GLOBAL CHALLENGES OF RANSOMWARE AND METHODS TO CURB ITS EFFECTS AND OCCURRENCE WITHIN ONLINE WORK ENVIRONMENT

BY

NAME: IFEOSE JUSTIN N

ADDRESS: Delta State University of Science and Technology Ozoro, Delta state

E-MAIL: realjusty@gmail.com

And

NAME: ADIGWE WINIFRED

ADDRESS: Delta State University of Science and Technology Ozoro, Delta state

E-MAIL: adigwew@gmail.com

ABSTRACT

Ransomware has recently become one of the most dangerous and frustrating malware to individuals and organisations in the current day computer and information technology world. Files of both individuals and organisations has increasingly been under serious attack and there is no sure-fire solution for defending against ransomware as these malware code uses polymorphic and metamorphic algorithms to create different versions therefore escaping signature detection. Hence, for individuals or organizations that wants their files in an adaptive security architecture has to deployed for constantly monitoring of the system as to detect new ransomware infection at its initial attempt stage such that it can be blocked before encrypting the files. This approach is defense in depth approach which supplements the network defenses such as patch management, anti-virus software, intrusion detection, firewalls, and content filtering. A model for the execution of the preempt and preventive security architectural structure via open source program is proposed and the presented model is implemented against the Petya and WannaCry ransomware. The proposed architectural model was successfully tested and able to alert of the ransomware attack and, it was capable to prevent the Petya ransomware from executing on the victim host.

Keywords: Ransomware, cryptocurrency, cryptovirology, Bitcoin

1.0 INTRODUCTION

The exist ransomware attacks has been until recently, when the attack became so recurring, common and devastating to organizations and individuals that many organizations and even individuals have lost valuable (files, documents, transaction records etc) worth Trillions of money. Most organisations / Individuals have been bankrupts owning to Ransomware activities that they have encounter

According to Fruhlinger (2018), ransomware is malware that encrypts files of victim's. The attacker now request for a ransom from the victim to recuperate access to the data when payment is made. Users are given procedure on how to make payment the fee to get the decryption key. The payment demand can varies from hundred dollars to millions, payment to cybercriminals in cryptocurrency.

According to Fruhlinger (2018), there are so many things the malware can do if it's gets access into the users device, but beyond,, the most common thing is to encrypt some or all of the victim’s data files. For further technical details look out for, the Infosec Institute has a great in-dept. But the important thing to know is that the files cannot be decrypted without a mathematical key known only to the attacker . The user is offered with a message illumination that their files are now inaccessible and will only be decrypted until they send an untraceable payment with Bitcoin to the attacker.

According to Mimoso (2016), Ransomware is a type of malicious software from cryptovirology that threatens to make public the victim's data or

continually block access to it unless a ransom payment is made .While some simple ransomware may lock the system so that it is not impossible for an erudite user to overturn,, more sophisticated malware uses a skill called cryptoviral extortion. It encrypts the users files, making them unreachable, and order for a ransom to be received to decrypt them. In a well implemented cryptoviral extortion attack, restoring of the files without the decryption key is a problematic problem, and tough to trace digital currencies such as Ukash and cryptocurrency are used for the ransoms, making tracing and prosecuting the perpetrators impossible.

Lutkevich et al. (2019) “describe ransomware as an integral part of malware. The victim’s data on a computer is locked -- basically by encryption -- and payment then requested for the ransomed data to be decrypted and access regain by the victim. The reason behind attacks by ransomware is normally monetary distinct from other types of attacks, the victim is normally notified that an exploit has occurred and is given procedure and instructions for recover from the attack. Payment is often requested to be made in a virtual currency, such as Bitcoin, to know the cybercriminal's identity”.

Lutkevich et al. (2019) add that ransomware malware may be multiplied through malicious email attachments, infected software apps, compromised external storage devices, and affected websites. Attackers mostly uses protocol of remote desktop and other procedures that cannot depend on any form of interaction with the users.

Lutkevich et al. (2019) reveal that “ransomware tools resident on the deep web allows cybercriminals to buy and use software tools to generate ransomware with unambiguous capabilities. They then crate this malware for

their own distribution, with ransoms paid to their cryptocurrency accounts. Just with much of the rest of the IT world, it is then easy for those with little or no technical background to order inexpensive ransomware as a service (RaaS) and deploy attacks with minimal effort.

Lutkevich et al. (2019) states that encryption ransomware is among today's most effective ransomware forms". As stated above, an attacker gets to files and encrypts the users data then asks for payment to regain access back on the files. Attackers uses a complex encryption algorithms to encrypt all data saved on the system. A direction is normally given on the attacked device with information on how to go on recovering the encrypted data when payment is done. Equated to screen lockers, encryption ransomware keeps the user's data in serious danger, and there is no guarantee of data been returned to the user after cooperation. In all situations, the victims will receive a pop-up messages or email ransom notifications threatening that if the requested sum is not paid at a given date, the private key for regaining access to the system or decrypt files will be smash up.

The damages caused by ransomware virus to computer users around the universe can be very devastating. The defy faced by users whose device is under attack is mentioned below:-

Loss of data: Valuable data is lost to the ransomware as it affect the most frequently used files used by the computer user.

Loss of money: Enormous amount of money are paid to the developers of ransomware software by distressed computer users who need to receive their data well again

Time Waste: Projects files saved on a workplace computer system that have

been compromised are usually lost to this attack, and much time is wasted in redoing the file again.

System Damage: The procedure of encrypting the files that ransomware makes use of system assets will overload it and cause dame to operating software.

Hard Drive Damage: The duplication of multiple encryption files in the system hard drive causing the hard disk's corruption, leading to destruction to the unit and preventing normal storage of files.

Antivirus Detection Failure: Most Antivirus software cannot detect newer editions of ransomware malware until its too late

2.0 PROPOSED SYSTEM AND IMPLEMENTATION

This research aims to develop an Anti-ransomware Model for the Protection of the Computer System from File Encryption-based Ransomware. To deploy a model, a software application developed that can achieve the following actions:-

i. crate data on system files and saved to the Hard Disc Drive

ii. Save the data in an electronic relational database

iii. Monitor the data kept on files then compare their properties against those saved in the database.

iv. Report any activity of change in file property if discovered.

v. Run a system protection mechanism if the files have been assumed to be tampered with by ransomware application.

vi. Generate a log report of the activities performed

2.1 REVIEW OF PAST LITERATURE

Kolodenker et al (2017), In ‘Paybreak: Defense against Cryptographic

Ransomware' proposed a new system, PayBreak, to effectively combat ransomware, then prevent any data loss. It does this by essentially creating a key escrow inaccessible to ransomware that holds every key used in encryption in a secure manner thus allowing the decryption of any file encrypted by ransomware. PayBreak demonstrates the ability to restore all files lost to twelve different ransomware families, and it does so with negligible performance overhead. While complete data recovery or complete prevention of data loss is the ideal result of combating ransomware, PayBreak only manages to effectively work with only 60% of all ransomware families leaving eight common families of ransomware that can decimate a users system to go uninhibited. PayBreak also lacks a basic robustness allowing it to be evaded simply by ransomware authors rolling back to older versions of crypto libraries or through basic obfuscation and evasion techniques as stated by the authors themselves. Their approach was essentially just a proof-of-concept, and it is doubtful whether the authors will pursue any future work on PayBreak or not.

According to Schofield (2016), ransomware is a kind of malware from cryptovirology that warns will make public their victim's data or perpetually deny access to it except ransom payment is recieved . Whereas simple ransomware can lock the device with anyone who is technical knowledgeable can reverse, but more advanced malware uses a technique called cryptoviral extortion. It encrypts the target's files, making them inaccessible, and ask for ransom payment to decrypt them

2.2 Types Of Ransomware

According to Johansen (2019), there are seven common types of ransomware

which are:

· Crypto malware. This ransomware can cause much damage because it encrypts things like your files, folders, and hard-drives. One of the most familiar examples is the destructive 2017 WannaCry ransomware attack. It besieged thousands of computer systems worldwide running onWindows Operation Software and spread itself within corporate networks globally. Victims were asked to pay the ransom in Bitcoin to retrieve their data. Lockers. Locker-ransomware is known for infecting your operating system software to completely deny you access of your computer or devices, making it impossible to access any of your files or applications. This type of ransomware is most often Android-based.

Scareware. Scareware is fake software that acts like an antivirus or a cleaning tool. Scareware often claims to have found issues on your computer, demanding money to resolve the problems. Some types of scareware lock your computer. Others deluge your screen with annoying alerts and pop-up messages.

Doxware. Commonly described as leakware or extortion ware, doxware threatened to display the hijacked information online if payment of the ransom is not made. As more people saves their important data, files and personal photos on their systems, it's understandable that some people out of fear pay the ransom when their files have been over taken.

Mac ransomware. Their first ransomware infiltrated Mac operating systems in 2016. Known as KeRanger, this malicious software infected Apple user systems through an app called Transmission, which could encrypt its victims' files after being launched .

3.0 METHODOLOGY

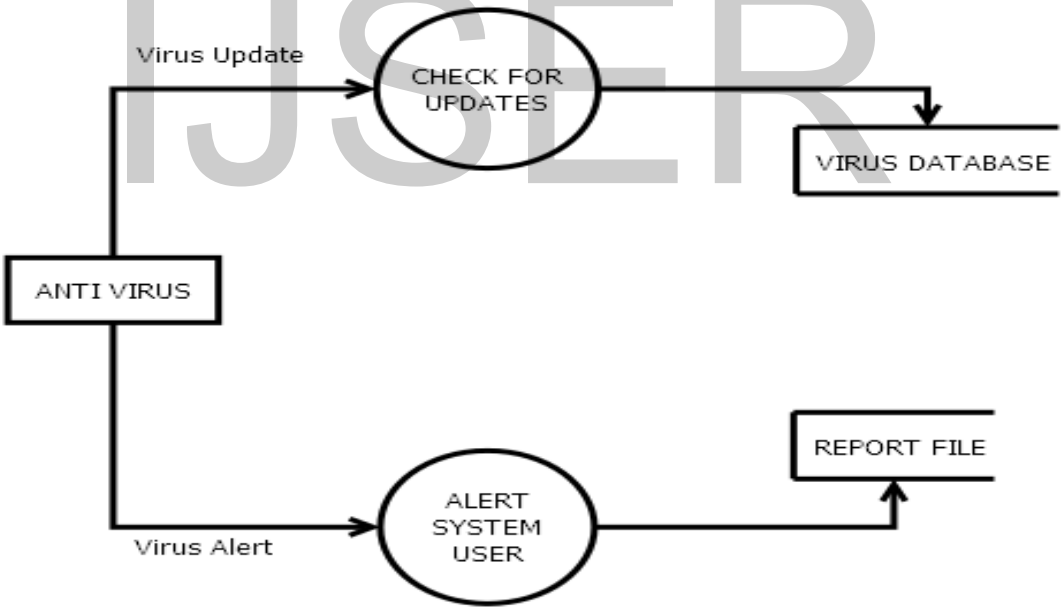
The software development methodology that is used is Object-Oriented Programming (OOP). The four core concepts of object-oriented programming are an abstraction, encapsulation, inheritance, and polymorphism. By the abstraction, a programmer hides many details about an object and displays only the most applicable information. This increases efficiency and reduces complexity

3.1 ADVANTAGES OF THE CURRENT SYSTEM

The current anti-malware software detection system is advantageous in weeding out and detecting malicious software which has gained access or attempting to gain access into the computer system's resources with a bid to compromise its performance.

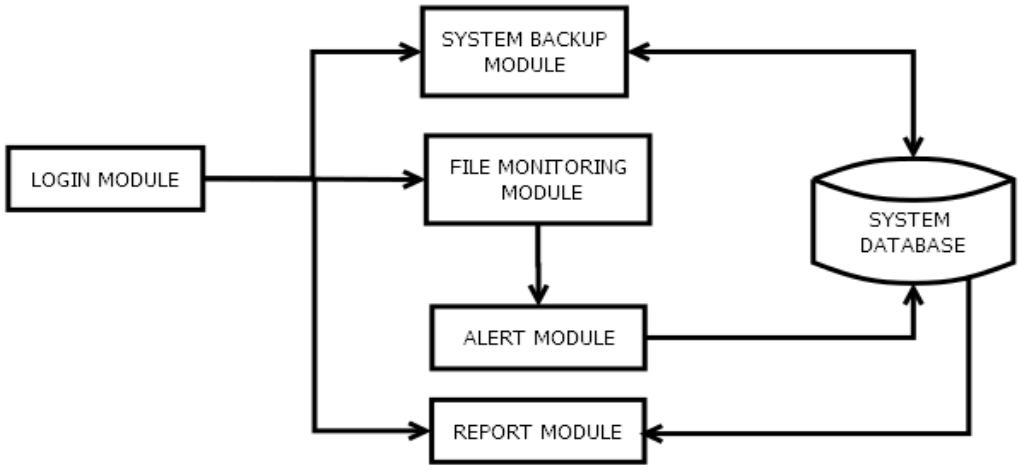
DATAFLOW OF THE EXISTING SYSTEM

The dataflow diagram of the current system is illustrated in the diagram below



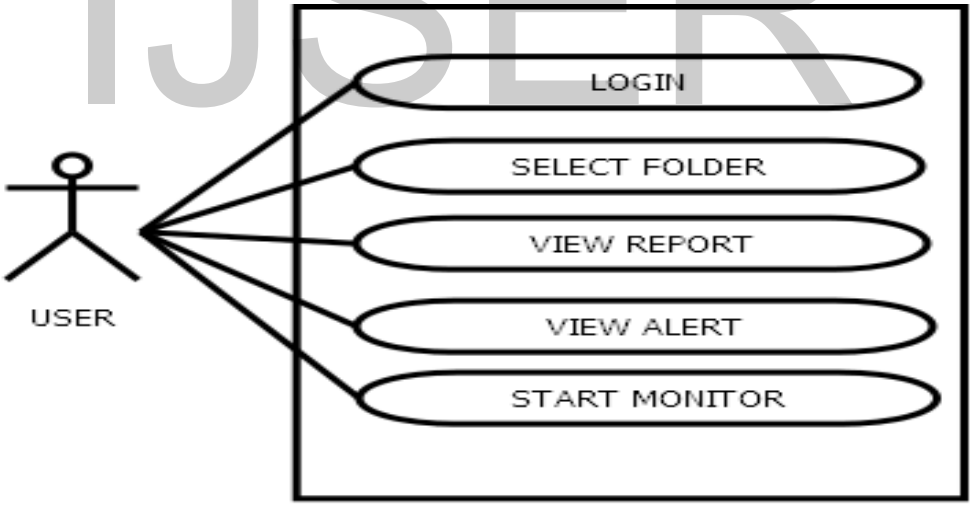
HIGH LEVEL MODEL FOR THE NEW SYSTEM

The High Level Model of the proposed system is illustrated in the figure below.

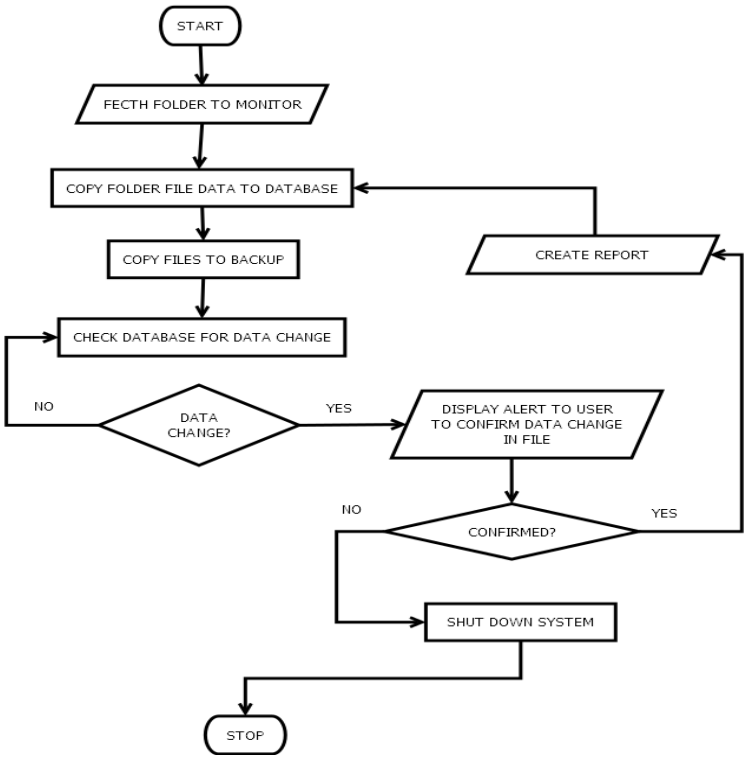


3.8 USECASE DIAGRAM

Below is the use case diagram of the proposed system.



System Operation Flowchart:-



Systems Flowchart

4.0 RESULTS

This system is designed specifically for the detection of ransomware activities on the system. It is used to monitor the changes in the files of any selected folder to detect any sudden changes in the file properties, which could signal that the files are being encrypted.

The system used a model that monitored selected files and backed them up as a proactive measure against ransomware virus attacks. This way, the user's information is safe as this is how to protect the file without payment of the ransom, as if the files get encrypted by ransomware application, it will be impossible to decrypt.

5.0 CONCLUSION:

When attacked by ransomware, it is almost impossible to undo the malicious software changes, hence the best method of combating the problem is to use a pre-emptive and preventive approach in tackling the problem to detect the ransomware activity before damaging the files on the PC. This lead to the development of an Anti-malware Model for the Protection of the System from File Encryption based Ransomware.

REFERENCES

Fruhlinger, Josh (2018) "Importance of Location-Based Mobile App in Business" CSO United States [online] Available From (19 Dec 2018)

Lutkevich, Ben; Richardson, Robert (2019) "ransomware" [online] TechTarget Available From

Mitre Finch (2016) "STAFF ALLOCATION ISTHE SOLUTION TO FRUITFUL STRATEGIC MANAGEMENT" [online] Available From (14 October 2016)

E. BRAUN (2017) " Importance of Effective Resource Allocation" Available From (February 14, 2017)