ISSN(Online) : 2456-8910
International Journal of Innovative Research in Applied Sciences and Engineering (IJIRASE)
Volume 3, Issue 7, DOI: 10.29027/IJIRASE.v3.i7.2020, 498-502, January 2020

Ransomware Remedial Through Virtualization

[1]R. Ilangovan, [2]Y.K. Chua, [3]S.H. Kok
Taylor's University, 47500 Subang Jaya, Selangor, Malaysia
[1] rishiilangovan@sd.taylors.edu.my
[2] kennethyiken.chua@sd.taylors.edu.my
[3]koksimhoong@sd.taylors.edu.my

***Abstract* –Ransomware is a growing threat to the global population. There are many attacks such attacks since 2012, notable ones namely WannaCry and Petya. These attacks had costed millions, maybe even billions of dollars in economic losses. Ransomware employs a method known as cryptoviral extortion, a three-step protocol that aims to take the user's data hostage and demand a ransom for it. There are existing defensive countermeasures against these ransomwares such as Paybreak; a decryptor for files, ShieldFS; a filesystem to detect malware based on adaptive models that is constantly being updated and SSD-insider; a mechanism that uses the NAND flash delayed deletion feature to recover files. Studies have also shown that awareness is important in defending against ransomware attacks, and end-user habits may increase the likelihood of being at risk. Therefore, to address the issue where defence mechanisms are not addressing, the awareness aspect, we have proposed a solution to address both the technical aspect of defence and the socio-cultural aspect. Our solution aims to educate the user to improve and supplement our defence. The end-user plays an active role rather than a passive stance in the other solutions listed above. In the worst-case scenario, the end-user should be able to deal with the scenario appropriately by not giving in to the demands of the attacker via our solution.**

***Index Terms* – Crypto-currency, Cyber security, Encryption, Malware, Ransomware**

I. INTRODUCTION

Ransomware is a type of malicious software that "kidnaps" the user's data. The attacker can then threaten the user by publishing the data or denying access to their data until the user pays the ransom to the attacker. Advanced ransomware employ a method known as cryptoviral extortion. This method has three steps in its protocol [1].

Step 1

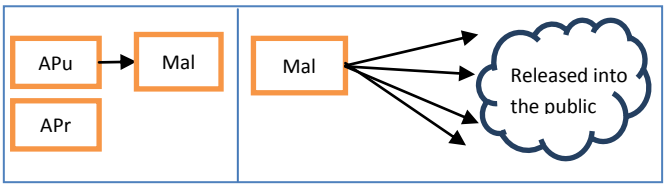

FIGURE 1: Ransomware Dissemination Step 1

The attacker will first generate an asymmetric pair of keys. The public key (APu) will be placed into the malware (Mal), which will be released into the public. The private key (APr) will be kept by the attacker. This is shown in Figure 1 above.

Step 2

The malware will first generate a symmetric key (SK), which it will use to encrypt the victim's data (VD) as shown in 1 and 2. As seen in 3, the symmetric key will be encrypted with the public key (APu) that was placed in the malware. Part 4 illustrates the original symmetric key (OSK) and the victim data (OVD) will be erased so that it cannot be recovered. The victim will then be asked for a payment by the attacker alongside the asymmetric ciphertext of SK (ASK). This is shown in Figure 2 below.

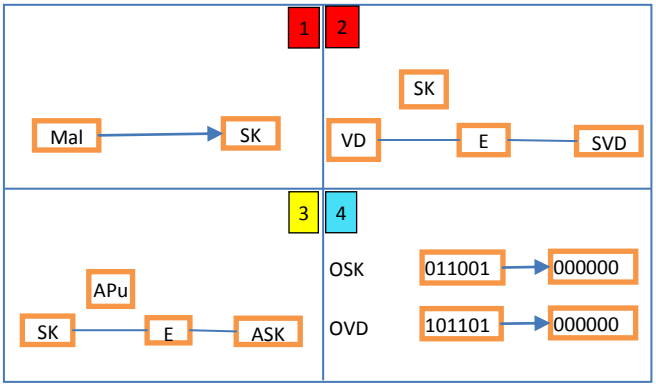

FIGURE2: Ransomware Dissemination Step 2

Step 3

The victim sends the ransom and the asymmetric ciphertext to the attacker. The attacker then uses their own private key to decrypt the symmetric key, which will then be sent to the victim so that they can decrypt their data.

To summarize, the victim essentially pays a ransom for the key to their data. Since the private key is kept safely, there is no other way. It also employs hybrid encryption given the combination of symmetric and asymmetric encryption methods involved. However, the hardest part of attacking is finding a way to infect the victim's computer with the malware. It is unfeasible to decrypt the data without the attacker's private key. The symmetric key is also randomly generated so it cannot be recycled for other victims.Table 1 below shows well-known ransomware attack in detail.

ISSN(Online) : 2456-8910
International Journal of Innovative Research in Applied Sciences and Engineering (IJIRASE)
Volume 3, Issue 7, DOI: 10.29027/IJIRASE.v3.i7.2020, 498-502, January 2020

TABLE 1: Ransomware Attack

Where	Ukraine (then global)	United States	United States	United Kingdom
How	Spread via a backdoor in a Ukranian tax preparation program,MeDoc	Cloned email address masqueradi ng as a department' s email address [2]	- N/A	- Eternal Blue exploit was used [3]
What was damag e? Who were victims ?	- Ukranian business firms [3] - Accounting information	- Cockerel Hill Police Department of Texas - Evidence data	- Hospital Presbyterian Medical Center (HPMC) [4] - Access to email, network and patient data was locked.	- National Health Services in England - MRI scanners and blood storage
Impact	- Affected about 90% of Ukranian businesses - Had already collected at least $10 billion USD after one week [5]	- Loss of critical evidence data worth 8 years.	-Department that used data affected were closed down. - At least, $1 million USD	- Economic loss of over $4 billion USD [6]
Recove ry	- Ransom were paid - Businesses were made aware of ransomware source.	- Unable to recover files since they did not pay the ransom [7] - They merely stopped the infection by wiping the servers	- after 10 days of manual handling, they resorted to paying up the ransom	- Windows released an update to prevent the exploit - Kill Switches were discovere d
Attack type	Petya	Osiris	- N/A	WannaCry
Vulner ability	Backdoor in MeDoc's software update feature.	Email Masqueradi ng	- N/A	- Windows OS exploit

II. RELATED WORKS

Simoiu et. al.[8]analyses the habits of users. It is interesting to note that only 4% of those affected with ransomware paid up the ransom. The aim of this study to develop a risk assessment model for ransomware victimization based on habits to enable identification of potential victims. It is found that demographics attributes such as gender and age can influence the likelihood of being a victim besides the number of hours spent online. They found that pre-paid cash voucher as the leading method of ransom payment instead of cryptocurrency, slightly contradicting other studies in the field. It is also found that ransomware that lock the computer is more common than encrypting ransomware. The majority of the respondents (30%) of the study who were infected with a ransomware dealt with it by restarting the computer. Users who used a backup to restore constitute only 22% of the respondents. The behavioural change after the attack was careful monitored. The rest are buying an anti-virus software and updating them. Despite having being attacked by ransomware, only 26% began to backup or backup more frequently. Backup are the most effective way to combat ransomware attacks. The study states that more awareness is needed. They proposed a heuristic risk assessment model based on self-reported security habits. Several questions relating to their online habits are developed. These questions are correlated to the risk of infection though not causally related. The study then concluded that ransomware attacks can cause losses over $100 million per year. The estimated victimization rate was 2-3% of the population in US per year.

Shashidhar[9]perform a static and dynamic analysis of the WannaCry malware. As discussed earlier, WannaCry uses the EternalBlue exploit, vulnerability in the Server Message Block protocol. It is found that WannaCry uses the kernel library and the user library. This gives access to local registry functions and functions that display graphics and GUI creation. It also seems that WannaCry is packed with Microsoft Visual Studio. This malware uses try/catch/finally blocks as well as memory manipulation to prevent itself from being removed from the RAM, to achieve its goal. The study also found that, upon removing any of the try/catch files, it would be corrupted and fail to execute. It is also found that it attacks approximately 151 file types. The WannaCry ransomware is also capable of deleting Shadow Volume Copies while also disabling backup restoration. The notable difference between the WannaCry variant in the study and the one involved in the attack is the absence of the kill-switch. If the WannaCry malware is denied admin privileges, the malware continues with the encryption, however, it will not be able to delete Shadow Volumes. The WannaCry malware uses RSA keys for encryption and decryption purposes. It was also discovered that Wanakiwi is viable as a decryptor for WannaCry. Since WannaCry deletes the entire registry keys and adds its own ones, it is best to reinstall the OS after retrieving the decryption key.

Surati and Prajapati [10]entails the overview of ransomware deployment as well prevention methods. It also compared 13 other studies based on the pros and cons of each ransomware countermeasure proposed by the studies. The study described the anatomy of a ransomware attack. The first phase is Deployment: install components used to infect, encrypt and lock the system. The second phase is installation: ransomware installs itself on system. The third phase, Command and Control is where the code will begin to look for instruction to reach out to its command server. This phase may vary depending on ransomware used. The fourth phase, Destruction phase, is when the files that have been identified in the third phase will be encrypted. The last phase, Extortion, is when the malware delivers the message

that the attackers have written to get victims to pay them the ransom for their files. There are three commonly used attack methods in ransomware which are exploit kit, malicious email attachments and email links. Detection and prevention methods are Honeypot, Heldroid, Cryptolock and Sandbox while steps that users can take are backup regularly, disabling macros, being cautious when opening suspicious attachments and use an anti-virus[11]. This study was a comprehensive review on each of the studies involved. Defensive measures were discussed based on feasibility as well.

Baek et al.[12] proposed an approach to detection of ransomware as well as recovery. Several features were designed to detect ransomware behavioural characteristics. The authors of this paper have also built a ransomware detection method through a machine learning[13] technique via a binary decision tree. By utilising the delayed deletion feature of NAND flash, a Flash Translation Layer scheme that accommodates an instant recovery of files can be designed. This study also involves a prototype of this concept working against eight examples as well as in-house examples. It has a 100% detection accuracy and detection latency being less than 10 seconds. Through this test, encrypted files have been recovered within 1 second without any data loss. This study shows how potential defences against ransomware can be developed. Although ransomware is always evolving, defences against it have to catch up and adapt accordingly.

Continella[14] states that the monitoring of ransomware activity should be at the filesystem since it is a strategic point. This study introduces ShieldFS, a preventive method against ransomware. It is an add-on driver to supplement the Windows native filesystem so that it is immune to ransomware attacks. This driver dynamically activates a protection layer depending on the outcome of the detection mechanism. It monitors the low-level filesystem activity so that its models of the system activity profile can be updated over time. In the case a process or more violates the models, it is identified as malicious and the effects are rolled back. ShieldFS was designed after an analysis of numerous I/O filesystem requests from clean machines in use. This study utilised a novel way of measuring filesystem activity such that it gathers data from real-world environments. Besides that, they have also tested ShieldFS against real threats which yielded positive results.

III. CHALLENGES

1) Awareness

The lack of awareness in society of the existence of ransomware is the most important reason why ransomware is a major threat. Ransomware is spread by taking advantage of users' lack of awareness. Companies usually provide social engineering training to employees so that they do not fall for phishing techniques [15]. Some malware masquerade as law enforcement agencies. Unaware people are fooled into being paid the ransom. Suspicious and unsolicited email attachments should also be cautioned upon since the CryptoLocker malware attack was propagated through email as well [16].

2) Poor security habits

Users who do not practice good online security habits are prone to ransomware attacks. It is found that 25% of home users do not have any backups at all. This leaves a huge portion of the population exposed to ransomware attacks [17]. According to [8], of the users who are previous victims of ransomware, only 26% began to backup. This shows that users tend to set themselves up for an attack with their habits passively. That study also showed that many users tend to visit P2P sites which increased the likelihood of being attacked.

3) New exploits being developed and new threats

The famous WannaCry attack occurred due to the EternalBlue exploit developed by the NSA[18]. Exploits like these cause the emergence of a new threat. For a period of two days, users' systems were being infected without any external support. Then, Microsoft quickly rolled out a new patch to address that exploit [17]. Defensive countermeasures were developed but much later. It is difficult to defend as it would need to address all issues and loopholes. However, for the attacker, they would only need one loophole to use it against the users.

4) Targeted ransomware attacks

Ransomware attacks that are directed to a certain organisation to fully exploit its weaknesses leave the organisation relatively defenceless especially if the organisation does not allocate a budget for its IT department. For example, the healthcare service industry shares this problem. Traditional honeypot systems are not viable anymore since attackers are able to detect it. Ransomware that are targeted to specifically exploit an organisation's flaws are difficult to defend against [19].

5) Lack of defence mechanisms

Many users' systems lack the presence of antivirus software. This opens up more opportunities for attackers to infect users with their malware. For organisations, they lack a proper incident plan to deal with such a scenario should the occasion rise [17]. Companies that are prone to ransomware attacks have very lenient user policies. While there needs to be a consideration of the user experience of the employees, there needs a greater consideration for the safety of the company. In addition, ransomware is equally harmful for the internet of things, smart homes, cellular networks, and other networks including wireless sensor networks, E-health IoT based applications as well [21-26]. Furthermore, ransomware makes easy target cyber security application as well as to the smart phone applications [27-29], including Android and IOS based applications.

ISSN(Online) : 2456-8910
International Journal of Innovative Research in Applied Sciences and Engineering (IJIRASE)
Volume 3, Issue 7, DOI: 10.29027/IJIRASE.v3.i7.2020, 498-502, January 2020

IV. PROPOSED SOLUTION

Antivirus works via static analysis or at most signature scanning. However, the more recent approach is heuristic scanning (dynamic analysis) is more reliable since it detects the pattern of file activity to identify its trust[20]. Through heuristic scanning, dynamic analysis can be applied to form a checkpoint based system where new applications will be screened in a sandbox where it is free to do whatever it wants. Through the observation of the behaviour of the application in this sandbox, we can determine how safe the application is. If the application requests the use of other files, we can safely assume that is malicious depending on what it wants. Figure 3 below shows an overview of how the system is implemented with comparison to conventional systems.

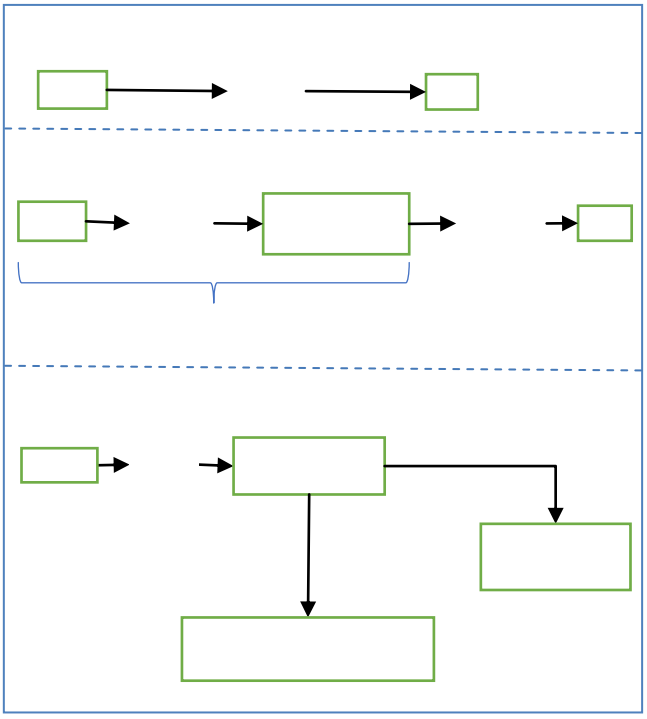

FIGURE3: Ransomware Protection Using Virtualization

For example, given two apps are downloaded. App A and app B, app A is malicious while app B is not. App A and B are both put into the untrusted zone and are tested to detect any malicious behaviours. App B will be put into the trusted once it passes. App A on the other hand will be screened since it will be requesting access to certain files. This can be reviewed by the user to check if it is truly malicious or not.

This solution was designed based on the WannaCry attack and using ShieldFS as inspirations. WannaCry and most of the commonly ransomware tend to encrypt or hijack the system. Taking WannaCry as a theoretical example, suppose that our system has implemented our solution and has been infected with WannaCry. This malware will immediately ask for admin privileges and our solution will detect it. If the user decides to test it further and give it admin privileges in the sandbox zone, it would have an illusion of control since it would not have direct access to the kernel libraries as it would have to request for it through the hypervisor. This will then indicate that it is indeed malicious. Cryptoviral ransomware would need the permission to read/write already existing files, this will be examined by our system and will be tested further and then it can assume that it is malicious. We have designed this to mirror ShieldFS since the use of the adaptive models to indicate malicious behaviours have been proven to be quite effective in its study. It also states that the filesystem is a good starting point for defence against ransomware.

Since the need to sandbox and monitor multiple processes, it is best to implement the solution on a hypervisor level. This allows an isolated environment for the untrusted zone, this way the malware is given an illusion of freedom. The hypervisor used would be a type 2 hypervisor since it would be hosted on a native OS. This allows for a separation in zones based on trust levels. The hypervisor also allows for the dynamic allocation of memory to the untrusted zone.

The disadvantage to this solution is that the system might run slower than usual considering how it has an additional hypervisor for the untrusted zone. The second point to note is that certain application may be able to determine that they are being screened so they may not do anything suspicious to prevent detection. This can be fixed by calibrating the system to not trust anything and be paranoid. It is possible to also employ a method similar to IOS systems, application containerization. Possible attack vectors are existing malware and exploits being developed to allow an escape from the sandbox.

V. CONCLUSION

As a conclusion, it is the end-users that determine whether an attack is successful or not. It would be better if the different defence mechanisms are able to be combined and optimized to be a complete security suite to properly medicate ransomware attacks. While preventive methods should be prioritised more, recovery methods should not be ignored since there is no 100% guarantee to any preventive measure. The solution that was proposed is merely a conceptual design so it may not be comprehensive enough. However, this solution, on a conceptual level, draws inspiration from a similarly proposed solution fromShieldFS. In our solution, the end user plays an active role; this will give the user a hand-onwith the approach to ransomware education.

The future direction of research on ransomware is payment tracking and better defences. There are many researches on ransomware behaviour to properly devise a new and efficient method to deal with such issues. However, due to the convenience of cloud solutions, the ransomware threat can be reduced.

REFERENCES

[1] A. Young and M. Yung, "Cryptovirology: Extortion-Based Security Threats and Countermeasures," in *IEEE Symposium on Security and Privacy*, 1996, pp. 1–12.

[2] E. Nakashima, "Osiris Ransomware: New Addition to the Locky Family," *Acronis Security Team*, 2017. [Online]. Available: https://www.acronis.com/en-us/blog/posts/osiris-ransomware-new-addition-locky-family.

[3] "NSA officials worried about the day its potent hacking tool would get loose. Then it did.," *The Washington Post*, 2017. [Online]. Available: https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html.

[4] B. JACK DANAHY, "Next wave of ransomware could demand $millions," *VentureBeat*, 2016. [Online]. Available: https://venturebeat.com/2016/03/26/next-wave-of-ransomware-could-demand-millions/.

[5] A. GREENBERG, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, 2018. [Online]. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ .

[6] J. BERR, "'WannaCry' ransomware attack losses could reach $4 billion," *CBS News*, 2017. [Online]. Available: https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/.

[7] D. Storm, "Police lost 8 years of evidence in ransomware attack," *ComputerWorld*, 2017. [Online]. Available: https://www.computerworld.com/article/3163046/police-lost-8-years-of-evidence-in-ransomware-attack.html.

[8] C. Simoiu, C. Gates, J. Bonneau, and S. Goel, "'I was told to buy a software or lose my computer. I ignored it': A study of ransomware," *Proc. 15th Symp. Usable Priv. Secur. SOUPS 2019*, pp. 155–174, 2019.

[9] J. Jones and N. Shashidhar, "Ransomware Analysis and Defense," *J. Colloid Interface Sci.*, vol. 374, no. 1, pp. 45–53, 2012.

[10] S. B. Surati and G. I. Prajapati, "A Review on Ransomware Detection & Prevention," *Int. J. Res. Sci. Innov. Issue IX*, vol. IV, no. Ix, pp. 2321–2705, 2017.

[11] S. H. Kok, A. Abdullah, N. Z. Jhanjhi, and M. Supramaniam, "A Review of Intrusion Detection System using Machine Learning Approach," *Int. J. Eng. Res. Technol.*, vol. 12, no. 1, pp. 9–16, 2019.

[12] S. Baek, Y. Jung, A. Mohaisen, S. Lee, and D. Nyang, "SSD-Insider: Internal Defense of Solid-State Drive against Ransomware with Perfect Data Recovery," in *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*, 2018, pp. 875–884.

[13] S. Kok, A. Abdullah, M. Supramaniam, T. R. Pillai, and I. A. T. Hashem, "A Comparison of Various Machine Learning Algorithms in a Distributed Denial of Service Intrusion," *Int. J. Eng. Res. Technol.*, vol. 12, no. 1, pp. 1–7, 2019.

[14] A. Continella *et al.*, "ShieldFS: a self-healing, ransomware-aware filesystem," 2016, pp. 336–347.

[15] "Ransomware: Facts, Threats, and Countermeasures," *Center for Internet Security*. [Online]. Available: https://www.cisecurity.org/blog/ransomware-facts-threats-and-countermeasures/.

[16] A. G. Johansen, "What is ransomware and how to help prevent ransomware attacks," *NortonLifeLock*. [Online]. Available: https://us.norton.com/internetsecurity-malware-ransomware-5-dos-and-donts.html.

[17] Kevin Savage, P. Coogan, and H. Lau, "Symantec SECURITY RESPONSE The evolution of ransomware," 2015.

[18] S. H. Kok, A. Abdullah, N. Z. Jhanjhi, and M. Supramaniam, "Ransomware , Threat and Detection Techniques : A Review," *Int. J. Comput. Sci. Netw. Secur.*, vol. 19, no. 2, pp. 136–146, 2019.

[19] Z. H. Wang, C. G. Liu, J. Qiu, Z. H. Tian, X. Cui, and S. Su, "Automatically Traceback RDP-Based Targeted Ransomware Attacks," *Wirel. Commun. Mob. Comput.*, vol. 2018, 2018.

[20] S. H. Kok, A. Abdullah, N. Z. Jhanjhi, and M. Supramaniam, "Prevention of crypto-ransomware using a pre-encryption detection algorithm," *Computers*, vol. 8, no. 4, pp. 1–15, 2019.

[21] Z.A. Almusaylim and N. Zaman, "A review on smart home present state and challenges: linked to context-awareness internet of things (IoT) Wireless Networks", 25 (6), 3193-3204.

[22] A. Almusaylim, Z., Jhanjhi, N. Comprehensive Review: Privacy Protection of User in Location-Aware Services of Mobile Cloud Computing. Wireless PersCommun (2019). https://doi.org/10.1007/s11277-019-06872-3

[23] M. Almulhim, and N. Zaman, "Proposing secure and lightweight authentication scheme for IoT based E-health applications", 2018 20th International Conference on Advanced Communication Technology (ICACT), 481-487.

[24] M. Almulhim, N. Islam and N. Zaman, "A Lightweight and Secure Authentication Scheme for IoT Based E-Health Applications", International Journal of Computer Science and Network Security 19 (1), 107-120.

[25] K. Hussain, S.J. Hussain, NZ. Jhanjhi and M. Humayun, "SYN Flood Attack Detection based on Bayes Estimator (SFADBE) For MANET", International Conference on Computer and Information Sciences (ICCIS), 1-4, 2019.

[26] K Hussain, NZ Jhanjhi, H Mati-ur-Rahman, J Hussain, MH Islam, Using a systematic framework to critically analyze proposed smart card based two factor authentication schemes, Journal of King Saud University-Computer and Information Sciences

[27] S. Jawad Hussain, Usman Ahmed, H. Waqas, S. Mir, NZ. Jhanjhi, and M. Humayun, "IMIAD: Intelligent Malware Identification for Android Platform," IEEE 2019 International Conference on Computer and Information Sciences (ICCIS), Al Jouf, Saudi Arabia, 2019

[28] Adeyemo Victor Elijah, Azween Abdullah, NZ JhanJhi, Mahadevan Supramaniam and Balogun Abdullateef O, "Ensemble and Deep-Learning Methods for Two-Class and Multi-Attack Anomaly Intrusion Detection: An Empirical Study" International Journal of Advanced Computer Science and Applications (IJACSA), 10(9), 2019. http://dx.doi.org/10.14569/IJACSA.2019.0100969

[29] Humayun, M., Niazi, M., Jhanjhi, N. et al. Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. Arab J Sci Eng (2020). https://doi.org/10.1007/s13369-019-04319-2