Analysis of Ransomware Using Reverse Engineering Techniques to Develop Effective Countermeasures

Naif Alsharabi [1,2,*], Mariam F. Alshammari [1], and Yasser Alharbi [1]

[1] Department of Computer Engineering, College of Computer Science and Engineering, University of Ha'il, Ha'il 55476, Saudi Arabia; Email: s20200325@uoh.edu.sa (M.F.A.), y.alharbi@uoh.edu.sa (Y.A.)
[2] College of Engineering and IT, Amran University, Amran 00977, Yemen
*Correspondence: n.sharabi@uoh.edu.sa, sharabi28@hotmail.com (N.A.)

***Abstract*—Ransomware is the most severe threat to companies and organizations, snowballing daily. Ransomware comes in various types that are difficult for non-specialists to distinguish and evolve and change encryption techniques to avoid detection. Ransomware has become a worldwide incidence during the Corona pandemic and remote work, accountable for millions of dollars of losses annually; This malware threatens victims to lose sensitive data unless they pay a ransom, usually by encrypting the victims' hard drive contents until the ransom is paid. The study focused on literature reviews and publications issued by international organizations interested in ransomware analysis to build a strong background in this field. Used static analysis and reverse engineering methodology to investigate ransomware to understand its purpose, functionality, and effective countermeasures against it. Finally, after Dearcry and Babuk ransomware were analyzed, written the Yara rule to detect and suggested countermeasures against them to help cybersecurity professionals better understand the inner workings of real ransomware and develop advanced countermeasures against similar attacks in the future.**

***Keywords*—ransomware, encryption, malware, crypto, reverse engineering, static analysis**

I. Introduction

The rapid development of the network has increased sensitivity toward security threats. Security is considered one of the essential components of remote systems management [1]. Ransomware is one malware that has the world's attention due to the significant increase in cyberspace. One malware family also significantly impacts businesses and institutions [2]. Ransomware attacks use many social engineering techniques to enter the system. It uses the properties of viruses to spread and execute encryption techniques to lock system files, and exploit vulnerabilities in systems to infiltrate and encrypt the system [3]. Ransomware encrypts the victims' files containing different types of data, such as information related to money, business documents, personal data, and databases that hold great value to the victim, and attackers ask for a ransom to get the decryption key [1].

In Some Cases, Ransomware developers moved decryption services into the Tor network, making it impossible to trace and take down a server; Criminals use bitcoin as an anonymous and secure payment service [4]. In 1996, the discussion about ransomware and cryptographic bans began. In 2017, ransomware spread widely and targeted more than 150 countries, such as one of the WannaCry versions, and asked for a ransom of 0.1781 Bitcoin [3]. 2019 has plagued the rise of notorious ransomware families such as JSWorm (01/2019) and CLOP (02/2019) [5]. The annual report issued by Sophos for the year 2021 indicates a decrease in the penetration level of ransomware to 37% from last year. Still, this decrease is partly due to the remarkable development in the techniques of this attack. It also targets larger organizations and institutions because it is more profitable than small organizations. Also, 44% of these attacks were from the education and retail sectors [6].

Ransomware uses evasive techniques to evade detection while attacks against the victim. Polymorphic ransomware may create many decryption engines and use different methods to obfuscate the framework used to avoid analysis [7]. Also, permutation engines are used in metamorphic malware strains to convert its code body for innumerable clones. Important to note that malware uses different obfuscation techniques to avoid analysis and reverse engineering by researchers or anti-ransomware tools. Exacerbating the problem of anti-ransomware, it in turn evolves its mechanisms by constantly creating new polymorphic variants, adapting its engines to work for encryption in Crypto-jacking attacks, and pairing data theft with file system encryption. The logic of infection in ransomware also differs according to the family or classification to which this type belongs, leading to the fact that the detection solution will be complex and suffer from a great complexity of resources [5].

Data gathered from the most recent industry cybersecurity reports revealed a significant increase in ransomware attacks compared to previous years prior to the Corona pandemic. This increase is attributed to most

Manuscript received October 28, 2022; revised December 12, 2022, accepted February 2, 2023; published April 4, 2023.

industrial companies and educational institutions' complete reliance on remote work, as reported by 188.9 million attacks in the second quarter of 2021.

In 2022, ransomware is still the most common type of malware. Its popularity has grown due to its ability to extort large sums of money while posing little risk to cybercriminals (Cyberreason).

After phishing, ransomware is the second leading cause of data breaches in Q1 2022 (Identity Theft Rescue Center).

The world of cybercrime is transforming, and ransomware groups' techniques are adapting to it. In January 2022, REvil, the aggressive ransomware group that gained news after successfully assaulting Colonial Pipeline, was disbanded by Russian authorities. Several of its top leaders were apprehended in a massive operation that spanned 25 places across the vast country. BlackFoG has compiled information on some of the most concerning cybercrime groups observed in 2022 and some ransomware strategies and patterns they share. Cybersecurity solutions targeting these strategies, techniques, and processes may be the finest early-stage investments security executives can make [8].

REvil had developed a pattern of repeatedly extorting its victims with the same data. After receiving a successful ransom payment, the gang determined that phishing for new victims was more difficult than re-extorting old ones, so they would demand victims pay again. Many new groups are expected to follow in their footsteps [9].

Therefore, data is very valuable to any organization. Businesses are immediately paralyzed if something contaminates or stops its flow, so attackers use it through ransomware attacks and keep it for ransom [10]. Thus, malware analysts analyze ransomware using special malware analysis techniques to create countermeasures against it.

Techniques used for malware analysis:

- Static analysis: It analyses the malware file without executing, knowing the hash value, the encryption algorithm used, and some of the file's properties.
- Dynamic analysis: running the malware in an isolated environment or the virtual environment, and at this step, tracking the behavior of the malware efficiently [11].

Information Technology executives and senior decision-makers must establish solid plans to combat tomorrow's cybersecurity risks and the latest ransomware gang methods. Security teams that can accurately foresee today's cybercrime patterns will be better equipped to deal with future threats.

The importance of having the correct data cannot be overstated. Security resources must be deployed using comprehensive threat intelligence data. The more you understand modern ransomware attacks and their techniques, the more prepared you will be [12].

Ransomware constitutes a severe threat to digital assets, and unless there is an encryption error, it isn't easy to recover these assets. One of the technical challenges facing security professionals is that designing and detecting an effective solution against this category of malware is a huge technical challenge. Because of the different methods and patterns of this category of malware, there is no standard technique dedicated to reverse engineering malware, and modern ransomware can evade anti-ransomware. Using static analysis and reverse engineering techniques enables us to disassemble the ransomware's source code and discover the characteristics and structure of the ransomware sample.

- What makes ransomware one of the most dangerous threats in cybersecurity? What are the harms caused by ransomware?
- What techniques are used for ransomware analysis, and what are the benefits?
- What encryption algorithm is used in the ransomware sample?
- How can we take countermeasures against ransomware attacks?

II. Literature Review

Gallegos-Segovia *et al.* [13] conducted a deep study of ransomware and how it relates to the social engineering that contributes to deploying, considering that the end-user is the weakest link in security. This study simulated the spread of ransomware using social engineering techniques. Also, the study discussed Countermeasures that limit the spread of ransomware; Computer solutions should be based on the establishment of periodic information security assessment tests and the formulation of policies that should be implemented inside each company.

Adamove *et al.* [4] distinguished by choosing a specific set of 13 key characteristics to analyze popular ransomware in many operating systems that help determine the similarities and differences in the list of modern ransomware subject to manual analysis. This analysis was to describe the design trends and behavior of modern ransomware, and this eliminates contradictions in the description of the ransomware behavior published by the Malware analysis laboratories. Moreover, suggest techniques to mitigate these threats based on the results obtained.

The study of O'Kane *et al.* [14] adds to the authors' expertise by examining the shift from early-day frauds to ransomware-enabled extortion. The authors look at the progression from crude ransomware efforts to the most advanced ransomware attack operations at the time.

Naveen and Gireesh [11] provide a clear idea of the internal structure of ransomware, which contributes to building a reliable identification mechanism against distributed ransomware attacks. The study also focused on analyzing some ransomware samples using reverse engineering techniques by setting up a virtual environment and installing many tools used in reverse engineering to perform practical analysis on some WannaCry ransomware samples through static and dynamic analysis.

Chittooparambil *et al.* [15] light on ransomware families from 1989 to 2017 have been identified and

categorized, but the pattern hasn't changed significantly. This study has three different ransomware families, and five stages of ransomware operation are identified. This study analyzed existing ransomware classifications as well as detection and prevention methods. The study concluded that none of the available solutions attempt to detect or stop ransomware in the first two stages based on his analysis of the existing methods. Because detection of ransomware at a later stage increases the impact of the attack, a solution to detect ransomware in its initial two stages is desirable to decrease the effect of ransomware.

Zimba *et al.* [16] analyzed the latest cryptoviral attacks and associated malware. Also, they propose a novel and comprehensive taxonomy of cryptoviral attacks that depicts how an attacker acquires cryptocurrencies and characterizes the attack paths of the nodes involved in the attack and their associated attacks.

The study of Akbanov *et al.* [17] concentrated on the first contacts and infection process of WannaCry, as well as its persistence mechanism, encryption process, recovery prevention, and communication with C&C servers. Important traits and behaviors of WannaCry during execution have been identified by the analysis. The results of this study might be applied to the creation of efficient countermeasures for WannaCry and other ransomware families that display similar behavior.

Mos & Chowdhury [12] discuss the stages of a ransomware attack and dive into the most destructive ransomware attack, WannaCry. The study explained that the security knowledge from this attack motivates the preventive action that helps understand the attacker's mindset using ransomware. Also, staying informed about current ransomware threats is one of the most effective protection methods.

Tang *et al.* [18] suggested Introspection-based RansomSpector, a method to identify and analyze crypto-ransomware. To detect assaults, RansomSpector, specifically located in the hypervisor layer, examines the file and network activity of ransomware that operates in the virtual machine. It is hence transparent to ransomware and challenging to get around. According to the evaluation's findings, RansomSpector can identify ransomware assaults with less performance impact.

In the context of the automobile industry, ransomware assaults are examined in the paper of Bajpai *et al.* [19]. The authors describe the limitations of ransomware in the context of cars and show examples of possible ransomware assaults. To encourage research to stop such attacks, they finally define the new ransomware tactics that the attackers may use in the context of vehicle systems.

The review of McIntosh *et al.* [20] has proposed a two-tier access control decision-making framework to help make more accurate and efficient access control decisions when needed. To monitor the file system's response to such an access request and, if necessary, roll back modifications. Also, it makes operating systems more resistant to damage caused by ransomware or software flaws.

Olaimat *et al.* [5] explain why developing and deploying an effective and efficient detective solution for this type of malware (ransomware) is a complex technical task. Also, they present a Ransomware taxonomy. The anatomy of the malware's invariant intrusions and infection pathways is shown. Furthermore, the study navigates and examines the different anti-analysis and evasive strategies that might be deployable by ransomware. The technical challenge that this ransomware poses is enlightened. This study discussed several technical issues that obstruct the development of reliable Crypto-Ransomware detection methods. The technical challenges raised in this study should push the research community to develop more effective and efficient anti-Ransomware algorithms and processes, especially since the world is more than ever bent toward adopting online work and education.

Oz *et al.* [21] provide a thorough analysis of ransomware defensive research with regard to PCs, workstations, etc. in this study. They provide a thorough analysis of the major components of ransomware, a taxonomy of significant ransomware families, and a complete summary of studies on ransomware protection. They also provide a detailed overview of the evolution of ransomware from 1990 to 2020. The authors think that this study will be essential in illuminating ransomware research with regard to target platforms and inspiring more studies.

III. Methodology

This research project was implemented according to the methodology and sequence of phases, First, with the literature review, and publications issued by governmental organizations specialized in raising awareness against ransomware and showing its damages.
Second, Data Set: The purpose of virtual machine software is to offer a platform that enables the effective and acceptable level of isolation execution of different operating systems concurrently. It makes virtualization a very potent tool for investigation by offering a real environment in a highly secured way. It would be essential to have a Windows 10 installation ISO file in a Virtual box to set up a malware analysis environment. The FlareVM installation, on the other hand, is a script you can execute that will convert a copy of Windows 10 into a reverse engineering environment with all the tools required for binary analysis, reverse engineering, and a secure location to run malicious software.

And in this research project, ransomware samples got from the project MalwareBazaar website, this is an initiative to gather and disseminate malware samples to the threat intelligence providers and infosec community. and analyzed real ransomware samples known as Dearcry and Babuk ransomware, which are executable files of 1.2 MB and 30KB.

Third, ransomware analysis: One of the most popular programs for malware analysis, PeStudio [Pestudio V.9.46] [22], was employed in the static analysis. It offers a wealth of details about the sample. then, using CAPA,

draw upon years of combined knowledge in reverse engineering to determine what a program accomplishes.

Following that began the reverse engineering process using IDA Pro Ghidra [IDA Pro] are excellent tools for studying malware samples from various backgrounds. This program transforms assembly language into pseudocode that is simpler to comprehend. It could help you comprehend the operation of the code more rapidly.
Fourth, results and countermeasures: The extracted data from the ransomware analysis was usable, accurate, complete, and relevant to the samples and took appropriate countermeasures. This step used Yara Rule and proposed effective countermeasures to increase security and avoid attacks.

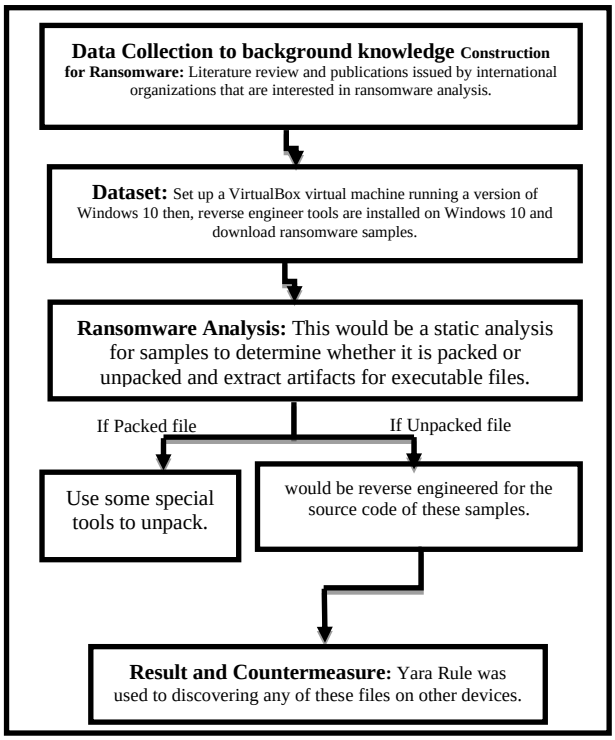


Figure 1. The Project Methodology.

Fig. 1 depicts the project's phase flow process: first, data collecting via literature review and international organization publications. Also, clarify the dataset required for the ransomware sample analysis investigation. Then, a ransomware sample is analyzed in a simulated environment that has all the study's tools. To write the findings using the Yara rule, as well as the required countermeasures to boost safety and avoid risk.

IV. Implementation

If one of the essential requirements for security and maintaining operating systems and the network is to extract unique strings from the programs that show unwanted behavior on devices or in the network.

Using static analysis and reverse engineering on ransomware samples in a virtual environment that simulates the functions of the actual computer is an alternative to the existing operating systems during malware analysis. Using reverse engineering tools that install in Virtual Machine, the code of the binary executable file (.exe) is examined and extracted, the functionality of ransomware samples and the encryption used for each, and Indicators of Compromise (IOC) are written and added to the Yara rule for discovery on other devices.

In this part, both Dercry and Babuk ransomware are analyzed using FLARE VM in Windows 10. FLARE VM is the first kind of reverse engineering and malware analysis distribution on the Windows platform. FLARE VM includes many tools such as IDA 7.0, radare, YARA, PEstudio, etc.(M., n.d.)

A. *DearCry Ransomware*

In March 2021, DearCry ransomware targets the four zero-day vulnerabilities known as CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065. The attack chain is aimed toward a Microsoft Exchange server that can accept untrusted connections from the internet. The DearCry ransomware encrypts the files it attacks and deletes the originals once it is copied.[23]

When performed, DearCry ransomware utilizes AES-256 and RSA-2048 to encrypt target files while altering file headers to include the string 'DEARCRY!'.

This project analyzed the DearCry ransomware sample available in "Malware Bazaar" (MalwareBazaar - E044d9f2d0f1260c3f4a543a1e67f33fcac265be114a1b135fd575b860d2b8c6.Bin (DoejoCrypt), n.d.). It is a portable executable file, and it is approximately 1.2 MB in size.

1) *Static analysis*

Static analysis is usually the initial step of malware analysis. Typically, the samples are examined with antivirus software and IOC scanners. This step includes the analysis of sample metadata, embedded strings, resources, imports, and exports (in Portable executable files, EXE), presence of macros, and auto-open or auto-close actions (in the case of Office Documents) [23].

In the Fig. 2, use the Pestudio tool to extract hash values and language in which the Dearcry ransomware file was written.

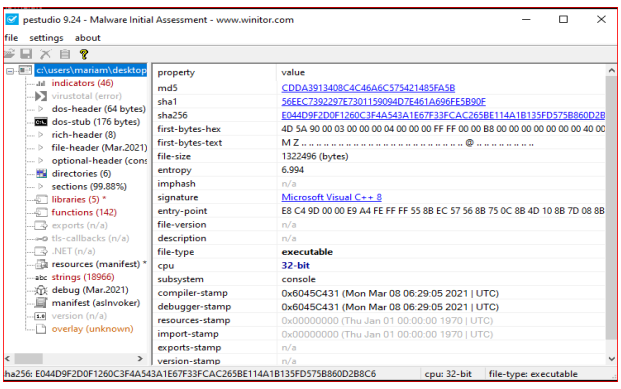


Figure 2. Associated DearCry hashes and signature.

The Pestudio tool is an essential tool that shows us the technical details for the files, which is one of the essential tools used in static analysis.

In the figure above, the hash value containing a series of numbers and letters appears unique and special for this file. The hash value of files is important in ensuring the file's integrity from tampering; It is also represented by more than one algorithm, as shown in the figure above. The md5 hash algorithm, which consists of a 128-bit string as a hex number, shows us 32 digits. Also explained the file value using the Secure Hash Algorithm 1 (SHA1), which consists of 40 numbers, i.e., a string containing 160 bits as a hexadecimal number. It also shows the secure hash value (sha256), which creates a 32-bit string of unique numbers for the file.

Also, the initial sequences of bytes are important details in the figure above. These bytes are not randomly typed but are represented using ASCII as signatures to identify the file format. The file included in the Pestudio tool was an executable file, which stands for "MZ" and is represented as a hexadecimal number "4D 5A". As shown in the above figure, the entropy value means the randomness in the file to be analyzed. The value of entropy ranges from zero to eight. If it rises about seven or higher, then it can be suspected. So Uses entropy in executable files to be undetected by Antivirus to verify its contents by encrypting completely. Thus, the value of entropy gives a rough idea of the methods of analysis that should be done.

Fig. 2 also showed us the type of programming language in which the ransom file was written, which is Microsoft Visual C++8; the type of the executable file and its version is 32-bit; The compiler stamp of the file is March 8, 2021, at 6:29.

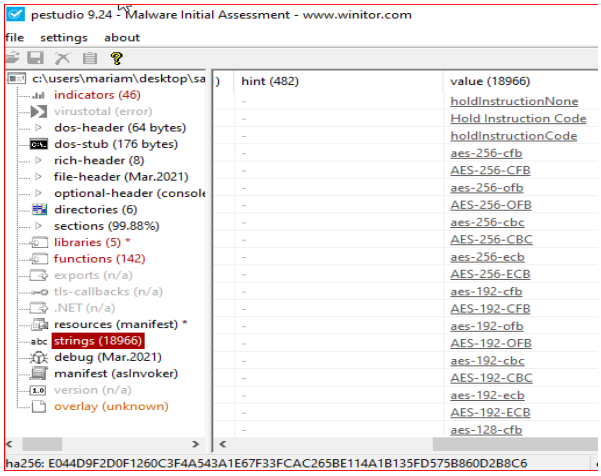


Figure 3. Associated DearCry encryption algorithms.

Strings:

When files are suspicious, the strings must be extracted to look for clues about the functions and pointers associated with the suspect executable. It is possible that the strings extracted from the executable file containing URLs and we can extract attack commands and references to the names of files and processes that will stop working if this malicious program is run. Strings hint at what the malware will do but do not give a clear view of the file and its capabilities.

DearCry ransomware did not contain any obfuscation; all strings are visible. For example, it used the Advanced Encryption Standard (AES) algorithm for encryption, such as in Fig. 3, one of the most widely used algorithms in the block cipher. In the AES encryption algorithm, the block size is fixed, which is 128 bits, but it supports three sizes of encryption keys, which are 128, 192, 256 bits; As the above Fig. 3 shows us, two types of the key were used, which are 192 and 256 bits. Also, some algorithms such as Cipher Block Chaining (CBC), Ciphertext Feedback (CFB), Output Feedback (OFB), and Electronic Codebook (ECB) could be used for padding blocks when the block is insufficient for the plaintext size. Also, use OpenSSL is designed in C, and it's responsible for the cryptography library implements the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols in an open-source manner. The library contains utilities for generating RSA private keys and Certificate Signing Requests (CSRs) and checksums, certificate management, and encryption/decryption. See that multiple crypto libraries call from OpenSSL inside the ransomware file in Fig. 4. it's a clear indication of facing a ransomware attack.

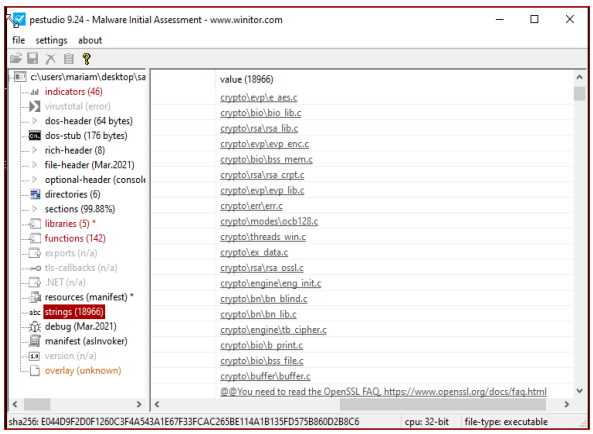


Figure 4. Interesting strings

2) Reverse engineering

Used IDA Interactive Disassembler for reverse engineering to DearCry sample, a portable Executable file produced by the Microsoft Visual Studio compiler. The analyzing objective is to determine what ransomware does and how it works.

The first time, Dearcry would begin to construct a new windows service called 'msupdate' this service is particularly liable for an encryption approach and is deleted after completion, shown in Fig. 5.

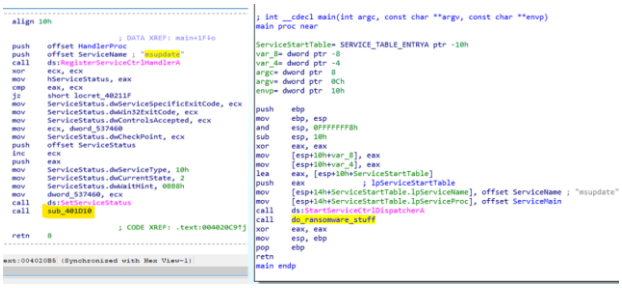


Figure 5. Main function.

A fixed list of extensions to queue for encryption is included, and the list covers the most common file types including ASPX shown in Fig. 6. The author of this ransomware can also encrypt and destroy the Exchange web shell, allowing access to the target PC via a remote shell.

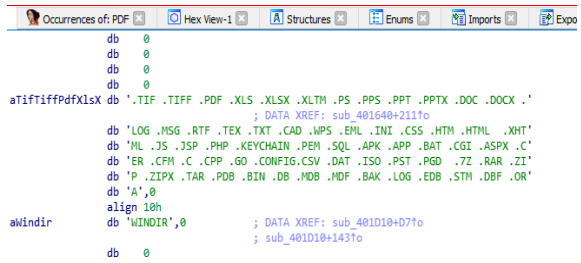


Figure 6. File extensions to be encrypted.

The DearCry ransomware encrypts files with AES-256 encryption during the encryption routine and then encrypts the AES key with an RSA-2048 key for additional harm. The ransomware will try to find encryptable data on all logical and accessible drives.

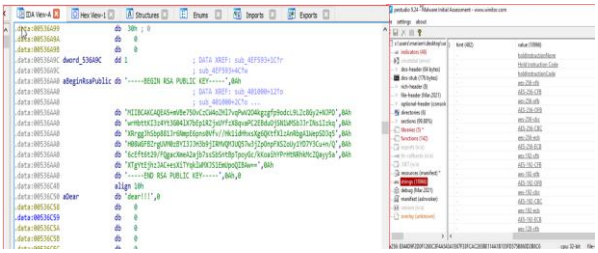


Figure 7. Extracted strings for RSA public key.

The encryption method begins with a copy of the original file. Then, the new file containing the original file after encryption. The string ". CRYPT" appears to be an extension of the ransomware-encrypted files as shown in Fig. 7. It's only used in one function; thus, it should oversee writing an encrypted file to a disk like Fig. 8. Therefore, when examining the encrypt file function. The mode "rb+" indicates that the original file is opened for update. For reading and writing, to be more specific. The "wb" mode means that a file with the extension ".CRYPT" is being opened for writing. DearCry uses copy encryption rather than in-place encryption of files. And appends a "DEARCRY!" tag at the beginning of the encrypted . CRYPT files.

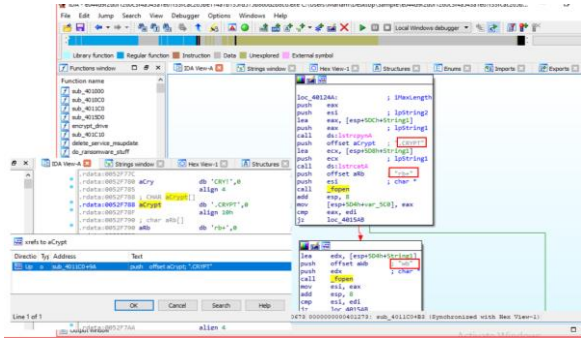


Figure 8. Cross-references to ". CRYPT" and creating the encrypted file by ransomware.

Fig. 8 and Fig. 9 showed this ransom note includes two email addresses for the threat developer and hashes for the file, an MD4 hash of the RSA public key hardcoded into the binary file.

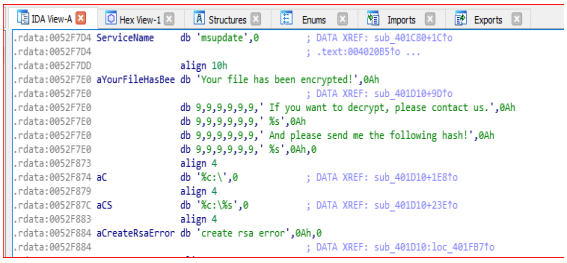


Figure 9. Ransom note template.

DearCry employs a stand-alone encryption mechanism in which the RSA public key is hardcoded into the ransomware file. The ransomware does not communicate with any command-and-control server to get more encryption keys or update the encryption operation's progress during the infection process.

B. Babuk Ransomware

Babuk ransomware is a new threat identified in 2021 that has infected at least five large businesses, one of which has already paid the attackers $85,000 following negotiations. Babuk ransomware like other malware is spread through targeting and penetrate the companies' networks by attackers. Babuk's developers have used the same methodologies as previous ransomware authors and have exposed the stolen data. The hash for the sample used in this project is 8203c2f00ecd3ae960cb3247a7d7bfb35e55c38939607c85dbdb5c92f0495fa9. This hash is associated with Babuk version 1. It is a 32-bit executable with a minimal file size of 30kb. This first version isn't protected or obfuscated [24].

After acquiring the Babuk ransomware sample, the static analysis was performed and confirm the file is ransomware through some characteristics extracted from metadata, strings, resources, etc., that are embedded in the executable file for the sample without viewing the instructions.

1) Reverse engineering

Babuk ransomware encrypts the file, tries to destroy the shadow volume through utilizes "vssadmin.exe" and "ShellExecuteW" before and after encryption shown in Fig. 10.

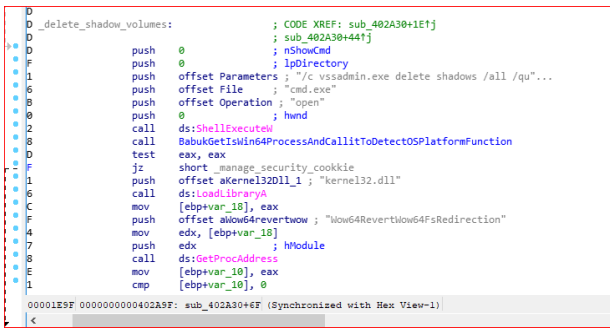
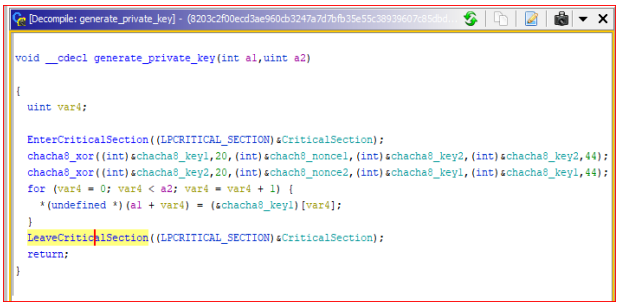


Figure 10. Destroy the shadow volumes.

Also, encrypts remote disks, and utilizes the Windows Restart Manager to terminate any process or service that may prevent it from encrypting files. Fig. 11 shows Excel.exe, notepad.exe, sql.exe, firefox.exe, outlook.exe, ocssd.exe, dbsnmp.exe, and isqlplussvc.exe are some of the processes or services that it terminates.

Figure 11. List of processes and services to be closed [7].

Fig. 12 shows Babuk ransomware utilizes SHA256 hashing, ChaCha8 encryption, and the Elliptic-curve Diffie–Hellman (ECDH) algorithm for generating keys to secure its keys and encrypt files.



```
void __cdecl generate_private_key(int a1,uint a2)

{
  uint var4;

  EnterCriticalSection((LPCRITICAL_SECTION)&CriticalSection);
  chacha8_xor((int)&chacha8_key1,20,(int)&chacha8_nonce1,(int)&chacha8_key2,(int)&chacha8_key2,44);
  chacha8_xor((int)&chacha8_key2,20,(int)&chacha8_nonce2,(int)&chacha8_key1,(int)&chacha8_key1,44);
  for (var4 = 0; var4 < a2; var4 = var4 + 1) {
    *(undefined *)(a1 + var4) = (&chacha8_key1)[var4];
  }
  LeaveCriticalSection((LPCRITICAL_SECTION)&CriticalSection);
  return;
}
```

Figure 12. Randomly generating ECDH private key.

Babuk traverses and encrypts files using a recursive technique. It searches each directory for files and subdirectories using the FindFirstFileW and FindNextFileW functions shown in Fig. 13. It recursively invokes the main encrypt function when it encounters a directory. Babuk on the other hand only goes down 16 directory levels deep. Thus, it may not encrypt all drive folders to save time. To prevent encrypting the ransom note or encrypted files, it will check if the file name is How to Restore Your Files.txt or if the file extension is. __NIST_K571__.

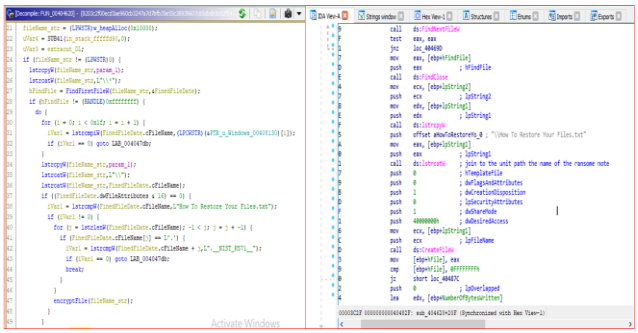
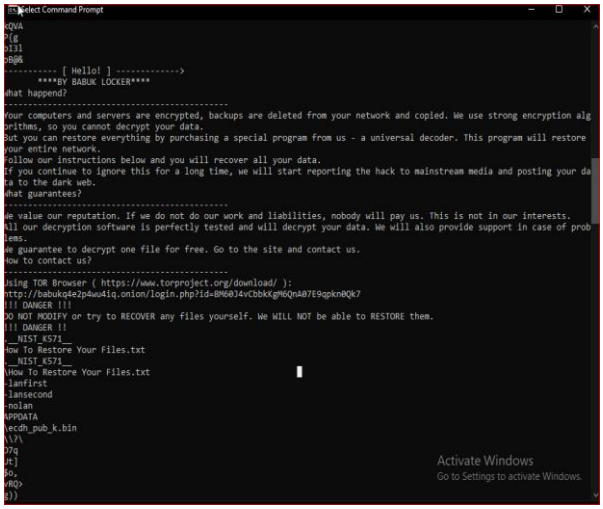


Figure 13. Traversing through folders.

Fig. 14 shows babuk ransomware victims have been notified that they would be unable to retrieve (decrypt) their files unless they purchase decryption software from the ransomware's producers. Victims are advised to contact developers through the given Tor website to receive advice on how to pay for the program.



```
Select Command Prompt
xQVA
?(@
b131
b@@6
---------- [ Hello! ] ---------->
      ****BY BABUK LOCKER****
What happend?
---------------------------------------------
Your computers and servers are encrypted, backups are deleted from your network and copied. We use strong encryption alg
orithms, so you cannot decrypt your data.
But you can restore everything by purchasing a special program from us - a universal decoder. This program will restore
your entire network.
Follow our instructions below and you will recover all your data.
If you continue to ignore this for a long time, we will start reporting the hack to mainstream media and posting your da
ta to the dark web.
What guarantees?
---------------------------------------------
We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests.
All our decryption software is perfectly tested and will decrypt your data. We will also provide support in case of prob
lems.
We guarantee to decrypt one file for free. Go to the site and contact us.
How to contact us?
---------------------------------------------
Using TOR Browser ( https://www.torproject.org/download/ ):
http://babukq4e2p4wa4iq.onion/login.php?id=BM6014vCbbKKgM6QnA87E9qpkn0Qk7
!!! DANGER !!!
DO NOT MODIFY or try to RECOVER any files yourself. We WILL NOT be able to RESTORE them.
!!! DANGER !!
__NIST_K571__
How To Restore Your Files.txt
__NIST_K571__
\How To Restore Your Files.txt
-lanfirst
-lansecond
-nolan
APPDATA
\ecdh_pub_k.bin
\\?\
)?q
Jt]
$o,
$RQ>
$))
Activate Windows
Go to Settings to activate Windows.
```

Figure 14. Extracted strings with a ransom note.

C. *The Effective Countermeasures*

The phishing emails and vulnerabilities are the reason for the spread of this type of malware, which calls for companies, organizations, as well as individuals to take many countermeasures to protect their digital assets from encryption.

Also, ransomware used different encryption algorithms and file encryption methods and access to operating systems, which researcher [5] assure that there is no solution to prevent it.

Accordingly, after analyzing the samples, the study suggested signature-Based Protection, Yara rules depend on your analysis and extraction of the valuable data. When extracting data professionally and more accurately and adding it to Yara Rule and running Yara on all other devices and servers in your environment to ensure the safety of machines and servers, or to find out infected devices and servers to isolate them.

1) Detect dearcry and babuk ransomware by Yara rule

Wrote effective Yara rules that enable us to check whether the operating system has this ransomware or not by using these rules shown in the Fig. 15.

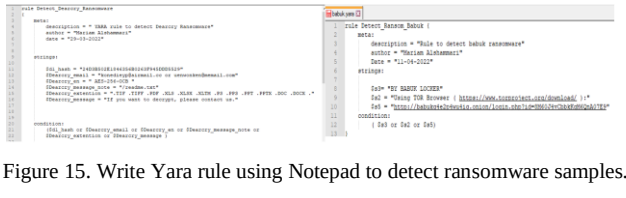


Figure 15. Write Yara rule using Notepad to detect ransomware samples.

This Yara rule was written using the Notepad ++ program; This rule bears information such as, the rule name, author, and the date to explain to us in the future who wrote this rule. The most important part, the extracted strings, must be written professionally and accurately to meet the below condition using the Boolean expressions.

Then I used the yara32 tool to detect this ransomware using the rule written above by the comment lines as in the Fig. 16.

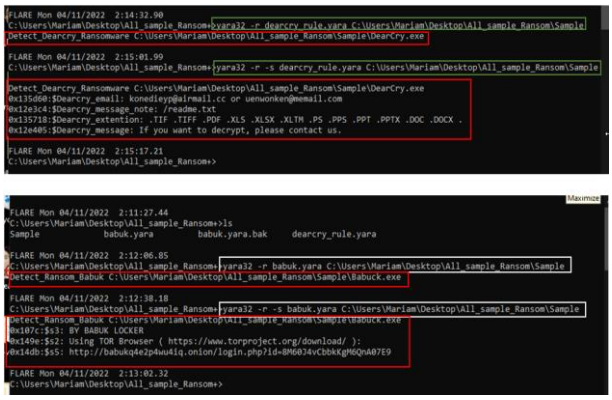


Figure 16. Running Yara rule to detect Dearcry and Babuk ransomware.

As shown in the previous figure, yara32 was used with the rule we wrote. Then the search was specified in the path of the file in which the Yare rule is saved. identified some commands that speed up the search process in yara32, which are -r and -s to search in the specified path and display all detected text strings along with the file name, which leads to the discovery of the Dearcry and Babuk ransomware file and success the extract unique data during the sample analysis phase.

So, Yara rules depend on your analysis and extraction of the valuable data. When extracting data professionally and more accurately and adding it to Yara Rule and running Yara on other devices and servers in your environment to ensure the security of machines and servers or to find infected devices and servers to isolate them.

Worthy of mentioning, depending only on signature-based protection is not adequate. Therefore, the most important countermeasures that must be taken to increase safety and avoid danger using anti-virus such as Windows Defender by enabling each of the following features: Virus and threat protection with Real-time protection and Ransomware protection. Available in the latest version of Windows Defender to detection of ransomware files while downloaded to your computer.

2) The simulations of project countermeasures

The flowchart in Fig. 17 shows a simulation of the project countermeasures recommended and the level of risks involved.

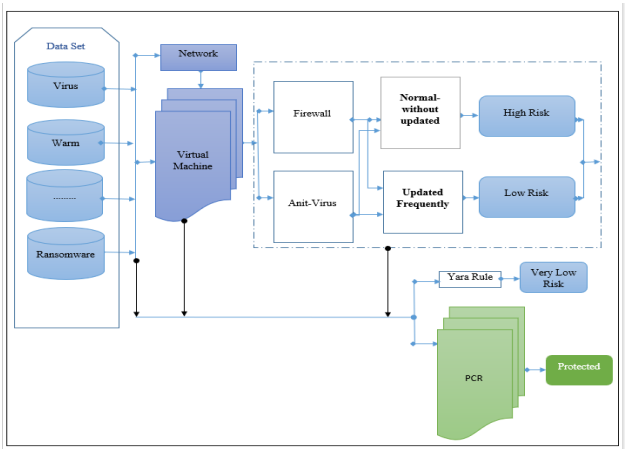


Figure 17. Project Countermeasures (PCR).

Whether these countermeasures are implemented on the ransomware samples analyzed in this study or from any malware dataset, their risk is assessed as follows:

First, Malware are downloaded using the network from many sources, whether through e-mail attachments, from suspicious and undocumented sites, or by exploiting security vulnerabilities in systems...etc. It is downloaded on the physical system or virtual machines such as the Virtual Box.

As the simulation flowchart shows, there are some possibilities for the risk level: high-risk level, low-risk level, very low-risk level, and protected system.

High-risk level: If the default settings of the firewall are used and without continuous updates, the risk of malware will become high, leading to the possibility of data loss and serious damage.

Low-risk level: Antivirus programs such as Windows Defender detect and prevent Malware from spreading on the computer, as they work in the background to detect this Malware. Its continuous update protects files and programs, which reduces the risk of malicious programs on devices.

Very low-risk level: Writing Yara rules and activating them in the work environment devices leads to detecting malicious programs long enough before the occurrence of critical damage.

Protected system: For the system to be protected, all the suggested countermeasures must be applied, which are the continuous update of anti-virus programs, updating the firewall and putting the settings according to the organization's policies, and the regular update of Yara's rules; In addition to the need to implement strict policies, which are divided into two parts:

D. Policies Within the Organization

They are policies that are imposed on the employees within the organization, especially the organizations that have critical systems; this is done through:

- Enforce stringent policies on the use of the Internet.
- The policy of blocking external files from entering the institution's devices and not exchanging files over the Internet.
- Enforce a policy of limited use of network resources for authorized persons.
- Enforce the strong passwords policy.
- Enforce a daily data update policy and backup them.

E. Countermeasures from the National Institute of Standards and Technology (NIST)

The essential countermeasures that must be taken to increase safety and avoid danger are recommended by Veeam, using a cybersecurity framework developed by the National Institute of Standards and Technology (NIST) because it is used worldwide as a starting point for managing cybersecurity. NIST provided a unified set of guidelines and standards for organizations and companies of different sizes and industries. This cybersecurity framework can also be used as a high-level security management tool and helps assess cybersecurity risks in

organizations. NIST consists of five phases: Identify, Protect, Detect, Respond, and Recover [10].

1) Identify

Determine the risks associated with cyber security to the operations, assets, and people of the organization by identified and prioritized threats and vulnerabilities, both internal and external. Establish risk management procedures that are overseen and accepted by all parties in order to support choices on operational risk [25]

a) The human firewall

Everyone in the organization should be aware of security risks and potential incidents and report any suspicious activity to build a multi-layered defense. It is worth noting the importance of the human firewall, an essential layer of defense against ransomware of any kind. It can also identify threats, prevent data security breaches, and mitigate their damage.

2) Protect

The objective of the task is to create and put in place the necessary safeguards to guarantee the provision of essential infrastructure services. A possible cyber security event or incident's impact can be limited or contained with the help of the Protect procedure [26].

a) Controlling folder access

Controlled Folder Access helps protect sensitive and valuable data from malicious threats such as ransomware; This is done by examining the applications and comparing them to a list of trusted and known applications. The effectiveness of controlling folder access lies with Microsoft Defender for Endpoint, which gives detailed reports on the events and blocking of access to the folder. It allows only applications included in the list of trusted programs to access protected folders [27].

b) Backup offline

One of the countermeasures is to keep offline backups wholly isolated from the hacked systems, and they are periodically updated according to the organization's policy. they are kept in a safe place and not brought online except when necessary.

c) Using immutable backup storage

This type of backup is located outside the target network and cannot be modified or deleted by anyone for a specific period, whether a week, a month, or more. It is impossible to modify the immutable copies by administrators or those with administrator privileges, unlike standard backup copies that are easy to modify or delete by system administrators. The hacker cannot alter, change, encrypt or delete backup files of this type, even with full administrator access to the backup server [10].

3) Detect

To detect cybersecurity events and confirm the efficacy of preventative measures, the information system and assets are continuously monitored at specific intervals. Additionally, anomalous behavior is promptly spotted, and the potential consequences of events are recognized [28].

a) Filter and monitor incoming emails

E-mail messages are one of the essential doors that attackers use to distribute and spread malware, such as attaching files or sending malicious links to the user. The best solution is to filter and monitor these incoming spam messages and ensure that these files and links are not malicious. When it is suspected that this file or link is suspicious, it is sent to the information technology department to examine its status [29].

4) Respond

The objective of the Respond function is to create and put into practice the necessary actions to address a detected cybersecurity event. Considering it, it is possible to limit the effects of a prospective cybersecurity incident. Planning your response, communicating with others, doing an analysis, mitigating risks, and making improvements are a few examples of result categories under this function [30].

a) Creating an incident response plan

Defining methods for identifying, communicating, controlling, and remediating security problems in a well-defined incident response plan will allow you to specify procedures for staff to know how to respond to cybersecurity events as they emerge effectively [10].

5) Recover

The recovery function permits a speedy return to regular operations as the frequency of cyberattacks and data breaches grows. To enable prompt restoration of systems or assets affected by cybersecurity incidents, recovery protocols and procedures are implemented and maintained [31].

Therefore, strongly recommend taking all the countermeasures mentioned in this research to reduce and counter ransomware, primarily in organizations that contain sensitive information, such as banks, governmental and private organizations, and educational institutions, as they show their effectiveness for users with different specialties.

V. Discussion

Most previous studies analyzed ransomware using static or dynamic analysis, or both. Some of these studies prefer dynamic analysis to static analysis due to the development of ransomware and its ability to use obfuscation methods or multi-format or metamorphic attacks to evade or hide from static analysis. However, some other studies revealed that modern ransomware developers could hide the activities of malicious files and stop their work if it was discovered that it was in a virtual environment to evade dynamic analysis. But we can't say that all ransomwares took this approach to hide and escape analysis; Based on the experience in this study, which was conducted on samples of ransomware that appeared in recent years, which did not use any obfuscation or hide code from the use of reverse engineering tools. Both Dercry and Babuk ransomware were thoroughly investigated and analyzed during this experiment. The cause of their occurrence was security vulnerabilities in operating systems; The encryption

mechanism followed in each sample was also identified. One of the countermeasures that I recommended was to find quick solutions to close these vulnerabilities to avoid cyber-attacks that occur because of them. Also, after the static analysis and reverse engineering of these samples were completed, a Yara rule was established to discover such malicious files in other devices in the same organization. Also, the results of the Yara rule are based on the signature of the file and achieve good results about the samples that have been analyzed or known.

Yet, the Yara Rule is inadequate for modern ransomware because malware analysts do not have its signatures. A study presented [32], whose results showed the effectiveness of continuous monitoring of system file activities and registry activities against ransomware. According to the study conducted by [33], the most effective countermeasure recommended by Microsoft is the folder access control, that requires the user to allow other files to access or modify protected folders [27]. Furthermore, immutable backup is one of the best countermeasures, but they need specialists to make these backups.

VI. Conclusion

Ransomware attacks are widespread and expand their coverage of attacks to other areas targeting individuals, countries, law enforcement agencies, government agencies, and other sectors like financial institutions. The project described reverse engineering tools and approaches for performing effective ransomware analysis. As a result, analyzing these ransomware samples provides a clear idea of how it works, and the encryption algorithm used. And creates an efficient Yara rule to detect cyberthreat information based on an accurate analysis done for Dearcry and Babuk ransomware. Due to this issue, many in-depth studies and analyses have been conducted to examine and identify effective countermeasures to combat ransomware attacks. Finally, simulated the project countermeasures and the level of risks involved. Now know what dangers, how ransomware works, and how it developed to avoid detection. The best defense is to be educated about current ransomware threats and how to protect against future modern ransomware. In terms of future work, it is planned to create a tool that can detect ransomware in real time and prevent it from spreading throughout the enterprise network.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Conceptualization, N. A., and M.A.; methodology, M. A. and N. A.; software, M.A.; validation, N.A., and Y.A.; formal analysis, M. M., N. A. and Y. A.; investigation, M. A. and N. A.; resources, M. A; data curation, M. A.; writing—original draft preparation, M. A., and N. A.; writing—review and editing, N. A. and Y.A.; visualization, Y. A.; Supervision, N. A.; project administration, N. A.; funding acquisition, N. A., and M. A. All authors have read and agreed to the published version of the manuscript.

Funding

This research has been funded by Scientific Research Deanship at University of Ha'il, Saudi Arabia through project number GR-22 006.

References

[1] S. D. Mukesh, "An analysis technique to detect ransomware threat," in *Proc. 2018 International Conference on Computer Communication and Informatics (ICCCI)*, 2018, pp. 1–5. doi: 10.1109/ICCCI.2018.8441502

[2] N. Ariffin, A. Zainal, M. A. Maarof, and M. N. Kassim, "A conceptual scheme for ransomware background knowledge construction," in *Proc. 2018 Cyber Resilience Conference (CRC)*, 2018, pp. 1–4. doi: 10.1109/CR.2018.8626868

[3] K. P. Subedi, D. R. Budhathoki, and D. Dasgupta, "Forensic analysis of ransomware families using static and dynamic analysis," in *Proc. 2018 IEEE Security and Privacy Workshops (SPW)*, 2018, pp. 180–185. doi: 10.1109/SPW.2018.00033

[4] A. Adamov and A. Carlsson, "The state of ransomware. Trends and mitigation techniques," in *Proc. 2017 IEEE East-West Design & Test Symposium (EWDTS)*, 2017, pp. 1–8. doi: 10.1109/EWDTS.2017.8110056

[5] M. N. Olaimat, M. A. Maarof, and B. A. S. Al-Rimy, "Ransomware anti-analysis and evasion techniques: A survey and research directions," in *Proc. 2021 3rd International Cyber Resilience Conference (CRC)*, 2021, pp. 1–6. doi: 10.1109/CRC50527.2021.9392529

[6] Blackfog. (2020). The state of ransomware in 2020, April. [Online]. Available: https://www.blackfog.com/the-state-of-ransomware-in-2020/#%0Ahttps://www.blackfog.com/the-state-of-ransomware-in-2020/

[7] X. Deng and J. Mirkovic, "Polymorphic malware behavior through network trace analysis," in *Proc. 2022 14th International Conference on Communication Systems & Networks (COMSNETS)*, 2022, pp. 138–146. doi: 10.1109/COMSNETS53615.2022.9668396

[8] D. Williams. (2022). Ransomware group tactics in 2022. BlackFog. [Online]. Available: https://www.blackfog.com/ransomware-group-tactics-in-2022/

[9] S. Jarjoui, R. Murimi and R. Murimi, "Hold My Beer: A Case Study of how Ransomware Affected an Australian Beverage Company," in *Proc. 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 2021, pp. 1–6. doi: 10.1109/CyberSA52016.2021.9478239

[10] R. Vanover and E. Weijdema, (2021). 5 Ransomware Protection Best Practices. [Online]. Available: https://www.veeam.com/wp-protection-yourself-from-ransomware.html

[11] S. Naveen and T. G. Kumar, "Ransomware analysis using reverse engineering," in *Advances in Computing and Data Sciences*, M. Singh *et al*., Eds. Singapore: Springer Nature Singapore Private Limited., 2019, pp. 185–194.

[12] M. A. Mos and M. M. Chowdhury, "The growing influence of ransomware," in *Proc. 2020 IEEE International Conference on Electro Information Technology (EIT)*, 2020, pp. 643–647. doi: 10.1109/EIT48999.2020.9208254.

[13] P. L. Gallegos-Segovia, J. F. Bravo-Torres, V. M. Larios-Rosillo, *et al.*, "Social engineering as an attack vector for ransomware," in *Proc.* 2017 *CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON)*, 2017, pp. 1–6. doi: 10.1109/CHILECON.2017.8229528

[14] P. O'Kane, S. Sezer, and D. Carlin, "Evolution of ransomware," *IET Networks*, vol. 7, no. 5, pp. 321–327, 2018. doi: 10.1049/iet-net.2017.0207

[15] H. J. Chittooparambil, B. Shanmugam, S. Azam, *et al*., "A review of ransomware families and detection methods," in *Proc. IRICT 2018: Recent Trends in Data Science and Soft Computing*, F.

Saeed, *et al.*, Eds. Berlin, Germany, 2018, vol. 843, pp. 588–597. doi: 10.1007/978-3-319-99007-1_55
[16] A. Zimba, Z. Wang, H. Chen, *et al*., "Recent advances in cryptovirology: State-of-the-art crypto mining and crypto ransomware attacks," *KSII Transactions on Internet and Information Systems*, vol. 13, no. 6, pp. 3258–3279, 2019. doi: 10.3837/tiis.2019.06.027
[17] M. Akbanov, V. G. Vassilakis, and M. D. Logothetis, "WannaCry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms," *Journal of Telecommunications and Information Technology*, vol. 1, pp. 113–124, 2019. doi: 10.26636/jtit.2019.130218
[18] F. Tang, B. Ma, J. Li, *et al.*, "RansomSpector: An introspection-based approach to detect crypto ransomware" *Computers and Security*, vol. 97, 101997, 2020. doi: 10.1016/j.cose.2020.101997
[19] P. Bajpai, R., Enbody, and B. H. C. Cheng, "Ransomware targeting automobiles," in *Proc. the 2nd ACM Workshop on Automotive and Aerial Vehicle Security*, 2020, pp. 23–29. doi: 10.1145/3375706.3380558
[20] T. McIntosh, P. Watters, A. S. M. Kayes, *et al.*, "Enforcing situation-aware access control to build malware-resilient file systems," *Future Generation Computer Systems*, vol. 115, pp. 568–582, 2021. doi: 10.1016/j.future.2020.09.035
[21] H. Oz, A. Aris, A. Levi, and A. S. Uluagac, "A survey on ransomware: Evolution, taxonomy, and defense solutions," ACM Computing Surveys, vol. 54, no. 11s, pp. 1–37, 2022. doi: 10.1145/3514229
[22] Pestudio 9.46. [Online]. Available: https://www.winitor.com/
[23] LIFARS. (2021). DearCry ransomware malware analysis and reverse engineering. [Online]. Available: https://lifars.com/wp-content/uploads/2021/04/DearCry_Ransomware.pdf
[24] A. Mundo, T. Seret, T. Roccia, and J. Fokker. (2021). Technical analysis of Babuk ransomware. McAfee, SAN Jose, California, USA. [Online]. Available: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-babuk-ransomware.pdf
[25] A. Ibrahim, C. Valli, I. McAteer, and J. Chaudhry, "A security review of local government using NIST CSF: A case study," *Journal of Supercomputing*, vol. 74, no. 10, pp. 5171–5186, 2018. doi: 10.1007/s11227-018-2479-2
[26] N. Teodoro, L. Gonçalves, and C. Serrão. (2022). NIST Cybersecurity Framework Compliance. 351. [Online]. Available: https://www.complianceforge.com/reasons-to-buy/nist-cyber-security-framework-csf.html
[27] Microsoft. (2022). Protect important folders from ransomware from encrypting your files with controlled folder access. Microsoft Docs. [Online]. Available: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/controlled-folders?view=o365-worldwide
[28] Detect. (2018). NIST. [Online]. Available: https://www.nist.gov/cyberframework/detect
[29] M. U. Kiru and A. B. Jantan, "The age of ransomware: understanding ransomware and its countermeasures," in *Artificial Intelligence and Security Challenges in Emerging Networks*, R. Abassi, Ed. IGI Global, Hershey, Pennsylvania, USA, 2019, pp. 1–37. doi: 10.4018/978-1-5225-7353-1.ch001
[30] Respond — CSF Tools. (2021). CSF Tools — The Cybersecurity Framework for Humans. [Online]. Available: https://csf.tools/reference/nist-cybersecurity-framework/v1-1/rs/
[31] Recover. (2018). NIST. [Online]. Available: https://www.nist.gov/cyberframework/recover
[32] Monika, P. Zavarsky, and D. Lindskog, "Experimental analysis of ransomware on windows and android platforms: Evolution and characterization," *Procedia Computer Science*, vol. 94, pp. 465–472, 2016. doi: 10.1016/j.procs.2016.08.072
[33] C. Beaman, A. Barkworth, T. D. Akande, *et al.*, "Ransomware: Recent advances, analysis, challenges and future research directions," *Computers and Security*, vol. 111, 102490, 2021. doi: 10.1016/j.cose.2021.102490

Naif Alsharabi is an associate professor of computer network at Amran University in Amran, Yemen. He obtained his undergraduate degree in computer Sc. (1997) from Technology University in Baghdad, He received his master and Ph.D. in wireless communication networks from Hunan University at Hunan province, China in 2005 and 2008. Currently Naif is working as an associate professor in Computer Engineering Department at College of Computer Sc. and Engineering, University of Hai'l from March 2021. His research interests span both computer networking, information security, deep learning, and data science.

Mariam Alshammari is a master's degree student in College of Computer Science and Engineering, Cyber Security Program. Her areas of interest are cyber security, big data security and IoT.

Yasser Alharbi is currently an assistant professor in the College of Computer Science & Engineering at the University of Hail in Saudi Arabia. He obtained his Ph.D. in computer sciences from the University of Essex, the United Kingdom in 2018. His areas of interest are big data in the network, IoT, fog computing and grid and cloud computing systems & network, which include resource and application management in clouds (VMs allocation and migration), performance analysis, modelling and optimization, and energy efficiency (green cloud).