ISSN No:-2456-2165

Event Reconstruction Study Using Windows Restore Point and Reverse Engineering Concepts

Moza M, Zahra H, Sara R, Alya K, Hoda M, Charles Shibu
Abu Dhabi Polytechnic, P.O. Box 111499, Abu Dhabi, United Arab

Abstract:- In this internet era almost all smart devices relate to eachother depending upon their uniqueness and usage pattern. Vivid applications were created and with multiple features thereby makingthem easy targets to be exploited [1]. Exploits usually are malwares that pose to be genuine and productive applications. These malwaresenter the system and cause serious losses in terms of information, hardware and other types of monetary losses. It is a well-known fact that information stealing malwares and spywares steal personalinformation thereby making them available in social media or become seeds for furthermore attacks in the future [2]. Several researches have been carried out in the recent years in areas of Malware analysis to emphasize on the alarming increase of malwarethreats for a variety of platforms even in the presence of anti-malware checks. In our article we are focusing on event reconstruction considering different malware analysis techniques and tools. Our focuss would be mainly to reconstruct and known attack with practical emphasis and thereby proposing mitigation solutions.

Keywords:- *Malware, Reverse Engineering Technology, Event Reconstruction, System Restore Point.*

I. INTRODUCTION

System Restore point is a procedure that allows the user to restore important operating system files and applications in theevent of a failure. The terminology was first coined for Windows Millennium Edition (ME) and later got applied in Microsoft Home and Professional versions of Windows OS. System Restore was created to keep track of modifications to system and application data. Moreover, it could restore different points in time by creating so-called restore points, which are often known as System Restore Points (SRPs). Moreover, these restore points are known to provide us with primary evidence about attackers**,** such as malicious code, configuration, and logging parameters, that may have been wiped off completely from the observed system memory. It is understood that in most versions of Windows operating systems, the System Restore Point is enabled by default. A variety of events create System restore point such as the first boot of the OS, system uptime cycle per 24 hours, while new softwares get installed, during the process of restoring a restore point, while installing new softwares in the system, manual updation of the operation system and etc. [3].

II. BACKGROUND LITERATURE

Cybercrime has steadily increased with the advent of Information technology and with easy-to-use tools causing serious consequences for both individuals and society. Although technological advancements have made our lives easier and more comfortable, they have also come up with detrimental effects. As a result, professional and advanced digital forensics techniques are required to deal with such crimes. To make matters worse, criminals attempt to erase traces of their illegal activities with anti-forensic tools and techniques. Anti-forensic techniques are known to jeopardize the availability of evidence and/or utility of evidence in the forensic process. Because anti-forensics tools and techniques are constantly begin improved and updated, digital investigations may become increasingly difficult. A digital forensic investigator typically analyzes information stored in an electronic device's memory, such as RAM (also known as volatile memory) and hard disks (also known as non-volatile memory) to find evidence. As a result, only an in-depth analysis of such media could reveal illegal methods and manipulations used against the already evaluated electronic equipment with its content, such as the use of malicious software or, more broadly, evidential information to be submitted to the court of law. Technically speaking, Windows' System Restore Point data structure are known to reveal "anti-forensic" techniques used against the artefacts under investigation, for example, deleted files with formidable source of evidential data. An investigator might, for instance, discover a evidential data related to key loggers using such analysis. In fact, forensic investigators may also encounter difficulties as a result of the SRP data repository's format.[3]

Investigating computer intrusions is a difficult task. Hackers and attack methodologies are constantly evolving and so is thelevel of maliciousness in their code. Concealing their malicious code, deleting, or changing log files, and re-engineering new methods to reduce the amount of traceability come at a cost to malware analysts. Upon reviewing almost 200 compromised systems, the authors [3] have expressed their frustration due tothe lack of evidential data in victim machines after the intrusions from the perpetrators. It as to be taken into consideration that the latest exploitation tools and post-exploitation techniques have become a serious weapon to beat traditional techniques practised in the analysis of physical media by investigators and analysts. Hence it is imperative to improve our tools and techniques to accommodate uncommon investigation steps in support of cybercrime investigations and malware analysis. One such uncommon technique is the use of System Restore Points in windows machines and in-depth analysis. This article is based on a practical analysis of an investigation that took place in the United States [4]. This analysis throws light to the fact that investigators can review System Restore Points to establish their analysis parameters with respect to event timeline and unravel hidden information to help figure out how the system got compromised [4].

Currently, digital surveys are primarily used for research and the collection of digital evidence. On-the-market, computer forensics tools preserve the state of a system or examine a system in search of evidence, but they do not attempt to determine why an object can be evidence. It's fun to collect an object and examine its properties, but in order for the proof to be useful, we need to figure out what's causing these properties. In the physical world, it boils down to recognizing and drawing blood at a crime scene without using scientific methods to determine where it came from.

Event reconstruction is a critical stage in digital forensic investigation since it helps to identify the whole sequence of the event while it occurred. The findings of this stage is usually helpful for the forensic investigators to generate reports to be submitted to the court of law. It is imperative that outcomes be reproducible and hence the entire event reconstruction procedures must be done in a thorough manner [5].

The Importance of Reconstruction of Crime Scenes It is frequently important to narrow down the alternatives that lead to the crime scene or physical evidence discovered to ascertain the real path of the crime. One of the primary reasons for preserving the integrity of a crime scene is the probable necessity to recreate a crime.

Author Jayaraman [12] says reconstruction of the events and the series of occurrences is vital for digital forensics' investigation since it evidently leads to the incidental phase. The ability to analyse the quality of automated event reconstruction during malware analysis is an important step towards standardizing the digital forensics investigation process involving malwares. This has always given positive outcomes in creating antiviruses, patch to systems, creating a more malware resistant infrastructure, etc.

A. Introducing Maliciousness Triggering SystemRestore

In is important to understand the originality of System restorewhile it was launched. Malware authors and analysts claimedthat they could remove viruses and fix issues arising in computers due to malware with ease and with the help of Windows System restore. But the reality was that System Restore created copies of infected files where the extreme case was the viruses being capable of infecting the actual and restore volumes. The viruses also get restored in the system when the system gets cleaned with the help of antivirus softwares and Windows system restore. Otherwise, the virus removal fails when System Restore gets used as a tool to remove the virus. Fake hard disk defragmenters are another source of problems. For example, the Trojan horse "Trojan virus" - is a malicious program that performs malicious operations under the guise of the requested process. Also, Worms - malicious code that replicates itself by exploiting vulnerabilities in networks independently. Usually, worms slow down networks. System Restore virus scans the computer for known errors in the system and inbuilt hard disks.

B. Fake Applications and System Restore

This fake application is known to provide computer performance metrics and theft analysis outcomes which usually display falsified information mentioning configuration errors, bad sectors in hard disks, and any other critical errors. The application also displays fake pop-up alerts to inform the users of hard disk failures and system issues. These alerts specifically make users believe that the computer needs a licensed version of System Restore so as to be able to fix the system issues. Malware authors are always known to raise their bar and push their custom-built software to the edge so as to disable legitimate antivirus software in the target device. Hence it is understood that System Restore and restore point prevails to be the only security and optimization solution available in windows-based systems. An optimum solution in such cases, otherwise, would be to remove the maliciousness itself manually. Based on the above discussions the advisory given [6] is to use only legitimate version of softwares and in our case that would be System restore point.

III. ANATOMY OF A CYBER ATTACK

Windows has a default configuration that creates a system restore point once a week and before any important actions, such as installing a new program or driver. If this protection isn't enough for you, you may have Windows build a restore point every time you start your computer. The mechanism that recovers a point is a useful tool. It may assist you in recoveringyour device and resolving a variety of issues. Because this willrestore your device to a prior state, you will be able to undo most of the modifications made to your PC since the restore point was created. Installed or removed software and drivers, changes made to the registry and settings files by applications, and Windows updates are all examples of these modifications. Two actions are necessary to modify the default configuration of the Windows restore point.

First, you'll alter the frequency with which Windows may trigger automatic restore points in the Windows registry, and then you'll utilize Process Scheduler to establish a starting task that produces a restore point.

Step 1: Alter the Creation Frequency of Restore Points. Windows has a default option that creates an automated restoration once every 24 hours. You may still do a manual restore point and create restore points as a result of a program or driver installation. You must deactivate this frequency option to build a restore point every time you start.

By editing the registry, you may change the frequency at whichrestore points are created. Click Start and put "Regedit" into thesearch box. To launch Registry Editor, press Enter and grant itpermission to make changes to your computer. Step 2: Create aNew Restore Point by scheduling a Startup Task. You must nextuse the Windows Task Scheduler to establish a task that runs onWindows startup and produces a new restore point after you have set the restore point frequency to zero in the registry. TapStart, type "Task Scheduler," then use the Enter key to launch the Task Scheduler.

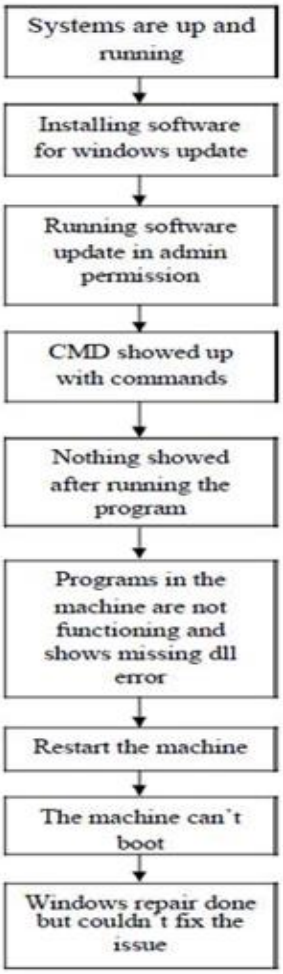

Systems are up and running
Installing software for windows update
Running software update in admin permission
CMD showed up with commands
Nothing showed after running the program
Programs in the machine are not functioning and shows missing dll error
Restart the machine
The machine can't boot
Windows repair done but couldn't fix the issue

Fig 1. Flow chart indicating practical demo of attack metrics

IV. MALWARE ANALYSIS

Malware analysis is the science of extracting as much information as possible about a piece of malware while using selective tools and techniques. To better comprehend the malware's capabilities and extent, how the system was infected, and how to protect against future assaults, the information retrieved helps enormously.

A. *Basic Static analysis*

The most frequent approach for malware analysis is Basic staticanalysis. This is usually accomplished by analysing the malware without executing it. As understood, the malware is examined without the malware sample being executed, static analysis is thought to be safe.

In this type of analysis, we examine the software without havingto look at the code. File information such as File name, File size, File type and any related hash values which are recognized by antivirus software, are among the technical metrics acquired with basic static analysis. Other parameters of analysis include malicious infrastructure, libraries, and compressed files.

In this type of analysis, we have used various tools such as Virus total, PEid, Dependency Walker, etc. As shown in Figure below virus total has indicated 56 0f 68 anti-virus scanners clarified that it is a malware. This malware was a sample tested to prove the concept of event reconstruction where in we have achieved first success in Basic static analysis.

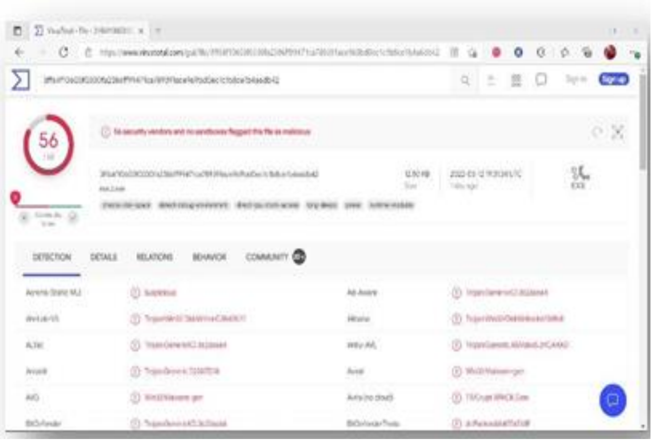
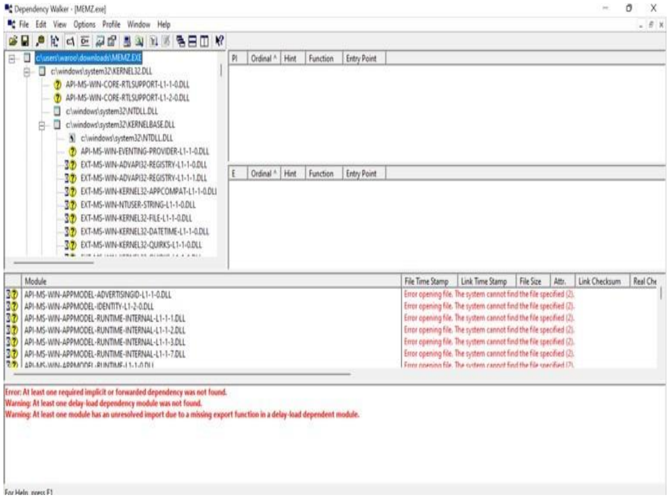


Fig 2. Basic static analysis (Virus total)



```
c:\users\waroo\downloads\MEMZ.EXE
  c:\windows\system32\KERNEL32.DLL
    API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL
    API-MS-WIN-CORE-RTLSUPPORT-L1-2-0.DLL
    c:\windows\system32\NTDLL.DLL
    c:\windows\system32\KERNELBASE.DLL
      c:\windows\system32\NTDLL.DLL
      API-MS-WIN-EVENTING-PROVIDER-L1-1-0.DLL
      EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-0.DLL
      EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-1.DLL
      EXT-MS-WIN-KERNEL32-APPCOMPAT-L1-1-0.DLL
      EXT-MS-WIN-NTUSER-STRING-L1-1-0.DLL
      EXT-MS-WIN-KERNEL32-FILE-L1-1-0.DLL
      EXT-MS-WIN-KERNEL32-DATETIME-L1-1-0.DLL
      EXT-MS-WIN-KERNEL32-QUIRKS-L1-1-0.DLL
```

```
API-MS-WIN-APPMODEL-ADVERTISINGID-L1-1-0.DLL        Error opening file. The system cannot find the file specified (2).
API-MS-WIN-APPMODEL-IDENTITY-L1-2-0.DLL             Error opening file. The system cannot find the file specified (2).
API-MS-WIN-APPMODEL-RUNTIME-INTERNAL-L1-1-1.DLL     Error opening file. The system cannot find the file specified (2).
API-MS-WIN-APPMODEL-RUNTIME-INTERNAL-L1-1-2.DLL     Error opening file. The system cannot find the file specified (2).
API-MS-WIN-APPMODEL-RUNTIME-INTERNAL-L1-1-3.DLL     Error opening file. The system cannot find the file specified (2).
API-MS-WIN-APPMODEL-RUNTIME-INTERNAL-L1-1-7.DLL     Error opening file. The system cannot find the file specified (2).
API-MS-WIN-APPMODEL-RUNTIME-L1-1-0.DLL              Error opening file. The system cannot find the file specified (2).
```

```
Error: At least one required implicit or forwarded dependency was not found.
Warning: At least one delay-load dependency module was not found.
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.
```

For Help, press F1

Fig 3*:* DLL files analysis using dependency walker

B. *Basic Dynamic Analysis*

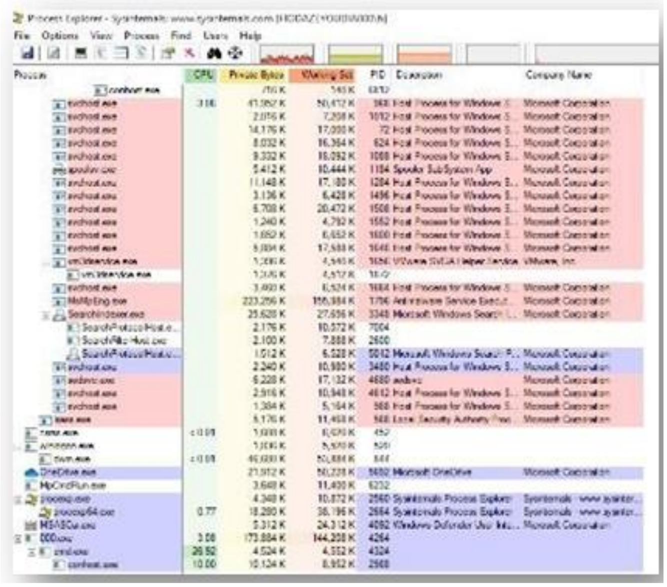


Fig 4. Basic dynamic analysis (Process Explorer)

Dynamic analysis is the process of monitoring a program's behaviour while it is running in a safe environment. In basic dynamic analysis, we execute the malware to analyse and understand the behaviour of it. It is not necessary to deconstruct the malicious binary before doing the analysis. The tool used in this technique actively monitors malware's behaviour during execution, making it more adaptable than static analysis. Basic dynamic analysis gives details such as domain names, specific IP addresses, registry keys and values, file path with locations, and any other files on the system or network been used by the malicious software. This type of analysis may not be able to produce useful findings in certain circumstances since malware may need extra information to execute which may be restricted in a safe environment. As a result, Advanced dynamic analysis is used, which involves extracting extensive information from the malware file as it is being run using a debugger or other specialtools.[8]

In our practical analysis we have used Process Explorer toimplement basic dynamic malware analysis. As can be seen inFigure 3 below, the malware (000.exe) runs in the system without a signature or a company name and not even from verified source.

C. *Advanced Static Analysis*

Strings, the linked library files (.dlls), and the exported and imported functions of the DLL files could be analysed with the help of such disassemblers. Knowledge of the basic operating system and understanding of disassembly are required for sophisticated static analysis since it catches undiscovered malware. Antivirus scanning, hashing, strings, and reverse compiling are a few more of the techniques used in advanced static analysis.[9]

D. *Advanced Dynamic Analysis*

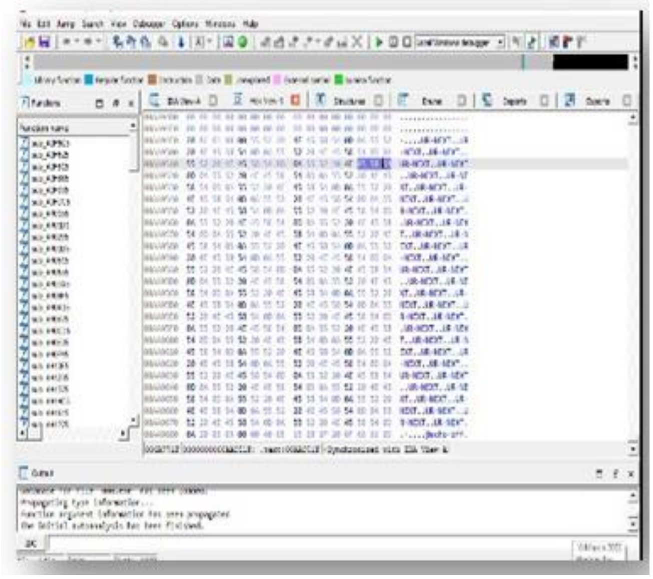


Fig 5. Advanced static analysis (IDA Pro)

Advanced static analysis is the process where we analyse themalware with the help of a disassembler, which allows it to be reverse engineered and analyzed. This sort of analysis revealsinformation about malware that isn't exposed by static analysisnor behavioural analysis [8]. The fundamental code that makesthe malware functional could be understood with the help ofdisassemblers such as IDA Pro as shown in Figure below orRADARE, another example serving the same purpose [7].

Advanced static analysis uses the debugger and disassembler toproduce instructions that define the semantics of the program.

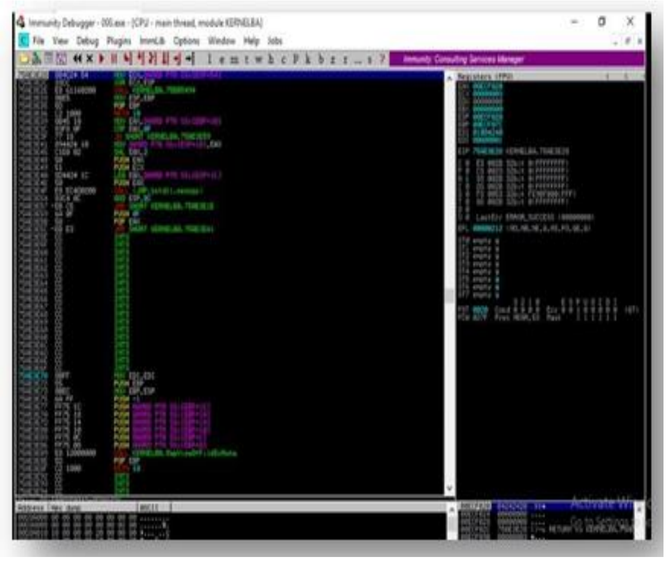


Fig 6. Advanced dynamic analysis (Immunity debugger)

Advanced dynamic analysis is an elated step towards viewing the low-level code in action. In this analysis technique, theentire analysis depends on the tool of usage. A thorough knowledge of setting breakpoints and analysing the code with the help of techniques such as Single stepping, stepping over and stepping into is vital. Registry based malwares, respective monitoring process and in-depth data analysis on malwares could be carried out with the help of debuggers such as OllyDbg, Immunity Debugger, WinDbg.

As part of a sophisticated dynamic analysis, a debugger may beused to get access to functionality that would otherwise be impossible to acquire via normal methods. It's more difficult tooverlook essential actions since it's behavior-based rather than static.[7]

In our analysis, we have used Immunity debugger to implement advanced dynamic malware analysis. We didn't have to go toodeep in the analysis process with Immunity debugger since thegiven maliciousness was already confirmed by Basic static, Basic dynamic, and Advanced static analysis with IDA Pro. The code was analysed with disassemblers, and we managed to acquire similar codes with the help of Immunity debugger as could be seen in the Figure.

E. Code Analysis

In order to figure out how the specimen behaves, reverse-engineering the malware was necessary as explained in Advanced static analysis. If you're looking at an application's low-level assembly instructions or byte code, you'll need a disassembler, debugger, and maybe a decompiler. The binary instructions are decoded by a disassembler into human-readable assembly code. It is the goal of the decompiler to re-create the original source code of the application. When a debugger is used, the analyst can interact with the code and see the results of its instructions to get a better understanding of the code's purpose. Both OllyDbg and IDA Pro Freeware, well-known free disassemblers and debuggers for Windows applications, are available for download.[10]

As a sophisticated approach, we analysed the binary code to comprehend its inner workings. A sample of the screenshot has already been provided (Figure 4). Static and dynamic analysis alone cannot provide the information that is revealed by this method. Strictly speaking, static vs dynamic code analysis is themain distinction between the two types of code analysis. Code analysis methods may be divided into two categories: static and dynamic. Static analysis entails disassembling the suspicious binary and examining the program's code, while dynamic analysis involves debugging the binary in a controlled way. It is imperative that grasp of programming languages, and operating systems is necessary for code analysis [11]. Knowledge of low-level languages depending on the application getting analysed is also essential. Examples of Low-level languages are not limited to Intel based X86 processor, ARM processors, Smali language, etc.

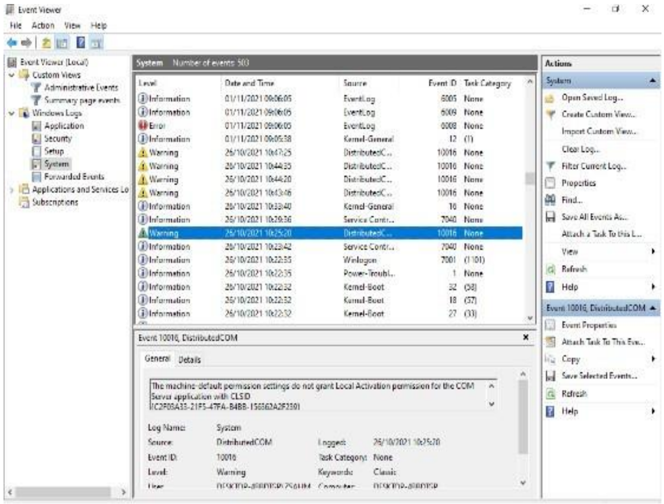
F. Analysis Conclusion (Including Subspinous Malware Behavior)

Whenever there's a security issue and malware being the culprit, malware analysis is an essential part of the incident response process. ' It provides guidance on how to get back on track. It aids in the identification of the hosts, servers, and systems impacted by the malware attack. As a result of malware analysis, companies are provided with actionable knowledge that they may use to avoid or lessen the dangers posed by malicious software. Using this method helps to avoid any more compromises.

V. SECURITY ANALYSIS AND DETECTION TECHNIQUES

As it shows in the below screnshot, Windows Event Viewer haslogged the suspoicious activites happened after the virus got downloaded into the system. There is also an option inside the windows server settings called threats and virus which providesus with details of any maliouces in the system.

As it is known that the event viewer used to check the logs thathappened in the system such as when we have downloaded thevirus in the system.



System Number of events: 503

Level	Date and Time	Source	Event ID	Task Category
Information	01/11/2021 09:06:05	EventLog	6005	None
Information	01/11/2021 09:06:05	EventLog	6009	None
Error	01/11/2021 09:06:05	EventLog	6008	None
Information	01/11/2021 09:05:38	Kernel-General	12	(1)
Warning	26/10/2021 10:47:25	DistributedC...	10016	None
Warning	26/10/2021 10:44:35	DistributedC...	10016	None
Warning	26/10/2021 10:44:20	DistributedC...	10016	None
Warning	26/10/2021 10:43:46	DistributedC...	10016	None
Information	26/10/2021 10:33:40	Kernel-General	16	None
Information	26/10/2021 10:29:36	Service Contr...	7040	None
Warning	26/10/2021 10:25:20	DistributedC...	10016	None
Information	26/10/2021 10:23:42	Service Contr...	7040	None
Information	26/10/2021 10:22:35	Winlogon	7001	(1101)
Information	26/10/2021 10:22:35	Power-Troubl...	1	None
Information	26/10/2021 10:22:32	Kernel-Boot	32	(58)
Information	26/10/2021 10:22:32	Kernel-Boot	18	(57)
Information	26/10/2021 10:22:32	Kernel-Boot	27	(33)

Event 10016, DistributedCOM

General Details

The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A33-21F5-47FA-B4BB-156362A2F239}

Log Name:	System		
Source:	DistributedCOM	Logged:	26/10/2021 10:25:20
Event ID:	10016	Task Category:	None
Level:	Warning	Keywords:	Classic
User:	DESKTOP-[illegible]	Computer:	DESKTOP-[illegible]

Fig 7: Log alert from event viewer

VI. IMPLEMENTATION

- *Reconstruction Pre-Requisite*

The significance of backup and recovery is that at some time a representative copy of the data is available for use. Transferring duplicated data from one place to another and performing different procedures on those files are all included under the umbrella phrase "backup and recovery."

In order to keep your data safe, you'll need a solid backup plan.Having a backup is your final line of defense against losing important data, since it allows you to retrieve the originals. The following are some of the benefits:

Prevent unwanted alterations by an attacker; safeguard againsthardware failure, unintentional erasure, or calamity. By looking at old and archived backups, you may learn about an intruder's activity.

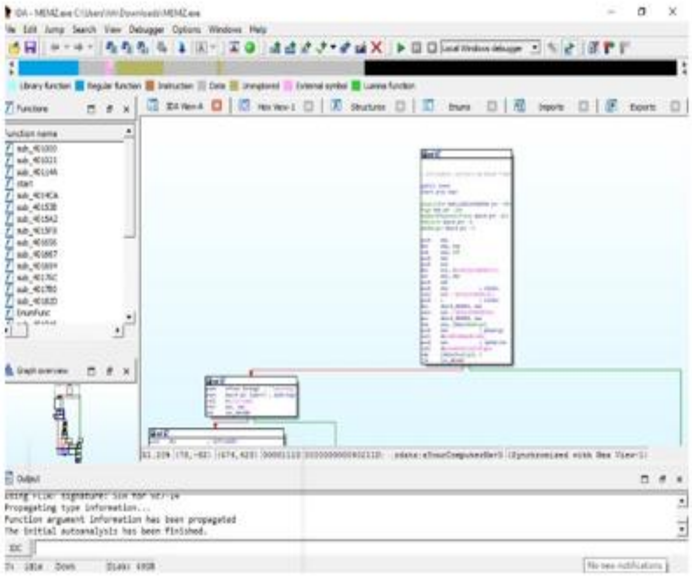
- *Reconstruction Environment*

The reconstruction environment is a windows server 2012 R2server and it is the 5th generation of Microsoft's Windows Server operating system, and its component of the Windows Operating systems. windows server 2016 Microsoft Windows Server 2016, formerly known as Windows Server vNext, is a server operating system developed by Microsoft (OS). The server operating system is designed particularly to be used as a basis for executing communicate effectively.in the environment the firewall was down to apply the viruses that are created and downloaded from github easly.

- *Reverse Engineering*

It is a technique or approach in which someone attempts to comprehend how a successfully made item, procedure, system, or software application achieves a purpose through logical logic with little (if such) knowledge into how it already does.

As an analysis process we applied reverse engineering technique by deploying IDA Pro. The Interactive Disassembler generated assembly language source code from machine-executable code as shown in Figure 7 and we were able to analyse in Grpahical mode and textual mode.



```
Using FLIRT signature: SEH for vc7-14
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished.
```

Fig 8: Graphical overview from IDA Pro

VII. CONCLUSION

In this research we were able to reconstruct the event with conventional systems using Microsoft platforms. We were able to identify the maliciousness of the malware and the target point using windows restore point and windows systems restore. Additionally, we made use of Windows Event Viewer to conclude system-based analysis in addition to the four malware analysis techniques.

Upon analysis, we were able to conclude that malicious nature of the malware and propose mitigation techniques. ConsideringData Loss Prevention (DLP) we propose adequate measures toensure Backups are in place to make use of System restore functionality. In addition, System Restore Point frequency needs to be increased to ensure restore points get generated at frequent intervals so that future investigation process could getsimplified. This also provides inherent roll back feature if the system gets compromised with alternate malicious softwares orsystem crash.

REFERENCES

[1]. N. Leavitt, “Mobile phones: the next frontier for hackers?” Computer, vol. 38, no. 4, pp. 20 – 23, april2005.

[2]. S. Thurm and Y. I. Kane. (2010, Dec.) Apps are caught stealing private data stored on smartphones(Android and iOS).

[3]. S. M. Yun, A. Savoldi, P. Gubian, Y. Kim, S. Lee, and S. Lee, “Design and implementation of a tool for System Restore Point analysis,” Proc. - 2008 4th Int. Conf. Intell. Inf. Hiding Multimed. Signal Process. IIH-MSP 2008, pp. 542–546, 2008, doi: 10.1109/IIH-MSP.2008.256.

[4]. K. Harms, “Forensic analysis of System Restore points in Microsoft Windows XP,” *Digit. Investig.*,vol. 3, no. 3, pp. 151–158, 2006, doi: 10.1016/j.diin.2006.08.008.

[5]. S. Soltani and S. A. H. Seno, “A formal model for event reconstruction in digital forensic investigation,” *Digit. Investig.*, vol. 30, no. August, pp. 148–160, 2019, doi: 10.1016/j.diin.2019.07.006.

[6]. “System Restore Point - an overview | ScienceDirect Topics.” https://www.sciencedirect.com/topics/computer-science/system-restore-point (accessed Apr. 25, 2022).

[7]. Saurabh, “Advance Malware Analysis Using Static and Dynamic Methodology,” *2018 Int. Conf. Adv. Comput. Telecommun. ICACAT 2018*, 2018, doi: 10.1109/ICACAT.2018.8933769.

[8]. E. Gandotra, D. Bansal, and S. Sofat, “Tools & Techniques for Malware Analysis and Classification,”*Int. J. Next-Generation Comput.*, vol. 7, no. 3, pp. 176–197, 2016.

[9]. O. Aslan, "Performance Comparison of Static Malware Analysis Tools Versus Antivirus Scanners To Detect Malware Performance Comparison of Static Malware Analysis Tools Versus Antivirus Scanners To Detect Malware," *Int. Multidiscip. Stud. Congr.*, no. December, pp. 1–6, 2017.

[10]. "4. Types Of Malware Analysis | Learning Malware Analysis." https://subscription.packtpub.com/book/networking- and-servers/9781788392501/1/ch01lvl1sec13/4-types- of-malware-analysis (accessed Mar. 22, 2022).

[11]. "SANS Digital Forensics and Incident Response Blog

[12]. | 3 Phases of Malware Analysis: Behavioral, Code, and Memory Forensics | SANS Institute." https://www.sans.org/blog/3-phases-of-malware-analysis-behavioral-code-and-memory-forensics/ (accessed Mar. 22, 2022).

[13]. Sundararaman Jeyaraman, Mikhail J. Atallah, An empirical study of automatic event reconstructionsystems, Digital Investigation, Volume 3, Supplement, 2006, Pages 08-115, ISSN 1742-2876, https://doi.org/10.1016/j.diin.2006.06.013.