International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 3, April 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Comparative Study of Fileless Ransomware

Krishna B L

Department of Computer Science & IT, Jain Deemed-To-Be-University, Bengaluru, Karnataka, India

ABSTRACT

A Fileless Ransomware is a new type of ransomware primarily follows the mechanism of both ransomware and fileless malware. Detecting and Defending these kinds of attacks becoming a great obstacle for IT firms. Cybercriminals found a new way of extorting ransom with vicious methods mainly from big organizations, government, Telecom Industry and many more. Traditional AV Engines are not able to defend Fileless Malware. This paper describes the mechanism of both ransomware and fileless malware, the working of fileless ransomware, what are the possible attack vectors of fileless ransomware, variations of fileless ransomware and their instances, Prevention methods and recommendation to defend against Fileless ransomware.

KEYWORDS: *Fileless Ransomware (FLRw), Anti-Virus (AV), Windows Management Instrument (WMI), Power Shell (PS), Command & Control (C&C)*

How to cite this paper: Krishna B L "Comparative Study of Fileless Ransomware" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-3, April 2020, pp.608-616, URL: www.ijtsrd.com/papers/ijtsrd30600.pdf

IJTSRD30600

Copyright © 2020 by author(s) and International Journal of Trend in Scientific Research and Development Journal. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0) (http://creativecommons.org/licenses/by/4.0)

1. INTRODUCTION

In current era computer science is major subject. It has many real-life applications such as cloud computing [1], artificial intelligence [2], virtualization environment [3], Internet of things [4,5,6,7,8,9,10,11], transportation problem [12,13], shortest path problem [14,15,16,17,18,19,20,21], internet Security[22], uncertainty [23,24,25,26] and so on. Malware is not a new threat in security where it exists for decades. Malware methodologies are updating so were countermeasures for the malware. Now it took a new approach to evade the traditional countermeasure and emerging of fileless malware.

A Fileless Malware (FLMw) is exactly not complete fileless rather it can be called as "bodiless malware" or "living off the land" is a new approach where the malware doesn't have any physical existence as such as a file but, a malicious exploit code injected directly to the RAM can be done by injecting the code to the currently running tasks. [27] These types of malware will be injected in various attack vectors like, victims visiting unsecured pages and redirected to malicious pages which leads to fileless malware injection.

Ransomware is one of the emerging Threats in Security. A type of malicious software or code which ciphers victim's files or even the entire system with a strong encryption process and demands a ransom amount for the decryption. Ransomware doesn't target any specific user, either it could be a big company or ordinary home user. Ransomware becoming a vicious method that helps cybercriminals to earn in millions of dollars by demanding a ransom amount. [28-29] Some of the ransomware is even worse that even after the receiving of ransom also, the ransomware destroys the entire victim's data. Most of the organization will never have a second thought for not paying ransom due to the level confidentiality of the data which is ciphered with strong asymmetric encryption (Most of the time it will Asymmetric encryption, where it will be stored in attacker C&C servers) where attacker demand for a huge ransom most of the time payment can be done through the bitcoin where the attacker will provide his bitcoin address. The transaction will be taking place in the dark web which can be accessed through Tor Browsers.

2. MECHANISM

FLRw is the combination of both FLMw and ransomware. [30] Precisely the mechanism is combined to stay stealth. For example, These FLRw's utilizes some of the Microsofts Utility tools specifically PS and WMI. Microsoft native scripting language a.k.a PS which helps users to perform custom tasks that need to be performed by the operating system. PS has access to core functions of O.S, so gaining access to PS by intruder also leads to adverse consequences.

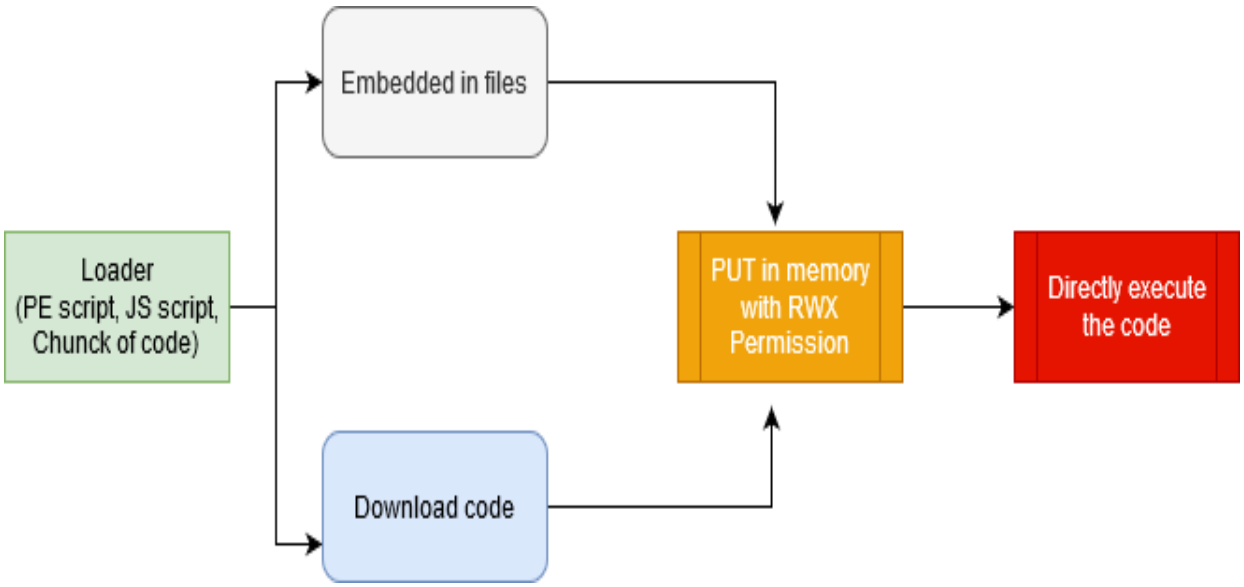

Figure.1 File less attack mechanism [31]

As you can see the Figure1. [31] First, the code will be written into native scripting language like JavaScript, PS script, etc:-. Second, the written code is either embedded into any files or the script is downloaded through any malicious website which directly enters into memory and code will be injected into any running processes which looks legitimate by this it won't be veiling to AV engines. After injecting into the process, secondly, the legitimate process execution memory space will be filled with malicious code and it will download additional scripts and encryption keys required from the host server. After getting the required script encryption will take place. The scale of the attack may differ from one system to overall enterprise network systems and a range of ransom will also be proportional.

3. FILELESS RANSOMWARE FAMILIES

PoshCoder / PowerWare: -

First-ever FLRw, named PoshCoder. Poshcoder leveraged on PS for an attack but it was unsuccessful due to programming flaw where instead of decrypting after the ciphering the files it was about to delete the encrypted files due to programming logic.

PowerWare a new version of PoshCoder can say; PowerWare working is similar to PoshCoder in which the flaw is patched. In Figure.3.1 An infected file is downloaded into the system through malicious campaigns or by sending emails. when the infected file is executed, the attached payload 1 which consists of connection script to host server will be executed and access PS in hidden mode will download the Payload 2, the actual ransomware script along with the keys for the encryption from the host server. The script consists set of file extension lists to encrypt the filetype according to the list. Meanwhile, in the background malware performs encryptions to files. It performs symmetric encryption using AES-256 to encrypt files and the encrypted files have an extension (<filename>.poshcoder). After the encryption, the key is transferred back to the host server. The key is sent back to the server using the HTTP protocol. Due to the weak mechanism of this ransomware, it was easier to decrypt the files by capturing HTTP requests sent in plain text which has a key to decrypt the files sent to the host server.

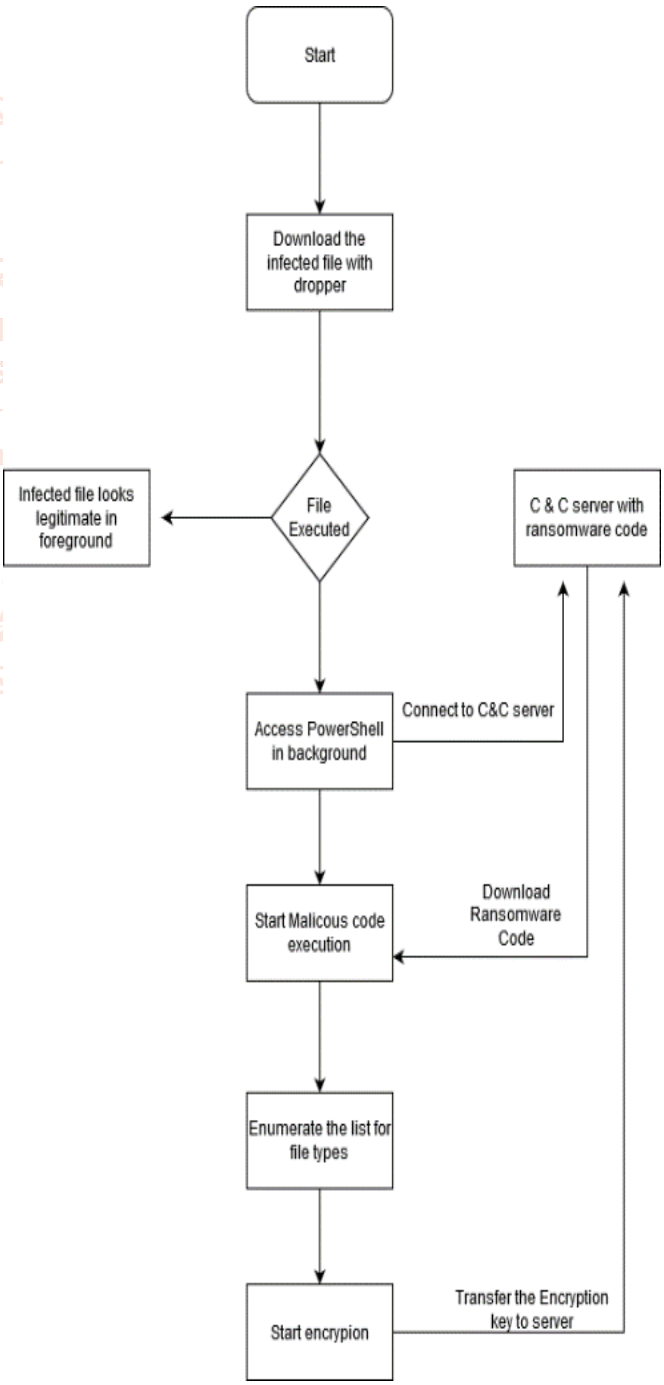

Figure2. PowerWare Flow Diagram

UIWIX:-

UIWIX is another variant of FLRw and made an effective impact. Unless PoshWarwe relays on PS, this ransomware is based on famous exploits EthernalBlue. [32] It exploits windows SMB v1, v2 protocol vulnerabilities. WannaCry and NotPetya ransomware were designed using EhternalBlue. UIWIX was considered to be far dangerous than WannaCry, because it doesn't have any kill switch in which WannaCry was performing network scan and trying to connect back to some unregistered domain, later it was mitigated by British Security researcher, who purchased the domain and helped in reverting the encryption.

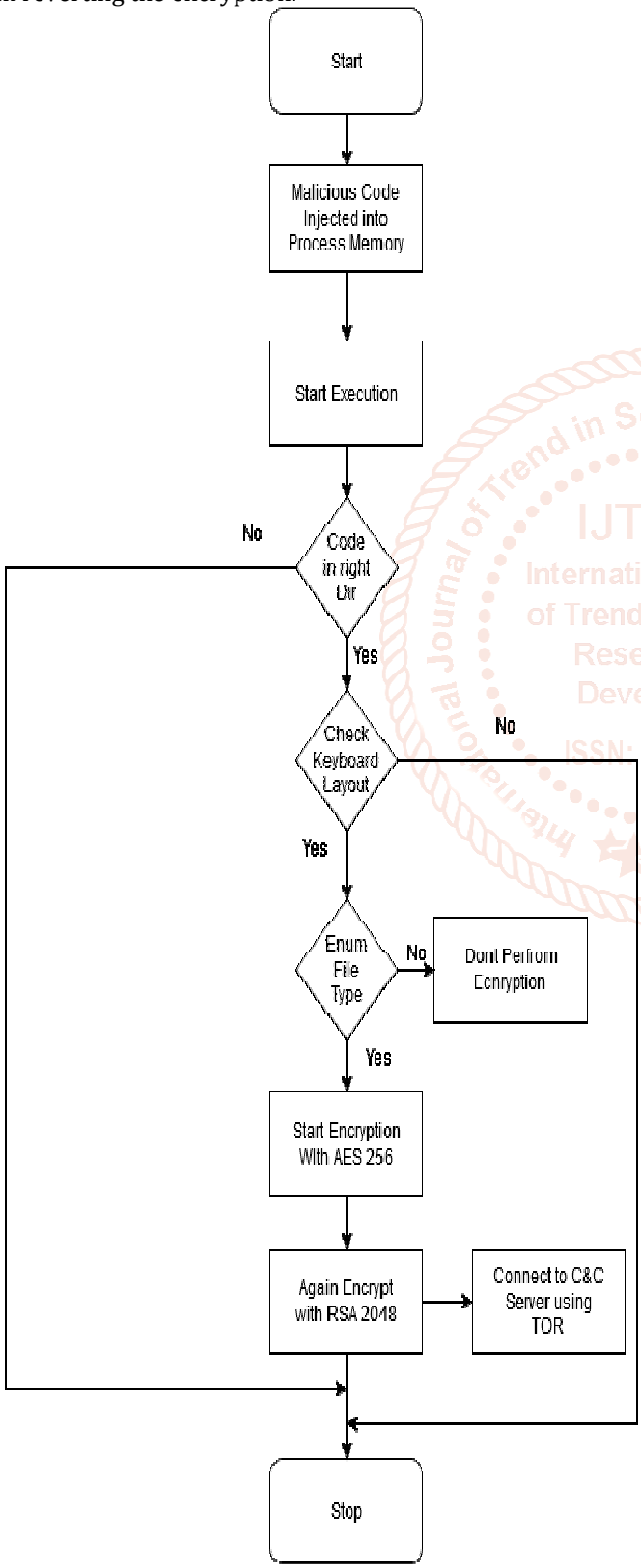

Figure3.2.1 UIWIX flowchart

In Figure3.2.1, UIWIX utilizes EthernalBlue exploit which performs remote code execution in memory due to buffer overflow vulnerability in Windows SMB v1 & v2 protocols will load the malicious DLL directly into the memory, rather than writing on disk, this made AV engines difficult to trace out this ransomware. It leaves no footprints to detect them because it directly resided into memory. Second, it goes through a series of inspections within the system for the existence of sandbox environments. First, it looks for the Debugging environment, next it looks for DLLs related to sandbox environments like Hypervisor software like VMware workstation, Virtualbox, Hyper-v, etc: - and sandboxes like Cucco. If any of these environments were found existing, it will be self-terminated. Another interesting fact is if UIWIX affected any system residing in countries like Kazakhstan, Russia, and Belarus. It again self-terminated. If none of the above environments are found, it will start the encryption process. In the encryption process first, the files are encrypted with a symmetric algorithm AES-256 with cipher blockchain mode and again with RSA 2048. WannaCry and PoshWare had a list of file extensions that needed to be encrypted. This ransomware encrypts all types of files existing in the system except files in the Windows folder and boot folder and again it performs RC4 encryption on the AES encrypted files. The encrypted files extension was <uniquecode>.uiwix, where unique code is 10 digit code which represents the victim ID and concatenated with .uiwix extension. It leaves a _DECODE_TEXT.txt file in the folder, which provides the instructions to the victim to pay ransom for the key to decrypt the files. After successful encryption, mini-tor.dll is loaded into memory will create a Tor connectivity to C&C server for transferring the key. It doesn't have a worm-like feature in WannaCry, which search for vulnerable systems in the network to continue the attack on those systems too.

SynAck:-

SynAck is meant for stealth and sophisticated technique, it is the first-ever FLRw which leverage the attack using the process injection technique called **Process Doppelgänging**. [33] This method utilizes the NTFS transaction also knows a TxF in windows which is the core functionality of the operating system for handling the files in the atomicity feature that will be used to inject the malicious code into the memory section looks like a legitimate process

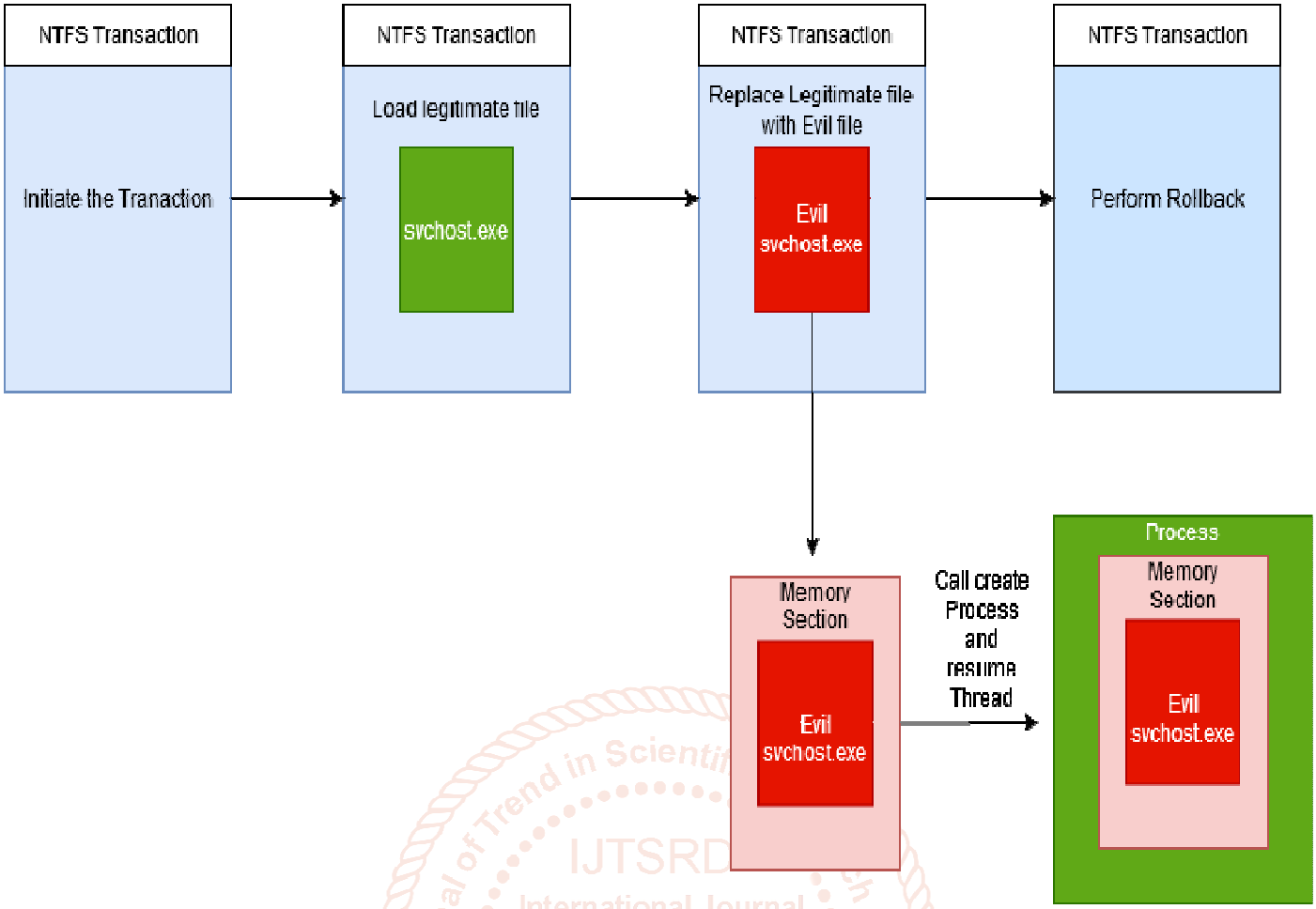

Figure3.3.1. Process Doppelgänging

Figure3.3.1 explains, First, it initiates the TxF transaction with a legitimate process file and that file is replaced with malicious code. Next, a section of memory is created for malicious code and it will reside in that section of memory. Later this will cancel the initiated transaction by calling the rollback function which makes the transaction never happened. Later it calls the process create function in the kernel to initiate a process of malicious code reside in the section of memory which starts the process without executable loaded. In Figure3.3.2 explains, The System library functions called indirectly by performing various arithmetic calculations and it does store the list of hash values, encode in the malware. These hash values are the running legitimate processes of application like hypervisors, backup applications, business applications, and script interpreters, etc: -. Like UIWIX, this ransomware scans for keyboard layouts and country region to determine whether the victim is from Belarus, Kazakhstan, Russia, and other soviet countries if so, it will be self-terminated. It has a list of directories that ransomware needs to perform the execution, the list determines whether the ransomware is in not in any of the sandbox environment, if it is not located in those directories it will avoid the execution and self-terminated. Later it goes through the hardcoded hash values to enumerate the running process and killing those processes will avoid locking the files from those processes and fasten the ransomware execution too. SynAck goes through multi-level encryption due to usage of ECIES hybrid encryption scheme combination of secp192r1 a standard NIST elliptic curve, PBKDF2-SHA1 as key derivation function (KDF), HMAC-SHA1 as Message authentication code (MAC) and XOR and AES 256 with EBC mode as ENC. This encryption scheme ensures no brute-force technique can be applied to obtain the key. This encryption also ensures the uniqueness of each victim because it collects the system information like system information, OS version, and username, along with some public keys generated by ransomware that will be taken as input for the encryption process. SynAck has a list of file extensions to encrypt the files which cover most of all the file types. Every encrypted filename is replaced with some random text which is generated by encryption scheme, running in the background. After the successful encryption, this will modify the registries and display the ransom message on the login screen with email id for the instruction and release the ransom note on the desktop with a ransom note. It consists of steps to follow to pay ransom for the decryption key and a unique base64 message which is generated by ransomware to authenticate the victim by the hacker

Sorebrect:-

Sorebrect is First ever FLRw, which utilizes another process injection technique called Process Hollowing. Like PoshWare, Sorebrect is a modified version of virulent AES-NI ransomware. Sorebrect affected middle east countries at the beginning, later it has affected all other regions in the world. The delivery method of this ransomware may use droppers to deliver to the system which uses PS to perform the injection.

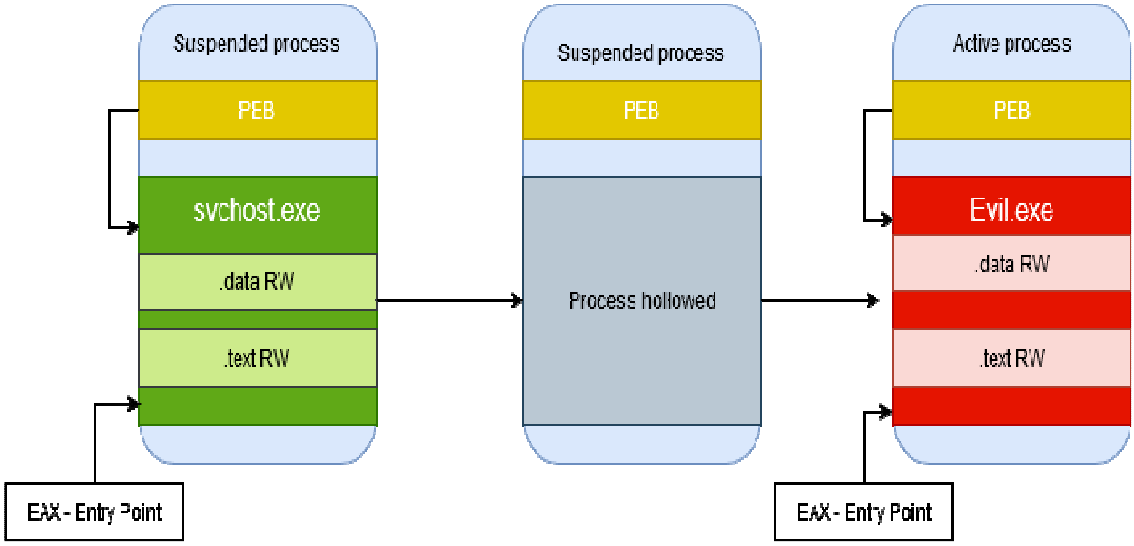

Figure3.4.1 Process hollowing

The injection technique is similar to SynAck where it uses Process Doppelgänging method, Sorebrect uses Process Hollowing method; In Figure3.4.1, [34-35] it looks for the legitimate processes like svchost, it will initiate the legitimate process in suspended mode, the process image loaded in memory will be overwritten with the malicious image, it will resume the existing process. When the process monitor is inspected, svchost will be displayed as normal and look like a legitimate process but in the background, ransomware will start execution.

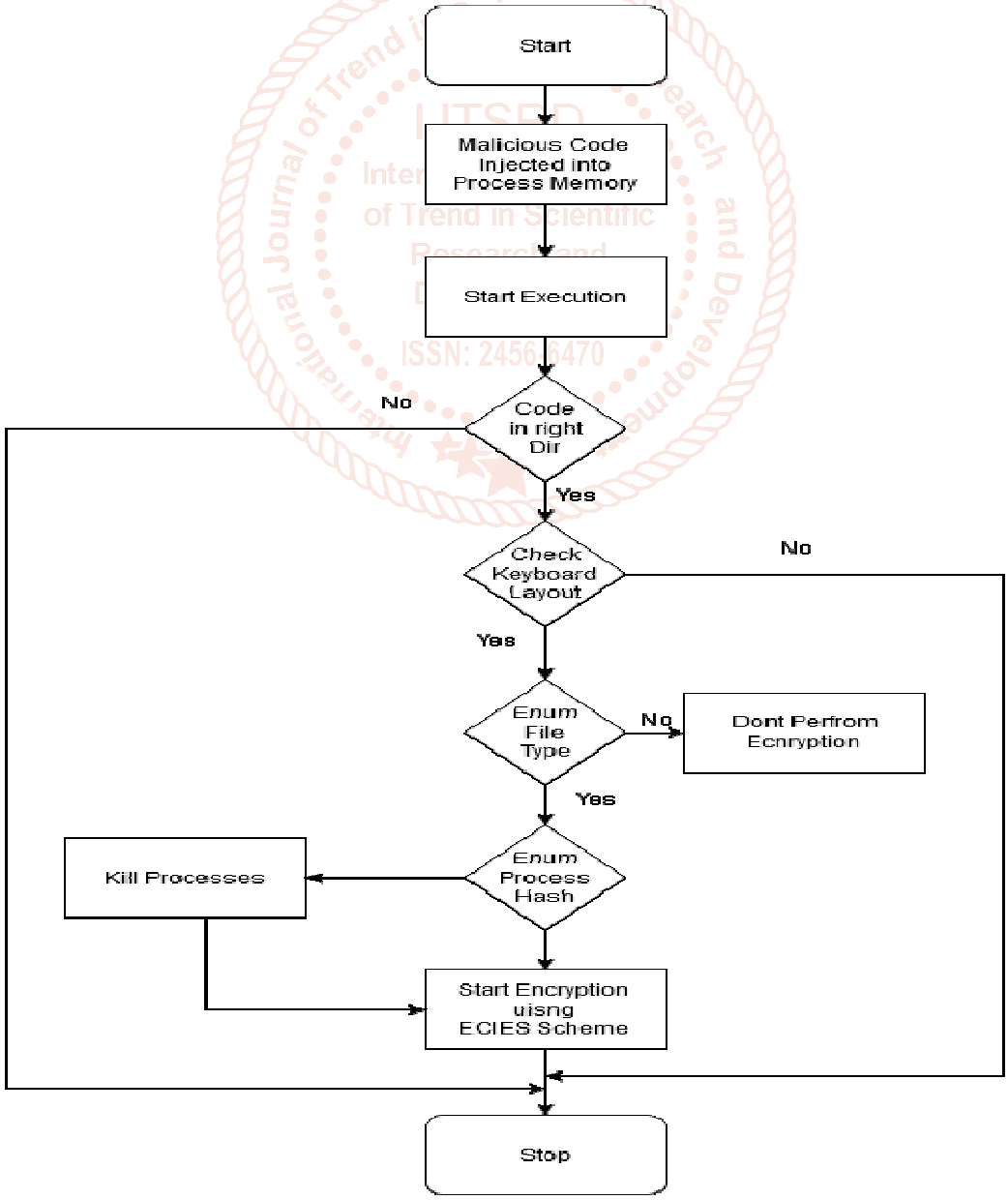

Figure3.3.2 SynAck Flowchart

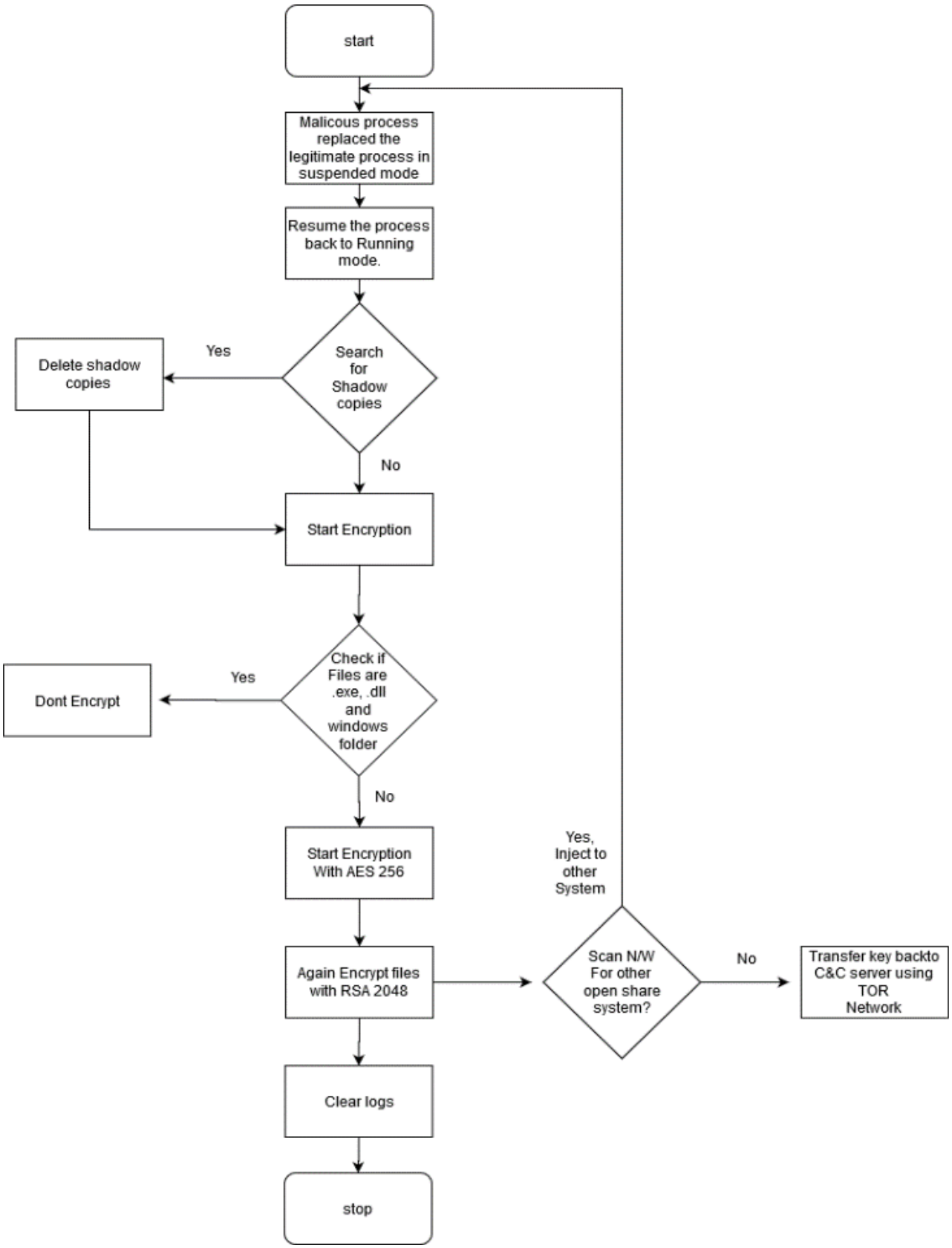

Figure3.4.2: Sorebrect Flow diagram

When it starts the execution, first it looks for all the restore points, shadow copies within the system. If it found any of it, it will be deleted. So, this user cannot revert to a normal stage. Except .exe, .dll, .msi and Windows folder, it will encrypt all files in the system. It goes through two stages of encryption, First, it will encrypt the files with AES-256 EBC mode and again the files and keys are encrypted with RSA-2048 and append the .pr0tect extension to the files. It has a worm-like feature like WannaCry; it performs network scans on the local network for other open share systems with read-write access. If it found any of the systems available, it will encrypt those systems. After the successful encryption, the keys are sent back to the C&C server using secured tor network connectivity for the anonymity and deletes the traces of malware by deleting all logs of the system using the wevtutil process. Later a ransom note is dropped on the system which has a unique id to identify the victim needed to send back to the attacker and further process to follow for paying the ransom to revert the decryption. This Ransomware was targeting primarily the manufacturing industries.

4. POSSIBLE ATTACK VECTOR

Attack vectors of ransomware are numerous methods. Traditional AV engines cannot defend every time against ransomware if users performed some dangerous tasks unknowingly and Some of them are attacker methods are mentioned below: -

- Visiting unsecured webpages is one the major way where the code will directly be downloaded when the user visited the page.
- Phishing campaigns help cybercriminals to inject the code.
- Downloading the file from untrusted sources.
- Trying to install pirated versions on systems where the cracker who made crack version previously mentioned about AV detection of malware as False Negative.
- Drive-by-downloads exploits
- Macro downloader
- DNSmessanger is another way delivering the payloads without files using DNS network protocol [36]
- Packers are mainly used to make the malicious payloads to be hidden. While the attacker will be embedded in the malicious code in the legitimate executable. So when the user loaded the legitimate file the malicious payload will be unpacked and injected directly into the memory.
- Malvertising.

5. DETECTION OF FILELESS RANSOMWARE

Setting up an event listener for any changes in registries can be useful enough detecting the ransomware which needs to modify the registries for persistence to stay on the system [37]. Executing the suspicious files in an isolated code execution engine. These engines provide an execution environment for executables. It will display how the memory will be allocated by the process and the user can interrupt the execution at any point when the user finds any suspicious activity like illegal memory alteration, string manipulations, etc: -. obfuscated code also be analyzed in these engines where the obfuscated need to be extracted at the memory level [38].

Goldilocks Principals determines the code type and requirements for code execution. Performing Advanced dynamic analysis using these engines also be helpful because most the FLRw uses PS, So we can view the list of Windows API which is calling by the code, we can detect the FLRw. [39] Detecting the process hollowing using memory forensics like by detecting the relation between parent and child process we can find out the suspicious execution. Because each process will be executed by a certain parent process. Comparing VAD and PEB structure will help in detecting process hallowing because a VAD node consists of a start, end addresses and full path of executables. Duplication of running services. Looking for isolated memory allocation will also be a good method for detecting process hallowing. [40] Real-time monitoring the shadow copies availability because the deletion of shadow copies is the first step performed by any ransomware where shadow copies helps in system restore to the copied version.

6. MITIGATION OF FILELESS RANSOMWARE

Prevention of an attack will be a bit easy compared to detecting the attack. Because one cannot defend an attack without knowing where the attack is originating from and what medium it is using. Process isolation for webpages, where isolated memory will be allocated for each page user visited so by this when a script is downloaded the malicious will be executed within that sandboxed memory so even when it tries to access for WMI or PS [41]. Blocking of all unused ports and services, turning off the banners of the service and modifying the default ports of the service will block the attacker from enumerating the system to intrude int the system.

Hiding the computer registries and setting proper access privilege and permissions for PS because the majority of FLRw depends on PS due to accessibility of core functionality of O.S Secure use of the internet is best the defense against these attacks all though attacker a new way intrudes into the system but still, we can defend these attacks to some extent and blocking all infected communications, emails, services, servers, etc: -.Disabling macro downloaders, using adblockers, Updating OS will help in fixing the newly discovered security process and keeping AV engines Up to date. This must be done for example SynAck utilizes the same vulnerabilities. Providing Cybersecurity awareness for users in an organization about secure usage of the organization resources and implementing appropriate security measures for organization and security policies for an organization [42]. Backup of any confidential data in a trusted and secured location or isolated place [43-55]. Not only the data for shadow copies of the systems will also help to restore the system to normal conditions if attack executed successfully. Creating multiple copies of shadow copies and storing them in an isolated environment will be easier enough to restore the system to normal.

CONCLUSION

Security is a myth and it cannot be applied 100 percent. Because Fileless Ransomware is evolving when compared to earlier releases. Currently, Security experts are putting tremendous effort to defend these kinds of ransomware by coming up with various proactive and detective techniques. As per the current security techniques, we can secure the system against the ransomware. But humans do make mistake by nature. FLRw is just a new beginning for this approach because it does use a fileless mechanism and the technique may differ from variant to variant. The chances of emerging of these type ransomwares are very high. A zero-day attack is far effective than an existing attack and the consequences can't be even imaginable. Practicing security as part of the development will be helpful.

ACKNOWLEDGEENT:

I would like to express my profound gratitude to professor Mr Subarna Panda, for their patient, encouragement and valuable assessments of this research work. I appreciate his willingness to generously contribute time.

REFERENCES

[1] X. Xu, "From cloud computing to cloud manufacturing," Robotics and Computer-Integrated Manufacturing, vol. 28, pp. 75-86, 2012.

[2] M. Haenlein and A. Kaplan, "A brief history of artificial intelligence: on the past, present, and future of artificial intelligence," California Management Review, vol. 61, pp. 5-14, 2019.

[3] H. Zheng, D. Liu, J. Wang, and J. Liang, "A QoE-perceived screen updates transmission scheme in desktop virtualization environment," Multimedia Tools and Applications, vol. 78, pp. 16755-16781, June 2019.

[4] Mohapatra, Hitesh; Rath, Amiya Kumar: 'Detection and avoidance of water loss through municipality taps in India by using smart taps and ICT', IET Wireless Sensor Systems, 2019, 9, (6), p. 447-457, DOI: 10.1049/iet-wss.2019.0081, IET Digital Library, https://digitallibrary.theiet.org/content/journals/10.1049/iet-wss.2019.0081.

[5] Mohapatra, Hitesh; Rath, Amiya Kumar: 'Fault-tolerant mechanism for wireless sensor network', IET Wireless Sensor Systems, 2020, 10, (1), p. 23-30, DOI: 10.1049/iet-wss.2019.0106, IET Digital Library, https://digital-library.theiet.org/content/journals/10.1049/iet-wss.2019.0106

[6] Hitesh. Mohapatra, "HCR using neural network," Biju Patnaik University of Technology, M.Tech. dissertation 2009.

[7] H. Mohapatra, S. Debnath, and AK. Rath, "Energy management in wireless sensor network through EB-LEACH," International Journal of Research and Analytical Reviews (IJRAR), pp. 56-61, 2019.

[8] VN. Nirgude, H Mahapatra, and SA. Shivarkar, "Face recognition system using principal component analysis & linear discriminant analysis method simultaneously with 3d morphable model and neural network BPNN method," Global Journal of Advanced Engineering Technologies and Sciences, vol. 4, p. 1, 2017.

[9] M. Panda, P. Pradhan, H. Mohapatra, and NK. Barpanda, "Fault Tolerant Routing In Heterogeneous Environment," International Journal of Scientific & Technology Research, vol. 8, pp. 1009-1013, 2019.

[10] Mohapatra, Hitesh; Rath, Amiya Kumar: 'Fault tolerance in WSN through PE-LEACH protocol', IET Wireless Sensor Systems, 2019, 9, (6), p. 358-365, DOI: 10.1049/iet-wss.2018.5229, IET Digital Library, https://digital-library.theiet.org/content/journals/10.1049/iet-wss.2018.5229.

[11] D. Swain, G. Ramkrishna, H. Mahapatra, P. Patra, and PM. Dhandrao, "A novel sorting technique to sort elements in ascending order," International Journal of Engineering and Advanced Technology, vol. 3, pp. 212-126, 2013.

[12] R. Kumar, SA. Edalatpanah, S. Jha, and R. Singh, "A Pythagorean fuzzy approach to the transportation problem," Complex and Intelligent System, vol.5, pp. 255-263, 2019.

[13] J. Pratihar, R. Kumar, A. Dey, and S. Broumi, "Transportation problem in neutrosophic environment," in Neutrosophic Graph Theory and Algorithms, F. Smarandache and S. Broumi, Eds.: IGI-Global, 2019, ch. 7, pp. 176-208.

[14] S Broumi , A. Dey, M. Talea, A. Bakali, F. Smarandache, D. Nagarajan, M. Lathamaheswari and R Kumar, "Shortest path problem using Bellman algorithm under neutrosophic environment," Complex & Intelligent Systems, vol. 5, pp. 409-416, 2019.

[15] R Kumar, SA Edalatpanah, S. Jha, S. Broumi, R. Singh, and A. Dey "A multi objective programming approach to solve integer valued neutrosophic shortest path problems," Neutrosophic Sets and Systems, vol. 24, pp. 134-149, 2019.

[16] R. Kumar, A. Dey, F. Smarandache, and S. Broumi, "A study of neutrosophic shortest path problem," in Neutrosophic Graph Theory and Algorithms, F. Smarandache and S. Broumi, Eds.: IGI-Global, 2019, ch. 6, pp. 144-175.

[17] R. Kumar, SA. Edalatpanah, S. Jha, and R. Singh, "A novel approach to solve gaussian valued neutrosophic shortest path problems," Int J Eng Adv Technol, vol. 8, pp. 347-353, 2019b.

[18] R. Kumar, SA. Edalatpanah, S. Jha, S. Gayen, and R. Singh, "Shortest path problems using fuzzy weighted arc length," International Journal of Innovative Technology and Exploring Engineering, vol. 8, pp. 724-731, 2019.

[19] R. Kumar, SA. Edaltpanah, S. Jha, S. Broumi, and A. Dey, "Neutrosophic shortest path problem," Neutrosophic Sets and Systems, vol. 23, pp. 5-15, 2018.

[20] R. Kumar, S. Jha, and R. Singh, "A different approach for solving the shortest path problem under mixed fuzzy environment," International Journal of fuzzy system Applications, vol. 9, pp. article--6, 2020.

[21] R. Kumar, S. Jha, and R. Singh, "Shortest path problem in network with type-2 triangular fuzzy arc length," Journal of Applied Research on Industrial Engineering, vol. 4, pp. 1-7, 2017.

[22] J. Sakhnini, H. Karimipour, A. Dehghantanha, RM. Parizi, and G. Srivastava, "Security aspects of Internet of Things aided smart grids: A bibliometric survey," Internet of Things, p. 100111, 2019.

[23] S. Gayen, F. Smarandache, S. Jha, and R. Kumar, "Interval-valued neutrosophic subgroup based on interval-valued triple t-norm," in Neutrosophic Sets in Decision Analysis and Operations Research, M. Abdel-Basset and F. Smarandache, Eds.: IGI-Global, Dec. 2019c, ch. 10, p. 300.

[24] S. Gayen, F. Smarandache, S. Jha, MK. Singh, S. Broumi and R. Kumar, "Introduction to plithogenic subgroup," in Neutrosophic Graph Theory and Algoritm, F Smarandache and S Broumi, Eds.: IGI-Global, Oct. 2019b, ch. 8, pp. 209-233.

[25] S. Gayen, S. Jha, M. Singh, and R. Kumar, "On a generalized notion of anti-fuzzy subgroup and some characterizations," International Journal of Engineering and Advanced Technology, vol. 8, pp. 385-390, 2019.

[26] J. Pratihar, R. Kumar, SA Edalatpanah and A. Dey, " Modified Vogel's Approximation Method algorithm for transportation problem under uncertain environment," Complex & Intelligent Systems, (Communicated).

[27] Fred O'Conner - Fileless Malware 101: Understanding Non-Malware Attacks - https://www.cybereason.com/blog/fileless-malware

[28] Daniel Gonzalez Thaier Hayajneh - Detection and Prevention of Crypto-Ransomware - ieeexplore.ieee.org/document/8249052

[29] Jeremy Kirk - Ransomware Payments: Where Have All the Bitcoins Gone? -

https://www.bankinfosecurity.com/ransomware-where-does-bitcoin-money-go-a-10747

[30] Nick Ismail - Defending against fileless malware - https://www.information-age.com/defending-fileless-malware-123466835/

[31] Fileless Ransomware Infections – How Does This Really Work? - https://www.asigra.com/blog/fileless-ransomware-infections-how-does-really-work

[32] Tal Liberman, Eugene Kogan - Lost in Transaction: Process Doppelgänging - https://www.blackhat.com/docs/eu-17/materials/eu-17-Liberman-Lost-In-Transaction-Process-Doppelganging.pdf.

[33] Nadav Grossman - EternalBlue – Everything There Is To Know - https://research.checkpoint.com/2017/eternalblue-everything-know/.

[34] KA. Monnappa - What Malware Authors Don't Want You to Know -Evasive Hollow Process Injection - https://www.blackhat.com/docs/asia-17/materials/asia-17-KA-What-Malware-Authors-Don%27t-Want-You-To-Know-Evasive-Hollow-Process-Injection-wp.pdf.

[35] Walter Glenn - What Is the Service Host Process (svchost.exe) and Why Are So Many Running? - https://www.howtogeek.com/howto/windows-vista/what-is-svchostexe-and-why-is-it-running/

[36] Tom Spring - New Fileless Attack Using DNS Queries to Carry Out PS Commands - https://threatpost.com/new-fileless-attack-using-dns-queries-to-carry-out-PS-commands/124078/.

[37] Ellen Zhang - What is Fileless Malware (or a Non-Malware Attack)? Definition and Best Practices for Fileless Malware Protection - https://digitalguardian.com/blog/what-fileless-malware-or-non-malware-attack-definition-and-best-practices-fileless-malware.

[38] Goverdhan Reddy Jidiga, P. Sammulal - The need for awareness in cybersecurity with a case study - https://ieeexplore.ieee.org/document/6726789/

[39] Monnappa K A - Detecting Deceptive Process Hollowing Techniques Using HollowFind Volatility Plugin - https://cysinfo.com/detecting-deceptive-hollowing-techniques/

[40] Travis Rosiek - The 5 Challenges of Detecting Fileless Malware Attacks - https://www.darkreading.com/attacks-breaches/the-5-challenges-of-detecting-fileless-malware-attacks/a/d-id/1332557

[41] Vasily Bukasov - How to provide process isolation and not destroy Windows - https://hackmag.com/security/win-isolation/

[42] Randell Jesup - Process Isolation in Firefox - https://mozilla.github.io/firefox-browser-architecture/text/0012-process-isolation-in-firefox.html

[43] Clemens Kolbitsch, Paolo Milani Comparetti, Christopher Kruegel, Engin Kirda, Xiaoyong Zhou, and XiaoFeng Wang - EffectiveandEfficient Malware Detection at the End Host - https://www.usenix.org/legacy/event/sec09/tech/full_papers/kolbitsch.pdf

[44] Chris Dale - Detecting if Volume Shadow Copies has been explicitly disabled through registry - https://www.securesolutions.no/detecting-if-volume-shadow-copies-has-been-disabled/

[45] Jason Faulkner - What Are "Shadow Copies", and How Can I Use Them to Copy Locked Files? - https://www.howtogeek.com/129188/htg-explains-what-are-shadow-copies-and-how-can-i-use-them-to-copy-or-backup-locked-files/

[46] Mohapatra H., Rath A.K. (2019) Fault Tolerance Through Energy Balanced Cluster Formation (EBCF) in WSN. In: Tiwari S., Trivedi M., Mishra K., Misra A., Kumar K. (eds) Smart Innovations in Communication and Computational Sciences. Advances in Intelligent Systems and Computing, vol 851. Springer, Singapore.

[47] Mohapatra, Hitesh A Debnath, Sourabh A Rath, Amiya Kumar, Energy Management in Wireless Sensor Network Through EB-LEACH, J International Journal of Research and Analytical Reviews (IJRAR), N Special Issue, ICFTEMST-19, P 56-61, D 2019, I e ISSN 2348 – 1269, Print ISSN 2349-5138.

[48] Fundamentals of Software Engineering: Designed to provide an insight into the software engineering concepts, Mohapatra, H, Rath, A.K. 9789388511773, https://books.google.co.in/books?id=puPJDwAAQBAJ, 2020, BPB PUBN.

[49] AndeVinay Kumar, Mohapatra, Hitesh, SSO Mechanism in Distributed Environment, image, 2015.

[50] Chawla, Harsha, Mohapatra, Hitesh, Globalization and its Impact on Indian Culture and Technology,2016.

[51] Raut, Shubham, Shinkar, Nilesh, Sathe, Dhananjay, Nehete, Lalit, More, Amey, Mohapatra, Hitesh.Four-way Integrated Authentication for Android Smart-phone.

[52] Mohapatra, Hitesh, Rath, Amiya Kumar Advancing Generation Z Employability through New Forms of Learning: quality assurance and recognition of alternative credentials.

[53] Masuti, Mayur, Mohapatra, Hitesh, Human Centric Software Engineering, 2015.

[54] Behura, Asmini, Mohapatra, Hitesh, IoT Based Smart City with Vehicular Safety Monitoring, 2516-2314, 2019, EasyChair.

[55] Mohapatra, Hitesh , Ground Level Survey on Sambalpur In the Perspective of Smart Water, 2516-2314, 2019, EasyChair