Using Blockchain to prevent Ransomware Attacks

Dr. Robert Steven Owor,
Robert.owor@asurams.edu;

Daylin Hart, dhart5@students.asurams.edu

Devonte Hawkins, dh

awki22@students.asurams.edu

Adia Sakura-Lemessy,
asakural@students.asurams.edu

Albany State University, 504 College Drive,
Albany GA 31705

Abstract

The rise of ransomware over the past few years is a major problem that has quickly become an extremely lucrative criminal business. Targeted organizations often believe that paying the ransom is the most cost-effective way to get their data back — and, unfortunately, this may currently be the only feasible option.

Abstract

The problem is that every single business which pays to recover their files is directly sponsoring the development of the next generation cyber-attack. Ransomware continues to evolve and become more and more sophisticated.

In this paper we propose a blockchain solution based on 4 proxy servers and a control server which all record exactly the same transactions. When one server is compromised by ransom ware, the control server uses a new encryption to block that server and hand it over to an investigation Team A new Server is created and the new four servers continue operations. Investigations can then be launched to determine the source and origin of the ransomware

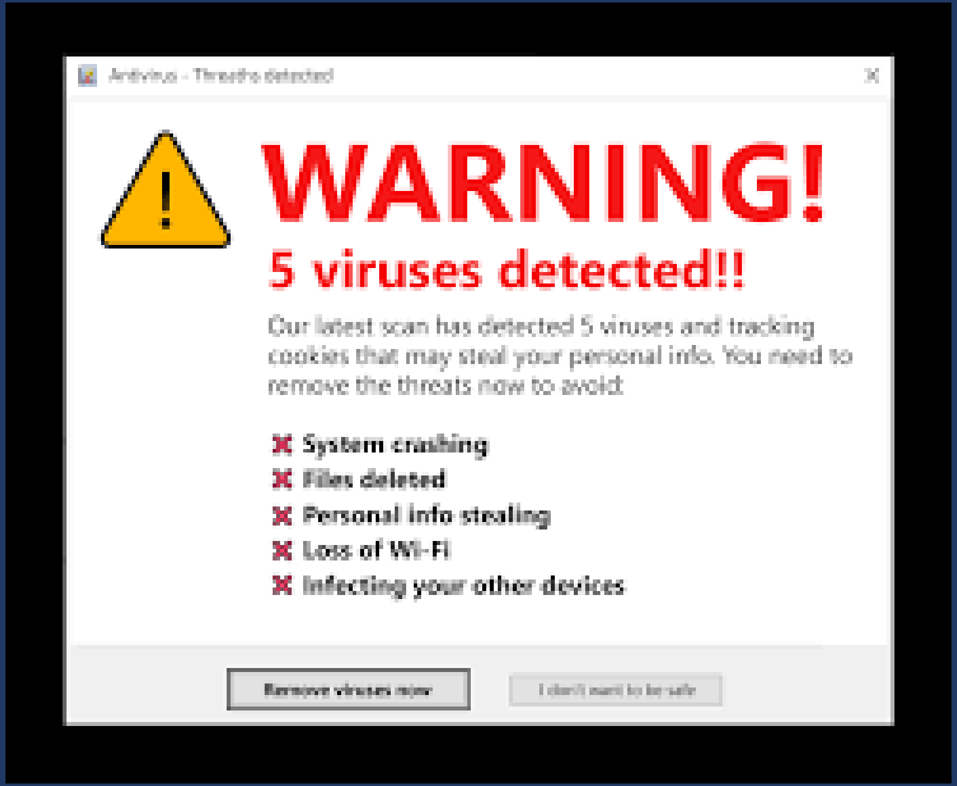
1.0 Introduction

Ransomware is a type of malicious software that prevents users from accessing their system or personal files usually by encrypting the files and data and demanding a ransom payment in order to regain access. Over the past decade, ransomware has become one of the most prolific criminal business models in the world, due to the fact that cyber-criminals usually target high profile individuals, corporations and even governmental institutions .

Ransomware is achieved by locking a victim's computer through encryption and demanding a substantial sum of money, usually in bitcoin (because it is the most valuable crypto and because it maintains a level of pseudonymity) for the decryption key necessary to decrypt the data. The Punishment for failure to pay, leads to a permanent loss of the data..

2.0 Types of Ransomware

Scareware is rogue security software and tech support scams. A user receives pop-up notifications which state that malware has been detected in the system and that the only way to remove it is to pay. Scareware coerces users to pay based on fear. In many cases users who don't pay are bombarded with more and more popups. Usually, the Scareware Mongers will simply give up. Scare ware Mongers can be tracked by monitoring their IP addresses and blocking them. Also, they can be tricked into a payment website where they will reveal their Bitcoin addresses, which can be tracked.



WARNING!

5 viruses detected!!

Our latest scan has detected 5 viruses and tracking cookies that may steal your personal info. You need to remove the threats now to avoid:

- ✗ System crashing
- ✗ Files deleted
- ✗ Personal info stealing
- ✗ Loss of Wi-Fi
- ✗ Infecting your other devices

2.0 Types of Ransomware

Screen lockers, also known as lockers, are a type of ransomware designed to lock a user out of their computer. When the victim starts their computer, they will see what seems to be an official governmental seal or the logo of the police department or institution responsible for tracking cyber misconduct. The victim user is informed that some unlicensed software or copyright violations such as illegal web content has been found on their computer and is provided with instructions to pay a fine. It is well known that the Government or IRS will never lock you out of your computer for failure to keep government rules and regulations. However, governmental institutions will never lock a user out of their computer, or demand payment for illegal activities

2.0 Types of Ransomware

Encryption ransomware (data kidnapping) attacks are a type of ransomware where hackers gain access to a user’s data, encrypt it and ask for payment to release the data. This type of ransomware is very painful for the victim because once hackers get a hold of a user’s data, no security software or system restore can return them unless they pay the required amount. The problem is that even if users pay up, there is no guarantee that the attackers will undo the damage. Furthermore, id it is sensitive data, the hackers can threaten to release the data into the public domain. The solution to such an attack is to have multiple servers recoding the same data. When one server is compromised, the compromised server is taken offline, re-encrypted so that the hackers cannot access the data ether. New Servers with new IP addresses are then loaded to continue operations. We will discuss this solution in more detail.

2.0 Types of Ransomware

Mobile ransomware specifically targets mobile devices. Attackers use mobile ransomware to steal data from a phone or to lock it. As with the encryption ransomware, the victim needs to pay a ransom to get their data back or to unlock the device. The solution to this type of attack is to always back up all the data on the phone to the cloud. iPhone data can be backed up in the iCloud while Android data can be backed up on the Google cloud. Once the victim realized they have been hacked and there is a demand for payment, they should contact their service provider immediately. The cell phone is taken offline. A new phone is issued to the victim with back up restored either form the iCloud or google cloud. Further investigations can be carried out on the malicious hackers.

3.0 Sample Cases of Ransomware Attacks

The Baltimore City Government was attacked on May 7th, 2019. Its computer systems were infected with a very aggressive ransomware called Robin Hood. The city was forced to take the system offline to prevent the ransomware from spreading further. The malware had managed to infect the voice mail system, the email system, a parking fines database system and a system used to pay water bills, property taxes, and vehicle citations. It is estimated that the aftermath of the attack cost the city at least $10 million

3.0 Sample Cases of Ransomware Attacks

A city in Florida, Riviera Beach also had its computer systems blocked by Ransom ware. Its email system, emergency response system, and water pump systems were all compromised and blocked from operation by encryption. It has been shown that ransomware attacks had a huge financial impact on the healthcare sector, with over $20 billion lost in impacted revenue, lawsuits, and ransom paid in 2020 alone. Over the course of the year, over 600 hospitals, clinics, and other healthcare organizations were impacted by 92 ransomware attacks.

4.0 Blockchain, a solution for ransomware

Bitcoin has the de facto standard for payments for cybercriminals. Blockchain, however can provide the solution to ransomware. This is because blockchain – if well implemented, can provide a very strong solution against ransomware [4].

.

4.0 Blockchain, a solution for ransomware

- Blockchain is a digital, distributed and decentralized ledger of transaction which stores transaction data in structures called blocks. Each block contains transaction data and metadata (a set of data which provides information about the respective block), the advantage of this structure is that each block is constructed upon the previous block, in a chain-like structure (hence the name blockchain) by the calculating the hash of the previous block and combining it with the hash of the second block of transactions.

- This complex design is what gives the data introduced in the blockchain its immutability and integrity. If a malicious actor attempts to alter the data from a block, every change will be immediately noticed by the system and every other network participant, because it will render all the following blocks invalid.

- These design choices make blockchain ideal for data storage because it is an append-only structure, which means that data can only be introduced into the system, it can never be completely deleted. Any changes made are stored further down the chain, but an admin can always see that when the changes occurred, who made them as well as the previous version of the data.

4.0 Blockchain, a solution for ransomware

- Blockchain can therefore provide the necessary principle of **integrity** and **immutability.**

The third principle of the blockchain is its **decentralization**. Decentralization means that the network does not rely on a central server to host all the data, but distributes it across every network participant, also known as nodes. There are many types of nodes in a blockchain network, full nodes for example store a copy of the entire blockchain.

- As a result, the entire system doesn’t have a single point of failure. If a node is compromised, admins just have to address the vulnerability which allowed the malicious user to access the network and restore the node to its previous version, or they can simply cut out the node from the network. In case of encryption by ransomware, the attacker would find it impossible to hold all the data hostage, because the entire network is distributed among thousands of users (even more depending on the size of the blockchain), and even if they manage to encrypt a node, admins close the proverbial backdoor through which the attacker entered and restore the node to its previous version. Moreover, the system can be designed to re-encrypt the data which has been compromised by a hacker. This means that the hacker has no access to the data and cannot maliciously expose it if it is sensitive data.

4.0 Blockchain, a solution for ransomware

- Blockchain can therefore provide the necessary principle of **integrity** and **immutability.**

The third principle of the blockchain is its **decentralization**. Decentralization means that the network does not rely on a central server to host all the data, but distributes it across every network participant, also known as nodes. There are many types of nodes in a blockchain network, full nodes for example store a copy of the entire blockchain.

- As a result, the entire system doesn’t have a single point of failure. If a node is compromised, admins just have to address the vulnerability which allowed the malicious user to access the network and restore the node to its previous version, or they can simply cut out the node from the network. In case of encryption by ransomware, the attacker would find it impossible to hold all the data hostage, because the entire network is distributed among thousands of users (even more depending on the size of the blockchain), and even if they manage to encrypt a node, admins close the proverbial backdoor through which the attacker entered and restore the node to its previous version. Moreover, the system can be designed to re-encrypt the data which has been compromised by a hacker. This means that the hacker has no access to the data and cannot maliciously expose it if it is sensitive data.

5.0 Modex BCDB

- Modex Blockchain Database (BCDB) was designed to help people without a background in tech, access the benefits of blockchain technology and remove the dangers posed by the loss of sensitive data.

- Currently, the majority of blockchain solutions present on the market are oriented towards blockchain as a service, limiting themselves to a rigid view and application of the technology. A company or the CTO of a company can come to the realization, after a bit of study that their business can solve several issues and streamline back-end processes by implementing blockchain. The problem is that in order for a company to implement blockchain technology only through its own tech team, they need to invest a significant amount of time and resources to study what type of blockchain is most suited for their needs, and commence a lengthy process of learning the development specificity of the respective blockchain, as well as scouting for developers proficient in the technology [7].

5.0 Modex BCDB

Modex BCDB is a new development in blockchain technology which removes the need to invest resources in blockchain training and facilitates fast adoption of the technology in businesses. The solution proposed by Modex is a middleware which fuses a blockchain with a database to create a structure which is easy to use and understand by developers with no prior knowledge in blockchain development [2]. As a result, any developer who knows to work with a database system can operate with this solution, without needing to change their programming style or learn blockchain.

5.0 Modex BCDB

Modex BCDB is a new development in blockchain technology which removes the need to invest resources in blockchain training and facilitates fast adoption of the technology in businesses. The solution proposed by Modex is a middleware which fuses a blockchain with a database to create a structure which is easy to use and understand by developers with no prior knowledge in blockchain development [2]. As a result, any developer who knows to work with a database system can operate with this solution, without needing to change their programming style or learn blockchain.

6.0 Conclusion

In Summary, Blockchains can be used to prevent against cyber attacks in general and ransom ware attacks in particular. Of particular interest is the Mode3ex Blockchain which allows any enterprise database to be ported into the Modex Blockchain. Modex Blockchain comes with the Encryption, integrity, immutability, decentralization and distribution capabilities to enable enterprise databases such as oracle, Microsoft, IBM, Mongo DB or even Access to secure the data from Ransom ware and other attacks. We hope that more and more companies and even individuals will take advantage of blockchains to prevent against Ransomware attacks.