International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307

OPEN ACCESS

Available Online at : www.ijsrcseit.com

doi : https://doi.org/10.32628/CSEIT243648

The Evolving Threat Landscape: How Cyber Threat Intelligence Empowers Proactive Defenses against WannaCry Ransomware

Jumoke Eluwa[1], Patrick Omorovan[1], & Dipo Adewumi[2] & Oluwafunmilayo Ogbeide[1]

[1]School of Science, Engineering and Environment, the University of Salford, Manchester, UK.

[2]School of Computing, Engineering and Digital Technologies, Teesside University, Middleborough, UK

ARTICLEINFO

Article History:

Accepted: 20 March 2024

Published: 03 April 2024

Publication Issue

Volume 10, Issue 2

March-April-2024

Page Number

403-411

ABSTRACT

Cyber threat intelligence (CTI) is a rapidly growing field that plays an essential role in ensuring the security of online systems. CTI refers to the intelligence that is gathered, analyzed, and disseminated to help organizations understand and respond to cyber threats. This information can be used to identify vulnerabilities, detect potential attacks, and develop strategies to mitigate risks. The field of CTI is constantly evolving, as cyber threats become more sophisticated and complex. Legacy security measures like firewalls and anti-virus software are no longer enough to protect organizations from the many threats they face. CTI provides a proactive approach to cybersecurity, by enabling organizations to anticipate and prepare for threats before they occur. CTI relies on the collection and analysis of data from multiple sources, such as open-source intelligence (OSINT), dark web forums, social media, and other threat intelligence streams. The data is analyzed using a wide range of tools and techniques, including machine learning and artificial intelligence, to identify patterns and trends that may indicate a potential threat. One of the key benefits of CTI is its ability to help organizations understand the tactics, techniques, and procedures of attackers. By analyzing the behaviors, strategies, tactics, and actions of threat actors, organizations can develop a more comprehensive understanding of the threats they face and can better prepare for potential attacks.

Keywords : Cyber Threat Intelligence, Threat Landscape, Ransomware

I. INTRODUCTION

Ransomware, a subset of malware, is considered as one of the most significant and rapidly expanding cyber threats to the digital world [1] and it is presently thought to be both the biggest threat to the Internet users and the main source of cash for hackers [2]. According to popular definitions, ransomware is one kind of virus that takes over a victim's computer or other device, encrypts a file, and demands that the

victim pay a ransom, usually in the form of cryptocurrency or another kindof payment, to regain access to the infected system [3]. Ransomware is disseminated by hackers and other persons with malicious intentions. Following its spread, this infection type is challengingto treat as all crucial files are corrupted. According to [4], employees contribute to the spreaddue to neglect or ignorance caused by a lack of awareness. Exploiting systems' known or unknown vulnerabilities, visiting infected websites, or using deep webs are some of the traditional ways that ransomware is propagated. In addition to WannaCry, TorrentLocker, CryptoWall, CryptoTear, Fusob, and Reveton, there are many different varieties of ransomware. The WannaCry ransomware, sometimes referred to as WanaDecrypt0r, WCry, WannaCry, WannaCrypt, and WanaCrypt0r, was found on May 12, 2017, following a large attack and had an approximate impact on more than 150 nations and 300,000 Windows systems [5]. Telecommunications, gas and oil production, healthcare, and government were among the industries that were impacted by the attack [6].

In the last five years, ransomware assaults have become one of the most common cyber-attacks hitting enterprises all over the world. The Verizon Data Breach Investigative Report (DBIR)2021 positions that 37% of international firms reported being attacked by ransomware [7]. After infecting a victim's machine, ransomware prevents users from accessing their resources. The infiltration by malware has evolved into a major security risk for modern individuals, businesses, and governments. Invading a computer system or network to steal information or cause disruption is called a cyberattack. By "malware," we mean malicious software such as computer viruses, worms, Trojan horses, ransomware, and spyware. Cybercriminals create these viruses, worms, and Trojan horses to steal information, blackmail victims into paying ransom, or otherwise cause mayhem in online systems.

Malware intrusion has become more sophisticated over the years, making it more challenging for cybersecurity experts to detect and prevent attacks. Malware intrusion is a significant threat to individualusers of computers and smartphones. Cybercriminals can put malicious software on these devices, whichlets them steal sensitive information like banking information, passwords, and personal identification information. Malware can also hijack the device and use it as part of a larger network to perform larger attacks or to spread the malware to other devices. In addition, ransomware has become a popular type ofmalware, which locks users out of their devices and demands payment to regain access. Malware intrusion is also a significant threat to organizations of all sizes. Cybercriminals can use malware to compromise the security of the entire network and access sensitive company data. This can result in many problems, such as data leaks, theft of intellectual property, financial leakages, anddamage to the company's reputation. Malware can also be used to launch distributed denial of service (DDoS) attacks, which can cause websites to crash and disrupt business operations.

Furthermore, malware infections can pose a serious risk to national security. The power grid, water supply systems, and transportation networks are all vulnerable to malware attacks. This can lead to a significant disruption in the functioning of the infrastructure and can have dire consequences for the safety and wellbeing of citizens. Malware can also be utilized to steal sensitive information from government agencies and launch cyberattacks against other countries. Malware intrusion is a significant threat to individuals, organizations, and nations. Cybercriminals use malware to exploit vulnerabilities in computer systems, steal data, extort money, or cause chaos. It is very necessary to be aware of the various types of malwares and take appropriate measures to protect against them. This includes installing and updating antivirus software, regularly backing up data, using strong passwords, and being cautious of suspicious emails and links. Additionally, keeping abreast of cybersecurity news and developments is

crucial for staying aware of emerging threats and developing countermeasures [8].

In recent years, there has been an unprecedented surge in the frequency of cyber-attacks, with some going unnoticed while others have gained media attention due to their severe impacts. One of the notable incidents that occurred in the past few years was the WannaCry Ransomware attack, which exploited a vulnerability in older Windows systems and affected many institutions. The NHS breach in the United Kingdom was one such example. The WannaCry attack had a wide-ranging impact and severely affected the NHS system's network architecture [9]. It spread through the computer networks of approximately eighty NHS Trust hospitals, completely taking over their systems (Figure 1). The ransomware infiltrated their systems, encrypted their files, and is now holding them for ransom.

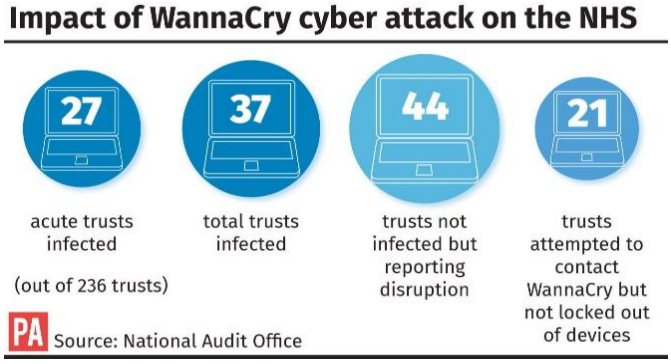

Figure 1: Impact of WannaCry Attack on the NHS

II. LITERATURE REVIEW

WannaCry, one of the largest and most damaging cyberattacks in recent history, a piece of malicious software released in May 2017 which quickly spread around the globe. This ransomware infected over 200,000 computers in 150 countries. The WannaCry malware targeted Microsoft Windows operating systems, encrypting victims' files, and demanding ransom payments in exchange for the decryption keys. In this literature review, we examine various studies and reports on the WannaCry malware, including its origins, propagation, and the impact it had on affected organizations and individuals. According to a report by Kaspersky Lab, the WannaCry malware wasdeveloped by the North Korean government-sponsored hacking group known as the Lazarus Group [10]. The Lazarus Group had previously been responsible for various other cyberattacks, including the Sony Pictures hack in 2014. However, the WannaCry malware was different in that it was the first time that the group had used ransomware as a means of attack. The WannaCry malware caused widespread disruption to businesses, hospitals, and government organizations, as well as individuals who fell victim to the attack. The UK's National Health Service (NHS) was particularly affected, with many hospitals forced to cancel appointments and procedures due to the malware infection [11]. Other affected organizations included Renault, Nissan, and FedEx, among many others. Damage from the WannaCry ransomware attack is expected to run into the billions of dollars.

In May 2017, the UK National Health Service (NHS) suffered a cyberattack that led to the shutdown of critical services in hospitals and health centers across the country (Figure 2). The WannaCry ransomware attack is regarded as one of the most significant cyberattacks in history, and its impact on the NHS was far- reaching. This literature review provides an in-depth analysis of the WannaCry attack on the NHS, its causes, consequences, and lessons learned. The WannaCry attack was facilitated by a vulnerability in the Microsoft Windows operating system that had been identified and fixed by the company two months before the attack [12]. However, some NHS organizations had failed to apply the security patch, leaving them vulnerableto attack. In addition, some NHS trusts were using outdated computer systems, which increased their vulnerability to the attack. The attack was also attributed to the widespread use of unsupported or unlicensed software in some NHS organizations [12]. The WannaCry attack had a significant impact on the NHS, with over 19,000 appointments cancelled, andmany hospitals and clinics forced to turn away patients [12]. The attack also

affected other critical services, including diagnostic equipment, laboratory services, and patient records, which were rendered inaccessible. In addition, the cost of restoring systems and upgrading security in the aftermath of the attack was estimated to be between £92m and £94m [13].

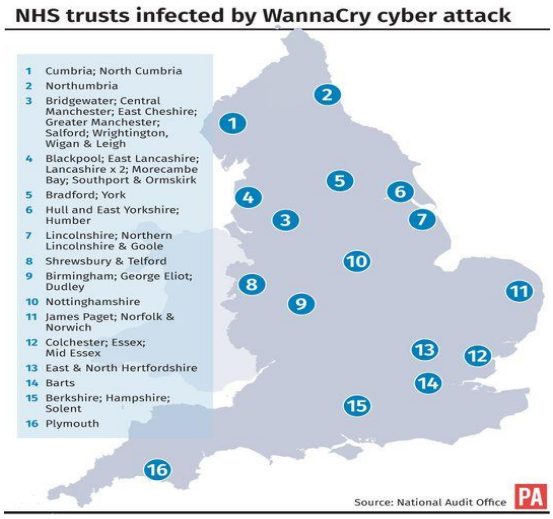

Fig 2. Map showing impacted areas of NHS

III. Methodology: The Threat Intelligence Cycle

This article utilizes the threat intelligence cycle (Figure 3) to examine WannaCry. Gathering, analyzing, and disseminating information about potential and actual threats to an organization's security is the goal of the Threat Intelligence cycle. The cycle comprises several distinct steps that work together to provide an organization with timely and accurate intelligence to make informed decisions [14].

Figure 3: The Threat Intelligence Cycle

3.1 Planning and Direction

Planning and Direction**:** The first step in the Threat Intelligence cycle is planning and direction. This step involves identifying the organization's critical assets that needs to be protected, determining the intelligence requirements, and developing a plan to gather the necessary information. This section explains the steps your team must take to develop a comprehensive CTI strategy and define its needs and objectives. The goal in this case is to have clear understanding of the threat profile (WannaCry) and gather relevant information requirements (Figure 4).

Fig 4. Intelligence Cycle planning model [15]

3.2 Data Collection: This step involves gathering relevant information from various sources such as open-source intelligence, human intelligence, and technical intelligence. The information collection phase in gathering intelligence around WannaCry covers internal information that must be protected against WannaCry or any ransomware. This includes an inventory of all windows OS servers within the organization landscape, Public IP addresses and domains exposed to the internet that are NATed to the infrastructure's DMZ environment, Inventory of Web servers Inventory of unpatched servers. On the other hand, external information refers to information that can be acquired from third parties such as regulators, service providers including web security, email security and domain security providers. Also, information from OSINT which could include general organization information available for free in open sourcewhich could be leveraged by cyber criminals. CVEs (Common Vulnerability Exposures) are also very

important external information as this addresses available vulnerabilities inclusive of zero-day vulnerabilities mostly applicable to WannaCry. Periodically checking the dark web for organization related information is critical for intelligence gathering as this could also be a major source of exploitation.

3.3 Processing: The processing component is a vital stage of the threat intelligence cycle that involves the collection, validation, and analysis of data to produce actionable intelligence. According to [14], the processing phase requires the integration of both human and technological capabilities to enable the ingestion, normalization, correlation, and enrichment of raw data. During this stage, various tools and techniques such as data mining, machine learning, and natural language processing are employed to transform unstructured data into structured formats that can be easily analyzed. Examples of tools for processing include Windows Server 2008 64-BIT – Exploitable Vulnerable system, Kali Linux – Metasploit Machine, Metasploit v6.2.26-dev, Virus Total, NMAP, Wireshark, OllyDbg – A binary code analysis software (Static Analysis), Pestudio, Process Hacker, Process Monitor, DNS query sniffer.

3.4 Analysis: This step involves looking at the structured data to find possible threats and figure out how bad they are. The objective is to look for patterns and trends that can tell about the threat actor's behavior and motivations. This article covers the static and dynamic analysis of the WannaCry ransomware.

3.4.1 Static Analysis: For the static analysis, we tried to explore the components of the binaries that make up the WannaCry malware. Figure 5 below shows the hash value (DB349B97C37D22F5EA1D1841E3C89EB4) of the malware and confirming that it is a PEEXE (Portal Executable file type).

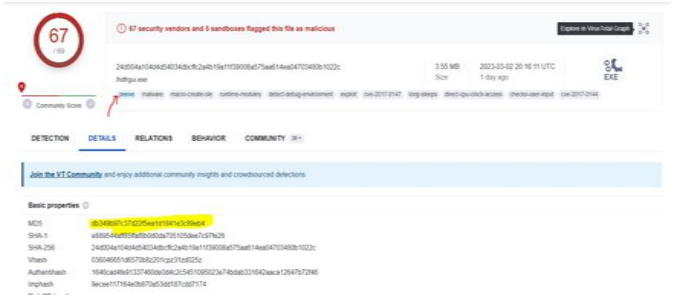

Fig 5. WannaCry Sample from Virus Total

Another important information about the malware is its current landscape obtained from virus total graph as can be seen in figure 6 below. Two key information from the graph which gives idea on the current spread and attack attempts is the contact domains and IPs. From the graph below this malware has been detected by 67 virus engines, interacted with 1430 IPs across the globe, it is confirmed that this binary is malicious as seen in figure 7.

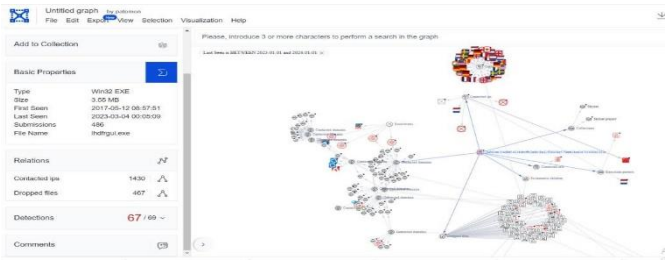

Fig 6. Total Virus WannaCry sample landscape

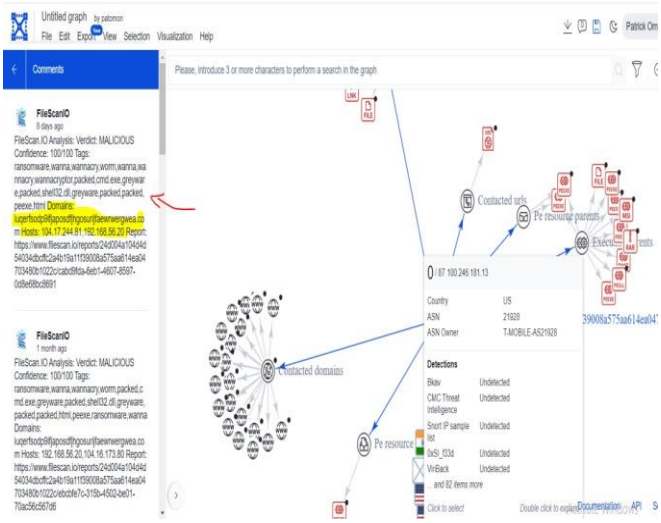

Fig 7. Virus Total Showing Industry Experts Comments About WannaCry

3.4.2 Dynamic Analysis: According to The Guardian newspaper Eternal Blue which is the vulnerability for exploiting WannaCry was released by the group named the "Shadow Group" and their reason was for pride rather than gain. They insinuate that they were “taking pride in picking adversary equal to or better than selves, a worthy opponent” and it has “always been about the Shadow Brokers vs the equation group, a sophisticated hacking team believed to be operated by the NSA" [16]. Therefore, the dynamic analysis covers all the steps involved the Cyber Kill chain (Figure 8).

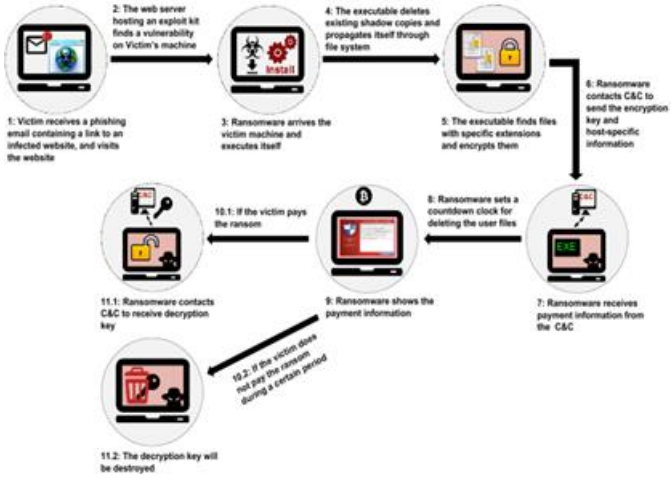

Fig 8. Cyber Kill Chain Anatomy of WannaCry [17]

Step 1: Reconnaissance

Nmap Version 7.93 installed in Kali **was** used to scan the virtual network environment network to find available systems with open port 139 and 445 (SMB) on which the exploitation of the eternal blue vulnerability (CVE-2017-0144) can be carried out. The figure 9 confirms that the system is a windows machine and is exploited due to the open port 445 SMB.

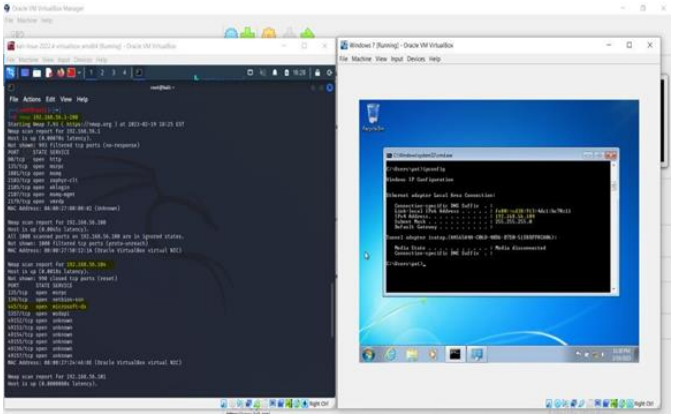

Fig 9. Scan result from Nmap

Step 2: Exploitation

Metasploit: The vulnerable port 445 can be exploited on the windows version (7, 8 and variation of 10), also on windows server 2008 and windows XP. This vulnerability allows attackers to gain remote root access (remote code execution) and control to be able to deploy any payload. To demonstrate this, we runthe script “**use exploit/windows/smb/ms17_010_eternalblue**”. Figure 10 below confirms a successful exploit gaining root access to the compromised system.

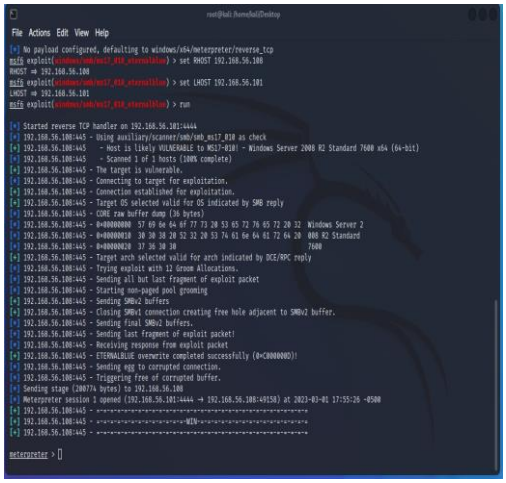

Fig 10. Successful Windows Exploit

Step 3: Execution: Downloading the WannaCry sample and copied it to the windows system in a controlled environment. This involves ensuring that the host system is not windows and that the VMs are in host-only network mode to prevent the virus from spreading across to the host machine. The malware was

executed and the below are the respective extracts showing it behavior. In figure 11 below, the DNS query sniffer tool was able to identify a process relating to the kill switchdomain which is imbedded in the binary. Another key process being executed by the malware is that it deletes all shadow copies of files from thesystem, this prevents any form of recovery. This means that a victim is left with no choice than to pay demanded ransom.

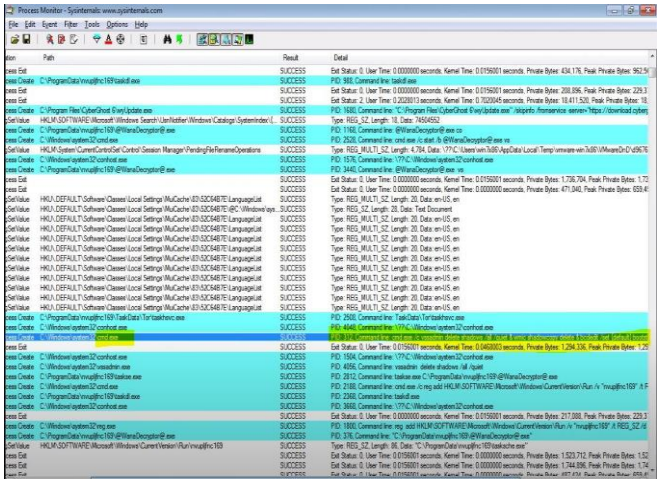

Fig 11. Malware File Deletion Binary

Step 4: Command and Control (C2): Further review of the binaries with Process Hacker tool reveals some of the inbuilt Tor directory communication IPs for communicating with C2 Servers in figure 12. Upon successful execution, the malware begins to encrypt the system files using a hybrid cryptographic. It uses both asymmetric and symmetric methods. AES keys are used during the encryption process with a binary "WanaDecryptor.exe" program, depicting a possible decryption after payment is made bythe victim. The malware also uses RSA public key called the adversary's public key (Apu) and generates 2048-bit RSA key pair called victim key pair (Vpu Vpr). The malwarethen encrypts the victims private key (Vpr) using the adversary's public key (Apu) and destroys the original private key of the victim. For every file in the affected system, it generates a unique AES key, encrypts the key using Vpu and the encrypted key is added to each file. Once encryption is completed, it deletes the original file by overwriting the memory space allocation and add a ".WNCRYT| extension to each file.

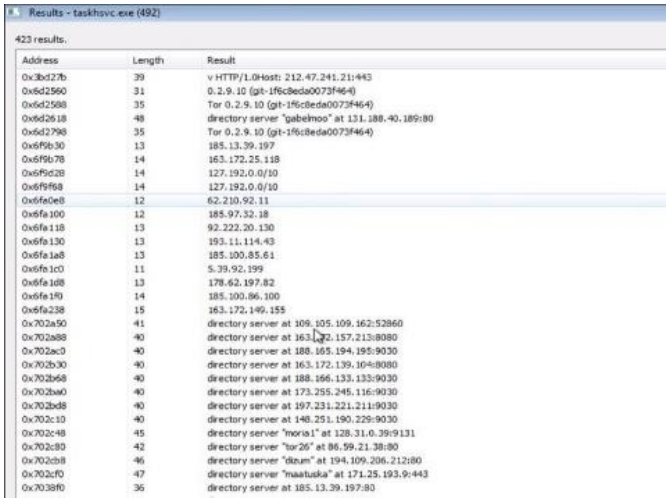

Fig 12. C2 Servers Communication IPs

3.5 Dissemination: From the analysis on WannaCry, key information to relevant stakeholders such as the CISO, CTO and Security Operation Team (SOC) is that this malware is still very potent, and the below actions need to be taken.

- Continuous assessment of our security landscape
- Applying regular patch updates
- Ensure all SIEM alerts are treated with utmost priority to identify potential attack
- All identified kill switch domain IPs are communicated to the Security Ops team for them to beblocked on our perimeter firewall
- Sensitize users of technology (end-users) on the need to stay secure by only visiting secured websites and opening email attachments that are confirmed to be authentic and free from virus
- The SMB port 445 and 139 are monitored by the SOC team for possible intrusion campaign

3.6 Utilization: This step involves gathering feedback from the stakeholders and evaluating the effectivenessof the intelligence operation to help refine the intelligence requirements and improve the intelligence-gathering process. The intelligence gathered from this exercise helps the SOC and Security Ops team to stay alert on potential threat actors and this is also shared with CIO and CISO to effectively engage business leaders and CEO on if there are tools or solutions to be put in place to booster the security posture of the organization.

IV. Conclusion:

In conclusion, the Threat Intelligence cycle is a critical process that enables organizations to make informed decisions to protect their assets from potential and existing threats. By following a systematicapproach to gathering, analyzing, and disseminating information, organizations can help to stay ahead of evolving threats and mitigate risks effectively [14].

V. Legal and Ethical Issues with WannaCry

One of the legal issues considered in this article is the violation of data privacy laws. WannaCry attackers exploited a vulnerability in the Windows operating system, which allowed them to access and encrypt users' data. This act violated data privacy laws such as the EU's General Data Protection Regulation (GDPR) (European Union, 2016). Secondly, the unauthorized access to computer systems is a violation of computer crime laws. The WannaCry attack exploited a vulnerability in the Windows operating system and propagated through a worm that spread rapidly across networks (FBI, 2017). The attackers gained unauthorized access to computer systems, and this act is a violation of computer crime laws, such as the Computer Fraud and Abuse Act (CFAA) (U.S. Department of Justice, n.d.). From an ethical standpoint, the WannaCry attack caused significant harm to individuals and organizations worldwide. The attackers demanded ransom payments from affected organizations, and failure to pay resulted in the loss of data. This act is an ethical concern as it causes significant harm to innocent parties and goes against the principles of justice and fairness.

6.0 Recommendation and Future Work

To counteract these evolving threats, new security measures are being developed. These include the use of blockchain technology to create secure and tamper-proof backups, as well as the development of new encryption techniques to protect against ransomware attacks. Additionally, there is a growing trend towards using "deception technology" to mislead attackers and prevent them from gaining access to critical systems [18]. Development of new legal frameworks and policy solutions to address the growing threat of ransomware is gaining attention [19].

Future work on ransomware involves the continued development of more sophisticated attacks, as well as the creation of more advanced security measures to counteract these attacks. This work will require collaboration between researchers, industry professionals, and policymakers to effectively mitigate the threat of ransomware. Future studies recommend the use of artificial intelligence (AI) and machine learning (ML) to find, mitigate and possibly stop ransomware attacks. For example, researchers have proposed using deep learning models to analyze network traffic and identify ransomware signatures, as well as using reinforcement learning algorithms to optimize response strategies [20].

VI. REFERENCES

[1]. Rudman, L., & Irwin, B., (2016). Dridex: Analysis of the Traffic and Automatic Generation of IOCs. Information Security for South Africa. 77-84. https://doi.org/10.1109/ISSa.2016.7802932.

[2]. O'Brien, N., Martin, G., Graß, E., Durkin, M., Darzi, A., & Ghafur, S. (2020). Safeguarding our healthcare systems: A global framework for cybersecurity.

[3]. Micro, T. (2017). Ransomware. Retrieved from https://goo.gl/nZaoAa.

[4]. Fimin, M. (2017). Are employees' part of the ransomware problem? Computer Fraud & Security. https://doi.org/10.1016/S1361-3723. 17. 30072-6.

[5]. Symantec (2017). What you need to know about the WannaCry ransomware. Threat Intelligence.

[6]. Akbanov, M., Vassilakis, V., Moscholios, I., & Logothetics, M. (2018). Static and Dynamic Analysis of WannaCry Ransomware. 12th IEEE – IET Intern. Symposium on Communication Systems, Networks and Digital Signal Processing.

[7]. Widup, Suzanne, W., Alex, P., David, H., Gabriel, B., & Philippe, L. (2021). Verizon Data Breach Investigations Report.

[8]. Rouse, M. (2019). Malware (malicious software). In Search Security. Retrieved September 5, 2021, from https://searchsecurity.techtarget.com/definition/malware

[9]. Duell, M. (2017, October 27). UK security minister blames North Korea for NHS ransomware hack. Mail Online. http://www.dailymail.co.uk/~/article-5023013/index.html?ito=link_share_article-image-share#i- 5761bfc009ed36a2

[10]. Kaspersky. (2017, May 16). WannaCry Ransomware: Everything You Need To Know. Kaspersky. https://www.kaspersky.com/blog/wannacry-ransomware/16144/

[11]. BBC News. (2017, May 15). What is WannaCry ransomware and how does it work? BBC News. https://www.bbc.com/news/technology-39901382

[12]. National Audit Office (2018). Investigation: WannaCry cyber-attack and the NHS. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf

[13]. Department of Health and Social Care. (2017). Lessons learned review of the WannaCry Ransomware Cyber Attack. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/636297/lessons_learned_review_of_wannacry_ransomware_attack.pdf

[14]. Sahrom, M., Rahayu, S., Aswami, A., & Robiah, Y. (2018). An Enhancement of Cyber Threat Intelligence Framework. Journal of Advanced Research in Dynamical and Control Systems. 10. 96-104.

[15]. Cyber Threat Intelligence in Government: A Guide for Decision Makers & Analysts. (2019).https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Cyber-Threat-Intelligence-A-Guide-For-Decision-Makers-and-Analysts-v2.0.pdf

[16]. Gibbs, S. (2017, May 17). Shadow Brokers threaten to unleash more hacking tools. The Guardian. https://www.theguardian.com/technology/2017/may/17/hackers-shadow-brokers-threatens-issue- more-leaks-hacking-tools-ransomware#:~:text=They%20said%20they%20were%20%E2%80%9Ctaking

[17]. Dargahi, T., Dehghantanha, A., Bahrami, P.N. et al. A Cyber-Kill-Chain based taxonomy of crypto-ransomware features. J Comput Virol Hack Tech 15, 277–305 (2019). https://doi.org/10.1007/s11416-019-00338-7

[18]. Biswas, S., Roy, S., & Ghosh, S. K. (2021). The economics of ransomware attacks: A systematic review. Journal of Business Research, 130, 703-718.

[19]. Munoz, D., Wang, W., Kulkarni, V., & Jain, A. (2021). Reinforcement learning for ransomware response. Journal of Information Security and Applications, 63, 102752.

[20]. Khan, U. A., Khan, M. U., Saeed, H., & Alqarni, A. (2021). Ransomware detection and prevention through deep learning: A review. IEEE Access, 9, 73717-73734