud computing techniques to IoT devices for preventing this attack. Our method is generalized means can be extended to any malware attack detection. In future work, firstly we implement our methodology on real world scenario and do changes in it as needed.

REFERENCES