International Journal of Multidisciplinary Research and Growth Evaluation.

A Disruptive Ransomware: Its Impersonation Process, Identification and Avoidance

Bhagwant Singh [1*], Dr. Sikander Singh Cheema [2]
[1, 2] Department Of Computer Science and Engineering, Punjabi University Patiala, Punjab India

* Corresponding Author: **Bhagwant Singh**

Article Info

ISSN (online): 2582-7138
Volume: 06
Issue: 02
March-April 2025
Received: 15-01-2025
Accepted: 09-02-2025
Page No: 238-245

Abstract
With science and technology advances, the capabilities and capacities of users' electronics gadgets are expanding at a rapid rate for saving more and more data, but meanwhile, such gadgets are always at high risk of compromising data security. Ransomware attacks are regarded as being very important, and they are extremely challenging to identify and handle. Here in this paper, the author introduces a disruptive Ransomware that is novel in its impersonation process to become a threat and can be discreetly installed by evading Windows Defender, Firewall, and Antivirus. It is also unique in that it is proficient at managing information. This article, along with its different sections, introduces various approaches to identify and avoid it.

Keywords: Disruptive Ransomware, Impersonation Process, Identification and Avoidance, Ransomware, Encryption and Decryption

1. Introduction

For internet users, ransomware is a critical issue that has lately mostly affected enterprises. Malicious malware known as ransomware prevents consumers from obtaining their data (often by encrypting it) and demands a fee in exchange for access. According to the latest report from Cybersecurity Ventures, by 2021, a ransomware assault will occur every 0.18 minutes [1].
The majority of the time, those who create ransomware do so by utilising tools intended to make the Internet more accessible and freer. Therefore, it's not surprising that they were among the first to adopt blockchain technology. At first, they sought ransom payments from their victims in a highly anonymous manner using bitcoins. Recent research, however, reveals that malware authors use blockchain-based services for a memory purpose or sometime to communicate with the ransomware [1]. Nonetheless, as blockchain is not best option for saving random data, transmitting files across they can be time-consuming and occasionally expensive.
There are different types of ransomware; the most typical kinds include crypto-ransomware or encryption tools, lockers, scareware, doxware or leakware, and RaaS [2]. Encryption as well as Crypto-Ransomware, is a very usual and dangerous variety of Ransomware [3]. Of this data and files within the computer are inaccessible without a suitable code. Locker, on the other hand, locked out the user's system, making data unavailable [4].
Scareware is phoney program which approaches for the money to fix problems that is under the scope of it including viruses and various other [5]. Some varieties of spyware lock the machine, but others only flood the display with a message without affecting the files. Similar to this, numerous people become worried and pay whenever they have been harmed by the making of sensitive information about individuals or businesses publicly available online. [6]. another type of ransomware is called Officers; it pretends to be law enforcement and alerts users to illegal internet activity and offers them the chance to escape jail time by paying a fine [7].

1.1 Attacks due to ransomware

Since its creation, ransomware has evolved into a variety of variations that serve their functions in distinct ways. By encrypting files and data on the hard drive, some software scares users into paying for phoney services or software, while other software restricts access to the operating system or uses sensitive user data to demand payment. The software security sector is well aware of these dangers and continuously assesses the dangers of new versions and types in order to offer an updated defense. This

Section looks into the impact of ransomware on the victim's machine [8].

- Payload persistence: The assault is carried out completely; typically accomplished by adding an executable to the startup folder, setting a task to run every time the computer starts up, or adding a startup item to the registry.
- Anti-system restores: Shadow copy save are typically deleted to implement anti-system restore, which stops system restore from undoing the changes.
- Stealth techniques: Malware attempts to run covertly in order to evade detection; this is typically accomplished by code injection into legitimate processes, executing from AppData.
- Environment mapping: Many ransomwares examine the system it attacked to ascertain the victim's value, additional potential targets (through the network), and if it is operating on a genuine computer or in a sandbox environment that might be attempting to analyse it.
- Network traffic: The majority of ransomware programmes require a web connection in order to obtain the files necessary for the payload and/or to transmit the encryption key.
- Privilege elevation: Using administrator rights to execute the attack; occasionally, just requesting administrator access or even other privilege escalation tactics, like click highjacking, may be effective.

Usually, all known types of ransomware programmes work similarly, but the disruptive ransomware described in this paper can install secretly without being detected by security software or antivirus programs. It even doesn't show its presence in the victim's system, as everything in the system continues to function normally after installation, including services, CPU use, disc usage, RAM consumption, etc. In addition to this, it does operate and install as a trustworthy programme. After installation, a single click instantly alters the machine's behaviour for several seconds or minutes. Following that, a user loses access to their data, which is upsetting for regular users and challenging to deal with. In the proceeding sections, the author has presented the, Proposed ransomware's action plan, algorithm of proposed ransomware with its pseudocode, the assault tactical phases of proposed ransomware, encryption and decryption techniques of proposed ransomware, and reactions to proposed ransomware. Further identification and avoidance of the proposed ransomware have also been given.

2. Material and methods

This section discussed about the framework of the proposed ransomware, its algorithm, encryption and decryption procedure.

2.1 Proposed ransomware's action plan

The proposed ransomware attack is divided into three stages. The name of these three stages are pre-attack stage, attack stage and post attack stage. In pre-attack stage, ransomware, perpetrator a design using a Command and Control (C&C) in which The PPK (Public-Private Key) Pair is created by the C&C server using RSA. Using this, offenders may trick the user into visiting their bogus website or message. Further in attack stage, a symmetric key has been created by ransomware. The user's computer's file system is then compromised by ransomware. The user's data is encrypted by the malware, and the unencrypted files are deleted if they weren't altered, and new documents are created that contain the encrypted data instead of the unencrypted files. The symmetric key is encrypted by the ransomware using the public key of the C&C server. In addition to this, an extortion message has been added in place of the plaintext symmetric key.

Finally, during the post-attack stage, victim displays the decryption key. The command-and- control server is where the ransomware gets its hands on the secret keys. The symmetric key is decoded using the private key, and finally, the user's data is decoded using the symmetric key. A three-stage working of proposed ransomware shown in figure 1

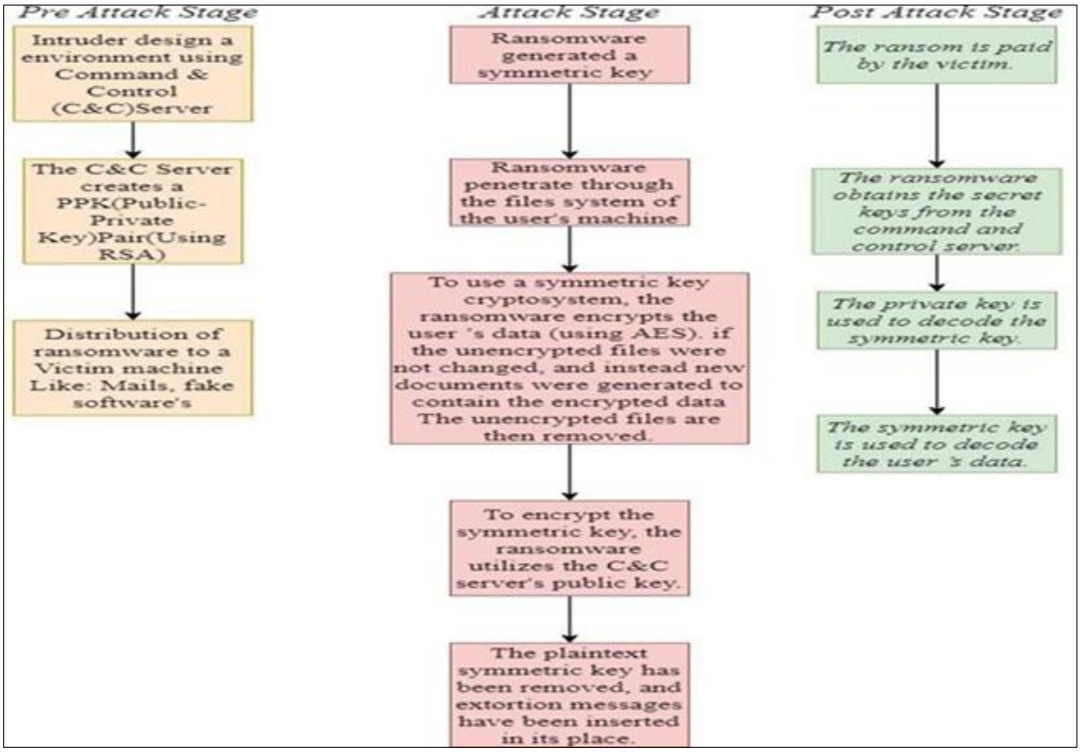

Fig 1: Action plan of proposed ransomware

2.2 Algorithm of proposed ransomware

The algorithm of the proposed ransomware is shown in Figure 2. As depicted in Figure 2, it consists of five steps to form a complete algorithm for the proposed ransomware.

These steps are connectivity to the browser and internet, accessing the victim's system's IP address and physical address, getting control of the system, and finally encrypting the user's data. The encrypted file has shown the. bhg extension.

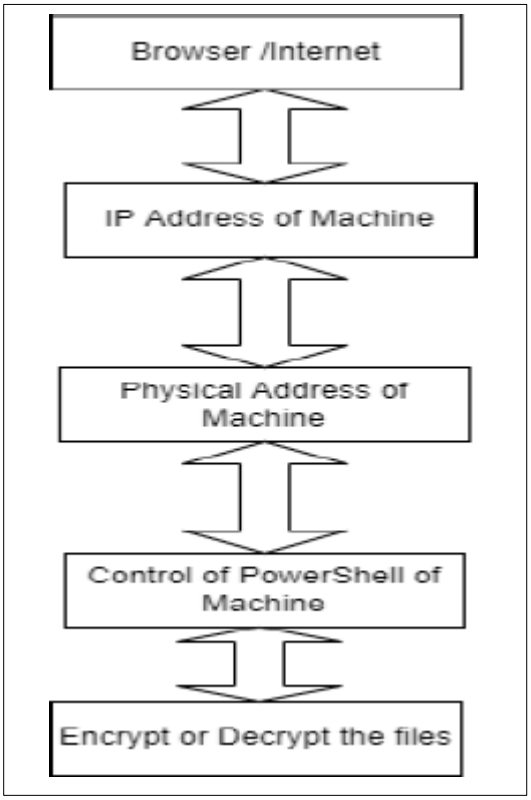

Fig 2: Flow chart of proposed ransomware

The basic code for encrypting the data has been presented in table 1 below.

Table 1: Pseudocode of proposed ransomware

1	If (run):
2	getListOfDrives():
3	return(drive_path)
4	get_all_files_of_pc():
5	dir_path = getListOfDrives()
6	dirs[ ]
7	for dirName, subdirList, fileList in dir_path:
8	for filename_1 in fileList_1:
9	if (filename not ends with ('ransomware extension')):
10	dirs.append(dirName + "\\" + fileName)
11	return(dirs)
12	encrypt_all_files():
13	dirs = get_all_files_of_pc()
14	for file_name in dirs:
15	encrypt_file(file_name)

2.3 Data encryption

The encryption process starts just after initiating communication with the PowerShell on the machine and receiving the IP address, port number, and physical address or Mac address. The programme starts by learning the number, extensions, and formats of all the discs and associated devices that are within the victim's machine and then starts the scanning process. Then, it sent the key to the server of Bulletproof Hosting using a reverse connectionAfter meticulously verifying each and every file, piece of data, and piece of information, proceed to scanning it to the server. The steps are started in case any specific files or data are missing after the scanning process. A step by step approach to data encryption has been in the flow chart shown below in figure 3(a). With that, an algorithm followed by the given progamme of Ransomware for data encryption is also shown in figure 3(b).

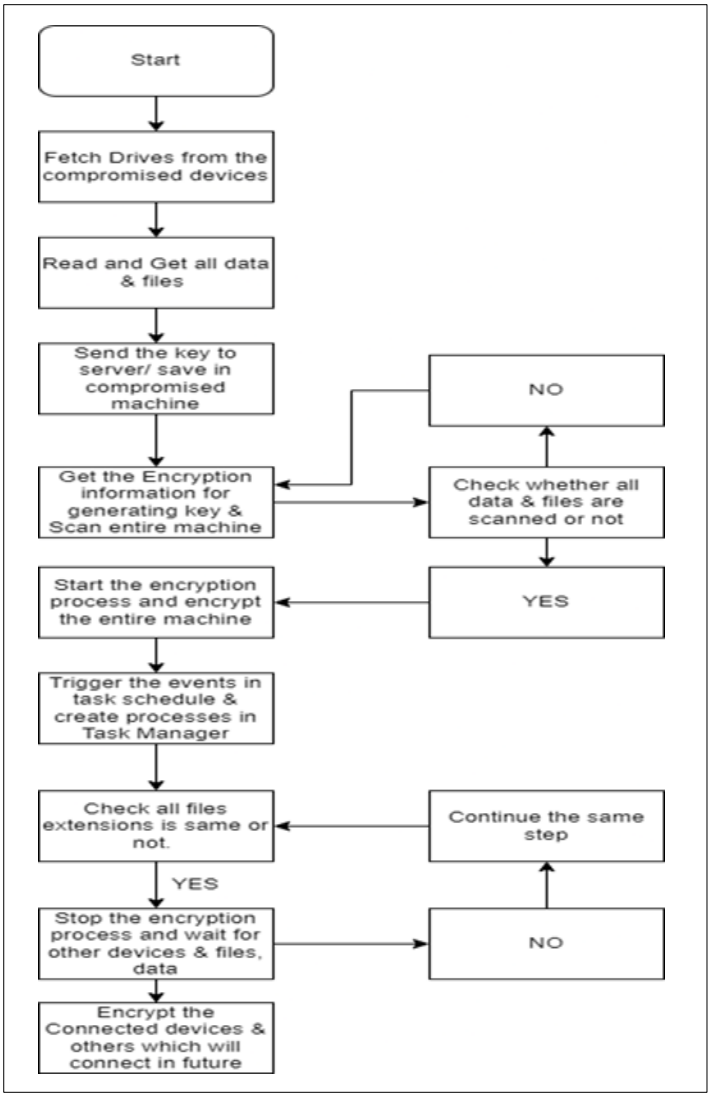

Fig 3: (a)

Table 2: (a) Flow chart of data encryption (b) Algorithm to data encryption

```
Step1: Fetch Drives from the compromised machine
For i in Unwanted_chars :
   For i in range (len(deviceID)):
      if (deviceID[i] == "C") :
      ["User_files = ["\\Pictures","\\Music","\\Documents","\\Downloads","\\Videos"]
      for loc in range(len(C_Drive_User)):
      continue
      else:
      dir_list.append(deviceID[i] +":")
      Step: 2 Get all files
      For j in range(len(dir_list)):
         for dirName, subdirList, fileList in os.walk(dir_path):
         if ( encryption format Is Not find Then encrypt the files)
         Step: 3 Sending key To the server
         def send_key()
         token = "abcdergshajklaxyz";
         chat_id = "2389XX21"
         user_id = os.getenv('Machine_name')
         response = requests.get(res)
         Return response
         Step: 3 Encryption Information For generating key
         key =        " ENCRYPTION_LEVEL = 256 // 8
         char_pool =          ''
         For i in range(0xe, 0xff):
            char_pool += (chr(i))
            try
            With open(file,        'rb') as f:
               data = f.read()
               If key_index >= max_index:
               key_index = 0
               else:
               key_index += 1 os.remove(file)
```

The ransomware begins operating and encrypting the user's data on disks, in folders, and in directories after it has been successfully installed on the victim's computer. In cases where a USB device is connected, ransomware encrypts the data on the USB device too. The unencrypted and encrypted data through the proposed ransomware has been shown in figures 4(a) and (b).

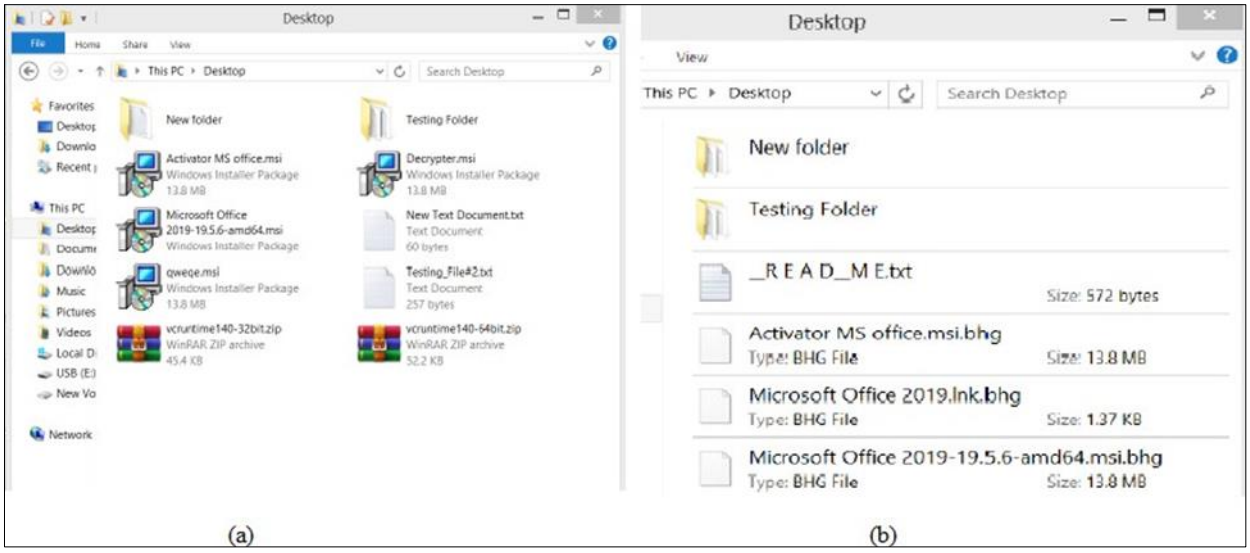

Fig 4: (a) Data before encryption (b) Data after encryption

Figure 3 demonstrates the results of a file conversion with the extension ". bhg through ransomware.
As all folders and files have been modified with the. Bhg extension, as seen in Figure 3, further, unless the victim uses the key that must be generated to decrypt the data, he or she is unable to access any directories, files, or folders. In the next section, the step by step approach to dataset decryption to retrieve the affected data by ransomware has been presented.

2.4 Data decryption

There are certain identical steps in the decryption process, like obtaining documents and information from the infected machine for the symmetric key. It is crucial to realise that in order to obtain a sufficient key from the server during the decryption process, the criminal needs access to all of the machine's data and files. Verify that almost all files, directories, and subdirectories have been closely investigated after regenerating the key. Next, after obtaining the victim's decryption key, the user uses it to start the decryption process. If the ransom is paid, the decryption key is probably sent solely to the user or victim; no decryption key is provided to anybody else. For the present affected data by proposed ransomware, the complete decryption process has been presented in figure 5.

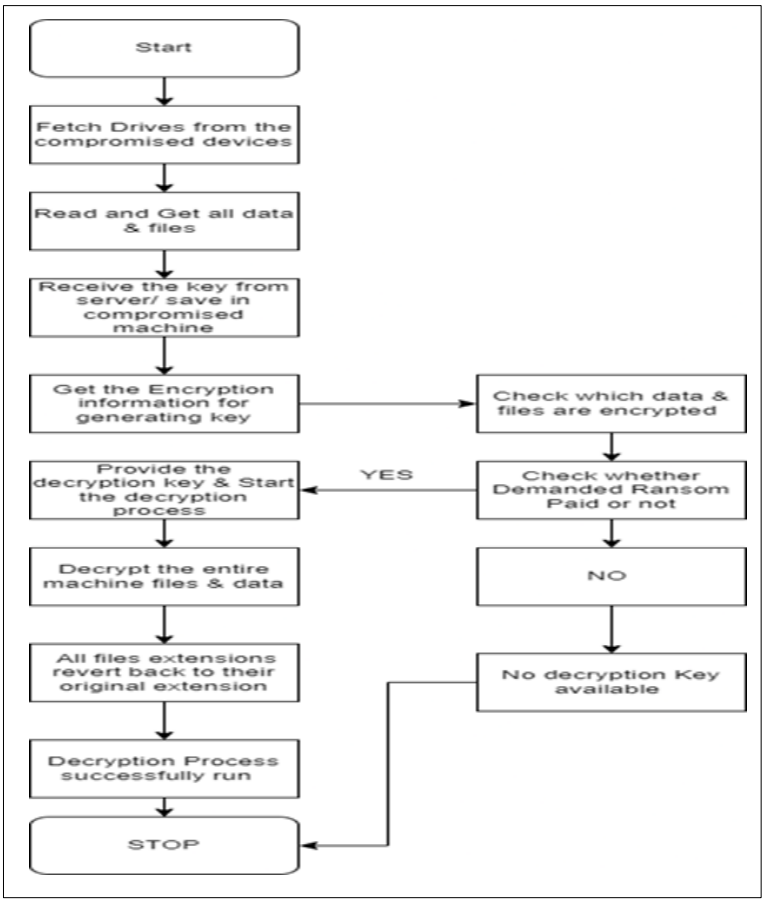

Fig 5: Circuit chart of data decryption

The detailed procedure for data decryption for the data affected by the proposed ransomware is shown in Figure 4. In the processing of data and encryption, the decryption key is found to be a major concern. For obtaining the decryption key to decrypt the data affected by the proposed ansomware, the step-by-step approach is shown in Figure 6.

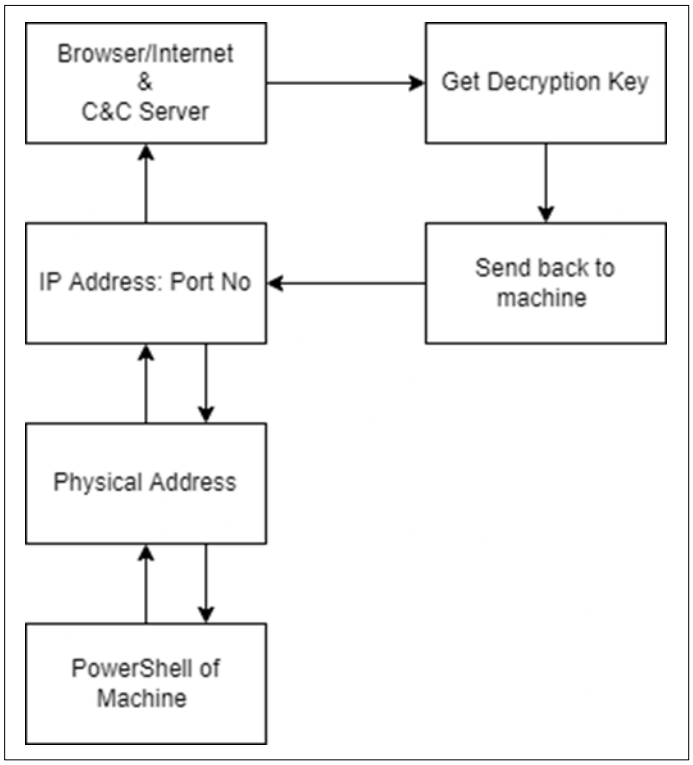

Fig 6: Proposed approach to decryption key generation

3. Results and analysis

The details of the proposed ransomware have been discussed below for its performance testing

3.1 Ransomware's State Report

The author has used the VirusTotal website to check the file's architecture to see if the file contains any harmful code or script. Following scanning, the author discovered that 57 antivirus programmers do not recognize the proposed ransomware, proving that the author has gotten beyond the antivirus mechanism and algorithm. Google Scan was also used to check the application of the proposed ransomware, but it failed to detect its configuration. It shows that the proposed design is effective and meets the needs of art. The generated report for proposed ransomware has been given below.

Table 3: Ransomware's State Report

Antivirus	Detected	Undetected
Ad-Aware	X	✓
ALYac	X	✓
Arcabit	X	✓
Avira (no Cloud)	X	✓
BitDefender	X	✓
Bkav Pro	X	✓
ClamAV	X	✓
Comodo	X	✓
Cyren	X	✓
Emsisoft	X	✓
ESET-NOD32	X	✓
FireEye	X	✓
AhnLab-V3	X	✓
Antiy-AVL	X	✓

3.2 Identification of proposed ransomware

There are various methods that can be applied to identify the proposed ransomware. Some of those methods are given below.

3.2.1 Application & file analysis

Once crypto-ransomware encrypts a file, it changes it. Modifications to a large number of files in a computer's file potentially signal a ransomware assault. To

recognize significant shifts in files, various measures can be utilized for example

3.2.1.1 File Complexity
This metric got a file's unpredictability. In comparison to plaintext data, encoded and compact files have a bigger level of complexity. Hence, determining if a file has been compromised by ransomware may be determined by formulating the file's complexities and compared the outcome to previous analyses for the same file**.**

3.2.1.2 File Format
The file's name or extension possesses its nature. Whenever a ransomware controls the file, it changes its extension.

3.2.1.3 File Variation
In contrast to benign file alterations like adding extra information or altering files and data, the information of a ransomware- encrypted file must be varied from the previous plaintext information. As a result, comparing two copies from the same file can determine whether or not ransomware is there.

3.3 Use of virustotal
To detect viruses and malware, using the virustotal web application is very fruitful. This helps the user know the legitimate behaviour of the file or application. Just drag and drop the file on the web interface of VirusTotal, and the user gets complete information about that file before installing any application; check the application's behaviour first, then install it on the machine. VirusTotal examines items using over 70 antivirus analyzers, Web address blocklisting providers, and various methods to identify information from the information under investigation. Any client can use their internet connection to choose a document from their PC and transmit it to VirusTotal. The leading public online portal, workstation uploaders, plug-ins, and a programming API are all options for submitting documents to VirusTotal. The WebClient has the greatest scanning priority among the freely released submission options. The Saas public API allows inputs to be programmed in any machine code.

3.4 Analysis of the readme.txt file
A ransom message in common left unaltered in case ransom ware assault occurs. This alarm could be recorded as a text document in the remote browser or presented. This letter tells the individual that his data is encoded, or unavailable when has been affected by the locker ransomware, and introduce them with the procedure about to pay and recover it. The ransomware's properties notes can be identified using static as well as dynamic analysis. Ransomware usually reflects a ransom note on the victim's machine to acquire payment. To determine if a ransomware attack is underway, various investigators employed static and dynamic monitoring to confirm the existence of such a note.

3.5 Fetch the analysis information from the system
Cuckoo Sandbox and Anubis can be used to assess all versions. After the analysis, the records and flow files were thoroughly examined, and the critical data was recorded. We discovered that the ransomware module tries to install itself in the device by causing significant alterations. File system operations, registry activity, and network communications all show these changes.

4. Avoidance of proposed ransomware
In order to avoid the effects of the proposed ransomware, some easy steps to implement in case the victim does not have a technical background have been presented below. These steps stop the encryption process as well as make sure that no more damage or infection occurs.

4.1 User Awareness
It doesn't matter how many prevention and safety tools any organisation or individual has taken, the first thing that can prevent the attack is the user's awareness of where to click, what to open or not to open, and where to download. Most of the time, it's all about the awareness that "machines are not vulnerable; humans are," so that's why you should be careful before doing anything and think twice before clicking on any link.

4.2 Temp folder files
When the ransomware starts the encryption process, some files are saved into the temp folder, which is mainly used to encrypt the data and files quickly. So, in that case, if the user wants to take some action, then the user can open the temp folder using the command in the Run window (Windows + R), then type (%tmp%) or (%Temp%) in the run and press enter. The window pops out of the temp folder, which then deletes the files and folder permanently or by forcing a format. Some files and folders are not formatted because they are in use by some process or service and they denied to format, so to delete those files and folders, check which exceptional service or process is running in the background of the machine and forcefully stop that service orprocess, and then delete the remaining files and folders. This helps users prevent ransomware from infecting more devices and data.

4.3 Startup folder files
The startup folder is also the prime target of perpetrators, where they can set their code or script to run whenever the victim's machine powers on or restarts. The increased number of restartsand power occur when the ransomware restarts its code and executes faster and more efficiently. So, in that case, the user can go to their startup folder using the command in

the run, i.e., "shell: startup). After applying this command in the run terminal, the Startup window appears, and the victim' has to delete the startup files that the user does not recognize. This also helps victims when their machines are compromised.

4.4 Task manager services & process

Task Manager is essential in every panic situation created by the perpetrator because the user can check all the services and processes and determine which are legitimate. Victims can stop those unusual activities and improve their machine's performance by checking the processes and services. Just find and stop the unwanted services and processes; this helps protect yourself from further infection and damage.

4.5 Task scheduler triggered events

Task Scheduler plays the prime role when the ransomware is infecting the data repeatedly. That is happening because ransomware creates an event in the task scheduler and triggers that event at a particular time, which automatically starts every day without permission from the victim or admin. That's why ransomware always infects the files, data, or devices connected to them. So,in that case, victims have to check which event is triggered automatically first, then find out which process is that and delete it from the Task Scheduler, which helps victims secure their dataor machine against further infection and damage.

5. Conclusion

The author of this paper offers disruptive ransomware that can be covertly deployed while evading detection by Windows Defender, the Firewall, and Antivirus. This ransomware is innovative in its impersonation method to become a threat. It is also exceptional in that it manages information well. The detailed information of action plan, algorithm, encryption, decryption procedure, and validity has been presented in this paper. Other than this, many techniques for identifying and avoiding it are introduced in this article.

6. References

1. Karam C, Kamluk V. Blockchainware-decentralized malware on the blockchain. Black Hat ASIA. 2015.
2. 5 most common types of ransomware: CrowdStrike [Internet]. CrowdStrike. 2023 [cited 2023 Mar 3]. Available from: https://www.crowdstrike.com/cybersecurity-101/ransomware/types-of-ransomware/
3. Kolodenker E, Koch W, Stringhini G, Egele M. Paybreak: Defense against cryptographic ransomware. In: Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security. 2017 Apr; p. 599–611.
4. Gómez-Hernández JA, Álvarez-González L, García-Teodoro P. R-Locker: Thwarting ransomware action through a honeyfile-based approach. Computers & Security. 2018;73:389–98.
5. Giles J. Scareware: the inside story. New Scientist. 2010;205(2753):38–41.
6. Moussaileb R, Navas RE, Cuppens N. Watch out! Doxware on the way…. Journal of Information Security and Applications. 2020;55:102668.
7. Puat HAM, Abd Rahman NA. Ransomware as a service and public awareness. PalArch's Journal of Archaeology of Egypt/Egyptology. 2020;17(7):5277–92.
8. Anghel M, Racautanu A. A note on different types of ransomware attacks. Cryptology ePrint Archive. 2019.