An Intelligent Defense Strategy to Counter Ransomware Menace

[1]Arindam Dan, [2]Sumit Gupta, [3]Prameya Saha, [4]Vivek Kumar, [5]Akash Verma

[1-5]University Institute of Technology, The University of Burdwan,

Golapbag (North), Burdwan-713104, West Bengal, India

[1]danarindam1233@gmail.com [2]sumitsayshi@gmail.com [3]pro.saha.16@gmail.com

[4]vivekrajwe1@gmail.com [5]akashverma9504@gmail.com

Abstract - The world today is experiencing the omnipresence of Internet and the ubiquitous use of digitalization like never before. But for enjoying these myriad offerings, users of this digital era are facing ballooning instances of intrusion, threats and attacks as its ripple effects. The cyber attackers or cyber criminals are always on the hunt to bank upon the vulnerabilities of online users, thus leading the latter into a big trouble. One such practice of putting a user into a compromising situation by attacking his/her computer system is through a ransomware. Ransomware is a malware which gets secretly installed on users' machines and in turn confiscates the control of crucial files, documents and other important resources. The attackers then raise the call for ransom payment (generally using cryptocurrency like Bitcoin) from the affected victim for relinquishing control on victim's sensitive information. Through this paper, we are proposing a simple and intelligent strategy to deal with ransomware; which often propagates when users' surf a sensitive or susceptible website or download any infected email attachment. Further, we are creating a Case Base and a Dupe List which can serve as important instruments for predicting beforehand the source of threat as well as occurrence of an unwanted attack. We have implemented our strategy and evaluated it against 30 samples of some popular ransomware. We have also tested these samples on machines with an inbuilt windows defender system and with paid antivirus installed on them. The results show that our approach is able to counter ransomware attacks more efficiently as compared to machines with other defense systems preinstalled on them by offering a cent percent success rate in providing defense.

Keywords: Ransomware, Virtual Box, Case Base, Dupe List

I. INTRODUCTION

As per (Kharraz et al., 2016), the emergence of ransomware dates back to the late 1980s, which has experienced a resurgence since 2013. Recently, ransomware has become one of the most important security threats on the Internet. Some of the most popular ransomware attacks are Cyborg (1989), GPcode.AK (2008), Trojan.Winlock (2011), Reveton (2012), CryptoDefense (2014), KeRanger (2016), WannaCry (2017) etc. It has been reported that the volume of targeted ransomware attacks has doubled in January 2017 from a comparable period in late 2016 (Yaneza, 2017).

In this paper, we have proposed an intelligent defense strategy to not only detect any ransomware attack but also to defend our computer against it.

II. PREVIOUS RELATED WORKS

A good amount of work has been done in the area of ransomware prevention and defense against ransomware. Few authors (Gonzalez and Hayajneh, 2017) have discussed about different types of crypto ransomware and have recommended few prevention measures by identifying suspicious patterns in the attack behavior. The authors (Shaukat and Ribeiro, 2018) have implemented RansomWall for Microsoft Windows OS and the authors (Vinayakumar et al., 2017) have used the notion of shallow and deep networks. In the paper (Siddiqui et al., 2017), the authors have proposed a hardware based access control policy to protect a computer from malicious software by securing BIOS configuration and boot files.

III. PROPOSED METHODOLOGY

Through this paper, we have proposed a working system that will provide a user with a mitigation plan to detect the occurrence of a ransomware attack and will also aid in protecting his/her computer system from the ransomware menace. As we know that a computer gets infected by a ransomware if any susceptible website is surfed or any malicious email attachment is downloaded, so we have

 DOI : 10.18231/2454-9150.2018.0931

proposed two different strategies to defend our computer against these two vulnerable scenarios. Our mitigation strategy to prevent the spread of ransomware can be divided into the following two phases:

Detection Phase: This phase helps in detecting whether any attack on our computer system is a ransomware attack or not. Based upon the source of the attack, we have proposed two different attack detection strategies:

1. If a user receives an attachment via an email, then our proposed system will check whether the sender of the mail is trusted or not. If it is found that the sender is not trustworthy, then the mail will be marked as a spam; otherwise the user will be permitted to download the said attachment(s). Figure 1 depicts our proposed defense strategy to deal with ransomware attacks through email attachment(s).

2. If a user surfs any website, then our proposed system will check whether the website is trusted or not. If it is found to be trusted, then the user will be permitted to visit the site; otherwise user's confirmation (via a warning message) will be sought for visiting a suspicious site. Figure 2 shows the defense strategy against ransomware while surfing an infected website.

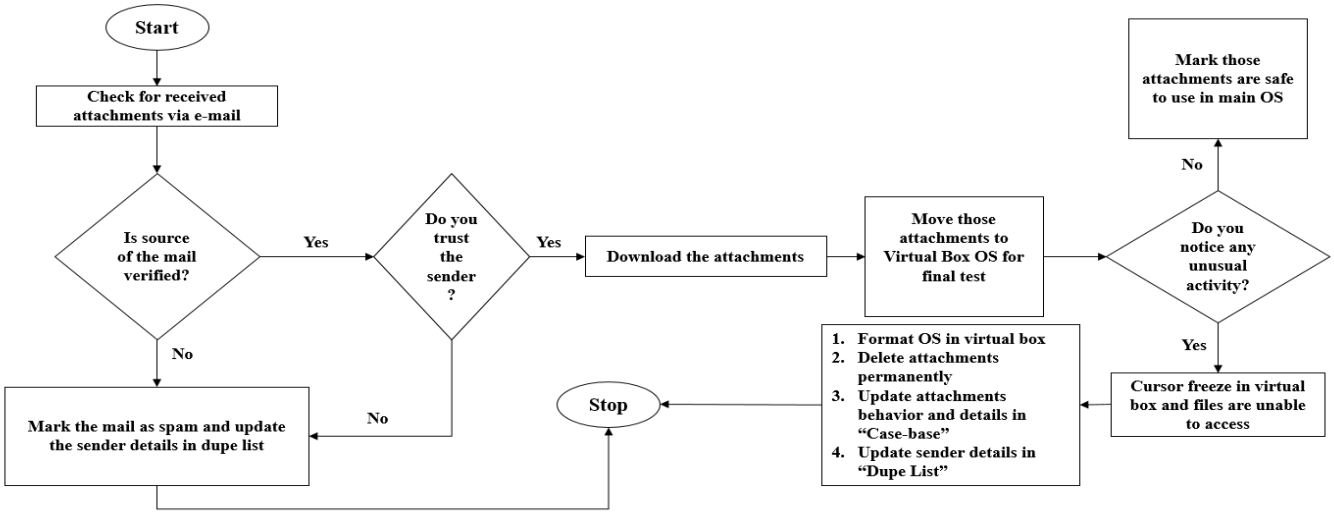

Figure 1. **Proposed Defense Strategy against Ransomware Attack through Email Attachments.**

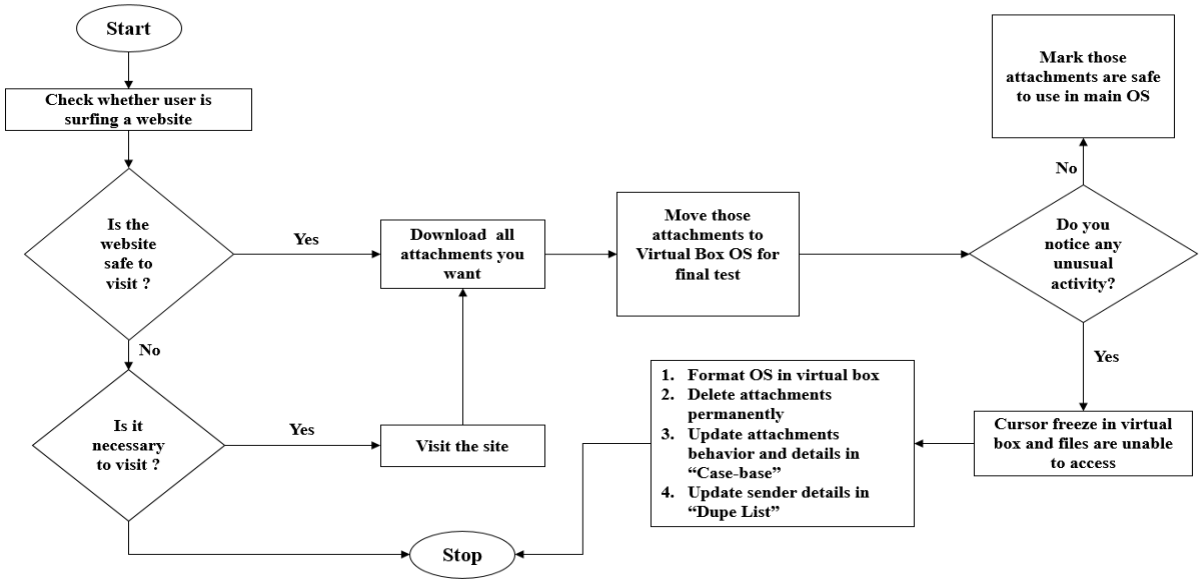

Figure 2. Proposed Defense Strategy against Ransomware Attack while Surfing Websites.

Defense Phase: This phase helps in providing defense against the spread of any ransomware which has been downloaded into our computer through attachment(s), either intentionally or unintentionally. We have proposed the following strategy to deal with it:

Firstly, every downloaded attachment will be checked in the Virtual Box Operating System (VBOS) before loading it into the system's primary or main OS. If any unusual activity is suspected or detected, then our proposed system will delete all the attachments by formatting the VBOS. Secondly, the behavior of the infected attachments or files will be recorded in a "Case Base" so that we can prevent future malware attacks based on the recorded behavioral patterns. Finally, the details of the sender and/or source of the infected attachment(s) (such as spam mail IDs and suspicious URL) will be updated in a "Dupe List" to trace the real culprit and defend our system from being affected in future.

 DOI : 10.18231/2454-9150.2018.0931

IV. RESULT AND ANALYSIS

To analyze the working of our proposed system, we have manually collected 30 samples of some popular ransomware (only for research purpose) and have tested them on 30 different machines; out of which 10 machines used our proposed approach (including VBOS), the other 10 machines had paid antivirus installed and the remaining 10 machines had an inbuilt windows defender system. Figure 3 shows the performance comparison using a horizontal bar chart.

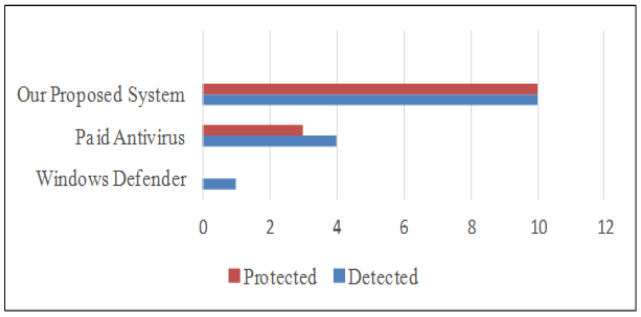

Figure 3. Horizontal Bar Chart showing the Comparative Performance Analysis.

The results show that all the 10 machines using our strategy were fully secured after being attacked using ransomware samples. Thus, our strategy countered ransomware attacks more efficiently as compared to machines preinstalled with other defense systems.

V. FUTURE WORK & CONCLUSION

This paper presented an intelligent defense strategy to protect our systems from the threat of ransomware. Unlike the over expensive antivirus and defender systems, our approach offers a cost effective panacea from ransomware. In near future, we aim to ameliorate our proposed strategy to track the real source of the ransomware in order to get hold of the real culprit beforehand. We are also working towards automating the entire system to reduce manual effort. Thus, we have initiated a strategic movement to quash the peril caused by ransomware.

VI. REFERENCES

[1] Gonzalez, D., & Hayajneh, T. (2017). Detection and prevention of crypto-ransomware. Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), IEEE 8th Annual, 472-478.

[2] Kharraz, A., Arshad, S., Mulliner, C., Robertson, W., & Kirda, E. (2016). UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware. 25th USENIX Security Symposium, USENIX Association, 757-772.

[3] Shaukat, S. K., & Ribeiro, V. J. (2018). RansomWall: A Layered Defense System against Cryptographic Ransomware Attacks using Machine Learning. 10th International Conference on Communication Systems & Networks (COMSNETS), IEEE, 356-363.

[4] Siddiqui, A. S., Lee, C. C., & Saqib, F. (2017). Hardware based protection against Malwares by PUF based access control Mechanism. 60th International Midwest Symposium on Circuits and Systems (MWSCAS), IEEE, 1312-1315.

[5] Vinayakumar, R., Soman, K. P., Velan, K. S., & Ganorkar, S. (2017). Evaluating shallow and deep networks for ransomware detection and classification. International Conference on Advances in Computing, Communications and Informatics (ICACCI), IEEE, 259-265.

[6] Yaneza, J. (2017). Brute Force RDP Attacks Plant CRYSIS Ransomware. Trend Micro. Retrieved from https://blog.trendmicro.com/trendlabs-security-intelligence/brute-force-rdp-attacks-plant-crysis-ransomware/

 DOI : 10.18231/2454-9150.2018.0931