2024 4th International Conference on Intelligent Technologies (CONIT)
Karnataka, India. Jun 21-23, 2024

Windows Forensic Analysis and Detection of Ransomware Attacks Using Event Logs and Tools

Yogeshwar Prajapati
Computer Engineering
Marwadi University
Rajkot, India
yogeshwar.prajapati120001@marwadiuniversity.ac.in

Krupali Gosai
Computer Engineering
Marwadi University
Rajkot, India
krupali.gosai@marwadieducation.edu.in

2024 4th International Conference on Intelligent Technologies (CONIT) | 979-8-3503-4990-0/24/$31.00 ©2024 IEEE | DOI: 10.1109/CONIT61985.2024.10626973

***Abstract*—This paper explores the vital domain of cybersecurity, specifically focusing on the forensic analysis of Windows systems to detect and combat ransomware attacks. Through the meticulous examination of event logs and the utilization of specialized tools, the study presents a comprehensive approach to identifying ransomware incidents, understanding their modes of dissemination, and implementing effective mitigation strategies. By analyzing event logs and employing state-of-the-art forensic tools, the research uncovers the sophisticated tactics employed by ransomware perpetrators and identifies crucial patterns essential for timely detection and response. Furthermore, this study integrates practical insights with theoretical frameworks to provide actionable guidance for cybersecurity professionals, empowering them to strengthen Windows environments against the evolving ransomware threat landscape. Ultimately, this paper contributes to enhancing the resilience of organizations to ransomware attacks, safeguarding critical data and infrastructure against the pervasive menace of cyber threats.**

***Index Terms*—WannaCry Ransomware, Event-logs, Cerber Ransomware, Windows Forensic, HijackThis-Tool**

I. Introduction

Ransomware attacks are quite dangerous for businesses and people alike since they target sensitive information and cause a lot of trouble. In order to combat this growing danger, it is essential to employ Windows forensic methods of analysis in conjunction with the review of event logs to detect and mitigate ransomware assaults. With the use of a variety of specialized tools and the vast amounts of data stored in Windows event logs, forensic investigators may deduce the origin, methods, and effects of ransomware occurrences [1]. Because they record a broad variety of system activities and events in real-time, Windows event logs are an excellent source of forensic evidence. Essential data including as file modifications, process executions, network connections, and user interactions are documented in the logs, providing a full timeline of system activities [2] [3]. By meticulously reviewing these event logs, forensic investigators can identify suspicious patterns, outliers, and indications of malware infection. Researchers can learn more about the attacker's tactics and goals by studying event logs, which also help them reconstruct the sequence of events leading up to and following a ransomware attack [4]. Expert forensic tools enhance the efficiency of ransomware detection and analysis on Windows machines when utilized in conjunction with event log analysis. Memory dumps, disk pictures, and network traffic are just a few examples of the many sources of data that these applications may collect, analyze, and link [5]. Volatility and other memory forensics techniques enable investigators to retrieve crucial evidence from volatile memory. This data may show how ransomware encrypted files, methods for inserting malware, and hidden processes [6] [7]. File system analysis tools like Autopsy and Encase Forensic provide useful details on ransomware-related file deletions, modifications, and encryption operations. Businesses may also lessen the impact of ransomware attacks by implementing proactive monitoring and alerting strategies, which help them spot threats quickly. In order to quickly identify and resolve ransomware issues before they escalate, security teams should employ heuristic analysis techniques and continuously monitor Windows event logs for any unexpected actions [8]. Enterprises may effectively contain, remove, and restore operations following ransomware attacks by implementing thorough incident response policies that are built using important information collected via forensic investigation. This safeguards important assets and keeps the company running smoothly.

II. Literature Review

Recent research indicates that by employing live forensic techniques, it is able to quickly discover the encryption keys for ransomware data in the volatile memory of the compromised machine during the execution of the ransomware. This method is referred to as a side channel attack. This paper presents research on the recovery of ransomware encryption keys that are encrypted using a single key per file. It also explores the extraction of the Salsa20 key from computer memory. Additionally, the paper discusses efforts to replicate the latest cryptographic management systems now in use [9]. The first half of the research will focus on examining various types of ransomware and common methods for recovering data. Furthermore, they propose a revolutionary architecture for the detection and recovery of ransomware, which enables the successful retrieval of data from infected folders. In order to maximize their benefits, they engage in this activity. This study aims to examine the techniques employed for the installation of the well-known WannaCry ransomware on a virtual system running Windows. To retrieve data that has been affected by WannaCry, digital investigations are carried out using the Autopsy tool. This demonstrates the feasibility of the suggested architecture. The suggested methodologies can be utilized to develop efficient algorithms for data recovery from WannaCry and other ransomware variants that exhibit similar behavior [10]. This paper examines numerous aspects of ransomware, including its propagation mechanisms, encryption techniques employed, and preventive measures. The subsequent articles detail a study in which the researchers utilized the RanSim simulator to detect malware in a computer system. This study utilized an exploratory research technique to examine the most recent literature on the issue. This paper provides a comprehensive analysis of emerging ransomware patterns, their corresponding consequences, and effective strategies to prevent or mitigate their impact [11].

The primary function of the ransomware is to encrypt the victim's files using an encryption key, which prevents the victim from accessing the original files unless he obtains the decryption key—which they will not have unless they pay the attacker a ransom. Considering the cryptosystems the ransomware employs in its attack, keys will be used to fulfil the ransomware's primary function of encrypting the victim's files [12]. The research area on ransomware encryption keys will be covered in this review paper by going over the earlier studies conducted by researchers who examined ransomware encryption keys from the perspectives of the ransomware authors, including where they obtain their keys, how they generate them, and how they manage them to keep them secure and away from the victim. In this paper, they present a ransomware classification system that considers attack designs that encrypt or delete files. To determine the severity of a ransomware assault, the method considers both the technical aspects of the attack's design and the overall efficacy of several ways for decrypting the data without paying the ransom [13]. Since the beginning of the COVID-19 epidemic, there has been a significant surge in attacks targeting ransomware. Criminals in the cyber world are continuously inventing new techniques to disseminate ransomware, such as phishing and social engineering. For that reason, this report surveyed recent advances in ransomware detection and prevention, mapped out the challenges, and suggested directions for future study [14]. Furthermore, after analyzing a handful of famous ransomware strains, they created AESthetic, a piece of experimental malware that evaded detection by eight prominent antivirus programs.

III. Methodology

This methodology section focuses on ransomware attack detection and forensic analysis in Windows environment. This methodology seeks to offer an in-depth understanding of ransomware actions and the related artifacts left behind in the system by utilizing event logs and specialized tools. This methodology aims to improve the identification and mitigation of ransomware attacks by methodically reviewing event logs and utilizing state-of-the-art forensic technologies. This approach provides valuable insights that are essential for developing successful incident response and preventive measures.

A. Proposed Work Flow

Fig. 1 represents the each components of ransomware attack and detection.Ransomware attacks target specific vulnerabilities within computer systems. Files are the primary targets of ransomware. By encrypting files like papers, images, and videos, attackers make them inaccessible to users. The encryption procedure scrambles data, rendering it illegible without the attackers' decryption key. This strategy attempts to persuade victims into paying a ransom to recover access to their files.

Registry: The Windows Registry is a key database that stores critical system configurations and information. Ransomware can do additional damage by modifying the registry, affecting system functionality, and making it difficult for users to restore control of their machines. This manipulation increases the attack's complexity and impact. During the attack phase, ransomware uses numerous tools and techniques to achieve its harmful objectives. Ransomware executables (such as WannaCry.exe and Cerber) are specialized instances of ransomware programs that encrypt a victim's files. Once executed, these malicious programs use sophisticated algorithms to encrypt data, thereby locking users off of their files until the ransom is paid. While the picture focuses on WannaCry and Cerber, it is crucial to remember that there are countless more ransomware strains, each with its own distinct characteristics and methods of operation. Ransom Notes (e.g., Read This [Quel].html, Read Me [Ada].txt, @WannaDecrypt.exe, @Please Read Me.txt): These files serve several functions inside the ransomware assault ecology.

Directions: Ransom letters frequently include directions for victims to reportedly decrypt their files. They may also include the attackers' contact information to facilitate communication about ransom payment and decryption.

Extortion Process: Ransom letters often include forceful language, threatening victims with irreversible data loss if they do not comply with the attackers' demands within a set timeframe. This psychological pressure is intended to compel victims to speed the ransom payment process.

Detecting and combating ransomware attacks is possible using available tools and tactics. Tools for identifying ransomware outbreaks include HijackThis Tool, which looks for suspicious entries and hijacked processes. Virus-Total is an online service that allows users to upload suspicious files and compare them to a large database of malware signatures kept by multiple antivirus companies. This collective information improves individual users' detection capacities, providing more comprehensive insights into new risks.

ID Ransomware: This specialist resource helps identify ransomware strains by providing a comprehensive database of ransomware families, as well as samples of ransom letters and file extensions commonly linked with each outbreak.

Forensic Tools: The DumpIt Tool creates forensic photographs of storage devices, providing a detailed snapshot of

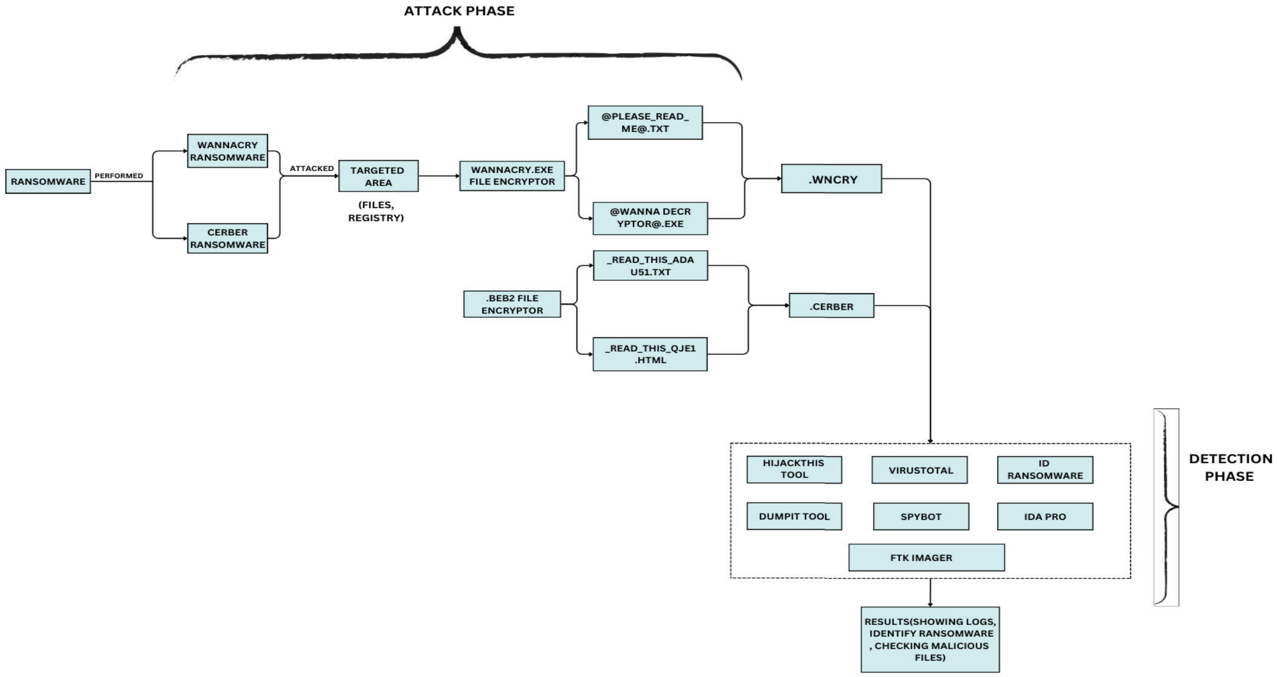


Fig. 1. Proposed Work Flow

their contents at a specified time. Forensic analysis of these photos can show evidence of malware activity, assisting with the investigation and mitigation of ransomware attacks.

FTK Imager: A more powerful forensic imaging tool for experts to collect and analyze digital evidence. FTK Imager has advanced capabilities for inspecting storage devices and detecting indicators of breach caused by ransomware attacks.

Spybot - Search and Destroy is a popular anti-virus software solution that detects and removes a variety of computer threats, including ransomware. Its thorough detection and eradication capabilities protect systems from harmful infiltration.

IDA Pro is an advanced disassembly tool used by security researchers to examine malware code. Analysts can use disassembly to disassemble machine code into a human-readable format, allowing for a better knowledge of how ransomware works and potentially uncovering weaknesses that can be exploited to produce decryption tools. The comprehensive features of IDA Pro enable researchers to uncover the complexities of ransomware assaults, allowing for the development of viable defenses.

B. *Architecture of Proposed Work Flow*

A ransomware forensic investigation is a demanding and complex procedure that requires a systematic way to determining the complexity of an attack. At its core, the inquiry focuses on the detailed collection, analysis, and preservation of digital evidence. The lower portion of the graphic focuses on the earliest stages: collecting ransomware samples from impacted systems, storing them in a secure database for future reference, and doing detailed analysis to understand the ransomware's behavior and features.

Simultaneously, on another side, incident response mechanisms are activated, with the objective of limiting the spread of the attacking, mitigating damage, and returning systems to normal operation. Forensic workstations with specialist tools are critical for conducting forensically sound examinations of digital data. These tools, which are part of the forensic toolbox, provide a variety of functions ranging from disk imaging to memory analysis, assisting in the acquisition and preservation of important evidence. Verification steps in the centre of the diagram verify that the findings are correct, dividing in fact ransomware encryption from technical failures. Investigators examine damaged files, attempting to recover encrypted data whenever possible, while methodically monitoring disk activity and studying system logs for signs of the attack. Quarantined file storage provides a safe refuge for dubious files, limiting their spread, and encrypted storage protects collected evidence. Fig. 2 represent the proposed architecture of detection of ransomware attacks. Overall, the outcome highlights the complex nature of ransomware forensic investigations, demonstrating the need for a complete and cautious approach to navigating these cyber threats. Investigators use meticulous research and rigorous methods to uncover the complex nature of ransomware attacks, identify criminals, and facilitate data recovery, all while protecting the integrity of digital evidence.

IV. Results and Discussion

This section presents our investigation's findings about the use of specialist tools and event logs for forensic analysis and ransomware attack detection in Windows environments. The outcomes are the result of using our methodology, which

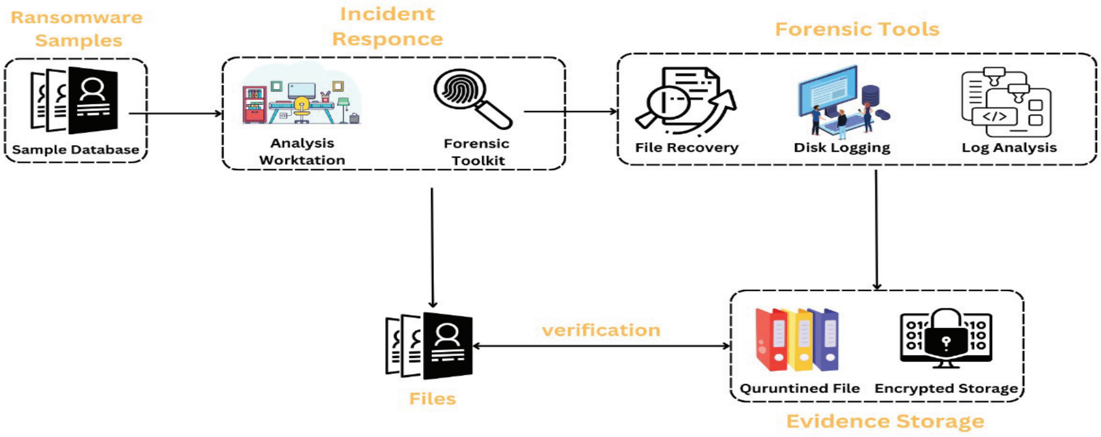
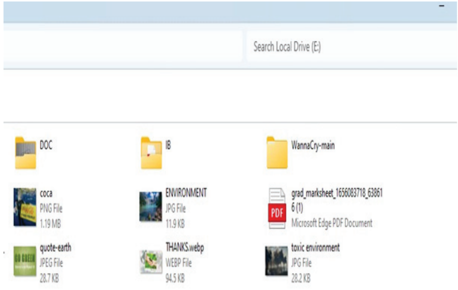


Fig. 2. Proposed Architecture

involves using sophisticated forensic tools and closely examining event logs. By examining gathered information and artifacts, we hope to clarify the traits, trends, and consequences of ransomware activity on Windows systems. The inspection of ransomware attacks on Windows 11 platforms involves an extensive approach involving proactive detection techniques and forensic analysis. In order to determine the ransomware's entry point, propagation vector, and encryption activity, forensic examination involves closely reviewing system logs, file information, and registry entries. Finding important artifacts left behind by the ransomware can be helped by the use of sophisticated forensic tools like IDA Pro and FTK Imager. In addition, putting in place proactive detection mechanisms like behavior-based anomaly detection and intrusion detection systems (IDS) can help in real-time identification of suspicious activity predictive of ransomware behavior, facilitating prompt response and mitigation efforts. The detailed process with its results are discussed further in the subsections below:

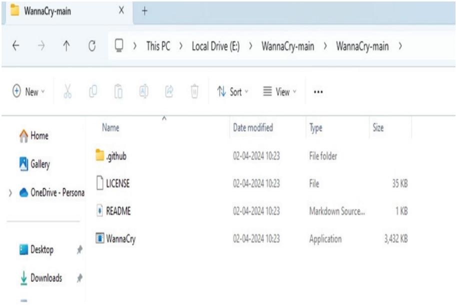
A. Results of Attacking Phase

- **Step : 1** To begin, select the single ransomware file that is depicted in the image below as the target of your investigation. Fig. 3 represents the ransomware samples that were used for the attack.
- **Step : 2** As seen in the Fig. 4 that follows, the ransomware that we use at this site is known by the name WannaCry.
- **Step : 3** At this stage, it is necessary to encrypt all of the data using the WannaCry ransomware, as demonstrated in the Fig. 5 that can be seen below.
- **Step : 4** When we attempted to see any files or folders after the ransomware attack, we were met by a pop-up notification that stated, "Your files have been encrypted." This occurred anytime we attempted to open any files or folders. Fig. 6 represent the same.



DOC
IB
WannaCry-main
coca PNG File 1.19 MB
ENVIRONMENT JPG File 11.9 KB
grad_marksheet_1656083718_638616 (1) Microsoft Edge PDF Document
quote-earth JPEG File 28.7 KB
THANKS.webp WEBP File 94.5 KB
toxic environment JPG File 28.2 KB

Fig. 3. Ransomware sample



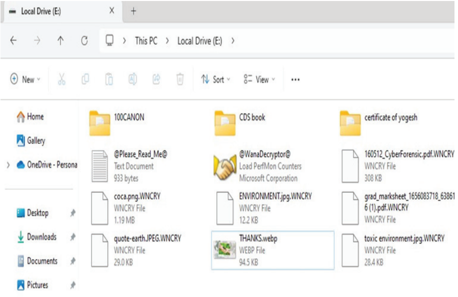
Name	Date modified	Type	Size
.github	02-04-2024 10:23	File folder	
LICENSE	02-04-2024 10:23	File	35 KB
README	02-04-2024 10:23	Markdown Source...	1 KB
WannaCry	02-04-2024 10:23	Application	3,432 KB

Fig. 4. WannaCry Ransomware

- **step : 5** An further ransomware attack, which we will refer to as Cerber is shown in Fig. 7, is being carried out, and based on that attack, we are attempting to analyze and identify all of the activity.

B. Results of Detection Phase

- **Step : 1** In the detection phase, with the assistance of HijackThis Tool, we investigate each and every one of the files and folders to ascertain whether or not they ought to be secured against ransomware attacks which is shown in Fig. 8.



Local Drive (E:)

This PC › Local Drive (E:) ›

New · Sort · View · ···

100CANON

CDS book

certificate of yogesh

@Please_Read_Me@ — Text Document — 933 bytes

@WanaDecryptor@ — Load PerfMon Counters — Microsoft Corporation

160512_CyberForensic.pdf.WNCRY — WNCRY File — 308 KB

coca.png.WNCRY — WNCRY File — 1.19 MB

ENVIRONMENT.jpg.WNCRY — WNCRY File — 12.2 KB

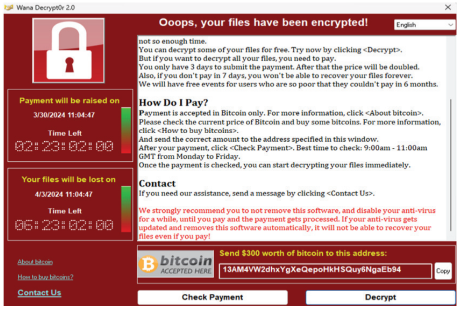
grad_marksheet_1656083718_63861 6 (1).pdf.WNCRY — WNCRY File

quote-earth.JPEG.WNCRY — WNCRY File — 29.0 KB

THANKS.webp — WEBP File — 94.5 KB

toxic environment.jpg.WNCRY — WNCRY File — 28.4 KB

Fig. 5. Encrypted files



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.
Once the payment is checked, you can start decrypting your files immediately.

Contact
If you need our assistance, send a message by clicking <Contact Us>.

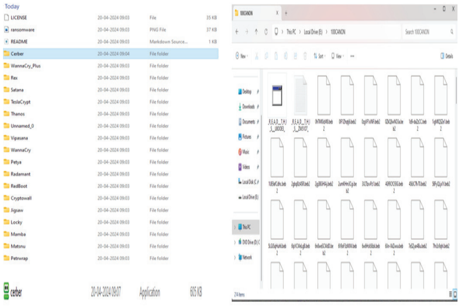
We strongly recommend you to not remove this software, and disable your anti-virus for a while, until you pay and the payment gets processed. If your anti-virus gets updated and removes this software automatically, it will not be able to recover your files even if you pay!

Payment will be raised on
3/30/2024 11:04:47
Time Left
02:23:02:00

Your files will be lost on
4/3/2024 11:04:47
Time Left
06:23:02:00

Send $300 worth of bitcoin to this address:
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

Fig. 6. Popup Window Generated



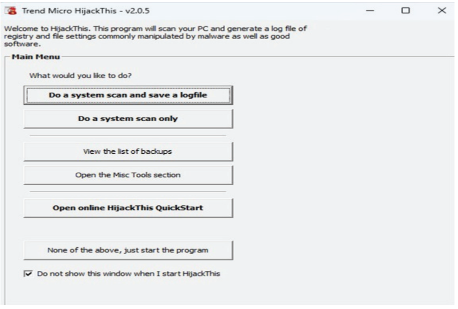
```
Today
LICENSE          20-04-2024 09:03   File                35 KB
ransomware       20-04-2024 09:03   PNG File            37 KB
README           20-04-2024 09:03   Markdown Source...   1 KB
Cerber           20-04-2024 09:04   File folder
WannaCry_Plus    20-04-2024 09:03   File folder
Rex              20-04-2024 09:03   File folder
Satana           20-04-2024 09:03   File folder
TeslaCrypt       20-04-2024 09:03   File folder
Thanos           20-04-2024 09:03   File folder
Unnamed_0        20-04-2024 09:03   File folder
Vipasana         20-04-2024 09:03   File folder
WannaCry         20-04-2024 09:03   File folder
Petya            20-04-2024 09:03   File folder
Radamant         20-04-2024 09:03   File folder
RedBoot          20-04-2024 09:03   File folder
Cryptowall       20-04-2024 09:03   File folder
Jigsaw           20-04-2024 09:03   File folder
Locky            20-04-2024 09:03   File folder
Mamba            20-04-2024 09:03   File folder
Matsnu           20-04-2024 09:03   File folder
Petrwrap         20-04-2024 09:03   File folder

cerber           20-04-2024 09:07   Application        605 KB
```

100CANON

This PC › Local Drive (E:) › 100CANON

Fig. 7. Cerber



Trend Micro HijackThis - v2.0.5

Welcome to HijackThis. This program will scan your PC and generate a log file of registry and file settings commonly manipulated by malware as well as good software.

Main Menu

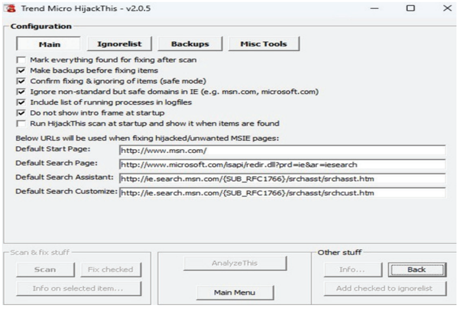
What would you like to do?

Do a system scan and save a logfile
Do a system scan only
View the list of backups
Open the Misc Tools section
Open online HijackThis QuickStart
None of the above, just start the program

☑ Do not show this window when I start HijackThis

Fig. 8. HijackThis Tool

- **step : 2** For the goal of conducting an analysis against ransomware, we have inspected each and every folder and disk, as seen in the Fig. 9 that can be found below.
- **step : 3** After the ransomware attack, in this step we are scanning the system and generating the malicious log files which is shown in the Fig. 10.



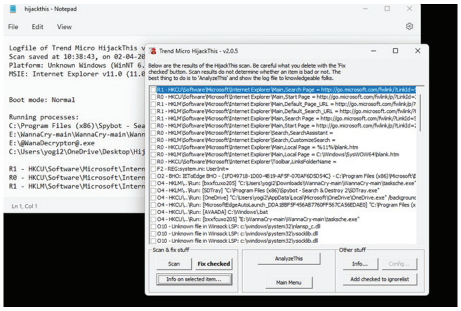
Trend Micro HijackThis - v2.0.5

Configuration

☐ Mark everything found for fixing after scan
☑ Make backups before fixing items
☑ Confirm fixing & ignoring of items (safe mode)
☑ Ignore non-standard but safe domains in IE (e.g. msn.com, microsoft.com)
☑ Include list of running processes in logfiles
☑ Do not show intro frame at startup
☐ Run HijackThis scan at startup and show it when items are found

Below URLs will be used when fixing hijacked/unwanted MSIE pages:
Default Start Page: http://www.msn.com/
Default Search Page: http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=iesearch
Default Search Assistant: http://ie.search.msn.com/{SUB_RFC1766}/srchasst/srchasst.htm
Default Search Customize: http://ie.search.msn.com/{SUB_RFC1766}/srchasst/srchcust.htm

Fig. 9. Configuration of HijackThis tool



hijackthis - Notepad

```
Logfile of Trend Micro HijackThis v
Scan saved at 10:38:43, on 02-04-20
Platform: Unknown Windows (WinNT 6.
MSIE: Internet Explorer v11.0 (11.0


Boot mode: Normal

Running processes:
C:\Program Files (x86)\Spybot - Sea
E:\WannaCry-main\WannaCry-main\Wann
E:\@WanaDecryptor@.exe
C:\Users\yogi2\OneDrive\Desktop\Hij

R1 - HKCU\Software\Microsoft\Intern
R0 - HKCU\Software\Microsoft\Intern
R1 - HKLM\Software\Microsoft\Intern
```

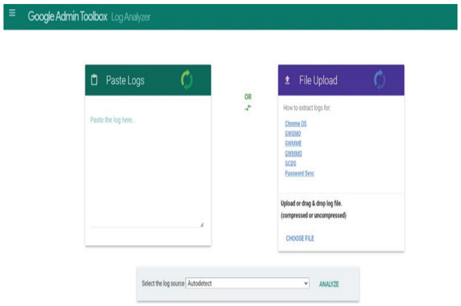
Trend Micro HijackThis - v2.0.5

Below are the results of the HijackThis scan. Be careful what you delete with the 'Fix checked' button. Scan results do not determine whether an item is bad or not. The best thing to do is to 'AnalyzeThis' and show the log file to knowledgeable folks.

```
R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Page = http://go.microsoft.com/fwlink/?LinkId=
R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Start Page = http://go.microsoft.com/fwlink/p/?LinkId=
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Page_URL = http://go.microsoft.com/fwlink/p/?
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Search_URL = http://go.microsoft.com/fwlink/?
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Search Page = http://go.microsoft.com/fwlink/?LinkId=
R0 - HKLM\Software\Microsoft\Internet Explorer\Main,Start Page = http://go.microsoft.com/fwlink/p/?LinkId=
R0 - HKLM\Software\Microsoft\Internet Explorer\Search,SearchAssistant =
R0 - HKLM\Software\Microsoft\Internet Explorer\Search,CustomizeSearch =
R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Local Page = %11%\blank.htm
R0 - HKLM\Software\Microsoft\Internet Explorer\Main,Local Page = C:\Windows\SysWOW64\blank.htm
R0 - HKCU\Software\Microsoft\Internet Explorer\Toolbar,LinksFolderName =
F2 - REG:system.ini: UserInit=
O2 - BHO: IEToEdge BHO - {1FD49718-1D00-4B19-AF5F-070AF6D5D54C} - C:\Program Files (x86)\Microsoft\E
O4 - HKLM\..\Run: [bxxfcuxo205] "C:\Users\yogi2\Downloads\WannaCry-main\WannaCry-main\tasksche.exe"
O4 - HKLM\..\Run: [SDTray] "C:\Program Files (x86)\Spybot - Search & Destroy 2\SDTray.exe"
O4 - HKCU\..\Run: [OneDrive] "C:\Users\yogi2\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /backgroun
O4 - HKCU\..\Run: [MicrosoftEdgeAutoLaunch_DDA1BBF5F456AB7760FF567CA56EDAE0] "C:\Program Files (x
O4 - HKCU\..\Run: [AVAADA] C:\Windows\.bat
O4 - HKCU\..\Run: [bxxfcuxo205] "E:\WannaCry-main\WannaCry-main\tasksche.exe"
O10 - Unknown file in Winsock LSP: c:\windows\system32\nlansp_c.dll
O10 - Unknown file in Winsock LSP: c:\windows\system32\vsocklib.dll
O10 - Unknown file in Winsock LSP: c:\windows\system32\vsocklib.dll
```

Fig. 10. Log analysis using HijackThis Tool

- **step : 4** Additionally, to perform an analysis of all the logs, we make use of a second tool called Google Admin Toolbox Log Analyzer which is shown in Fig. 11. This program is used for the goal of acquiring all of the logs from the system.



Google Admin Toolbox Log Analyzer

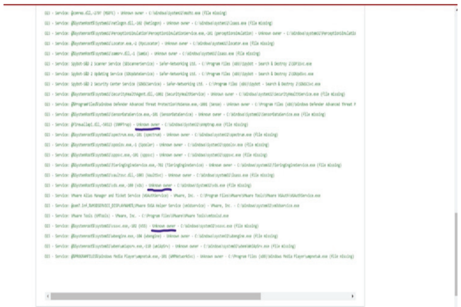
Select the log source: Autodetect

Fig. 11. Google analyzer tool for analysing log

- **step : 5** From this point forward, we have been able to identify all of the Logs, and within those Logs, we have recognized some of the malicious conduct that is indicated by blue underlines which is shown in Fig. 12. This has helped us to identifying malicious content.

V. Future Work

In the future, studies should focus on exploring how to make use of emerging technologies, such as artificial intelligence (AI) and machine learning (ML), into Windows forensic analysis. This mixture aims to improve the detection and mitigation of ransomware. These technologies have demonstrated potential in diverse cybersecurity applications and could be



```
O23 - Service: @comres.dll,-2797 (MSDTC) - Unknown owner - C:\Windows\System32\msdtc.exe (file missing)
O23 - Service: @%SystemRoot%\system32\netlogon.dll,-102 (Netlogon) - Unknown owner - C:\Windows\system32\lsass.exe (file missing)
O23 - Service: @%systemroot%\system32\PerceptionSimulation\PerceptionSimulationService.exe,-101 (perceptionsimulation) - Unknown owner - C:\Windows\system32\PerceptionSimulatio
O23 - Service: @%systemroot%\system32\Locator.exe,-2 (RpcLocator) - Unknown owner - C:\Windows\system32\locator.exe (file missing)
O23 - Service: @%SystemRoot%\system32\samsrv.dll,-1 (SamSs) - Unknown owner - C:\Windows\system32\lsass.exe (file missing)
O23 - Service: Spybot-S&D 2 Scanner Service (SDScannerService) - Safer-Networking Ltd. - C:\Program Files (x86)\Spybot - Search & Destroy 2\SDFSSvc.exe
O23 - Service: Spybot-S&D 2 Updating Service (SDUpdateService) - Safer-Networking Ltd. - C:\Program Files (x86)\Spybot - Search & Destroy 2\SDUpdSvc.exe
O23 - Service: Spybot-S&D 2 Security Center Service (SDWSCService) - Safer-Networking Ltd. - C:\Program Files (x86)\Spybot - Search & Destroy 2\SDWSCSvc.exe
O23 - Service: @%systemroot%\system32\SecurityHealthAgent.dll,-1002 (SecurityHealthService) - Unknown owner - C:\Windows\system32\SecurityHealthService.exe (file missing)
O23 - Service: @%ProgramFiles%\Windows Defender Advanced Threat Protection\MsSense.exe,-1001 (Sense) - Unknown owner - C:\Program Files (x86)\Windows Defender Advanced Threat P
O23 - Service: @%SystemRoot%\system32\SensorDataService.exe,-101 (SensorDataService) - Unknown owner - C:\Windows\System32\SensorDataService.exe (file missing)
O23 - Service: @FirewallAPI.dll,-50323 (SNMPTrap) - Unknown owner - C:\Windows\System32\snmptrap.exe (file missing)
O23 - Service: @%systemroot%\system32\spectrum.exe,-101 (spectrum) - Unknown owner - C:\Windows\system32\spectrum.exe (file missing)
O23 - Service: @%systemroot%\system32\spoolsv.exe,-1 (Spooler) - Unknown owner - C:\Windows\System32\spoolsv.exe (file missing)
O23 - Service: @%SystemRoot%\system32\sppsvc.exe,-101 (sppsvc) - Unknown owner - C:\Windows\system32\sppsvc.exe (file missing)
O23 - Service: @%SystemRoot%\system32\TieringEngineService.exe,-702 (TieringEngineService) - Unknown owner - C:\Windows\system32\TieringEngineService.exe (file missing)
O23 - Service: @%SystemRoot%\system32\vaultsvc.dll,-1003 (VaultSvc) - Unknown owner - C:\Windows\system32\lsass.exe (file missing)
O23 - Service: @%SystemRoot%\system32\vds.exe,-100 (vds) - Unknown owner - C:\Windows\System32\vds.exe (file missing)
O23 - Service: VMware Alias Manager and Ticket Service (VGAuthService) - VMware, Inc. - C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe
O23 - Service: @oem7.inf,%VM3DSERVICE_DISPLAYNAME%;VMware SVGA Helper Service (vm3dservice) - VMware, Inc. - C:\Windows\system32\vm3dservice.exe
O23 - Service: VMware Tools (VMTools) - VMware, Inc. - C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
O23 - Service: @%systemroot%\system32\vssvc.exe,-102 (VSS) - Unknown owner - C:\Windows\system32\vssvc.exe (file missing)
O23 - Service: @%systemroot%\system32\wbengine.exe,-104 (wbengine) - Unknown owner - C:\Windows\system32\wbengine.exe (file missing)
O23 - Service: @%Systemroot%\system32\wbem\wmiapsrv.exe,-110 (wmiApSrv) - Unknown owner - C:\Windows\system32\wbem\WmiApSrv.exe (file missing)
O23 - Service: @%PROGRAMFILES%\Windows Media Player\wmpnetwk.exe,-101 (WMPNetworkSvc) - Unknown owner - C:\Program Files (x86)\Windows Media Player\wmpnetwk.exe (file missing)
```

Fig. 12. Malicious File Detected

utilized to automate the analysis of event logs and the detection of ransomware tendencies. Through the utilization of extensive datasets containing labelled event log data, researchers have the potential to enhance the precision and effectiveness of machine learning models. This, in turn, enables the development of algorithms that can promptly identify ransomware behavior in real-time. In addition, AI-powered methods could facilitate proactive threat detection by constantly monitoring system behavior for unusual patterns that may indicate the presence of ransomware. This would decrease the need for manual intervention and enhance the overall effectiveness of detecting such threats. Moreover, it is necessary to investigate innovative methods for addressing and recovering from ransomware incidents specifically in Windows environments. Although detection is important, organizations must also establish strong procedures for containing and minimizing the consequences of ransomware attacks once they happen. Future research could concentrate on creating automatic reaction mechanisms that utilize event log data to detect and separate affected systems, so halting the propagation of ransomware throughout the network. Furthermore, researchers could explore novel methods for recovering from ransomware, such as utilizing backup solutions and data replication techniques to restore compromised files and systems to their original state before the attack. By focusing on these specific elements of ransomware incident response, future efforts can help improve the robustness of Windows systems against ransomware threats and reduce the consequences of attacks on enterprises.

VI. Conclusion

In conclusion, the combination of Windows forensic investigation, event log study, and specialist tools provides a strong defense against ransomware attacks. Forensic analysts can uncover significant evidence of ransomware activity by carefully examining event logs. This evidence may include illegal changes to files, strange execution of processes, and abnormal network connections. By providing a thorough understanding, enterprises can implement proactive detection systems that promptly notify security personnel of possible dangers as they occur. In addition, the use of sophisticated forensic technologies simplifies the analysis procedure, enabling quick identification and response to ransomware occurrences. Utilizing event logs as the main source of data also allows for the reconstruction of attack timings, which helps in comprehending attack pathways and guiding decision-making in incident response. It is crucial to continuously investigate and modify forensic techniques and tools in order to remain ahead of the ever-changing ransomware attacks. Organizations may enhance their cybersecurity by using a multi-modal strategy to detect and analyze ransomware. This will help protect important assets and maintain operational continuity in the face of evolving threats.

References

[1] A. El-Kosairy and M. A. Azer, “Intrusion and ransomware detection system,” in *2018 1st international conference on computer applications & information security (ICCAIS)*. IEEE, 2018, pp. 1–7.

[2] A. Ren, C. Liang, I. Hyug, S. Broh, and N. Jhanjhi, “A three-level ransomware detection and prevention mechanism,” *EAI Endorsed Transactions on Energy Web*, vol. 7, no. 26, 2020.

[3] M. M. Khan, M. F. Hyder, S. M. Khan, J. Arshad, and M. M. Khan, “Ransomware prevention using moving target defense based approach,” *Concurrency and Computation: Practice and Experience*, vol. 35, no. 7, p. e7592, 2023.

[4] R. Moussaileb, N. Cuppens, J.-L. Lanet, and H. L. Bouder, “A survey on windows-based ransomware taxonomy and detection mechanisms,” *ACM Computing Surveys (CSUR)*, vol. 54, no. 6, pp. 1–36, 2021.

[5] X. Ling, L. Wu, J. Zhang, Z. Qu, W. Deng, X. Chen, Y. Qian, C. Wu, S. Ji, T. Luo *et al.*, “Adversarial attacks against windows pe malware detection: A survey of the state-of-the-art,” *Computers & Security*, vol. 128, p. 103134, 2023.

[6] S. Karanam, “Ransomware detection using windows api calls and machine learning,” Ph.D. dissertation, Virginia Tech, 2023.

[7] Q. Kang and Y. Gu, “Enhancing ransomware detection: A windows api min max relevance refinement approach,” 2023.

[8] J. A. Herrera-Silva and M. Hernández-Álvarez, “Dynamic feature dataset for ransomware detection using machine learning algorithms,” *Sensors*, vol. 23, no. 3, p. 1053, 2023.

[9] L. F. de Loaysa Babiano, R. Macfarlane, and S. R. Davies, “Evaluation of live forensic techniques, towards salsa20-based cryptographic ransomware mitigation,” *Forensic Science International: Digital Investigation*, vol. 46, p. 301572, 2023.

[10] S. C. Nayak, V. Tiwari, and B. K. Samanthula, “Review of ransomware attacks and a data recovery framework using autopsy digital forensics platform,” in *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE, 2023, pp. 0605–0611.

[11] M. I. Sarwar, L. A. Maghrabi, K. Nisar, and I. Khan, “Cryptovirology ransomware: A review of dissemination and mitigation techniques,” *Inf. Sci. Lett*, vol. 12, no. 11, pp. 2277–2288, 2023.

[12] M. A. Aboud and K. Mariyappn, “Investigation of modern ransomware key generation methods: A review,” in *2021 International Conference on Computer Communication and Informatics (ICCCI)*. IEEE, 2021, pp. 1–5.

[13] A. Zimba, M. Chishimba, and S. Chihana, “A ransomware classification framework based on file-deletion and file-encryption attack structures,” *arXiv preprint arXiv:2102.10632*, 2021.

[14] C. Beaman, A. Barkworth, T. D. Akande, S. Hakak, and M. K. Khan, “Ransomware: Recent advances, analysis, challenges and future research directions,” *Computers & security*, vol. 111, p. 102490, 2021.