Comparative Study of Ransomwares

Vivek Kumar Anand, Karunesh Bamanjogi, Aryan Raj Shaw, Mahak Faheem
Computer Science and Engineering
NIIT University
Neemrana, India

2022 7th International Conference on Computing, Communication and Security (ICCCS) | 979-8-3503-0990-4/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICCCS55188.2022.10079369

***Abstract*— Over the past few years cyberattacks have increased significantly as we have moved to a digital world. In 2021 this number rises drastically. Ransomware Attacks are not only limited to attacking an organization or a group of people to steal/encrypt their data, but it also refers to attacking networks or servers to slow down the services to such an extent thus creating the services unusable for the user, but at the same time, unlike other malware whose detection and analysis is not much complex, in ransomware, we find that they cannot be reverse engineered easily, due to high obfuscation and packing techniques involved. Skilled attackers are always a step ahead thus they find ways to evade the security systems or execute zero-day vulnerabilities.**

Keywords—Ransomwares, Activation, Command & Control Server, Worming Component, IOCs

I. Introduction

Malware analysis is the process of dissecting a given sample or piece of malicious software to understand its working and find ways to identify, mitigate and defeat it. Any software or code that does something that causes harm to the user or the device or can simply trigger a chain of unwanted events can be considered malware. There are various kinds of malware, such as Worms: Computer worms are standalone malicious software that can self-replicate. It does not affect other programs but keeps replicating, once triggered. Hence, such code consumes the memory and slows down the network and the system. Worms require a propagation medium(file) to spread from one system or network to another. Examples of worms are Email-worm, IM-worm, P2P-worm, etc. Viruses: Computer viruses are malicious computer programs that manipulate the code upon execution and affect the system and data. Viruses need a host program to spread and get executed. They can delete files and data, modify programs and destroy the system. Examples of viruses are Boot Sector virus, Macro virus, Polymorphic virus, etc. Trojans: A Computer Trojan is a malicious software that impersonates a legitimate program and gets downloaded as an attachment hidden within an Email or Free Software. The activation of this malware is done by social engineering, hiding the malicious code within the credible software, thus gaining the user access to the host computer. Rootkits: A Computer Rootkit is a malicious software that remains camouflaged and contains a bunch of tools that infect the host computer to gain the user system access and steal personal information or manipulate it. Once gained access it can also download other malicious software into the host computer. Spyware: A Computer spyware is a malicious software that is designed to enter the host computer, capture and monitor the data related to the user, and send it to the attacker. Spywares also affect the network and device performance by slowing down the speed of data activities. However, many legitimate companies and computer software use spyware, like “tracking tools”, making data vulnerable to breaches and misuse. Ransomware: Computer Ransomware is the malicious software that attacks the host computer or the network and encrypts all the critical data which makes a whole organization come to a halt as they are unable to access any databases, files, servers, etc., and in return, the attackers demand a ransom to decrypt the data and provide the access. The purpose of malware analysis is to investigate all the unwanted and malicious activities and events that occurred on the computer after the malware has been run on the computer. The following should be the goals of malware analysis:

- Determine the exact attack.
- Find the root cause of compromise.
- Locate all the infected files, networks, and systems.
- Determine the scope of suspected binaries or executable files
- Determine the ways in which the infection can spread to other systems.
- Determine the kill switch or the ways to stop the attack and contain its damage.

A. Malware Analysis Techniques

While performing malware analysis, generally, the executable files are examined. Basically, there are two malware analysis techniques: static and dynamic. In static analysis, files are examined without running the executable while in dynamic analysis, the executable files are run to examine them.

1) Static analysis

a) *Basic static analysis:* This is performed without running the executable file. Basic static analysis can detect whether or not the executable is malicious. It can provide sufficient information that can be used to create network signatures. This analysis technique is simple and quick but not suitable for complex malware.

b) *Advanced static analysis:* This analysis technique involves the reverse-engineering of the malware’s internals. The executable is loaded into a disassembler and then the entire program is examined. Since the CPU executes

979-8-3503-0990-4/22/$31.00 ©2022 IEEE

the instructions, we can analyze what the program actually does.

2) *Dynamic analysis*

   a) *Basic dynamic analysis:* This analysis technique involves running the executable and then observing its behavior on the system. It can help to find the root causes of infection, and manipulations and also can be used to produce effective signatures. A properly isolated system should be used to perform dynamic analysis in order to avoid infection.
   b) *Advanced dynamic analysis:* In this analysis technique, a debugger is used to examine the internal structure of a running executable. It can provide extra detailed information that cannot be provided by other analysis techniques.

B. Related Terminologies

1) *Reverse engineering:* The process of tearing down or decompiling a software program is referred to as reverse engineering. It converts binary instructions into machine-level language so that the software engineers could inspect the program and how it may impact various systems, or which vulnerabilities it can exploit. Reverse engineering helps to develop software that may reduce or mitigate the potential risk of the malicious program.
2) *Anti-disassembly:* Malware authors use anti-disassembly techniques to delay and/or prevent reverse-engineering the malware. It also could prevent the detection of malware by a few or many anti-virus or anti-malware programs. It may also be referred to as malware obfuscation.
3) *DLL(Dynamic Link Libraries):* Dynamic link libraries help Microsoft Windows operating systems to use libraries to share part or whole of one program among multiple softwares. It executes only if an associated program is executed which requires some additional functionalities which a DLL file could provide.
4) *PE(Portable Executable):* It is a file format used by Microsoft Windows executable applications, object code, and DLLs. After .exe complies, a PE header is included, which describes its structure. It gives general information like where the executable can be loaded into the memory and/or from where the address of the executable will start.

C. Malware Analysis Tools

Before understanding the malware analysis tools let us look briefly at how malware analysis is performed. Firstly, we will do static analysis where the code will not be executed instead the information is gathered from the malware like about the suspicious indicators such as hashes and figure out if the malware is packed. Secondly, we will deploy the malware into a virtual machine that is specially configured for performing malware analysis. And third, we will do dynamic analysis to identify unique behaviours of the malware. This can be looking into C&C servers, network traffic or change in any registry etc.
These are the various tools used for malware analysis:

1) *For Static Analysis*

   a) PEiD: This application is used to identify small packers, crypters and compilers. The current version of PEiD can detect 470 different signatures in PE files which are downloaded from a text file called userdb.txt. Usually, malware creators obfuscate their malware to make the malware harder to detect or analyze.
   b) Dependency Walker: It is an application that is used to scan 32 and 64-bit Windows modules like .exe, .ocx etc. It also shows the dependencies of the file and detailed information about file path, version number, machine type etc.
   c) Resource Hacker: It is used to extract the resources from windows binaries. It can add, attract or modify different resources like strings, images etc.
   d) PEview: This application is used to provide information about the PE i.e, Portable Executable files, file headers and different sections of it.
   e) FileAlyzer: This tool is also used to give information about the PE files but in addition, it provides a separate VirusTotal tab that can be used for VirusTotal scanning. It also provides the feature of deobfuscating UPX and PEComapct packed files.

2) *For Dynamic Analysis*

   a) Procmon: Also known as Process Monitor is developed by Windows SysInternals that is used for monitoring file system registry and processing them in real-time. This tool is a combination of two tools: FileMon & RegMon. This tool provides a feature of Non-destructive filtering which means the tool will capture all the data but will only display the filtered data.
   b) Process Explorer: It is a tool made by Microsoft that is used to observe processes and display which handles and DLLs are processed and loaded for each process.
   c) Regshot: This tool is used to compare the current state of the registry to the state when malware has been executed on the system.
   d) Wireshark: This tool is used to analyze the

network by deep inspection, filtering packets, live packet capturing etc. This tool is also used to analyze packets and log network traffic to files.

II. Literature Review

Ransomware attacks are so successful because of the highly profitable business model, development of anonymous and seamless payment systems, untraceable transactions using crypto-currencies, and the evolution of RaaS (Ransomware-as-a-Service).

Ransomware with secondary payloads, worming capabilities, targeted attacks, and attacks against non-traditional systems have urged the need for smarter and advanced detection techniques and fast detection mechanisms in conjunction with layered security models.

Signature-based detection of malware is limited to "known" malware only. "The deferral in recognizing new types of malware makes companies powerless against genuine harm", M Satheesh et al [9], for zero-day attacks, such techniques cannot be relied upon. In such cases behavioral examination becomes mandatory. For the widely evolving framework-based ransomware, the proposed workflow and set of techniques would do as well as the signature-based detection for the known attacks.

SDN-based detection and mitigation solutions are limited to the ransomware families such as WannaCry, Cerber, Locky, Cryptowall, and ExPetr. The literature mentions that ransomware families that do not communicate with external endpoints such as C&C servers to exchange the encryption keys or other data cannot benefit much from the SDN-based approach. For example, in the case of BadRabit, the public key is integrated into its files. An additional layer of IDPS that can detect and block the self-propagating ransomware can be equipped.

As per Beaman C et al [10], "the focus of the state-of-the-art ransomware detection techniques mostly revolve around honeypots, network traffic analysis, and machine learning-based approaches. Prevention techniques mostly focused on access control, data and key backups, and hardware-based solutions.", it is clear that, despite the machine learning approaches being already in the application, there is no full-proof automation that can combat the attacks and so the need for more intelligent approaches for detection and prevention stands high in need.

The statistics of ransomware attacks also points to the ignorance, unawareness and unpreparedness amongst the users. To develop and propose better solutions, open-access ransomware libraries are the need of the hour. Other challenges include inadequate detection and false-positive rates. While the false alarms would cause network interruptions and needless blocking, the low and loose detection will make the system purposeless.

In this project, we are focussing on the analysis of ransomware and its different components.

III. Objectives

Objectives of our R&D project are as followed:

- To explore the ransomware and RaaS
- To study various malicious components found in ransomware families
- To study and compare different ransomware families based on selected parameters
- To find out the optimized and effective analysis techniques for different ransomware families
- To develop an application that can suggest effective analysis for given IOCs or keywords

TABLE I. SUSPICIOUS BEHAVIOR SETUP, SCOPE & WAYS

Suspicious Behaviour setup	***Scope***	***Ways***
Payload persistence	→ Ensures attack completion → Persists across reboots and restarts → Able to resume up on start	→ By placing a copy of the executable into the Windows startup dir. → Adding a registry key entry → Setting up a cron job/Scheduled tasks
Anti-system restore	→ Ensures malicious actions cannot be undone → Prevents encrypted data from being restored to unencrypted version	→ Disable system restore functionality → Delete Windows shadow copies
Stealth techniques	→ Executes in stealthy manner without being noticed or caught by the user or scanners	→ By injection into a legit process → Executing from %AppData% dir. → Using executables name same as Common Windows Executables
Environment mapping	→ Maps system env. before initiating its setup procedure → Determines if it is a real system or a sandbox → Determine security settings and policies	N/A

Suspicious Behaviour setup	***Scope***	***Ways***
Network traffic	→ Requires internet to download payload related files → For Encryption key communication → Ensure malicious C&C servers do not get shut down by the authorities	→ Using domain name registration tactics → Generate random domain names registered to anonymous top level domain

IV. Proposed Methodology

In this section, a complete overview of the project will be explained, which includes the complete process of how to identify the types of ransomware. A layman user does not have or may have very less knowledge of when malware compromises their system. The user only can tell if their system is behaving properly or if there is something that is not going well like PCs running slowly or weird pop-ups appearing on the screen. There are many of these indicators of compromises or IOCs. To help in malware detection and analysis, a web-based application has been designed. The working of this application is divided into three categories or steps. Not just for a normal user, but this application may also help cyber experts in malware analysis in a quicker and more effective way by recommending certain types of malware analysis tools that could detect or analyze a particular malware file sample when shared with that particular software/website.

1) Comparative study description

In our research, we have focused primarily on three parameters of any ransomware or its family. Any given specimen of ransomware has many parameters which include, but are not limited to, activation, kill switch, worming component, and C&C (command and control servers) communication. An astonishing thing about the variants of ransomware is that if one parameter is present in one ransomware specimen, its behavior may be entirely different or may not be even present in another variant. The procedure was to study a particular parameter in various ransomware. There are many research papers that have researched particular ransomware or its family based on the above-mentioned parameters but there is an absence of information about the different parameters in different ransomware families, and its comparative study.

Before we analyze ransomware, it's very important to identify that the system is being attacked by ransomware. Most of the time people or organizations are unaware of the fact their system is being attacked. And so this parameter is really important as early detection can minimize the damage caused. Slowing down of the system is a common symptom of any kind of attack as the attacker utilizes the processing power of the host system thus slowing down the machine. In the case of CryptoLocker when the system is under attack and if file access activity is monitored on affected files servers, this ransomware generates very large numbers of open, modify, and create events at a very rapid pace, and are fairly easy to spot. The generation of unnecessary network traffic is also a common symptom of a system under attack. This is evident when communication to the servers becomes extremely slow, or the user is unable to browse the internet even for simple tasks. If the system is protected by antivirus software, the antivirus gives warnings regarding the chances of potential ransomware attacks when the system shows unusual behaviors mentioned above. When the system is attacked by ransomware, a message window is shown demanding a ransom to decrypt the important or confidential files on the system.

2) Comparative study implementation into web app

Web application will be a simple form-based application that would take inputs and return a basic/detailed report to the user in a way that could help in detecting what ransomware could have potentially infected a system.
In the first step, the user will feed the input to the web app through a form-based interface. The input fields will have multiple options for the user to enter the IOCs. IOCs are indicators of compromise that a user may experience in the usage of their systems. This includes options like slow system, shady system behavior, weird file extensions, etc.
In the second step, the data provided by the user will be sent to the backend of the web app. Here the web app will process the inputs based on the data from the table.
In the third step, after analyzing input from the user, the web application will display the desired outputs.

3) IOCs table implementation

After going through the various research papers which provided insight into ransomware and its parameters, all of these researches were tried and brought together into these tables provided in this report. All of these tables are categorized based on the parameters and various ransomware and families. After the tables are ready, all of this data will be hard-coded, for now, in the web application. This would help one to check which IOCs are related to which ransomware and would then give its recommendation and related information. It will also mention the tools which may be required for further malware analysis.

4) Comparison between different ransomware families based on selected parameters

a) *Activation:* Every Ransomware has an infection vector through which it enters the system, either directly or indirectly. During this stage, ransomware is delivered to a

victim system (for example, a PC/workstation, mobile device, IoT/CPS device, and so on), Harun et al [6]. Malicious actors use a variety of infection vectors to deliver ransomware.

TABLE II: ACTIVATION & INFECTION VECTOR

Ransomware	***Activation***	***Infection***
AIDS Trojan	The malware didn't start encrypting the system at first. Instead, it hijacked the AUTOEXEC.BAT, a short form of a file named automatically executed batch file which gets executed after each boot. The malware gets activated around the 90th boot and starts encrypting the files on the C drive	Floppy drive
Petya	After getting installed in the system by the user unwillingly, Petya starts infecting the Master boot record (MBR). Once it is inside the MBR it forces the computer to restart and then starts encrypting the MFT(Master file table).	Phishing emails
TeslaCrypt	It starts with Social Engineering where the victim is made to click on a malicious link or attachments through phishing or spam emails resulting in redirection to compromised WordPress websites that have exploit kits installed like Angler Exploit kits, Neutrino Exploit Kits.	Phishing emails
Jigsaw	It is spread through phishing or spam mail which contains malicious attachments or links and once activated it encrypts the MBR(master boot record)	Phishing emails
Cerber	Emails with malicious Microsoft Word Documents attached once the attachment is opened it will result in a malicious macro running and contacting the attacker-controlled website to download the ransomware	Drive-by-download
CryptoWall	Malicious links in phishing emails when clicked redirect the victim to a number of compromised domains. Once followed a downloader is placed on the system, which connects to these compromised domains. Once connected it downloads and installs Cryptowall on the system.	Phishing emails
SamSam	It uses brute-force methods to crack weak passwords thus exploiting the vulnerabilities including Remote Desktop Protocol (RDP) thus gaining access to the victim's network.	Vulnerabilities
CrySIS	Malicious email attachments that use double file extensions through harmless-looking installers or installation files for various legitimate applications.	Phishing emails Malicious Apps Vulnerabilities

Ransomware	*Activation*	*Infection*
	Exploiting leaked or weak RDP Credentials	
LeChiffre	It infiltrates the network through scanning weak, unsecured vulnerable networks or desktops.	Vulnerabilities
Bad Rabbit	Infiltrates the system by downloading malicious adobe updates or apps through compromised websites.	Malicious Apps

b) *Command & Control Servers:* Following activation, ransomware connects to the Command and Control (C&C) server to exchange critical information with the attacker (e.g., encryption keys, target system information) Harun et al [6]. Although many ransomware strains communicate with command and control servers, there are some families that do not.

TABLE III: COMMAND & CONTROL COMMUNICATION

Ransomware	Command & Control	Communication
1. AIDS Trojan	The C&C was actually designed to work under offline conditions without connecting to any external server and executed once the boot count reached 90 after the malware entered the system M Satheesh et al [9]. It was not actually a C&C server, but a floppy disk that injected the payload of encryption malware.	Hard-coded
WannaCry	Post infection of the machine, it tries to contact a C&C server, www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com. If this happens, it will not perform encryption or self-propagation. Another killswitch domain www[.]ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com was discovered. A new variant surfaced soon after that did not have the domain contact killswitch functionality. Additional files with .wncry extensions may be created.	DGA-based
3. Jigsaw	Contacts the C&C server to generate asymmetric keys using RSA+AES double encryption, and only public keys are used to encrypt the files on the victim's computer. Each time, a new pair of keys is generated for encryption and no key is locally stored on the victim's computer.	DGA-based
TeslaCrypt	C&C servers are located on the tor network. Malware establishes communication via public tor2web services. Post communication, a pair of RSA-2048 keys, or encrypted using AES-256-CBC with a SHA256 hash; are generated and used to encrypt the victim's computer. It has a predefined static list of C&C addresses.	Hard-coded
CryptoWall	Contact the C&C to get encryption keys. The	DGA-based

Ransomware	Command & Control	Communication
	malware injected into the svchost encrypts files and malware code injected into	
Locky	Ab.	N/A

c) *Worming Component:* This component in any ransomware refers to the propagating and spreading capabilities of the ransomware from one infected system to another or from one network to another. The worm component can propagate within the local network.

TABLE IV:WORMING COMPONENT

Ransomware	Worming Component	Description
Wannacry	Present	Self-propagating within and outside the network.
ZCryptor	Present	It is a part of ransomware and part worm that is known for encrypting files and copying them onto external media.
Ex-Petr	Present	Drive-by download, watering hole attack. Stolen admin creds laterally within a network & across connected domains via 445 or 139
Petya	Present	Spreaded via malware-laden phishing emails. Designed to spread beyond the initially infected environment.
Cerber	Ab.	N/A
Cryptowall	Ab.	N/A
Locky	Ab.	N/A

d) IOCs(Indicator of Compromise): Indicators of attack differ from IOCs in that they focus on identifying the activity associated with the attack while it is occurring, whereas IOCs focus on what happened after the attack has occurred. IOCs serve as flags for cybersecurity professionals to detect unusual activity that could indicate or lead to a future attack. IOCs are classified into several types. Some contain simple elements such as metadata, while others are more complex, such as malicious code.It is frequently beneficial for information security professionals to collect multiple IOCs and then see if there is a correlation between them indicating details of a possible attack.

TABLE V: NETWORK IOCS IN RANSOMWARE DETECTION & PREVENTION TOOLS[8]

IOCs	Ransomware Detection Tools				
Network IOCs	***Hitman Pro***	**Cryptomonitor**	**Bit Defender**	**Cryptoprevent**	**CryptoDrop**
Perform HTTP requests	✓	✓			
Connect to tor2web		✓			
Too many DNS requests		✓			
Too many non-existing domain name responses		✓			
Request to high entropy domain names	✓	✓			

TABLE VI: SYSTEM IOCS IN RANSOMWARE DETECTION & PREVENTION TOOLS[8]

IOCs	Ransomware Detection Tools		
System IOCs	**Cryptomonitor**	**Bit Defender**	**Cryptoprevent**
Disable windows error recovery on startup	✓	✓	✓
Disable startup repair	✓	✓	✓
Disable UAC	✓		
Disable Task manager	✓		

IOCs	Ransomware Detection Tools		
System IOCs	**Cryptomonitor**	**Bit Defender**	**Cryptoprevent**
Stops windows security center service and prevents it from starting up on boot	✓	✓	✓

TABLE VII: BEHAVIOURAL IOCS IN RANSOMWARE DETECTION & PREVENTION TOOLS[8]

IOCs	Ransomware Detection Tools				
Behavioral IOCs	**Hitman Pro**	**Cryptomonitor**	**Bit Defender**	**Cryptoprevent**	**CryptoDrop**
Tries to unhook windows function		✓			
Untrusted processes spawning/ injecting into target processes	✓	✓		✓	✓
Fingerprints the system	✓	✓			
Dropped files	✓	✓	✓	✓	✓
Periodic Activity				✓	

e) IOCs and malicious features native to different ransomware families:

i) *Wannacry* - WannaCry exploits the **"**Windows SMB Authenticated Remote code execution Vulnerability(CVE-2020-1301)"[6] and search for file types with extensions like .odt, .doc, .pptx and 175 others and appends them with .WCRY at the end of the file name.

ii) *Bad Rabbit* - This ransomware downloads a malicious install_flash_player.exe via compromised websites . The user opens the file with access with administrative privileges which it prompts due to standard UAC prompt and after opening it with the same it saves the *"malicious DLL as C:Windowsinfpub.dat and launch it using rundll32* "[7].

iii) *LockBit2.0* - Thai ransomware uses bitwise operations for decoding the strings and loading of the modules and attacks only those systems that do not use a set list of Eastern European Languages.

iv) *RagnarLocker* - This ransomware instead of choosing which files to encrypt it chooses which it has to not encrypt. By applying this method the system operates normally while the ransomware encrypts the remaining files.

V. RESULT

After doing the literature survey and analysis of the data we collected, we figured out that:

A) While researching the parameter activation for different ransomwares we determined and labeled the studied ransomwares as infected via Phishing emails, Vulnerabilities, malicious Apps or Drive-by-download.

B) For the parameter C&C(Command & Controls) we determined two methods on which establishing the connections to the C&C servers is based i.e Hard-coded and DGA based.

C) For the parameter worming component we determined which ransomwares have a worming component present in it or not.

D) We determined about the IOCs which were categorized into network based, system based, static based and behavioral based IOCs based on which different ransomware detection tools work.

VI. COMPARISON WITH OTHER EXISTING WORK AND ANALYSIS

A lot of research work has been done on ransomwares. Other research works generally present either malware analysis of one ransomware or one type of ransomware families.While we have tried to abstract the common ransomware components and studied their roles in different ransomwares. Some works have listed the IOCs and related tools to detect them. We have focussed on determining

the IOCs native to specific ransomware or ransomware families. We have tried to implement the research work on IOCs present in M. Verma et al [8] in a working model i.e. a webapp. We are also working to implement our own comparative analysis into the webapp.

VII. Future Scope

The future scope of our project is to determine different components and characteristics of ransomwares such as kill-switches, locking mechanisms, encryption, data exfiltration, deletion of shadow copy, extortion mechanisms, etc., and extend the comparative study to different ransomware families. We can also work on IOCs of different ransomwares or ransomware families to determine unique characteristics of the ransomwares that might help in early detection, mitigation or simply the isolation so as to stop the propagation by damping the worming or contagious components found in the ransomwares. We can also utilize the comparative study to get a comprehensive overview of any ransomware, its characteristics and IOCs.

VIII. Conclusion

During our research work we explored a lot about different ransomwares and their malicious behavior. The very first challenge was to identify different parameters of ransomwares. As we researched further we were able to find out different parameters on which we can classify applications, due to the unavailability of appropriate APIs we ransomwares. There were also difficulties while making the web apd to hardcode the information and the data which we presented in the above tables, which was time-consuming. We also could have made use of different APIs so that instead of hardcoding the information we could have added better functionalities to our web application. Our Web Application is based on different IOCs, we could have added more parameters from our research work i.e. activation, worming component, and C&C servers. Our web application is currently made for any malware analyst who has prior knowledge of malwares, IOCs, etc, but we can take this project in our Advanced R&D to make the web application more comprehensive so that it will not only be limited to the malware analyst but to a general user as well.

References

[1] A.K. Maurya, N. Kumar, A. Agarwal and R.A. Khan, “Ransomware: Evolution, Target and Safety Measures,” JCSE, vol. 6, no. 1, pp. 2347-2693, Jan. 2018

[2] Segun I. Popoola, Ujioghosa B. Iyekekpolo, Samuel O. Ojewande, Faith O. Sweetwilliams, Samuel N. John, and Aderemi A. Atayero, “Ransomware: Current Trend, Challenges, and Research Directions,” in Proc. WCECS 2017, Oct. 2017

[3] Maxat Akbanov, Vassilios G. Vassilakis and Michael D. Logothetis, “WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms,” JTIT, vol. 1, no.1 pp. 113-124, Jan. 2019

[4] Weijie Han, Jingfeng Xue, Yong Wang, Zhenyan Liu, Zixiao Kong, “MalInsight: A Systematic Profiling Based Malware Detection Framework,” JNCA, vol. 125, pp. 236-250, Nov. 2018, doi: 10.1016/j.jnca.2018.10.022.

[5] F. M. Alotaibi and V. G. Vassilakis, "SDN-Based Detection of Self-Propagating Ransomware: The Case of BadRabbit," in IEEE Access, vol. 9, pp. 28039-28058, 2021

[6] Q. Chen and R. A. Bridges, "Automated Behavioral Analysis of Malware: A Case Study of WannaCry Ransomware," 2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA), 2017, pp. 454-460

[7] Q. Chen and R. A. Bridges, "Automated Behavioral Analysis of Malware: A Case Study of WannaCry Ransomware," 2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA), 2017, pp. 454-460

[8] M. Verma, P. Kumarguru, S. Brata Deb and A. Gupta, "Analyzing Indicator of Compromises for Ransomware: Leveraging IOCs with Machine Learning Techniques," 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), 2018, pp. 154-159

[9] M. Satheesh Kumar, J. Ben-Othman and K. G. Srinivasagan, "An Investigation on Wannacry Ransomware and its Detection," 2018 IEEE Symposium on Computers and Communications (ISCC), 2018, pp. 1-6

[10] Beaman C, Barkworth A, Akande TD, Hakak S, Khan MK. Ransomware: Recent advances, analysis, challenges and future research directions. Comput Secur. 2021 Dec;111:102490