International Journal of Engineering Technology and Applied Science
(ISSN: 2395 3853), Vol. 9 Issue 8 October 2023

Evidance-Based Analysis of Malware Attackes and Analysis of Malwares Activities

MD Mumtaz
Department of Computer Application
School of Computer Application ,
SAGE University, Bhopal, India
mdmumtaz7480@gmail.com

Rijvan Beg
iNurture- Department of Computer Application, SOCA, SAGE University, Bhopal, India
rijvan.beg@gmail.com

Vaibhav Jain
iNurture- Department of Computer Application, SOCA, SAGE University, Bhopal, India
vaibhav.inurture@sageuniversity.edu.in

Abstract—**In recent years, malware has been developed using various obfuscation techniques. As a result, malware detection has become a serious problem, Hence the need for malware analysis. In this paper, we have explained the basics of malware well and also discussed the different types of malwares and its descriptions. Discuss static analysis and dynamic analysis. This survey paper outlines several types of malware analysis methods and tools and used different tools to create data sets of malwares and keep records of Semantic behavior of the program. The various steps of malware analysis is discussed in this paper comprise static analysis of malware and dynamic analysis of malware with tools which are used to analyze malware. This paper also provides proposed model for malware analysis and network forensics.**

Index Terms-- Malware, Security, Memory forensics, Malware Detection, Malware Behavior.

I. Introduction

Any software that performs malicious actions on the victim's machine is considered malicious. Sophisticated malware uses packaging and obfuscation techniques to complicate the analysis and detection process. In recent years, malware has been developed using various obfuscation techniques. As a result, malware detection has become a problem [1].

Malware is a collective term for many types of malwares (viruses, ransom ware, spyware, etc.). Malware actually threatens individuals and organizations. Malware is an acronym for malware, a generic term for viruses, worms, Trojan horses, and other malicious computer programs. Hackers use software to destroy and obtain confidential information.

Detecting malware is challenging. A large and growing ecosystem of malware and engineering tools poses significant challenges for network operators and IT administrators. Antivirus software is one of the most widely used for detecting malware and malware blocking tools [2]. Virus is the first malware, a virus is a type of malware, and so all viruses are malware.

Sometimes user confused and unable to find out the threat, that what threat has come and what malicious activities has performed, sometimes user unable to distinguish threat. So first user need to understand what type of threat or malicious action has performed and put it into a separate category. So that we can understand better then try to find out better solution compared to existing.

However, in terms of the privacy and security of user data, especially when collecting evidence to analyze malware, malware is a concern because users with the data cannot obtain material resources and equipment.When it comes to analyzing malware in cloud computing, virtualization and cloud computing are the last two topics in information technology. They provide transparent services and change the way they are created, delivered, managed and executed. Companies and institutions can benefit from lower costs and greater efficiency. At the same time, virtualization and cloud computing have opened the door to operational and security problems [3].

Someone must design the code so that no existing antivirus software can detect its presence in the system. When the system is found to be damaged by malicious software or malware or any other malicious action, the forensic expert will first look for malicious activities or software that should not exist [4].

Malware can perform malicious activity in any sector and area like Banking sector, which can cause hacking or Data theft, information leakage, in banking sector there are so many users they use internet banking on internet, there is very high chances of data theft, in the bank's website there is a lot of data and important information or credentials like user id and password and mobile numbers stored on the bank's website. Some banks malware such as Zeus, Citadel, Carberp, SpeEye and Soraya, which infected personal computers between 2006-2019[5].

Today, everyday life largely includes the use of information technologies and especially the use of internet like watching movies, games, communications personal to electronic banking and official communications. The extensive use of the computer has also triggered the great spread of malicious programs also known as malware. These days most malware you have got through files and through espionage, theft of information and even money theft. Hence the fraud financial is one of the activities with greater impact than a malware can perform when it affects a computer [4-5].

Most malware detection technologies use malware signatures to detect. It is not difficult to detect known malware on the system, but this problem occurs when the malware is unknown, because the available signatures of known malware cannot be used to detect unknown malware. Signature-based detection technology cannot detect unknown and zero-day attacks [6].Malware analysis is a major trend in the security industry. With declining analytical skills and knowledge, the number of new malware samples and toolkits being used to automatically generate malware is growing exponentially [7].

Malware is software that is very similar to other software. The main difference between malware and non-malware (benign) is the behavior of that particular software. Malware is considered harmful, if part of the software exhibits malicious activity such as theft of user data, copying, certain security features, disabling backdoor features, or executing commands that the user does not need. There is a possibility of malware is running [8].

Current malware has no specific type of malware. It is versatile and complex. To manage the various malware that appears every day on the Internet, security analysts and product vendors, use automated tools to easily identify the malware and distribute or analyze malicious code. Expert works as a unit. Before technical instructions to mitigate threats, you should understand how malware works [9].The increase in the number of these malicious files has increased the demand for malware analysts or forensic specialists. Today, malware has the ability to evade detection, that is, to evade detection. Therefore, it is important to conduct a thorough analysis to assess the impact or damage caused by malware [10].

A. Definition of malware and its types

When a software or program is executed intentionally to damage a system or files is called malware [11]. There are different types of malwares in security area like Trojan horses, worms, various virus, and ransom wares. Each malicious codes are working as payloads, payload target the system and run for a specific purpose. Virus normally is considered first malware in the world, because its behavior is like malware [12], now here we explore the malware types and their behaviors to better understand.

Table I
MALWARE TYPES AND THEIR CHARACTERISTICS

Malware types	Descriptions
Trojan Horses	Looks like a regular programTrojan Can grant access to your computer without your permissionYour credential information can be leaked
Backdoor	Direct access to the networkcan open computer without permissionIt is a way for virus and worms to enter the systemIt is installed by worms.
Root kit	Thorough can which can access administration access hide themselvesIt can attach with malware.
Ransom ware	When the system is infected, it converts the data in coded form so victim cannot view data, to view data victim has to pay for it.
Spyware	Spyware try to capture credentials sell it to otherLike internet banking details and cards information and passwords.
Virus	It is first malware knows by othersprogram replicate and attach itself.
Worm	Multiply by using networkIt can cause illegal access can cause for backdoor

II. RELATED WORK

In this paper author analyze, that recent years, it is seen that malware detection is becoming a very big problem. Detection is becoming a very big problem.re detection is becoming a very big problem. In this study the author has analyze that it is not easy to detect effectively the new generation of malware with the help of signature-based and traditional behavior-based malware detector. Author proposes a model which name is subtractive center behavior model (SCBM), which creates malware ka data set, and tries to capture semantically related behavior related programs [13].Figure 1 shows the new generation malware.

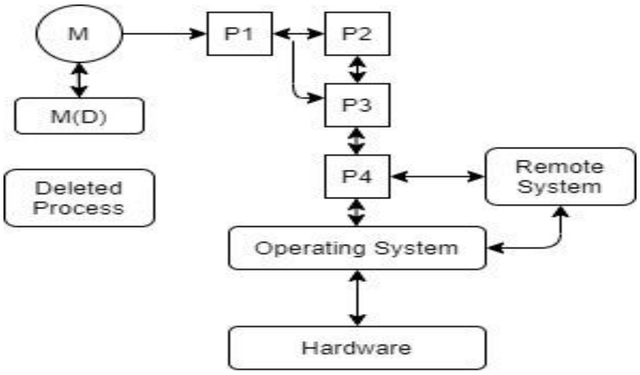


Fig. 1 New Generation Malware

In this paper it is observed Antivirus software that is used mostly to detect malware and to stop it, sometime unexpected malicious file comes and antivirus failed to detect that file, and antivirus sometimes failed to detect new generation modern malware, which is very effectively works and harmful for networks. So that author presents a new model for malware detection which helps to find out the malware for in cloud computing or cloud network service. This model uses multiple malware detection engines to identify malicious file and unwanted software, with the help of this model author can detect malware and vulnerabilities in the system [14].

A. Malware types

Although there are various types of malwares, the most common types today are as follows:

- Spyware: This is designed to collect information about the user without his/her knowledge and without being noticed. If the system is infected, it records the user’s keystrokes, file operations and important information such as usernames, passwords and credit cards saved in the Internet browser [15].

- Adware: This malware displays ads on the user’s screen. Although it is not defined as malicious software in itself, it can be transformed into a relatively more harmful type of software for stealing user information and capturing movements in the system when used together with a type of spyware [16].

- Virus: This malicious software, which can be hidden in any code or document, can cause problems such as deleting files on the system or stopping the operations of the system completely. It generally spreads through media such as CD/DVD, email and USB flash drives.

- Bot: This malware allows the attacker to gain control of the user’s system or perform a specific operation without being noticed by the user. Bot malware is normally used to exploit the computing power of the system in large-scale attacks[15-16].

- Bug: Bugs are accidental errors in the software. Although they are not seen as malicious software in themselves, they are used to give superuser powers to the attacker.

- Rootkit: This is designed to enable remote access of the system without being noticed by the user. If a rootkit runs successfully, it can perform many operations in the system, such as uploading files, installing programs, modifying system files or disabling programs such as anti-virus.

- Trojan: This kind of malicious software usually infects the system through the web or email without being noticed by the user. The malware hides itself after infiltrating the system (for example, taking on the appearance of an image file). As with rootkits, trojans can perform numerous operations once they get into the system.

- Worm: A worm is spread over the network using vulnerabilities in the system. Its objectives might include consuming network resources or creating a denial of service by overloading web servers.

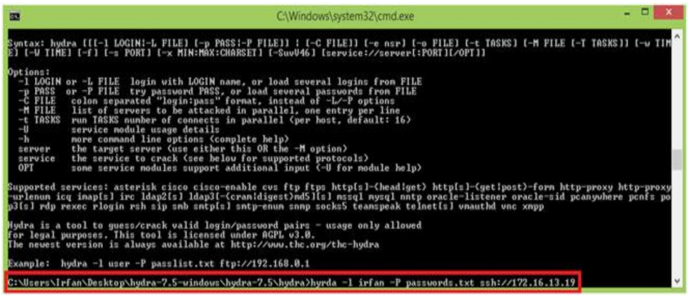
- Crypto malware: As the name suggests, this type of malicious software renders files or the system unusable. Generally, this type of malware is divided into two categories – lockers and encoders. The most widely known type is ransomware, which encrypts all files after infecting the victim computer. The user needs a specific password key to access the files again and the attacker wants a ransom in exchange for sending this password key[15-16].

B. Forms of malware attacks

Although malicious software types can be grouped under certain headings, it is not possible to examine all malicious software. So, let’s examine their general forms of attacks:16,17.

- Modification of the file system (for example, new file creation, editing, encryption, deletion).
- Modification of the file directory (for example, creating a new record, or changing an existing record).
- Infiltration into running processes (eg, adding a piece of malicious code into a running process).
- Creating and acquiring mutexes (eg, increasing access authorisation in the system).
- Network status monitoring (eg, monitoring ping scans).
- Starting and stopping system

There is a provision for different Transparent Service with utilization of resource in cloud computing, it is main features of cloud computing, in this paper author present a framework named is security information and event management (SIEM), with the help of this framework crime investigation is done and determine the evidence with effective proof and footprints. And also determine the issues rising during the malware detection, it can also focus on passive attack and try to give proper solutions [13].Author deploys the brute-force attack using Hydra tool. Show in figure 2.



```
Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIM
E] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-SuvV46] [service://server[:PORT][/OPT]]

Options:
  -l LOGIN or -L FILE  login with LOGIN name, or load several logins from FILE
  -p PASS  or -P FILE  try password PASS, or load several passwords from FILE
  -C FILE   colon separated "login:pass" format, instead of -L/-P options
  -M FILE   list of servers to be attacked in parallel, one entry per line
  -t TASKS  run TASKS number of connects in parallel (per host, default: 16)
  -U        service module usage details
  -h        more command line options (complete help)
  server    the target server (use either this OR the -M option)
  service   the service to crack (see below for supported protocols)
  OPT       some service modules support additional input (-U for module help)

Supported services: asterisk cisco cisco-enable cvs ftp ftps http[s]-{head|get} http[s]-{get|post}-form http-proxy http-proxy
-urlenum icq imap[s] irc ldap2[s] ldap3[-{cram|digest}md5][s] mssql mysql nntp oracle-listener oracle-sid pcanywhere pcnfs po
p3[s] rdp rexec rlogin rsh sip smb smtp[s] smtp-enum snmp socks5 teamspeak telnet[s] vmauthd vnc xmpp

Hydra is a tool to guess/crack valid login/password pairs - usage only allowed
for legal purposes. This tool is licensed under AGPL v3.0.
The newest version is always available at http://www.thc.org/thc-hydra

Example:  hydra -l user -P passlist.txt ftp://192.168.0.1

C:\Users\Irfan\Desktop\hydra-7.5-windows\hydra-7.5\hydra>hyrda -l irfan -P passwords.txt ssh://172.16.13.19
```

Fig. 2: Brute-Force attack using Hydra

A detailed analysis of traditional file-based malware and multifarious file less malware, file less malware is type of malware which does not use traditional activities, it means it does not use file. This survey focusses on traditional and file less malware activities, sometimes analyzer or forensics experts use digital forensic tools for detecting malware, like cuckoo sandbox to detect attacker, but attacker also use anti-forensic tool to delete their footprints. In this paper author also propose a model related to the file less malware attack [14].

There are several sectors where malware can affect, and can effects on their networks, similarly malware can affect in banking sector also. There are several types of malwares in banking sector like Zeus, Citadel, Carberp, SpeEye and Soraya, through which banking sectosare infected between 2006-2014. These malwares are described in detailed by author and comparison between them [15].

Signature-based technology is used to detect malware most of the time. Detecting identified malware is easy, but when the problem occurs when malware is not recognized before, because new generation malware is not detected due to its new signature which in not knows by malware detector before. So a new approach are required to identified malware effectively, in this paper author analyze he malware behavior and identified its characteristics, properties and its features by different analytical techniques with the help of some available open source tools [16].

In security area malware analysis is on the top trend, there are some new malware and tools kit are available, author noted that malware analysis and knowledge of experts are not enough, in this paper author create a infrastructure they for malware analysis with traffic of data packets and files travelling thorough on the networks, author claim about the architecture which perform malware analysis fast comparing the result of existing model or architectures and multiple different antivirus that uses customized kernel-drivers [17]. Author shows static analysis in figure 3.

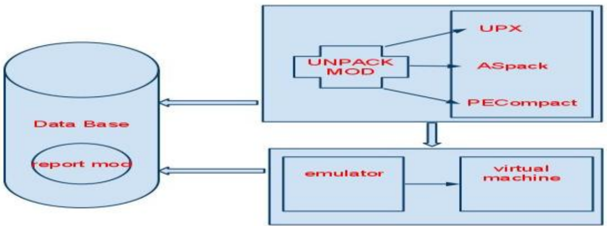


Fig. 3 Static Analysis

Author tries to analyze the opened binary data to analyze malware, static analysis is done when malware is not active.

Many methods are suggested by researchers to analyze the malware and there are also visualization methods for analyzing traditional malware and the visualization method focuses on repressing the features of malware. There is a lot work done in the field of visualization of malware but unfortunately author identified a lack of focus of behavior in the visualization malware. In this paper author focuses on classification of malware for its benefit, and find out its behavior according to existing methods. This research provides high accuracy and comparison with existing model to identified malware behavior [18].

Author proposed this malware behavior visualization model through which visualization of malware can bedone. Figure 4 shows the processes model in malware behavior visualization.

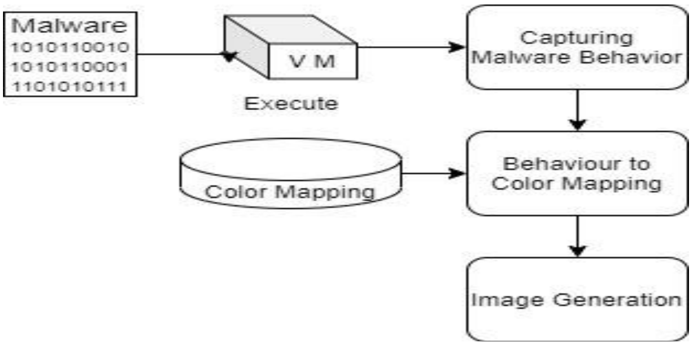


Fig. 4 Processes in Malware behavior visualization

Now a day’s malware is spreading very fast, some malwares are identified by the antivirus and with the help of malware analysis detecting tools, but some are identified and some can't be identified. Author discusses a new analysis technique which is reverse engineering and signature-based analysis. This paper discusses existing subverting techniques and discusses how to overcome the new developed techniques for malware analysis. This paper explores the variety of malware and classification of malware category [19].

As we all know, we are becoming very much dependent on the computer and attacks like Trojan and malware activities are increasing day by day. Malware codes are very difficult to understand. It is designed to damage the computer without the owner knowing. In this malware analysis we focus on the behavior of the malware and its components, for analyzing malware there are two methods like static malware analysis and dynamic analysis. In the static analysis malware tested without running in the environment and in the dynamic analysis malware tested with running virtual environment. In this research author try to malware analysis with static analysis and dynamic analysis of malware to know how much damage have done in the system and how to forensics on malware and try to know the level of the attacker [20]. Figure 5 shows the methods of malware like static analysis and dynamic analysis, advance static analysis and advance dynamic analysis, at last finally got report of malware analysis.

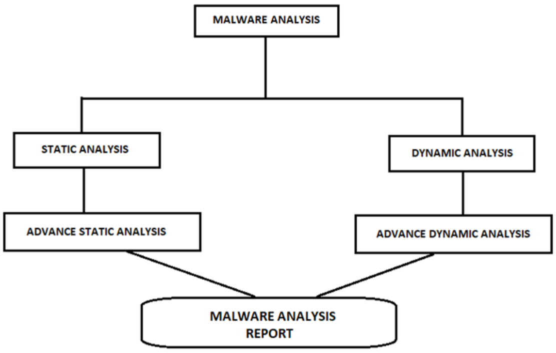


Fig. 5Methods for Malware Analysis

Malware analysis is the very important factor in security field. In this paper malware are analyzed statically and dynamically also. Author uses machine learning concept to extract the samples which is collected by tools running for malware detection. Cuckoo sandbox tools are used for malware analysis dynamically. Tools generated some different combinations from APIs, and summary information, DLLs and registry keys. Cuckoo tools are used for provide high accuracy. In this paper more than 2300 features are extracted dynamically. This paper provides accuracy of dynamic analysis of malware is 94.64%, and static analysis of malware is 99.36% [21].

III. BACKGROUND DETAILS

A. WindowsVulnerabilities for malware

In this section windows vulnerabilities are identified andcategorized onthe basis of windows layers. Attacker canperform the attack by exploiting these vulnerabilities whichare represented in Table 2.

Table 2: Classification of Windows Vulnerability for Malwares

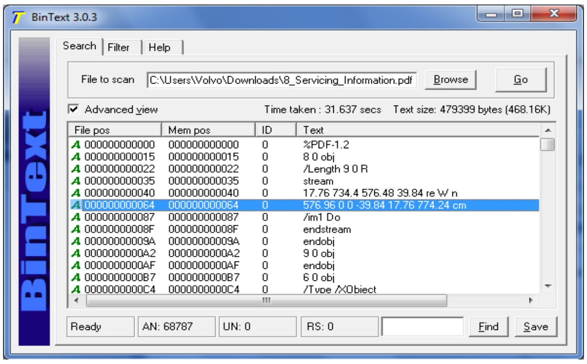
Layers	Vulnerability
Application Layer	Applications Vulnerabilities
Application Framework Layer	Content Provider Vulnerabilities
Library Layer	Vulnerability related to Web-Kit and SQL Lite Libraries
Runtime System Layer	Privilege Escalation attacks
Linux Layer	Cross Layer Vulnerabilities

B. Steps to Perform Malware Analysis:

Malware is a type of virus and analysis is to analyze malware. In computer security area we have to analyze the malicious activities. Here we discuss about the malware analysis like how can be analyze malware, how can malware effects on systems, how it works. Here detailed overview about the steps of malware analysis[21].

1- Performa static malware analysis- in this phase when malware is in disable form means it is in inactive form. Static malware is not running at that time, In other words when malware is not active in the system the static malware analysis is done by the expert [1-2].

2- Need to get information from malware and its activities like string value should be collected through the bin text tools, it is windows-based tools is to collect the string value. It also shows the hexadecimal value and it also shows the hidden text which was hidden behind of value [22].
UPX is the tools used for compression and packaging techniques. In this tool explain how the malware is compressed and how it is packed; these are all information provided by UPX Tools.



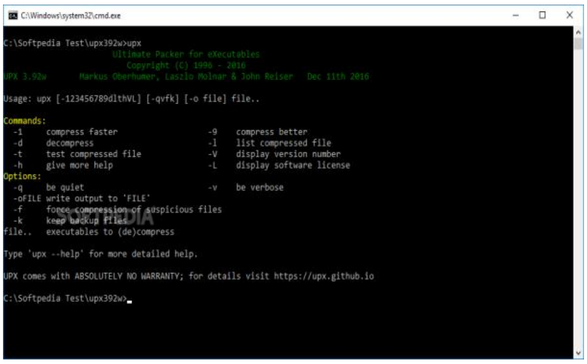
File to scan C:\Users\Volvo\Downloads\8_Servicing_Information.pdf

☑ Advanced view   Time taken : 31.637 secs   Text size: 479399 bytes (468.16K)

```
File pos        Mem pos         ID   Text
A 000000000000  000000000000    0    %PDF-1.2
A 000000000015  000000000015    0    8 0 obj
A 000000000022  000000000022    0    /Length 9 0 R
A 000000000035  000000000035    0    stream
A 000000000040  000000000040    0    17.76 734.4 576.48 39.84 re W n
A 000000000064  000000000064    0    576.96 0 0 -39.84 17.76 774.24 cm
A 000000000087  000000000087    0    /im1 Do
A 00000000008F  00000000008F    0    endstream
A 00000000009A  00000000009A    0    endobj
A 0000000000A2  0000000000A2    0    9 0 obj
A 0000000000AF  0000000000AF    0    endobj
A 0000000000B7  0000000000B7    0    6 0 obj
A 0000000000C4  0000000000C4    0    /Type /XObject
```

Ready   AN: 68787   UN: 0   RS: 0

Fig. 6 BinText Tool



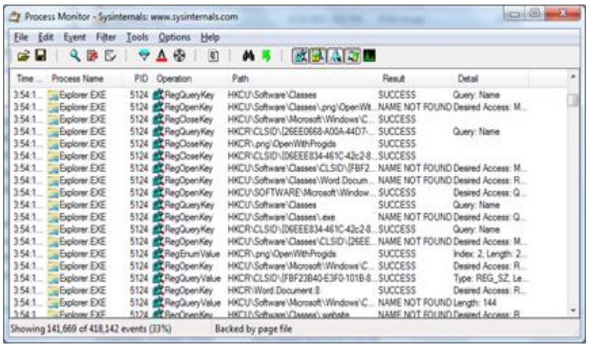
```
C:\Softpedia Test\upx392w>upx
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2016
UPX 3.92w       Markus Oberhumer, Laszlo Molnar & John Reiser   Dec 11th 2016

Usage: upx [-123456789dlthVL] [-qvfk] [-o file] file..

Commands:
  -1     compress faster                   -9    compress better
  -d     decompress                        -l    list compressed file
  -t     test compressed file              -V    display version number
  -h     give more help                    -L    display software license
Options:
  -q     be quiet                          -v    be verbose
  -oFILE write output to 'FILE'
  -f     force compression of suspicious files
  -k     keep backup files
file..   executables to (de)compress

Type 'upx --help' for more detailed help.

UPX comes with ABSOLUTELY NO WARRANTY; for details visit https://upx.github.io

C:\Softpedia Test\upx392w>_
```

Fig. 7 UPX Tool

3- In this step ensure about the network connection. When we need to analyze the malware, we need to install virtual machine or virtual box then need to install operating system in this virtual box. This operating system should be run virtually and whenever operating system is running the network should be disabling [3].

4- in this step the process monitors and process explorer tool is used to malware analysis and need to run malware and virus and also need to monitor action of process and information of the system. This tool needs to install in same virtual machine where you have found the malware. So that you can get the information of the process [23].

5-

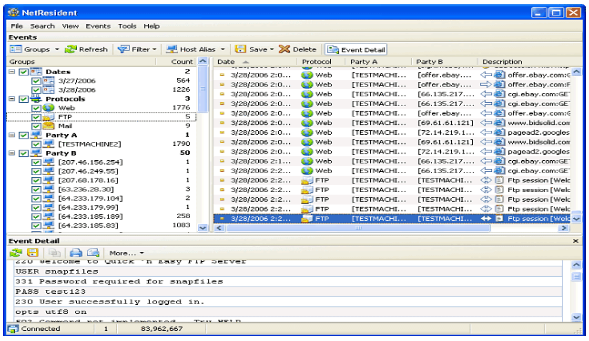


Time ...	Process Name	PID	Operation	Path	Result	Detail
3:54:1...	Explorer.EXE	5124	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
3:54:1...	Explorer.EXE	5124	RegOpenKey	HKCU\Software\Classes\.png\OpenWit...	NAME NOT FOUND	Desired Access: M...
3:54:1...	Explorer.EXE	5124	RegCloseKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	
3:54:1...	Explorer.EXE	5124	RegQueryKey	HKCR\CLSID\{26EE0668-A00A-44D7-...	SUCCESS	Query: Name
3:54:1...	Explorer.EXE	5124	RegCloseKey	HKCR\.png\OpenWithProgids	SUCCESS	
3:54:1...	Explorer.EXE	5124	RegCloseKey	HKCR\CLSID\{06EEE834-461C-42c2-8...	SUCCESS	
3:54:1...	Explorer.EXE	5124	RegOpenKey	HKCU\Software\Classes\CLSID\{FBF2...	NAME NOT FOUND	Desired Access: M...
3:54:1...	Explorer.EXE	5124	RegOpenKey	HKCU\Software\Classes\Word.Docum...	NAME NOT FOUND	Desired Access: R...
3:54:1...	Explorer.EXE	5124	RegOpenKey	HKCU\SOFTWARE\Microsoft\Window...	SUCCESS	Desired Access: Q...
3:54:1...	Explorer.EXE	5124	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
3:54:1...	Explorer.EXE	5124	RegOpenKey	HKCU\Software\Classes\.exe	NAME NOT FOUND	Desired Access: Q...
3:54:1...	Explorer.EXE	5124	RegQueryKey	HKCR\CLSID\{06EEE834-461C-42c2-8...	SUCCESS	Query: Name
3:54:1...	Explorer.EXE	5124	RegOpenKey	HKCU\Software\Classes\CLSID\{26EE...	NAME NOT FOUND	Desired Access: M...
3:54:1...	Explorer.EXE	5124	RegEnumValue	HKCR\.png\OpenWithProgids	SUCCESS	Index: 2, Length: 2...
3:54:1...	Explorer.EXE	5124	RegOpenKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Desired Access: R...
3:54:1...	Explorer.EXE	5124	RegQueryValue	HKCR\CLSID\{FBF23B40-E3F0-101B-8...	SUCCESS	Type: REG_SZ, Le...
3:54:1...	Explorer.EXE	5124	RegOpenKey	HKCR\Word.Document.8	SUCCESS	Desired Access: R...
3:54:1...	Explorer.EXE	5124	RegQueryValue	HKCU\Software\Microsoft\Windows\C...	NAME NOT FOUND	Length: 144
3:54:1...	Explorer.EXE	5124	RegOpenKey	HKCU\Software\Classes\.website	NAME NOT FOUND	Desired Access: R...

Showing 141,669 of 418,142 events (33%) Backed by page file

Fig. 8Tool for Process Monitor

6- When Malware runs, network traffic is increased so we have to record that traffic and information related to network with the help of network connectivity and packet log content monitoring tools like Net resident and TCP View. The traffic of the network is generated by the malware analyzed by Netresident.



Groups	Count
Dates	2
3/27/2006	564
3/28/2006	1226
Protocols	3
Web	1776
FTP	5
Mail	9
Party A	1
[TESTMACHINE2]	1790
Party B	50
[207.46.156.254]	1
[207.46.249.55]	1
[207.68.178.16]	1
[63.236.28.30]	3
[64.233.179.104]	2
[64.233.179.99]	1
[64.233.185.189]	258
[64.233.185.83]	1083

Date	Protocol	Party A	Party B	Description
3/28/2006 2:0...	Web	[TESTMACHI...	[offer.ebay....	offer.ebay.com:G
3/28/2006 2:0...	Web	[TESTMACHI...	[offer.ebay....	offer.ebay.com:P
3/28/2006 2:0...	Web	[TESTMACHI...	[66.135.217....	cgi.ebay.com:GE
3/28/2006 2:0...	Web	[TESTMACHI...	[66.135.217....	cgi.ebay.com:GE
3/28/2006 2:0...	Web	[TESTMACHI...	[offer.ebay....	offer.ebay.com:G
3/28/2006 2:0...	Web	[TESTMACHI...	[69.61.61.121]	www.bidsolid.com
3/28/2006 2:0...	Web	[TESTMACHI...	[72.14.219.1...	pagead2.googles
3/28/2006 2:0...	Web	[TESTMACHI...	[69.61.61.121]	www.bidsolid.com
3/28/2006 2:0...	Web	[TESTMACHI...	[72.14.219.1...	pagead2.googles
3/28/2006 2:1...	Web	[TESTMACHI...	[66.135.217....	cgi.ebay.com:GE
3/28/2006 2:2...	Web	[TESTMACHI...	[66.135.217....	cgi.ebay.com:GE
3/28/2006 2:2...	FTP	[TESTMACHI...	[TESTMACHI...	Ftp session [Welc
3/28/2006 2:2...	FTP	[TESTMACHI...	[TESTMACHI...	Ftp session [Welc
3/28/2006 2:2...	FTP	[TESTMACHI...	[TESTMACHI...	Ftp session [Welc
3/28/2006 2:2...	FTP	[TESTMACHI...	[TESTMACHI...	Ftp session [Welc
3/28/2006 2:2...	FTP	[TESTMACHI...	[TESTMACHI...	Ftp session [Welc

Event Detail

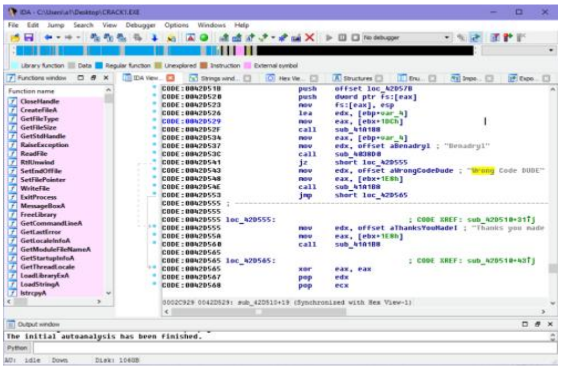
```
220 Welcome to Quick 'n Easy FTP Server
USER snapfiles
331 Password required for snapfiles
PASS test123
230 User successfully logged in.
opts utf8 on
502 Command not implemented - Try HELP
```

Connected 1 83,962,667

Fig. 9NetResident Tool

7- In this step registry tools is used to determine what changes has done in registry and what file is added and process spammed by the malware. The tool is Regshort.

8- Information and data debugging is the main step to perform malware analysis, to analysis we need to collect the information and start debugging with the help of debugging tools like ollyDbug and Procdump. Ensure that what type of service request information needed like service request and DNS table information, when malware is running what attempts is happening on the network incoming and outgoing traffic. In this lever we can use IDA Tools also. The IDA tool providedescriptive data of malware activities or malicious activities. IDA describe each and everything about malicious activities in detail like a reverse engineering.



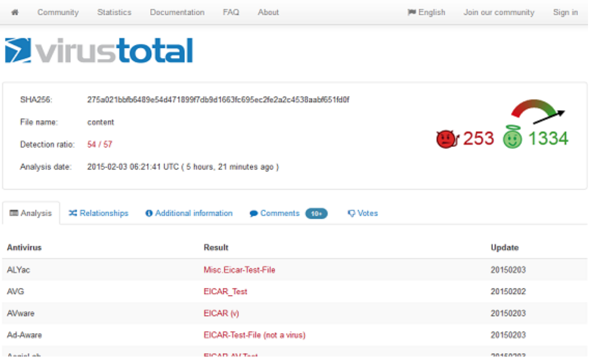
Function name
CloseHandle
CreateFileA
GetFileType
GetFileSize
GetStdHandle
RaiseException
ReadFile
RtlUnwind
SetEndOfFile
SetFilePointer
WriteFile
ExitProcess
MessageBoxA
FreeLibrary
GetCommandLineA
GetLastError
GetLocaleInfoA
GetModuleFileNameA
GetStartupInfoA
GetThreadLocale
LoadLibraryExA
LoadStringA
lstrcpyA

```
CODE:0042D518                 push    offset loc_42D578
CODE:0042D520                 push    dword ptr fs:[eax]
CODE:0042D523                 mov     fs:[eax], esp
CODE:0042D526                 lea     edx, [ebp+var_4]
CODE:0042D529                 mov     eax, [ebx+1DCh]
CODE:0042D52F                 call    sub_41A188
CODE:0042D534                 mov     eax, [ebp+var_4]
CODE:0042D537                 mov     edx, offset aBenadryl ; "Benadryl"
CODE:0042D53C                 call    sub_403BD8
CODE:0042D541                 jz      short loc_42D555
CODE:0042D543                 mov     edx, offset aWrongCodeDude ; "Wrong Code DUDE"
CODE:0042D548                 mov     eax, [ebx+1E8h]
CODE:0042D54E                 call    sub_41A188
CODE:0042D553                 jmp     short loc_42D565
CODE:0042D555 ; ---------------------------------------------------------------
CODE:0042D555
CODE:0042D555 loc_42D555:                             ; CODE XREF: sub_42D510+31↑j
CODE:0042D555                 mov     edx, offset aThanksYouMadeI ; "Thanks you made
CODE:0042D55A                 mov     eax, [ebx+1E8h]
CODE:0042D560                 call    sub_41A188
CODE:0042D565
CODE:0042D565 loc_42D565:                             ; CODE XREF: sub_42D510+43↑j
CODE:0042D565                 xor     eax, eax
CODE:0042D567                 pop     edx
CODE:0042D568                 pop     ecx
0002C929 0042D529: sub_42D510+19 (Synchronized with Hex View-1)
```

```
The initial autoanalysis has been finished.
AU: idle   Down      Disk: 106GB
```

Fig. 10OllyDbug

9- Malware testing can be done online also. There are some website which provide online services to scan the virus or malware for analysis. Like VirusTotal and cuckoo sandbox. In this website we have to submit malware or virus after that website take some time to process it and provide report regarding malware activities. The report contain the malware levels like how malware are critical and how much it suspicious and what is rank of malware, how much API Calls called by it, how much fake calls and what API Calls are truly called. These tools provide free service for malicious files or malware.



SHA256: 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f

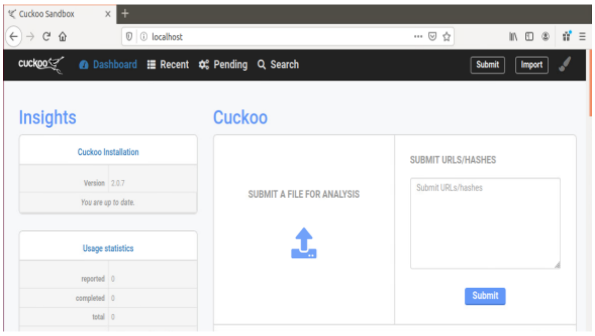
File name: content

Detection ratio: 54 / 57

Analysis date: 2015-02-03 06:21:41 UTC (5 hours, 21 minutes ago)

Antivirus	Result	Update
ALYac	Misc.Eicar-Test-File	20150203
AVG	EICAR_Test	20150202
AVware	EICAR (v)	20150203
Ad-Aware	EICAR-Test-File (not a virus)	20150203
AegisLab	EICAR-AV-Test	20150203

Fig. 11VirusTotal



Version 2.0.7

You are up to date.

reported 0

completed 0

total 0

Fig. 12 Cuckoo Sandbox

C. *Analysis method*

Malware analysis is a procedure used to look at the behaviors and components of malware and, if possible, pinpoint the attacker. Figure 13 displays the suggested malware analysis technique.

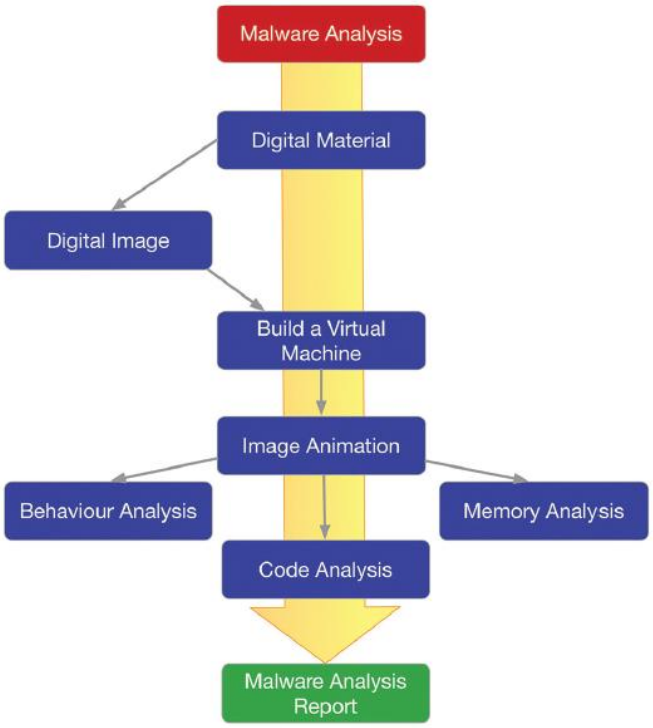


Figure 13: Basic Malware Analysis Method

To avoid tampering with the original, all research and analysis must be done on a copy (image) of the evidence.18 The image needs to be created using specialized technology or software. The process of creating an image entail using a tool or application to copy every file on the system (computer, mobile device, portable memory, etc).

The image contains every piece of data on the data storage device, whether it is currently accessible, deleted, hidden, or otherwise. It is necessary to confirm in the image that every piece of evidence's data has been accurately copied. Because of this, worldwide standards should be followed during the image generation process[23].

The process of malware analysis begins with the picture production stage. The process as a whole may be impacted by taking pictures properly and in accordance with international standards. Therefore, it's important to ensure that the pictures are accurate. The information on the storage devices is checked to see whether there have been any changes using the hash validation value. It is concluded that there has been no change to the data in the system and the image if the hash validation value is the same before and after the operation. MD5 (Message-Digest algorithm 5), SHA-1 (Secure Hashing Algorithm), or SHA-256 hash validation values are applied throughout the forensic examination. The hash values need to be computed and checked frequently in forensic analysis.

Software image production and physical image creation are the two main categories into which the picture generation process may be separated.

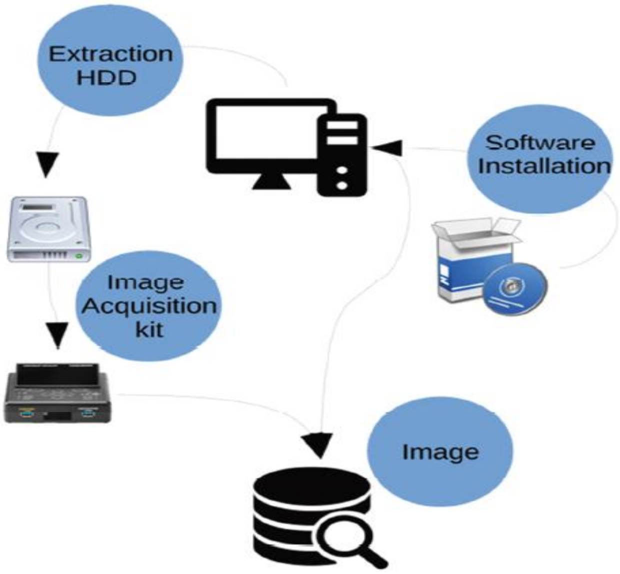


Figure 14: Image Creation Procedure

The detailed image generation processes are shown in Figure 14. Forensic Replicator, PDA Seizure, Palm dd, FTK Imager, Image (DOS), SMART (Linux Redhat), ByteBack (DOS), ILook, Automated Image & Restore, Forensic Explorer, Sans Acronis True Image, EnCase Forensics, and other programs are installed on the system's primary drive or an external disk to create software images. Tools used in image creation software are typically designed with hardware in mind. These programs might be as simple as a few lines of code or as complex as software with millions of lines. The software used in forensic investigations is typically complicated and provides low-level hardware connection capabilities [26-27].

The technique most frequently utilized in forensic cases is the generation of physical images. The target system's hard disk is deleted using this technique. The image recovery kit (Tableau TD1, TD2, etc.) is next linked to the removed drive[28-29].

IV. PROPOSED MODEL

Detection of malicious activities is done by learning behaviors of attack. Detection of malware we can develop a framework according to client-server paradigm.

Client is taking services and server is providing services on the network the framework can be divided into three levels, first one is to capture the samples second one is tagging the data and last is learning from samples data. Client can capture the samples which are generated by the tools and preprocess it. To forensic analysis preprocessing is the first and important part of analysis of malware.

This is the proposed model for Memory Forensics to analysis of malware.

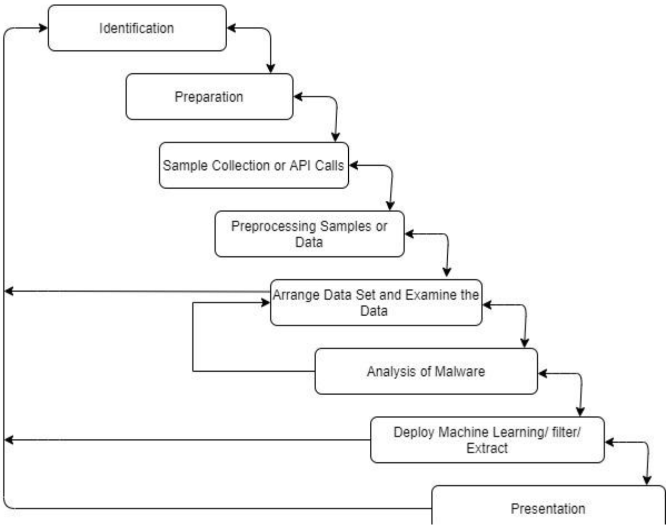

Identification
Preparation
Sample Collection or API Calls
Preprocessing Samples or Data
Arrange Data Set and Examine the Data
Analysis of Malware
Deploy Machine Learning/ filter/ Extract
Presentation

Fig. 13Model for Malware Analysis& Network Forensics

The proposed model is basically used for malware analysis and digital forensics. The block diagram is explained in detail.

A. Identification:

As we know we have to identify ka behavior of system on network, malware or malicious activities increasing day by day, so we need to identify the threat which can cause to damage the system. First this model tries to identify malware and threat through which we can try to prepare further process to malware analysis.

B. Preparation:

The main motive of this phase is contentiously watching the samples which is collected from identification phase and plays the important role in risk assessment, this phase need to regular training to arrange the samples data like API calls and DLLs files, Ready to arrange to keep threats and new security attack and tools which can analyze the malware or malicious program like malware, botnet, APT (Advanced Persistence Threat) and DDoS.

C. Sample collection and API Calls:

In this phase we need to arrange API calls and DLLs files, we need to arrange the data set of API calls so manage data set arranging in proper manner then next step to extract it with the help of machine learning application.

D. Processing Samples or data:

In processing phase first need to preprocessing of collected data from previous phase, Data may be malware footprints or may be details information of malware where from it travels. The evidence of malware travels on the system, the leave footprints and try to erase their evidence, we need to collect that evidence which malware can unable to erase and try to collect API Calls called during the malware traveling, there are some fake API calls and some are truly called. In this phase data extraction is done. I t is similar to the extraction process.

E. Arrange data set and examine the data:

In this phase evidence are traces and targeted though the security tools on extracted data sent on which analysis of malware is to performed, the data set need to be filtered by category like API calls, DLLs, Registry Keys. The data set may be having duplicate data which have to arrange in proper manner.

F. Analysis of malware:

While analysis of malware or threats experts should have monitor and analysis of network communication, registry keys, foot printing data, memory analysis dynamically and process analysis to analyze the malware activities. For investigation of malware activities tools has to be performed like cuckoo sandbox and collect the sample data and report and try to find out where the actual attack action is performed.

G. Deploying Machine learning Application:

In this phase after we got the report and arranged data set with registry entries and process analysis, network information, footprint of malware. These data should be arranged in proper manner after that this need to be extract the data set with the help of machine learning application. There are so many machines learning application through which we can filter the data samples and get proper analysis.

H. Presentation:

All the data found in previous levels such as identification, preparation, sample collection of data, detection, analysis and examination are arranged in proper manner and presented for understanding legal evidence, purpose. The detailed report can be represented as visualization so that they can be easy understood.

V. EXPERIMENTAL SETUP

A. Virtual Machine

Analysis must be done in a safe environment to prevent the impact of the malware on the workstation under investigation. A virtual machine needs to be set up on the workstation for this purpose. By using a virtual machine, it is possible to utilize an operating system other than the one that is currently installed, such as Windows Vista, Windows 7, Windows 10, MAC OS X, etc. The most popular virtual machine program is VMware.

To enable viewing of the contents, it is necessary to mount the image that was obtained for analysis on the workstation. The picture files are mounted read-only as a virtual hard drive on the workstation since the hash validation value will be determined after the investigation to make sure that the image content is accurate. This makes it possible to export the images' files and directories.

B. Behaviour analysis

The behavior of malware, including registry activities, network operations, file and directory transfers, is examined in the behavior analysis. Malware development occasionally introduces unintended problems. Debugging is thus possible via behavior analysis. It's crucial to note this erroneous information. Debugging occasionally reveals details about the attacker. Process Monitor, Process Explorer, Regshot, Wireshark, CaptureBat, Cuckoo Sandbox, Anubis, Volatility, and other tools are frequently used for behavior analysis.19,20.

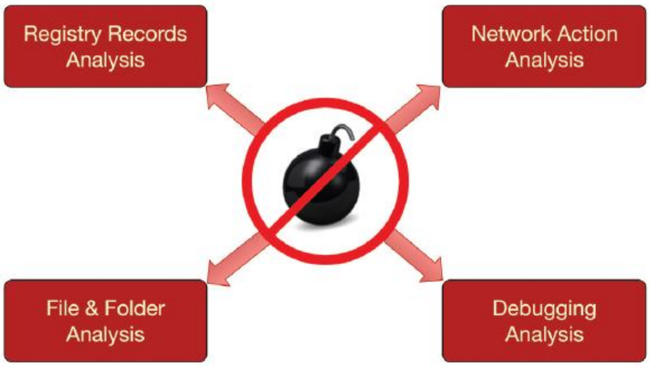


Figure 15: Algorithm for behavior analysis

Table 3: Brief Overview of Behavior Analysis Tool

Process Monitor	able to show a snapshot of the operating system's file system, registry, and background processes.

Process Explorer	displays background programs, running apps, and the.dll files that the system's running programs need.
Regshot	used to check system changes and file and registry activity. Regshot creates an image of the system's registry for this purpose, enabling rapid comparison and viewing.
Wireshark	able to examine all TCP/IP communication on any network card (modem or Ethernet card) plugged into the computer.
CaptureBat	able to real-time display files and registry entries.
Cuckoo Sandbox	a free, open-source tool that makes it possible to keep an eye on system processes, the registry, and the file system. In order to determine whether any malware has already been identified, it also compares the files with signature samples that are maintained in the database.

C. *Malware Code analysis*

The targets, intent, and actions of malicious software can be ascertained with the aid of dynamic and static analysis, as well as how the malware is propagated.

- *Static analysis:*Before malware is executed, static analysiscomprises a structural examination. Static analysis makes it possible to learn details about malware, including any text it may include, functions used, the contents of file-directory structures, if the files are compressed, hash verification values, and the date it was first activated on the system [25].

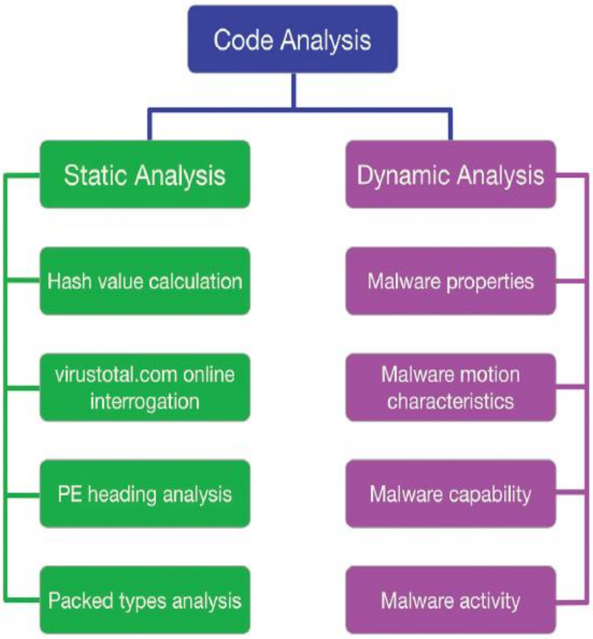


Figure 16: Algorithm for Code Analysis

- *Malware packing technique*: In order to prevent malicious software from being detected by anti-virus programs, attackers compress their data.22 After infecting the target system, malicious software first decompresses its payload, if compressed, and then the 'wrapper' is decompressed and the actual malware section is executed. For this reason, during analysis, it is necessary to examine the malware by working step-by-step in order to understand its functioning.

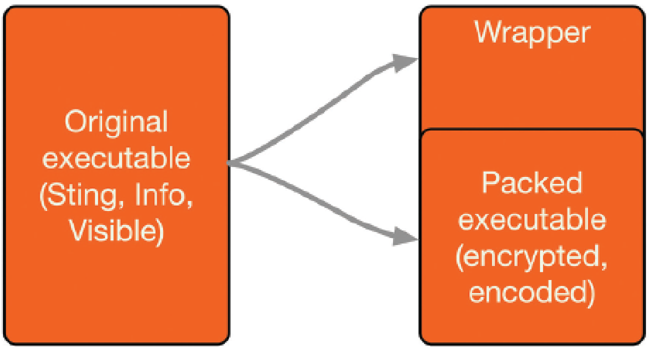

Original executable (Sting, Info, Visible)
Wrapper
Packed executable (encrypted, encoded)

Figure 17: General Rationale of Packing

- *Dynamic analysis*: In order to regulate the malicious software's file-directory, registry, operating system, IP traffic, and network activities, dynamic analysis involves running the malicious software in a restricted environment (on a virtual machine or in a sandbox).23 We can see the malware's traits, mobility, activity, and capacity thanks to dynamic analysis. Attackers use a variety of concealment techniques, such as anti-sandbox[26], anti-VM, and anti-debug, to avoid having malware recognized by anti-virus software in the system before it is executed. As a result, the information gathered by running malware is more crucial than that gathered from static analysis.

D. *Malware analysis export*

In order to preserve data integrity, the analysis of digital material should be conducted utilizing the Write Blocker feature and photos acquired in accordance with international standards within the context of forensic IT applications. This requirement must be met, and the analysis report must include the verification values for the constructed and examined images (hash algorithm, MD5, SHA-1, and SHA-256 values).

All of the concepts researched should have explicit definitions in the analysis reports that summarize the findings of the forensic IT investigation. The analysis reports should also clearly explain the tools and techniques that are employed for technical investigations. It is essential to be able to draw the same conclusions from the same facts using the same methods and tools as other experts.

Another scenario that occurs regularly today is when multiple countries, as opposed to just one, are involved in the crime. As a result, the reports need to be drafted in accordance with industry standards. To do this, laboratories must be accredited in order to meet global standards. According to both national and international norms, such accreditation is a trustworthy indicator of technical ability. By offering governmental certification of the proficiency of laboratories, laboratory accreditation enables clients to quickly discover and choose trustworthy test, analysis, and calibration services.

Table 4: Device Information

Description	Actual Storage, 621.392.321 Sectors, 132.7GB
Total size	350.141.221.127 bytes (301.1GB)
Total sectors	499.481.012
Acquisition MD5	cgh2112g144g2abf0stnx33314f77cdynddir4
Verification MD5	Cnf35g217h2cavafvgbh5833gte66bcdundrs4
Acquisition SHA-1	1dy456l1385kdye466293ya3353by620nsd9832
Verification SHA-1	1dy456l1385kdye466293ya3353by620nsd9832

Acquisition SHA-256	54sdcfGght96gh82937f8891m8001jkA124665
Verification SHA-256	54xsdfGtgfee95gh82937f8891m8001uıA12565

Table 5: Windows OS Information

Product name	Microsoft Windows 10 Pro
Registered owner	Bey
System root	C:\Windows
Product ID	65XXXX-7X0-60XXXX3-2XXXX
Version	6.2
Install date	02.09.2023 – 20:19:20IST
Last shutdown time	18.10.2023 – 23:15:23IST

Table 6: Information about the Malware

File information	
Filename	Your line 23446715’s Vodafone Invoice for the Month of August 2023
Creation time	17.10.202323:12:32 (2023-10-18 -11:21:23 UTC)
Last write time	20.10.2023 17:21:07 (2023-10-20 -15:21:09UTC)
File size	3,3567 bytes
MD5 hash value	1bdb92cadcea8ea47e801e8c6ba3705b
SHA-1 hash value	a6427be2eebb30e549f48723686aad0d5b19db46
SHA-256 hash value	2ce7932a940cf20d368890ea286ca64549b356e9738645a1bcf 59b5bcb296e4d
Submit time	20.10.2023 22:12:31 (2023-10-20 06:26:47 UTC)
Delivery time	20.10.2023 22:13:41 (2023-10-20 06:27:49 UTC)
Message ID	C21F73BH6714BZ582DD7E4F7G10ENDK8@exdf
File path	IMAGE.015/Partition 1/NONAME [NTFS]/[root]/Documents and Settings/pc/Local Settings/Application Data/Microsoft/Outlook/Outlook.pst»Personal Folders» Inbox »Your Vodafone Invoice for OCTOBER-2023 Period of your line 23446715

E. Analysis

In the light of the proposed model, a real malware attack was examined in detail. The image of the victim computer, which had been exposed to a malware attack, was taken using the TD2 device. Since the malware would attack user data quickly upon running the system, it was executed in a virtual machine mode of the workstation. For a behaviour analysis of the malware, FTK, Process Monitor, Wireshark and Cuckoo Sandbox programs were preferred. Code was examined using static and dynamic analysis. Volatility Frame Work was used for memory analysis. Static analysis results obtained with Cuckoo Sandbox are presented in Tables 4 and 5.

As the most common type of malware today, a cryptolocker was chosen as an example. This type of malware strongly encrypts files after infecting the user’s system. Then it asks a ransom from the user to allow access to the encrypted files, where names and extensions are also sometimes modified. It often creates on the victim system an ‘invoice’ that asks the user to click a link to view its contents. The file information of the malware obtained by Process Monitor is shown in Table 6.

In the analysis carried out on the image, it was seen that the malware had been cleaned, probably with the MalwareFox software installed and active in the victim system. Analysis of the file ‘mfx-log-2018-12-16 (12-07-47).xml’ found in the ‘IMAGE.001/Partition1/NONAME NTFS]/[root]/Documents andSettings/AllUsers/Application Data/MalwareFox/Logs/’ directory revealed that the malware had been indeed cleaned by MalwareFox after a malware scan in the computer.

Investigations on the forensic copy were continued, despite the fact that the malware had been removed. The file ‘B6500360.exe’ was found in the directory ‘IMAGE.001/Partition 1/NONAME [NTFS]/[root]/System Volume Information/_ restore{B4F7JDYF-CFT3-7354-CDT5-UCG65ENDGY623}/CF2653’. And the Volatility Framework program detected the ‘pacco_38972893.exe’ file in a compressed form in ‘mfx-log-2018-12-16 (12-07-47).xml’ in the memory dump.

The MD5 hash value of the pacco_38972893.exe file was queried via www.virustotal.com and it was found that 20 anti-virus companies detected it as malware. The query results are given in Table 7and the file-directory and registry actions of the malware were examined with the FTK program, with the results shown in Table 10.

After the completion of the examination of the registry and file-directory actions of the malware, decryption attempts were performed on the encrypted files. Due to the strong encryption feature of the malware, decryption was not successful.

VI. DISCUSSION &CONCLUSION

The sharp rise in malware attacks over the past few years demonstrates that many businesses, from huge multinational firms with substantial security budgets to small businesses and individual users, are unable to adequately defend their systems from these cunning cyber attackers.

Systems grow more open to attack due to rising security flaws and technological advancements, which also make them more appealing targets. Every day, new malware variants are created and disseminated in an effort to take advantage of this as a means of income. The few studies that have been done in this area and the inadequate recognition of the problem have led to a rise in the number of people who have fallen victim to malware. Without a doubt, victimization will remain a severe issue for a very long time.

In this paper, we put forth a model that goes into great depth about how malware analysis is carried out. An ordinary and current type of malware was examined as an example to demonstrate how the proposed model can be employed. It has been demonstrated that malware may be located using a study of its distinctive behavior and the Whois data of the server to which it connects. Every day, new hardware and software systems are being created to combat malware. The analytical programs suggested in this study are the newest and most widely used by professionals.

As a result, it is viable to design various attack methods in addition to performing malware analysis using various software and hardware systems that are not included in this study. Additionally, as the infrastructure of systems and operating systems often follows the same logic, developing a fundamental approach is a crucial step in providing insight into ongoing research and potential issues.

Table 7: The contents of the compressed file in B6500360.exe.

C:\RECYCLER\S-2-6-32-122258963-271533256-29128955642-2004\Ef291.zip\Trojan. pacco_49083904.exe
C:\Document and Setting\pc\Local Setting\Temp\C7611471.exe\ccdddi_49083904.exe

Table 8: Analysis results of the pacco_38972893.exe malware via the www.virustotal.com website.

Analysis	20 engines detected this file
	MD5: 2471c8c294743a0d0d6938f328ae273f
	SHA-1: e2d846226fe8afe22f051cdf4ac7ae55cbba76ba
	SHA-256: c18350240197ea578b73ec50c5c81e9d
	Filename: ccdddi_49083904.exe
	Last analysis: 2020-10-20 14:26:423 UTC
Al Yac	Trojan.Generic2132367
AVG	YnhgFGHY
AVware	Trojan.Win32ç.Generic!ZY
Agnitum	Trojan.kyrfv!2Gghgin7+I9B
Ad-Aware	Trojan.GenericHK.3911926
Yandex	Trojan.Filecoder!1Ey17kehnhhj
AhnLab-V3	Malware/Win32.Genericterm
Acrabit	Trojan.Generic. E1D32G
Avast	Win32:Malware-gen
Avira (no cloud)	TR/FileCoder.71156925.2
Baidu-International	Trojan.Win32. Filecoder.Gh
BitDefender	Trojan.GenericEF.3011926
CAT-QuickHeal	Ransom.Crowti.N6
Cyren	W32/Filecoder.XMQH-8836
DrWeb	Trojan.DownLoader17.64698
ESET-NOD32	Win32/Filecoder.FJ
Emsisoft	Trojan.GenericKD.2900815 (B)
F-Prot	W32/Filecoder.AE
Fortinet	PossibleThreat.P0
Ikarus	Trojan.Win32.Deshacop.big
Malwarebytes	Ransom.FileCryptor

Table 9: File-directory and registry logs of the ccdddi_49083904.exe malware.

Process	Process activity
Creates process:	C:\windows\temp\ B6500360.exe\ ccdddi_49083904.exe
Creates process:	[“C:\windows\temp\ B6500360.exe\ ccdddi_49083904.exe”]
Terminates process:	C:\Windows\temp\ B6500360.exe\pacco_38972893.exe
File folder activity	
Creates:	C:\USERS\ADMİN
Creates:	C:\Users\Admin\AppData\Local
Creates:	C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\ B6500360.exe
Reads from:	C:\Windows\System32\drivers\etc\hosts\B6500360.exe
Registry activity	
Process:	HKLM\SOFTWARE\Microsoft\Tracing\explorer_12334562
Process:	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\”C:\Windows\B6500360.exe”
Process:	HKU\S-1-4-12-764534351-3421244-18036362054-1000\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings
Process:	HKU\S-1-4-12-764534351-3421244-18036362054-1000\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings
Loaded DLL files	
Module name	C:\WINDOWS\system32\ntdll.dll
Module name	C:\WINDOWS\system32\kernel32.dll
Module name	C:\WINDOWS\system32\USER32.dll
Module name	C:\WINDOWS\system32\GDI32.dll

Table 10: Network actions of the ccdddi_49083904.exe malware as listed by Wireshark.

Time	Source	Destination	Protocol	Length	Info
23.12360	192.168.45.15	185.86.56.14	TCP	66	Standard query A xfbdc A xxxxx7gb.ru
26.12360	192.168.45.15	185.86.56.14	TCP	62	Standard query A xfbdc yxxxxda.ru
32.12360	192.168.45.15	185.86.56.14	TCP	66	Standard query A xfbdc yxxxxta.ru

VII. References

[1] Singh, Avinash, Adeyemi R. Ikuesan, and Hein S. Venter. "Digital forensic readiness framework for ransomware investigation." International conference on digital forensics and cybercrime. Cham: Springer International Publishing, 2018.

[2] R. B. Hadiprakoso, H. Kabetta and I. K. S. Buana, "Hybrid-Based Malware Analysis for Effective and Efficiency Android Malware Detection," 2020 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS), Jakarta, Indonesia, 2020, pp. 8-12, doi: 10.1109/ICIMCIS51567.2020.9354315.

[3] O. Or-Meir, A. Cohen, Y. Elovici, L. Rokach and N. Nissim, "Pay Attention: Improving Classification of PE Malware Using Attention Mechanisms Based on System Call Analysis," 2021 International Joint Conference on Neural Networks (IJCNN), Shenzhen, China, 2021, pp. 1-8, doi: 10.1109/IJCNN52387.2021.9533481.

[4] I. Muhamad Malik Matin And B. Rahardjo, "A Framework For Collecting And Analysis Pe Malware Using Modern Honey Network (Mhn)," 2020 8th International Conference On Cyber And It Service Management (Citsm), Pangkal, Indonesia, 2020, Pp. 1-5, Doi: 10.1109/Citsm50537.2020.9268810.

[5] M. Y. Khalil, Vivek, K. Anand, A. Paul and R. Grover, "PDF Malware Analysis," 2022 7th International Conference on Computing, Communication and Security (ICCCS), Seoul, Korea, Republic of, 2022, pp. 1-4, doi: 10.1109/ICCCS55188.2022.10079419.

[6] R. Murali, A. Ravi and H. Agarwal, "A Malware Variant Resistant To Traditional Analysis Techniques," 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), Vellore, India, 2020, pp. 1-7, doi: 10.1109/ic-ETITE47903.2020.264.

[7] M. F. Ismael and K. H. Thanoon, "Investigation Malware Analysis Depend on Reverse Engineering Using IDAPro," 2022 8th International Conference on Contemporary Information Technology and Mathematics (ICCITM), Mosul, Iraq, 2022, pp. 227-231, doi: 10.1109/ICCITM56309.2022.10031698.

[8] A. Walker and S. Sengupta, "Malware Family Fingerprinting Through Behavioral Analysis," 2020 IEEE International Conference on Intelligence and Security Informatics (ISI), Arlington, VA, USA, 2020, pp. 1-5, doi: 10.1109/ISI49825.2020.9280529.

[9] C. -D. Nguyen, N. H. Khoa, K. N. -D. Doan and N. T. Cam, "Android Malware Category and Family Classification Using Static Analysis," 2023 International Conference on Information Networking (ICOIN), Bangkok, Thailand, 2023, pp. 162-167, doi: 10.1109/ICOIN56518.2023.10049039.

[10] M. Dhalaria and E. Gandotra, "Android Malware Risk Evaluation Using Fuzzy Logic," 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, Himachal Pradesh, India, 2022, pp. 341-345, doi: 10.1109/PDGC56933.2022.10053179.

[11] B. Ramadhan, Y. Purwanto and M. F. Ruriawan, "Forensic Malware Identification Using Naive Bayes Method," 2020 International Conference on Information Technology Systems and Innovation (ICITSI), Bandung, Indonesia, 2020, pp. 1-7, doi: 10.1109/ICITSI50517.2020.9264959.

[12] Preeti and A. K. Agrawal, "A Comparative Analysis of Open-Source Automated Malware Tools," 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2022, pp. 226-230, doi: 10.23919/INDIACom54597.2022.9763227.

[13] H. A. Noman, Q. Al-Maatouk and S. A. Noman, "A Static Analysis Tool for Malware Detection," 2021 International Conference on Data Analytics for Business and Industry (ICDABI), Sakheer, Bahrain, 2021, pp. 661-665, doi: 10.1109/ICDABI53623.2021.9655866.

[14] I. Alsmadi, B. Al-Ahmad and M. Alsmadi, "Malware analysis and multi-label category detection issues: Ensemble-based approaches," 2022 International Conference on Intelligent Data Science Technologies and Applications (IDSTA), San Antonio, TX, USA, 2022, pp. 164-169, doi: 10.1109/IDSTA55301.2022.9923057.

[15] N. A. Anuar, M. Zaki Mas'ud, N. Bahaman and N. A. Mat Ariff, "Analysis of Machine Learning Classifier in Android Malware Detection Through Opcode," 2020 IEEE Conference on Application, Information and Network Security (AINS), Kota Kinabalu, Malaysia, 2020, pp. 7-11, doi: 10.1109/AINS50155.2020.9315060.

[16] T. Mantoro, M. E. Fahriza and M. Agni Catur Bhakti, "Effective of Obfuscated Android Malware Detection using Static Analysis," 2022 IEEE 8th International Conference on Computing, Engineering and Design (ICCED), Sukabumi, Indonesia, 2022, pp. 1-5, doi: 10.1109/ICCED56140.2022.10010587.

[17] B. Akram and D. Ogi, "The Making of Indicator of Compromise using Malware Reverse Engineering Techniques," 2020 International Conference on ICT for Smart Society (ICISS), Bandung, Indonesia, 2020, pp. 1-6, doi: 10.1109/ICISS50791.2020.9307581.

[18] A. Eltaher, D. Abu-juma'a, D. Hashem and H. Alawneh, "Design and Implementation of a Malware Detection Tool Using Network Traffic Analysis in Android-based Devices," 2023 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), Amman, Jordan, 2023, pp. 276-280, doi: 10.1109/JEEIT58638.2023.10185826.

[19] A. Eltaher, D. Abu-juma'a, D. Hashem and H. Alawneh, "Design and Implementation of a Malware Detection Tool Using Network Traffic Analysis in Android-based Devices," 2023 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), Amman, Jordan, 2023, pp. 276-280, doi: 10.1109/JEEIT58638.2023.10185826.

[20] S. Gülmez and I. Sogukpinar, "Graph-Based Malware Detection Using Opcode Sequences," 2021 9th International Symposium on Digital Forensics and Security (ISDFS), Elazig, Turkey, 2021, pp. 1-5, doi: 10.1109/ISDFS52919.2021.9486386.

[21] Omar Aslan, RefikSamet, and ¨Omer ¨Ozg¨urTanrı¨over, "Using a Subtractive Center Behavioral Model to Detect Malware," Hindawi

Security and Communication Networks, vol. 2020, pp. 17,Published 27 February 2020.

[22]HSafaa Salam Hatem, Dr. Maged H. wafy, Dr. Mahmoud M. El-Khouly "Malware Detection in Cloud Computing".,inInternational Journal of Advanced Computer Science and Applications, vol:5 no:4 2014.

Paper ID: IJETAS/August/2023/03

[23] Muhammad Irfan1and Haider Abbas1,2,Yunchuan Sun3, Anam Sajid4, Maruf Pasha5 "A framework for cloud forensics evidence collectionand analysis using security information and eventmanagement," insecurity and communication networks in 2016.

[24] Sudhakar, Sushil Kumar, "An emerging threat Fileless malware: asurvey and research challenges," unpublished in Cybersecurity open access 2020.

[25] V. Méndez-García, P. Jiménez-Ramírez, M. Á. Meléndez-Ramírez, F. M. Torres-Martínez "Comparative Analysis of Banking Malware,"proceedings of the 2014 ieee central america and panama convention (concapan xxxiv).978-1-4799-7584-6/14/$31.00 ©2014 IEEE.

[26] Om Prakash Samantray, Satya Narayan Tripathy, and Susanta Kumar Das, "A study to Understand Malware Behavior throughMalware Analysis" Proceding of international conference on system computation automation and networking 2019 @ IEEE 978-1-7281-1524-5.

[27] Rodrigo RubiraBranco, Udi Shamir, "Architecture for Automation of Malware Analysis" 2010 5th International Conference on Malicious and Unwanted Software. 978-1-4244-9356-2/10/$26.00c 2010 IEEE.

[28] Syed ZainudeenMohdShaid, MohdAizainiMaarof, "Malware Behavior Image for Malware VariantIdentification," 2014 International Symposium on Biometric and Security Technologies (ISBAST) ,978-1-4799-6444-4/14/$31.00 ©2014 IEEE.

[29] R. Beg, R. K. Pateriya and D. S. Tomar, "ACMFNN: A Novel Design of an Augmented Convolutional Model for Intelligent Cross-Domain Malware Localization via Forensic Neural Networks," in IEEE Access, vol. 11, pp. 87945-87957, 2023, doi: 10.1109/ACCESS.2023.3305274.