**Dynamic Analysis of Blackcat Ransomware using C2 framework for Malware Detection**

Shubhankar Hazra1, Geetanjali Surange1, Pallavi Khatri1

ITM University, Gwalior

**ABSTRACT**

In the composition that follows, it shows how to achieve malware dissection on a special ransomware infection called BlackCat, utilizing colourful open- source tools to examine the source law and identify pointers of concession (IOCs). It identifies the parameters that are being utilised for the functionality to introduce a trojan contagion or produce a backdoor to transmit the malware and compromise the fatality’s computer. The composition discusses the tools exercised to detect the lines through UAC bypass, IDS disabling, director access utilizing a C2 frame. Rear engineering was substantially exercised to anatomize the BlackCat Ransomware.

The purpose of serving dissection of this personal ransomware is to community the entire society about its evading parcels, disparate characters, lacings, IOCs, and all the double coequals. All these together will be rollicking an important part in mollifying the malware and escaping it into the discovery frame and bone should be suitable to duly detect the entry points, access points, UAC bypasses, admin access, and one should be suitable to all of these by actuating the malware in a further prescribed manner and it will be ready for the community to understand and they will try to get further out of any personal ransomware or the malware blood.

**Keywords: -** Malware analysis, C2 framework, Angler Exploit Kit, Ransomware, Havoc framework, Rust programming.

1. **INTRODUCTION**

**#Malware:-**

Any type of malware classified as ransomware aims to have users pay a ransom in exchange for full access to their machine. As mentioned earlier, there are two primary kinds of ransomware, namely the crypto locker and ones. In the first instance, the ransomware's objective is to lock by utilising either basic or sophisticated procedures, prevent the user from regaining access to the user's machine. After that, they usually present a message the display to request payment. Access is provided once more, only in the event the user pays the ransom**[1].** BlackCat is a Ransomware of type RaaS (Ransomware as a Service), which affects the system via the command line as it is an windows malware being deployed to abuse the victims and extort money. It is very similar to the previous ransomware like hive, blackbasta and many other ransomwares that had been used in past to extort money from the victims after they are being affected by the malware **[2][3].**

**The following are the indicators of (IOCs) of Exmatter malware in general:**

|  |  |
| --- | --- |
| **Name of files** | **MD5 Hashes** |
| Amd-Copy.ps1 | 82db4c04f5dcda3bfcd75357adf98228 |
| Ipscan.ps1 | 861738dd15eb7fb50568f0e39a69e107 |
| Run1.ps1 | 79fea7f741760ea21ff655137af05bd0 |

**Table-1 PowerShell common filenames**

|  |
| --- |
| **Additional Filenames** |
| [#].ps1 |
| Mim.ps1 |
| Systems.ps1 |

|  |  |
| --- | --- |
| **Name of files** | **MD5 Hashes** |
| http\_64.exe | |  | | --- | | 82db4c04f5dcda3bfcd75357adf98228 | |  | |
| Spider.dll | 861738dd15eb7fb50568f0e39a69e107 |
| Powershell.dll | 79fea7f741760ea21ff655137af05bd0 |
| Recpdump.exe | 615131e320b8f07e4b4bbb01d57a8eee |

**Table-2 Exe and dlls common filenames**

**1.1Common IOCs used in malware**

Unusual Network Outbound Traffic

IT teams utilize traffic exiting the network as a signal to identify possible problems. whether outbound traffic patterns appear to be strange, the IT team can keep a careful eye on them to see whether anything is wrong. Because this traffic originates within the network, it is frequently the easiest to monitor, and if action is taken immediately, it can be used to block a variety of threats.

Privileged User Account Activity Abnormalities   
Privileged user accounts frequently have access to sensitive or unique areas of the network or applications. As a result, recognizing irregularities can help IT professionals discover an attack early on, potentially before it causes severe damage.

#**Ransomware:-**

According to the FBI's FLASH alert, BlackCat, also known as "**ALPHV**" ransomware, gains access to a target system through stolen user credentials. It uses this access to compromise Active Directory user and administrator accounts. The malware may now configure malicious Group Policy Objects (GPOs) using the Windows Task Scheduler to spread its ransomware payload. To exfiltrate data before execution, BlackCat first disables security features on the victim's network. Following that, it uses multiple batch and PowerShell scripts to carry out the infection. There are two of these: "drag-and-drop-target.bat" and "est.bat," which run the ransomware executable for the MySQL Server, and "est.bat," which replicates the ransomware across several sites**[2].**

* 1. **TTPs used in most ransomware families**

|  |
| --- |
| **Blackcat Ransomware SHA256 Hashes:** |
| 72f0981f18b969db2781e874d249d8003c07f99786e217f84cf54a148de259cc (exe) |
| 69417ec104c1dd07e5067110d6e7f3c643c534d14db65a704bc0c14c223c3001 (elf) |
| 8ee191b51b853addc862307c8f641bd251a8b7dd88263d228453bb06882f2464 (dll) |

**Table-5 Blackcat ransomware hashes**

**1.3. Common Strings used (Ransomware)**

* **Methods of Analysis of a ransomware and malware: -**

1. **Method 1**

The analysis of ransomware and malware from the above findings can be concluded that we can perform the analysis via using the debugging tools or we can even try to do the analysis of the malware by deploying our own piece of code and then try to do the live analysis of the malware and ransomware families using honeypots or even debarring different terms of the analysis and make the analysis phase to run more smoothly.

1. **Method 2**

The next method of analysis done here can be done in accordance with the ransomware where all the infected vectors are taken into consideration and we must take the most redundant phase in which the initial access is gained easily and we would be able to get the most out of the analyzed malware or ransomware. We were able to find the common TTPS, strings, IOCs and the Yara rules that can be easily generated using these phases of ransomware analysis which will further help us in doing in depth analysis of the host machines or the whole system easily.

**2) Literature Survey**

This paper **[1]** investigated victims' decision-making processes during ransomware attacks. Fourth-one ransomware assaults were analysed using qualitative data acquired from organisations and police officers in the United Kingdom's cybercrime sections. In this work, the hypothesis is investigated that victims should thoroughly consider the scenario before deciding whether to pay a ransom. To be honest, not all patients who used the treatment options healed rapidly. Healthier has come under criticism. Twice in the previous few of months. Inadequate patching and anti-virus (AV) software allowed ransomware to infect hundreds of machines. Despite their lack of preparation, many organisations were fortunate. Because ransomware encrypts previously unencrypted data, the business continuity of Lawful (i.e., criminal evidence) is critical. Private enterprises must keep in mind that ransomware assaults are often much more costly It will be difficult for those in the public sector, with bankruptcy a distinct possibility. An extraordinary onslaught was launched against the educational institution Educes. Ransomware interrupted the network of hundreds of thousands of computers, encrypting massive amounts of data, including research data and findings. Data protection authorities determined that fear of incrimination is a major factor in the decision to pay a ransom. Dimmed refused to pay for fear of being victimised again. The victim was a little start-up company, and if they paid it, they would be obliged to take out a loan due to a lack of finances. Reduced ransomware criminality has emerged as a top concern for governments and businesses worldwide. There are numerous, according to the research Reasons why targeted firms may choose to pay a ransom even if they have backups. The following paper **[2]** describes Ransomware attacks, which have escalated in recent years all around the world. These attacks aim to lock victims' computers or encrypt their data in exchange for a ransom. These ransomware types differ in their implementation and approaches, beginning with how they spread, the vulnerabilities they exploit, ways for hiding their activity from antivirus software, encryption algorithms, and performance. Conti ransomware is a complex ransomware that provides ransomware-as-a-service. The researcher starts by setting up a separate test environment. . To begin, the researcher launches VirtualBox and runs a virtual version of Microsoft Windows 10. Then we install the 512 analysis tools, which include Studio and Process Explorer Monitor, Wireshark, 513, and x64dbg. The researcher begins by installing the Conti ransomware on a fresh Windows 10 computer that has not received any system or 544 Windows Defender updates. Windows Defender discovers the 545 attacks after the ransomware has already begun encrypting the contents on the PCs. As a result, the researcher tries an older version of the Conti ransomware, and Windows 548 Defender identifies and terminates the attack. The Conti ransomware source code release demonstrates that these 698 malwares are certainly current and sophisticated, employing distinct approaches. In this study, we analyze Conti 700 ransomware source codes revealed its ability to avoid antivirus software, as well as its unique multithread, Encryption 702. The researcher also revealed data on all 703 API function calls, as well as API obfuscation techniques. The researchers also plan to investigate the remaining 709 Conti leaks in the future. These files contain internal logs, Jabber chat communications, and more source code for various web programs. The Conti Group conducts its business through 711. The following paper **[3]** emphasizes the risks of Ransomware poses a serious threat to both home users and businesses. In the workplace, individual computers typically store only system and program files, with all documents available through shared servers. In these cases, a single crypto-ransomware-infected server can encrypt any shared files to which it has access, including the entire collection of data from a workgroup of computer users. We offer a technique for detecting and preventing crypto-ransomware activities using file-sharing traffic monitoring. Ransomware poses a serious threat to both home users and businesses. In the workplace, individual computers typically store only system and program files, with all documents available through shared servers. In such cases, a single crypto-ransomware-infected server can encrypt all It has access to all shared files, including the entire collection of data from a user workgroup. We offer a technique for detecting and preventing crypto-ransomware activities using file-sharing traffic monitoring. The researcher examined six alternative interval T values, ranging from 10 to 60 seconds. We created training and testing datasets for each value, trained each of these machine learning models, and analyzed the outcomes. The classification metrics were calculated. Here are the files. They provide a balanced representation of both groups ('infected' and 'not-infected') since they are an 80%-20% random split of a dataset. Contains 50 hours of ransomware traffic and 50 hours of normal application activity. NNs produce the best outcomes among the models investigated; yet, they can be improved. The true positive and false negative rates were determined using the time it takes to detect ransomware (true positive) in the 'infected' dataset. The model's average and maximum time to raise an alarm for the 150 Traces of crypto-ransomware activity are now available. To test our theory, the researcher employed SMBv3 and NFS file-sharing protocols to run the 'unseen' software protocols. The researcher created a novel scenario in which a Windows 10 client and an Ubuntu file server shared the same directory as the one used for model training. In this study, the researcher developed a deep learning model capable of detecting crypto-ransomware while reading and writing files from a network-shared volume. There's been no Previous research on this problem, which is extremely common on business networks. Thanks to a new feature known as the number of brief instructions, the model's input set of characteristics represented not only the intensity of file access activity, but also the number of files accessed. When compared to other papers in the literature, the researcher revealed that the detection technique given in this study produces equal or better ransomware detection results. The proposed architecture is only acceptable for critical files that are stored on a file server. The study focused on the usual enterprise deployment scenario. Because of their enormous profit potential, crypto ransomware attacks have grown significantly in recent years. Nature's expansion will undoubtedly increase up speed in the future. . This research **[4]** explores ransomware actions during the destruction phase using behavioral feature analysis in order to better understand this malware and assist developers of ransomware detection systems in generating more reliable solutions. The feature selection algorithms utilized in this work and comparable research strive for the highest performance; yet, they consider the two goals equally, resulting in indistinguishable features. Ransomware and goodware are both linked. To gain a better understanding of how ransomware works, we merged numerous API versions to add information gain to these tactics, which, if studied individually, would make it easier to delete via the feature selection process. Although the API is the best individual feature group for recognizing ransomware from legitimate software, an anti-ransomware system should Other essential traits to watch for include data from other groups being used to enhance detection rates, manifested files, strings mentioning DLLs, and efforts to access external storage media. The top ten APIs associated with ransomware occurrences were NtTerminateProcess, SetUnhandledExceptionFilter, WSAStartup, WriteProcessMemory, NtGetContextThread, NtSetContextThread, exception, NtResumeThread, GetComputerName(A,W), and NtDeviceIoControlFile. Security systems must closely monitor API calls. The file's entropy is Ransomware encryption increases the randomness of file contents, which is a strong indicator of crypto-ransomware. However, entropy-based ransomware detection has severe limitations, including the risk of misclassification when distinguishing ransomware-encrypted data from regular files with high entropy. Furthermore, the cost of assessing entropy throughout a complete file makes entropy-based detection impracticable for large files. In this investigation **[5]** the researchers offer two indicators for ransomware detection based on byte frequency: EntropySA and DistSA, both of which take into account the intriguing properties of file subareas known as "sample areas" (SA). In threshold-based detection, a good threshold is essential. The researcher illustrates how to create thresholds to detect ransomware attacks. The support vector machine is a machine learning technique for categorizing datasets. It can classify high-dimensional spaces using one or more hyperplanes and is capable of both linear and non-linear classification. Non-linear SVMs are more versatile than linear SVMs, but they are less efficient since they require polynomial and Gaussian Radial Basis Function (RBF) kernels. The study introduced two byte frequency-based metrics, EntropySA and DistSA. In contrast to most previous detectors' files The indicators focus on constrained (sampling) file parts, whereas entropy does not. Without comparing read and write file entropies, EntropySA and DistSA discriminate between encrypted and unencrypted files. The proposed indications identify whether a file is being encrypted in real time. This method, unlike previous process-centric detection methods, detects ransomware while reducing file loss. Furthermore, the indicators employed by the researcher guarantee deterministic worst-case complexity. According to the paper**[6]**, ransomware uses encryption techniques to prevent legitimate users from accessing data. Too many ransomware families have been produced and distributed, causing significant damage to governments, businesses, and private customers. As ransomware cyberthreats become more common, researchers have proposed a variety of detection and categorization strategies. To identify malware before and after an assault, Host-based detection methods track local system activities. Forensic analysis focuses on recovering, acquiring, and analyzing data from contaminated equipment. Determine the effects of malware (including any identifiable information). As a result, several research have been conducted. Malware authorship analysis examines the stylistic features of the principal malware code to determine its authors (creators). This information can be useful when conducting digital forensics or tracing down malware. Ransomware will continue to pose a concern in the foreseeable future. As a result, it is critical to stay current with these dynamic occurrences and develop effective detection and classification frameworks. Overall, the works included here constitute a significant body of work in this area. Ransomware is a kind of malware that encrypts Data files are inaccessible to common users. This paper**[7**] goes over. Many ransomware families have been released, resulting in extensive harm and financial losses for individual users, businesses, and governments. As a result, academics have suggested multiple ransomware detection algorithms that analyze data using a variety of machine learning (ML) approaches. The ongoing spread of ransomware presents a plethora of operational issues for organizations. Threat detection and mitigation. Most importantly, gathering and sending vast amounts of raw data from massive user bases is becoming increasingly difficult (if not impossible). to a common region for analysis. Ransomware poses a continuing threat to both individuals and organizations. Researchers devised many methods for detecting and categorizing malware by analyzing binary files and system/network events with machine learning (ML) algorithms. However, greater scalability and privacy considerations complicate implementation. Massive volumes of data are collected and processed centrally. As a result, this paper proposes a novel distributed ransomware analysis (DRA) paradigm for ransomware detection and attribution. Recent advances in machine learning have yielded promising results in detecting malicious software that acts. Behavioural modeling detects dangerous programs by analyzing attributes generated from their runtime behavior. Because behavioural traits are intrinsically linked to the activity of any virus and hence difficult to avoid, they hold great promise. While much work has been done to avoid static malware aspects, less has been done to avoid dynamic malware features. This study**[8]** analyzes the resistance of behavioral ransomware detectors to escape and suggests numerous new evasive techniques. The prior tests' detector features (Shields and Regard) were easily recognized. In a real-world assault scenario, this white-box configuration assumption may not be valid. Our final level of experimental evaluation focuses on black-box scenarios in which the detector characteristics remain undisclosed. We developed and tested a novel practical attack against behavioral malware detection. Our attack spreads viral activity throughout a network of interrelated systems. A behavioural process classifier will not identify any specific process behaviour as suspicious. The article**[9]** discusses a variety of Ransomware issues. First, it dives deeper into Ransomware, discussing how it operates, the various varieties of Ransomware, and Ransomware Attack Phases. Recent ransomware attacks are being examined to better understand the There is a continuous ransomware pandemic. Malware analysis employs a variety of methodologies, including the use of multiple unique sandbox environments for malware execution and the detection of changes in behavior under various conditions. Malware analysis is critical in dealing with ransomware attacks, which are growing more prevalent. A WannaCry Ransomware sample has been obtained and analyzed. Any. Run was utilized for automated analysis and yielded satisfactory results. A virtual machine was created to do static and dynamic analysis. Flare VM was configured to study the sample. The static and dynamic analysis results showed that it was a ransomware sample. Malware, a hazardous weapon used by cyber attackers, is advancing in terms of rapid deployment and self-replication. Furthermore, because it can elude detection and do digital forensics investigations in near real-time, contemporary malware is one of the most hazardous forms of cybercrime. Advanced evasive strategies can have disastrous consequences. It must be detected quickly and independently for effective analysis. This paper**[10]** presents a new systematic method for detecting current malware. It classifies and detects five types of modern malware: adware, redware, rootkit, SMS malware, and ransomware. We used embedded approaches to train our raw data using the random forest algorithm to identify the significance of our attributes in binary and multi-class classification. Because of its efficiency and precision, this method was selected. Our research tries to detect and categorize modern malware with low error rates. Two deep learning algorithms (CNNs) and DNN) with static feature heuristic detectors, as well as two basic machine learning approaches (RF and DT) were constructed. These models were trained using two forms of categorization (binary and multiple). Malware identification and analysis are popular topics in the cybersecurity business. Every year, malware attacks target a number of businesses and states. Financial loss, data exfiltration, and cyber espionage can all result from a malware-based breach. Malware scanners and traditional antiviral therapies are useless in guarding against malware. The following research study **[11]** shows how to use machine learning to identify zero-day vulnerabilities in multi-tier ransomware families. It contradicts how we can use the hypervisor learning process to identify zero-day exploits in specific ransomware. It then proceeds to discuss how it was able to identify the ransomware's zero-day vulnerabilities and how it plans to unearth more for various malware families in the future. This research paper**[12]** demonstrates how we may perform dynamic analysis on a specific ransomware software. Before paying the ransom, you may be able to identify it. It identifies malware using machine learning, deep learning, and databases. In the future, the researcher plans to undertake more of this type of detection using file hashing. The article**[13]** that follows explains how to perform behavioral malware detection and identification using multiple test datasets and machine learning (ML) supervised learning. They use an Ubuntu machine with a Cuckoo sandbox to evaluate the malware's behavior. The researcher provided examples of ransomware. This article**[14]** describes versions that behave similarly but use different payloads. The experimental findings give information on how to detect ransomware by checking for unique file systems. This is the approach used to maximise the monetization of malware. In the future, ransomware can be tested on a number of operating systems, including Linux and MacOS. The researcher then examined the current state of ransomware assaults on internet-connected devices in the following article. The authors of this study **[15**] aim to discover both the ransomware's behavioral analysis and the detection methodologies used for malware analysis. The tools used to trace the behavioural analysis will be seek or Suricata, and the ransomware's behavioural analysis will occur once it has gained access to the system. So, based on the findings, one may understand how the analysis was conducted and how to obtain additional dump logins from the system's behavioral structure. The author **[16]** explore the impact of ransomware on Windows Active Directory Domain Services (AD DS), highlighting how ransomware attacks can compromise AD DS, leading to severe disruptions in enterprise environments. Their study underscores the importance of safeguarding AD DS against ransomware to maintain operational integrity and continuity in organizations . The author examine **[17]** the classification of ransomware using different types of neural networks. Their research demonstrates the effectiveness of neural networks in accurately identifying ransomware, showcasing the potential of machine learning techniques in enhancing ransomware detection capabilities. The study compares various neural network architectures to determine the most efficient approach for ransomware classification . The author introduce **[18]** the concept of data flooding as a countermeasure against ransomware. The study outlines the theoretical foundations and practical implementations of data flooding, which aims to overwhelm ransomware processes, thereby inhibiting their ability to encrypt files. This innovative approach provides a novel perspective on disrupting ransomware operations and mitigating its impact . The author propose **[19]** a method for ransomware detection based on process memory analysis. Their technique involves monitoring and analyzing the memory usage patterns of processes to identify anomalous behavior indicative of ransomware activity. This approach leverages the unique characteristics of ransomware's interaction with system memory, offering a promising avenue for early detection . The author **[20]** present BigRC-EML, a big-data-based framework for ransomware classification using ensemble machine learning. Their research highlights the advantages of combining multiple machine learning models to improve classification accuracy and robustness. The framework utilizes vast amounts of data to train the models, ensuring they can effectively detect and classify various ransomware strains . The author **[21]** develop R-Locker, a honeyfile-based approach to inhibit crypto-ransomware on Windows platforms. By deploying decoy files that attract ransomware, R-Locker can detect and block malicious activities before significant harm occurs. This method capitalizes on the predictable behavior of ransomware, providing a proactive defense mechanism against encryption attacks . The author investigate **[22]** the role of government in shaping the ransomware insurance market. Their study delves into the regulatory and governance aspects, offering insights into how governmental policies can influence the availability and terms of ransomware insurance. They argue that effective governance can mitigate the financial impact of ransomware by promoting better risk management practices . The author analyze **[23]** the ransomware payments economy, exploring the dynamics between attackers and victims in the context of ransom payments. Their research highlights the economic incentives driving ransomware attacks and the effectiveness of different payment strategies. By examining this underground economy, the study provides valuable insights into the financial motivations behind ransomware and potential measures to disrupt these illicit activities .

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Reference no.** | **Ransomware family analysed** | **Malware Family Analysed** | **Methods used(static or dynamic approaches)** | **Limitations** |
| [1] | n/a | General malware | n/a | It describes mostly about the work of the cybercrimes used by these malwares to steal credentials access. So, it just specifies that much |
| [2] | Conti | Goot loader, Conti, royal family | Static and dynamic both the approach has been used | The findings are very similar pattern in which I found out it using dynamic analysis. But it does not specify the important TTP’s used |
| [3] | Crypto based ransomware | n/a | Neural networks and LLMs approach | It is suitable for few types of files or clickjacking attacks only |
| [4] | Any ransomware | n/a | Behavioural approach(static approach) | The limitations of this approach will not help us in getting the string and will make the ransomware more powerful |
| [5] | Crypto based ransomware | n/a | Empirical analysis(dynamic analysis | EntropySA and DistSA have three limitations for detecting ransomware. First, the indicators have problems detecting the DMA Locker2 ransomware. |
| [6] | Any ransomware | Any malware | Binary and source code analysis(dynamic approach) | It does not verify about the constraints that are affected |
| [7] | Any ransomware | n/a | Empirical analysis | It also describes about the analysis of the ransomware but fails to determine the path length for it |
| [8] | Any ransomware | Any malware | Behavioural analysis(static approach) | The family of assaults' fundamental drawback is that they target a specific set of features for evasion. |
| [9] | WannaCry ransomware | n/a | Static and dynamic both | It defines all the necessary components but it does not give the assembly code for the ransomware access points |
| [10] | n/a | Adware, redware, rootkit, SMS malware | Static and dynamic both | It does not define the network build from which we can collect the packets for further investigation |

**Table-7 Citation of the literature survey**

In short, the literature survey can be citated such as few of the authors follows both the dynamic and static approach for analysis and most of them use same methods for doing the investigation the only limitation, we can find is in the TTPs, strings, IOCs, are not all defined in the papers. The researchers that use behavioural analysis mostly everyone is using dataset in it, so the limitations from the most authors are related to not finding proper path, not getting the access points, and few of them are just analysing few files. Then some of the ransomware and malware are just using dynamic approach and the major misses in these are that some of them are not able to show or give the caller functions and some of them are unable to provide proper information on the code diffing. Lastly, the static approach is doing real time analysis and in these there are just two limitations, they are the logs might give some wrong timestamps and the tools should be used less to avoid getting improper credentials.

**3.Methodology**

**3.1 Ransomware Analysis**

Ransomware often progresses across multiple phases. When ransomware infects an Android device, it either prompts the user for administrator access or deceives them by displaying a pop-up requesting patch updates. It sends these messages and this data to the attacker. employing Transport Layer Security (TLS), which is frequently encrypted. In case of crypto ransomware, it receives a private key from the command and control server. It uses this key to encrypt selected files that are already on the Android device. After encryption is complete, it will display an alarm message and request payment from the victim. The locker ransomware, on the other hand, will reset the Android smartphone's PIN, after which it will demand payment to re-access the device**.[19]**

**Figure-2Ransomware extortion process 1**

The steps that any crypto family goes through when it comes to Windows are illustrated here. Each variant infects the PCs of its victims using any malicious website or email and then moves on by using an infected link or attachment. The victim's PC contacts the Command & Control server after becoming infected. The ransom payment message will be shown on the victim's PC after the encryption process. Malware passes through the same phases as locker ransomware, but does not encrypt data. When locker ransomware attacks a victim's computer, it acquires administrator privileges and takes control of the keyboard. The user's access to the device is restricted. It changes the desktop backdrop or displays a window warning users about the ransomware attack and describing steps to recover access. This article employs static and dynamic malware analysis approaches to detect potential ransomware on the device. The following

subsections provide a detailed description of all the findings**.[20]**

**Table-8:** **Parameters used in BlackCat Ransomware**

|  |  |
| --- | --- |
| Parameters to be used | Explanation of parameters |
| 1. ADDvectoredexceptionhandler Api | It is utilized or used to do vector attacks on the windows API |
| 1. Regopenkeyexw | This will be routing the system and find out all the cryptographic hashes in the system |
| 1. Bcryptrandomgen | It is generated after we inject the malicious code in the system a random token or operator is generated |

The **SetUnhandlerException** is used to determine the exception rate at which we can get the point of handler exception and try to access the handle requests intercepted by the communication protocols in the system.

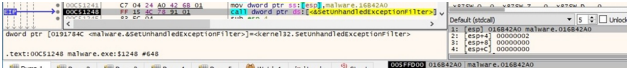


Figure- 1 **SetUnhandlerException**

**AddVectoredExceptionHandler API** it is used to bypass the api endpoints by just mutating the unhandled vectors form the registry key and then we can have an access to the user data from it.

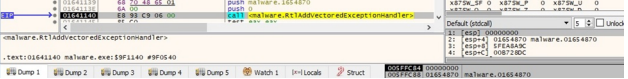


Figure- 2 **AddVectoredExceptionHandler API**

**RegOpenKeyExw** its simply opens the registry editor and changes all the default values either from “0” to “1” or from “false” to “true”.

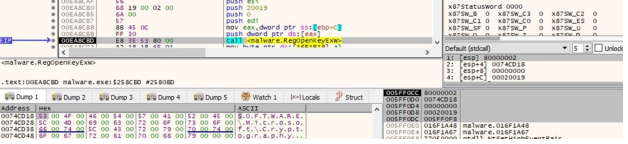


Figure-3 **RegOpenKeyExw**

**BcryptRandomGen** if functionality is to generate a random encryption key when the attacker gain access control over the victim’s system and it has been encrypted so it generates an encrypted key but only from the attacker side.

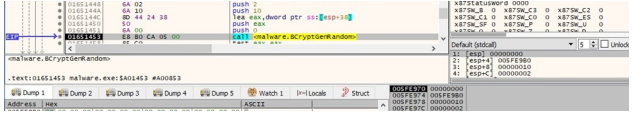


Figure-4 **BcryptRandomGen**

**CreateEventW API** it will create all the streamline of events which will follow the process of the events and it will help in eventually decrementing the chances of the attack.

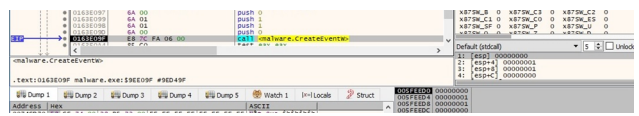


Figure-5 **CreateEventW API**

The methods to be used in analysing the Blackcat ransomware are as shown in figure 65:

**Figure-6 Ransomware analysis methodology for malware detection**

**4.Proposed framework for analysis of Blackcat ransomware**

The proposed system for this case study to be used is a C2 framework specifically named Havoc C2 framework to bypass the windows defender to gain the access of the system and get a shell or cmd access in one’s system. The other tool is Angler Exploit Kit which is to do offensive attacks against their rival organizations and look for the loophole. The main work of this toolkit is used to generate Payloads which cannot be detected by any antivirus or any defender making it undetectable. The Havoc C2 framework is a very recent framework and it mainly will be used to bypass the UAC for the privilege escalation techniques. Especially this framework will produce payloads in .dll, .exe, shell, etc types of formats which are also bit difficult to bypass them so the framework will be used particularly for this purpose as shown in the results section.

**5.Results and Discussion**

This ransomware can bypass the UAC privilege escalation via all the types of handlers and it had an encrypted AES file encryption which made it to encrypt the whole system and they were able to kill all the system utilities including the RAM memory also making it difficult for the defenders to retrieve information, although the information can be retrieved using different blue team tools like Retriever, etc. The results of the demon being created to bypass the windows defender and some of the antivirus threats are being as follows:-

**5.1. Identified vulnerabilities**

Following infected vectors could be found after the analysis:

1. CVE-2021-34473:- Microsoft Exchange server remote

Code Execution Vulnerability.

1. CVE-2021-34523:- Microsoft Exchange server Elevation of

Privilege Vulnerability.

1. CVE-2021-31207:- Microsoft Exchange Server Security

Feature Bypass Vulnerability.

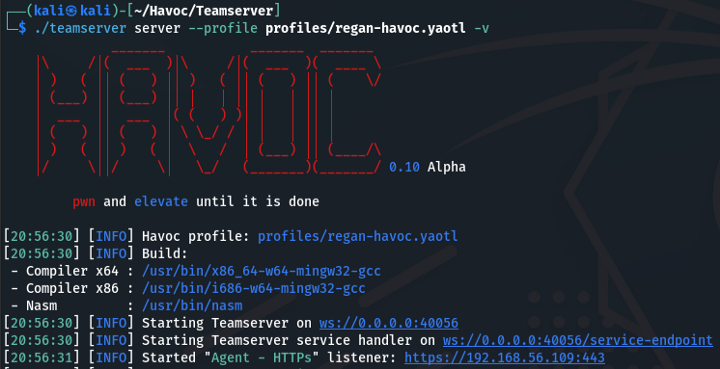


Figure -7 **Teamserver Startup**

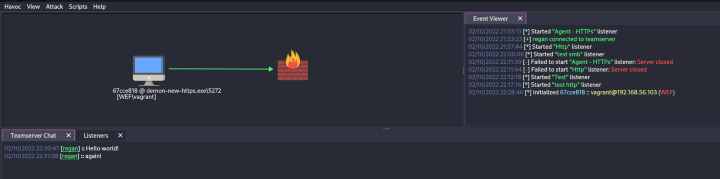
******

Figure-8 **Connected to victim’s server**

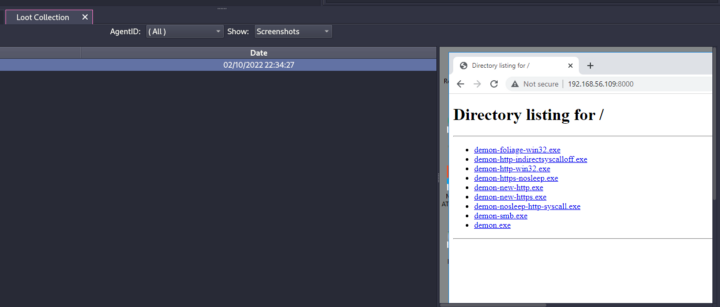
******

Figure 9 -**list of files in victim’s machine**

**Table-9 Results acquired after C2 attack**

|  |  |
| --- | --- |
| **Infection resource** | **Effect of the resource** |
| 1. Svchost.exe | It enables the service host and we can make changes in the DLL files by injecting payload |
| 1. Lsaas.exe | We have complete control over the local system |
| 1. Notepad.exe | We will get a notice of paying crypto currency in the note and how to pay it |
| 1. Powershell.exe | After running any of the PowerShell script files the whole system will be obfuscated and we can send as many as malicious warnings possible |
| 1. Config | We can change the config settings and make the IP address and MAC address completely disable from the victim’s machine. |

**6.Conclusion**

Thus, from all the above takings it can be concluded that a C2 framework can be used to abuse or bypass the windows C2 system for the BlackCat Ransomware too. The ransomware can be used for creating a demon file in specific formats like(.msi , .exe, .dll, shell, .wmic , etc.) and we can use this to create a small malware or payload. I also mentioned about the Angler Exploit Kit but as I mentioned I cannot show demos for it as it is an Illegal hacking tool and not easily available in the market, but we can use this tool to completely bypass the EDR-AVASION of the system and create payloads which will be totally undetectable.

**7.Future scope**

The ransomware analysis process takes a lot of time to find any strings or even the constraints that we are looking for to find, that will help us to at the most find 2-3 vulnerabilities or sometimes even 0-days and the more important thing is that we must do rigorous testing and transparency to find anything particular like that. So, we transude to that thing and then we would be able to find the strings, IOCs, etc. things that we want to find.

**8.References**

1. <https://news.sophos.com/enus/2022/07/14/blackcat-ransomwareattacks-not-merely-a-byproduct-of-badluck/>
2. https://unit42.paloaltonetworks.com/blackcat-ransomware/
3. https://www.microsoft.com/security/blog/2022/06/13/the-many-lives-ofblackcat-ransomware/
4. Forensic Analysis of a Ransomware(Animesh Kumar Agrawal, Sumit Sah, Pallavi Khatri)
5. Araba, A., Dijoux, R., Poulain, T., & Chevalier, G. (2020). Detecting ransomware using process behaviour analysis. *Procedia Computer Science*, *168*, 289-296. https://www.sciencedirect.com/science/article/pii/S2667096821000069
6. Zavarsky, P., & Lindskog, D. (2016). Experimental analysis of ransomware on windows and android platforms: Evolution and characterization. *Procedia Computer Science*, *94*, 465-472.
7. Internet of things and ransomware: Evolution, mitigation, and prevention(Mamoona Humayuna, NZ Jhanjhi, Ahmed Alsayat, Vasaki Ponnusamy)
8. Benkhelifa, E., Welsh, T., Tawalbeh, L., Jararweh, Y., & Al-Ayyoub, M. (2016). Leveraging software-defined-networking for energy optimisation in mobile-cloud-computing. *Procedia Computer Science*, *94*, 479-484.
9. Khan, N., & Al-Yasiri, A. (2016). Identifying cloud security threats to strengthen cloud computing adoption framework. *Procedia Computer Science*, *94*, 485-490.
10. Khanna, P., Zavarsky, P., & Lindskog, D. (2016). Experimental analysis of tools used for doxing and proposed new transforms to help organizations protect against doxing attacks. *Procedia Computer Science*, *94*, 459-464.
11. S ur Rehman, S., & Khan, M. U. (2016). A reliable and secure virtualized clinical assistance tool for doctors and patients. *Procedia Computer Science*, *94*, 441-446.
12. Ahmed, Y. A., Kocer, B., & Al-rimy, B. A. S. (2020). Automated analysis approach for the detection of high survivable ransomware. *KSII Transactions on Internet and Information Systems (TIIS)*, *14*(5), 2236-2257.
13. Poudyal, S., & Dasgupta, D. (2021). Analysis of Crypto-Ransomware Using ML-Based Multi-Level Profiling. *IEEE Access*, *9*, 122532-122547.
14. Alzahrani, S., Xiao, Y., & Sun, W. (2022). An Analysis of Conti Ransomware Leaked Source Codes. *IEEE Access*, *10*, 100178-100193. s
15. Zuhair, H., Selamat, A., & Krejcar, O. (2020). A multi-tier streaming analytics model of 0-day ransomware detection using machine learning. *Applied Sciences*, *10*(9), 3210.
16. McDonald, Grant, et al. "Ransomware: Analysing the impact on Windows active directory domain services." *Sensors* 22.3 (2022): 953.
17. Madani, Houria, et al. "Classification of ransomware using different types of neural networks." *Scientific Reports* 12.1 (2022): 4770.
18. Berardi, Davide, et al. "Data flooding against ransomware: Concepts and implementations." *Computers & Security* 131 (2023): 103295.
19. Singh, Avinash, Richard Adeyemi Ikuesan, and Hein Venter. "Ransomware detection using process memory." *arXiv preprint arXiv:2203.16871* (2022).
20. Aurangzeb, Sana, et al. "BigRC-EML: big-data based ransomware classification using ensemble machine learning." *Cluster Computing* 25.5 (2022): 3405-3422.
21. Gómez‐Hernández, José Antonio, Raúl Sánchez‐Fernández, and Pedro García‐Teodoro. "Inhibiting crypto‐ransomware on windows platforms through a honeyfile‐based approach with R‐Locker." *IET Information Security* 16.1 (2022): 64-74.
22. Baker, Tom, and Anja Shortland. "The government behind insurance governance: Lessons for ransomware." *Regulation & Governance* 17.4 (2023): 1000-1020.
23. Oosthoek, Kris, Jack Cable, and Georgios Smaragdakis. "A tale of two markets: Investigating the ransomware payments economy." *Communications of the ACM* 66.8 (2023): 74-83.
24. https://cybersecurity.att.com/blogs/labs-research/blackcat-ransomware
25. https://www.vaultree.com/blog/what-is-the-black-cat-ransomware-attackand-why-is-it-unique
26. https://blogs.blackberry.com/en/2022/06/threat-thursday-blackcat
27. <https://www.sentinelone.com/labs/blackcat-ransomware-highly-configurable-rust-driven-raas-on-the-prowl-for-victims/>